在 GCP 上部署 Firewall Threat Defense Virtual

您可以在 Google 云平台 (GCP) 上部署 Firewall 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**中选择该项目。
- 要访问控制面板，请点击**导航菜单** > **主页** > **控制面板**。

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 Firewall Threat Defense Virtual 实例。以下程序介绍了如何准备 GCP 环境并启动 Firewall Threat Defense Virtual 实例，以便部署 Firewall Threat Defense Virtual。

概述

Firewall 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。Firewall 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

GCP 机器类型和 Threat Defense Virtual 版本

选择 Google 虚拟机类型和大小以满足 Firewall Threat Defense Virtual 需求。目前，Firewall Threat Defense Virtual 支持计算优化和通用机器类型（标准、高内存以及高 CPU 机器类型）。

注释 支持的计算机类型可能会更改，恕不另行通知。

表 *1:* 支持的计算优化计算机类型

计算优化计算机类型	属性		vNIC	Threat Defense Virtual 版本
	vCPU	内存 (GB)		
c2-standard-4	4	16 GB	4	7.0 或更高版本
c2-standard-8	8	32 GB	8	7.0 或更高版本
c2-standard-16	16	64 GB	8	7.0 或更高版本

表 *2:* 支持的通用计算机类型

通用计算机类型	属性		vNIC	Threat Defense Virtual 版本
	vCPU	内存 (GB)		
n1-standard-4	4	15	4	7.0 或更高版本
n1-standard-8	8	30	8	7.0 或更高版本
n1-standard-16	16	60	8	7.0 或更高版本
n2-standard-4	4	16	4	7.0 或更高版本
n2-standard-8	8	32	8	7.0 或更高版本
n2-standard-16	16	64	8	7.0 或更高版本

通用计算机类型	属性		vNIC	Threat Defense Virtual 版本
	vCPU	内存 (GB)		
n2-highmem-4	4	32	4	7.0 或更高版本
n2-highmem-8	8	64	8	7.0 或更高版本
n1-highmem-4	4	8	4	7.0 或更高版本
n1-highmem-8	8	16	8	7.0 或更高版本
n1-highmem-16	16	32	8	7.0 或更高版本
n2d-standard-4	4	8	4	7.0 或更高版本
n2d-standard-8	8	16	8	7.0 或更高版本
n2d-standard-16	16	32	8	7.0 或更高版本
c2d-standard-4	4	8	4	7.0 或更高版本
c2d-standard-8	8	16	8	7.0 或更高版本
c2d-standard-16	16	32	8	7.0 或更高版本

- Firewall Threat Defense Virtual 至少需要 4 个接口。
- 支持的最大 vCPU 数量为 16 个。

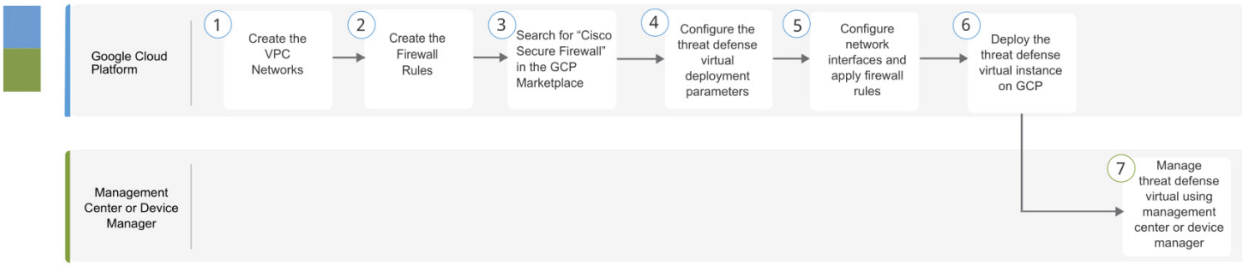
您可以在 GCP 上创建帐户、使用 GCP 市场上的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品来启动 VM 实例，以及选择 GCP 计算机类型。

注释

- 默认情况下，使用 UEFI 模式部署 Threat Defense Virtual 实例。
- 用户可以在部署 Threat Defense Virtual 实例时启用安全启动。

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	在 GCP 上部署 Threat Defense Virtual：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	在 GCP 上部署 Threat Defense Virtual：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	在 GCP 上部署 Threat Defense Virtual：在 GCP 市场中搜索“Cisco Secure Firewall”。
4	GCP	在 GCP 上部署 Threat Defense Virtual：配置 Threat Defense Virtual 部署参数。
5	GCP	在 GCP 上部署 Threat Defense Virtual：配置网络接口并应用防火墙规则。
6	GCP	在 GCP 上部署 Threat Defense Virtual：在 GCP 上部署 Threat Defense Virtual。
7	管理中心或设备管理器	管理 Firewall Threat Defense Virtual： • 使用 防火墙管理中心 来管理 Firewall Threat Defense Virtual • 使用 防火墙设备管理器 来管理 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 Firewall Threat Defense Virtual。
  - 所有安全服务的许可证授权均在 防火墙管理中心中配置。

- 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 Firewall 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 Firewall Threat Defense Virtual 连接到 防火墙管理中心，另一个用于诊断；无法用于直通流量。
- 流量接口 (2) - 用于将 Firewall 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 21 页。

通信路径

- 用于访问 Firewall Threat Defense Virtual的公共 IP。

Firewall 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 防火墙管理中心。从 Cisco Secure Firewall 版本 7.2 开始，还支持 防火墙设备管理器。

Firewall Threat Defense Virtual 智能许可的性能层

Firewall 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 ***Firewall 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 Firewall Threat Defense Virtual 设备时的准则。

注释 要更改 vCPU/内存值，必须先关闭 Firewall Threat Defense Virtual 设备的电源。

性能优化

为实现 Firewall 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 - Firewall 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。

部署

运行版本 7.4.3 或更高版本的 Threat Defense Virtual 实例会在首次启动期间执行多项初始化任务，这会导致控制台在大约五分钟后可用。这种延迟是正常的。如果设备在首次启动后大约两分钟内关闭，重要的初始化步骤可能会中断，从而可能导致设置不完整和意外行为。

要解决此问题,必须使用新映像重新安装虚拟平台。

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 Firewall 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 Firewall 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 Firewall 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
- Firewall Threat Defense Virtual 本地 HA
- 透明/内联/被动模式
- 巨型帧

UEFI 和安全启动限制

在 GCP 上，仅支持绿地（全新）部署，并且必须在初始部署期间启用 UEFI 固件。

现有的棕色地带部署可以升级到版本 10.0.0，而不会受到影响。不支持在部署后更改启动模式或启用 UEFI 安全启动。

升级限制和局限性

恢复升级限制

⚠

注意　不支持恢复升级。

确保在升级前进行备份。升级到 Threat Defense Virtual 10.0.0 后，您无法回滚到以前的软件版本。要返回到较早的版本，必须重新部署管理中心。

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

.

.

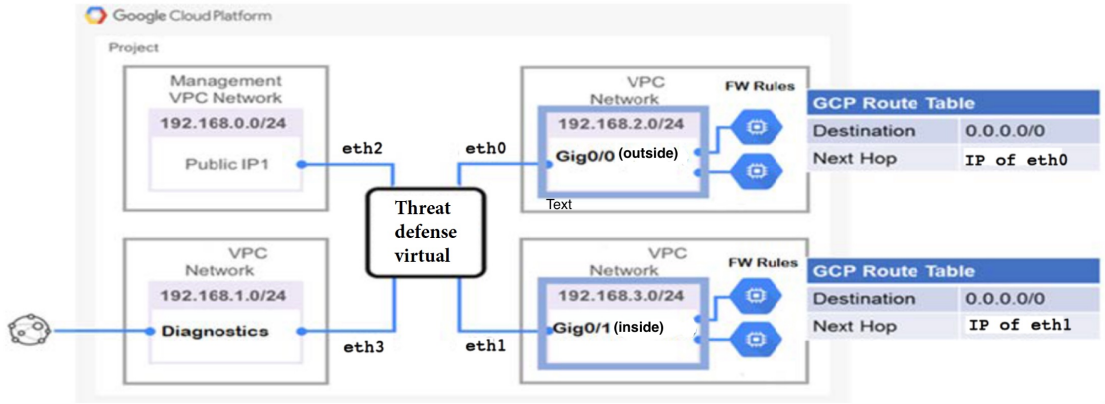
.

- 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 Firewall Threat Defense Virtual 的拓扑，在 GCP 中为 Firewall Threat Defense Virtual 配置了 4 个子网（外部、内部、管理和诊断）。

图 *1: GCP* 上的 *Firewall Threat Defense Virtual*部署示例



如何管理 Secure Firewall Threat Defense Virtual 设备

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

Secure Firewall Management Center

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 防火墙管理中心（而不是集成的 防火墙设备管理器）来配置您的设备。有关详细信息，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual

重要事项 您不能同时使用 防火墙设备管理器 和 防火墙管理中心 来管理 Firewall Threat Defense 设备。在启用 防火墙设备管理器 集成管理功能后，将无法使用 防火墙管理中心 来管理 Firewall Threat Defense 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 防火墙管理中心。另一方面，当您向 Firewall Threat Defense 注册 防火墙管理中心 设备时，防火墙设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 防火墙设备管理器 配置迁移到 防火墙管理中心 的选项，反之亦然。选择为 Firewall Threat Defense 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

防火墙设备管理器 是大多数 Firewall Threat Defense 设备上都包含的 Web界面。它可以配置小型网络最常用的软件基本功能。此产品专为仅包含一台或几台设备的网络而设计，在这种网络中，无需使用高性能多设备管理器来控制包含大量设备的大型网络。有关详细信息，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

注释 有关支持的 防火墙设备管理器 设备的列表，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。

云交付的防火墙管理中心

云交付的防火墙管理中心是一个基于云的管理平台，让您可以集中管理 Secure Firewall Threat Defense Virtual 设备。云交付的防火墙管理中心支持 Secure Firewall Threat Defense Virtual 7.0.3、7.2.0 及更高版本。有关详细信息，请参阅使用 云交付的防火墙管理中心 来管理 Secure Firewall Threat Defense Virtual。

重要事项 您不能将云交付的防火墙管理中心与 防火墙设备管理器 配合使用来管理同一台 Secure Firewall Threat Defense Virtual 设备。

配置 GCP 环境

Firewall Threat Defense Virtual 部署需要四个网络，您必须在部署 Firewall Threat Defense Virtual 之前创建这些网络。网络如下：

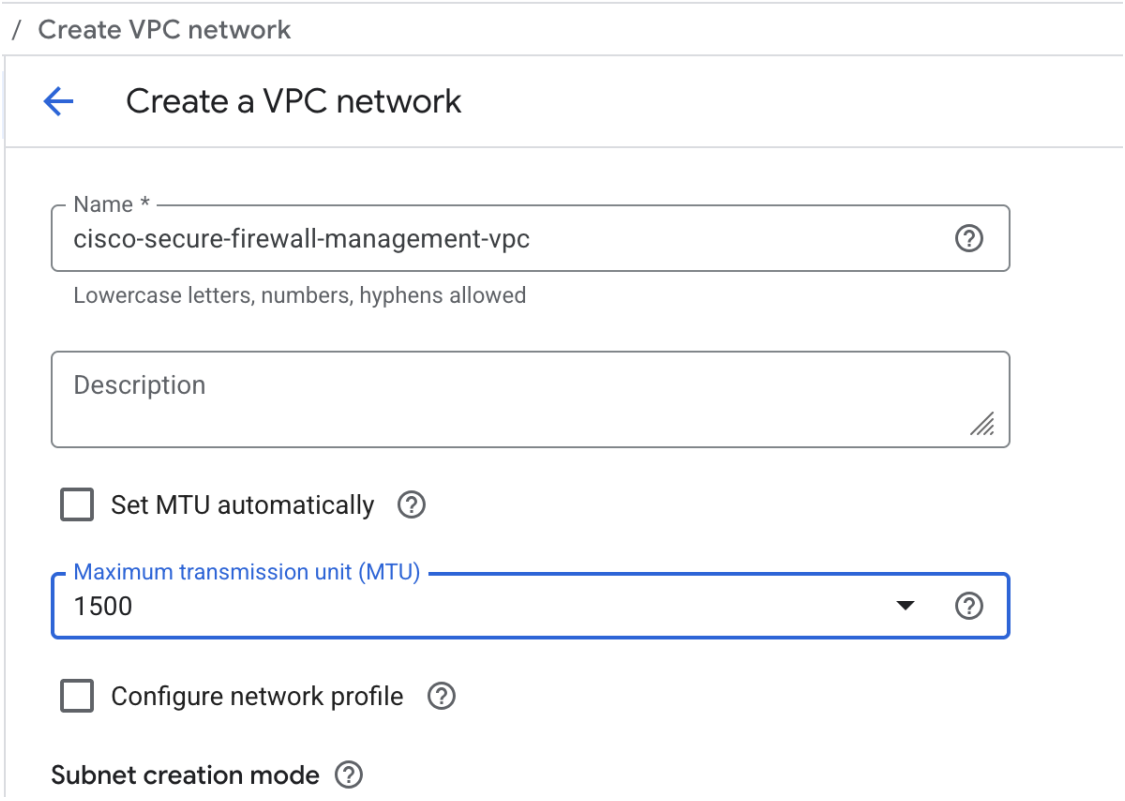
- 外部子网的外部 VPC。
- 内部子网的内部 VPC。
- 管理子网的管理 VPC。
- 诊断 VPC 或诊断子网。

此外还设置了路由表和 GCP 防火墙规则，以允许流量流经 Firewall Threat Defense Virtual。路由表和防火墙规则与在 Firewall 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 GCP 上 FTDv 的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**，然后点击**创建 VPC 网络**。

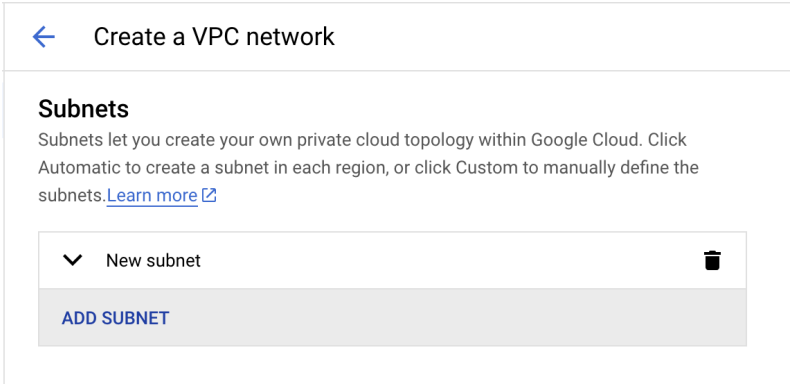


步骤 2 在**名称 (Name)** 字段中，输入所需的名称。

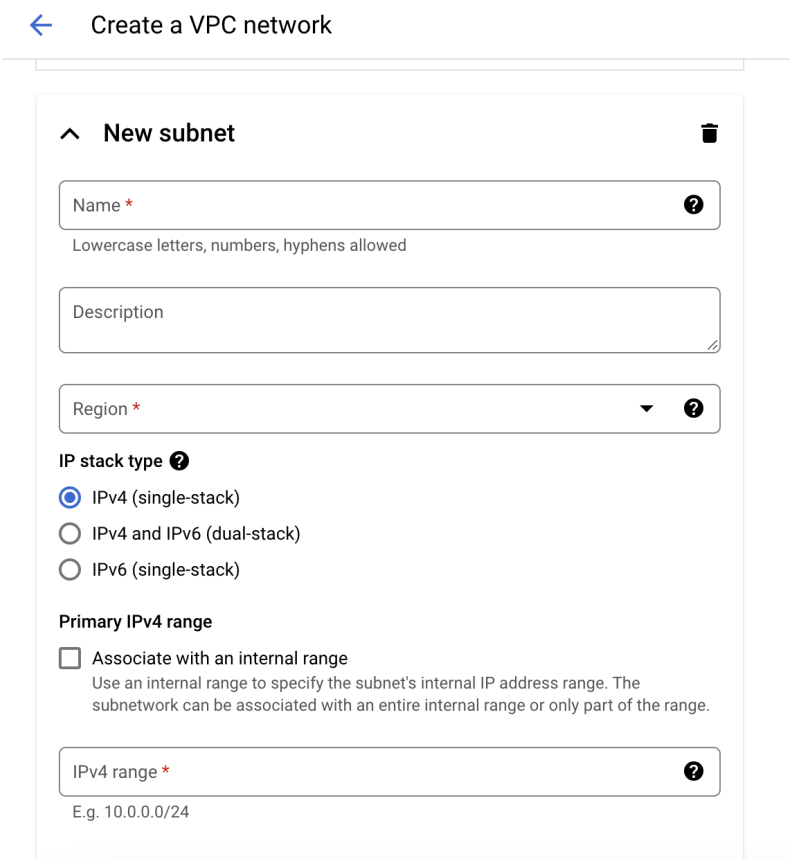
步骤 3 取消选中**自动设置 MTU**，然后从**最大传输单位 (MTU)** 下拉菜单中，选择适当的 MTU 值。

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 **IPv4** 范围字段中，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)**。

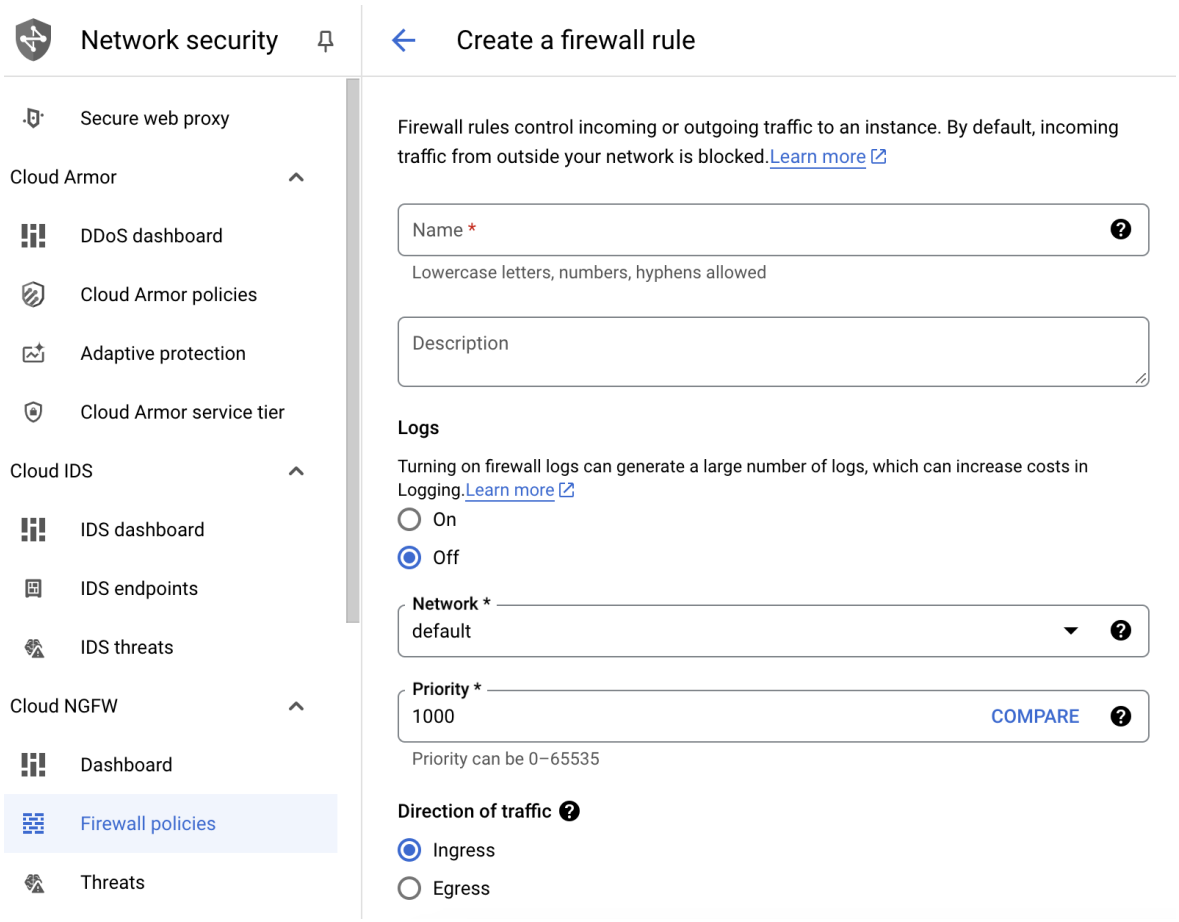
步骤 10 重复步骤 1-7，在您的 VPC 中创建其余三个 VPC 网络。

创建防火墙规则

在部署 Firewall Threat Defense Virtual 实例时，请为管理接口应用防火墙规则（以允许使用 防火墙管理中心 的 SSH 和 HTTPS 连接），请参阅部署 Firewall Threat Defense Virtual，第 16 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** > **VPC 网络** > **防火墙**，然后点击**创建防火墙规则**。

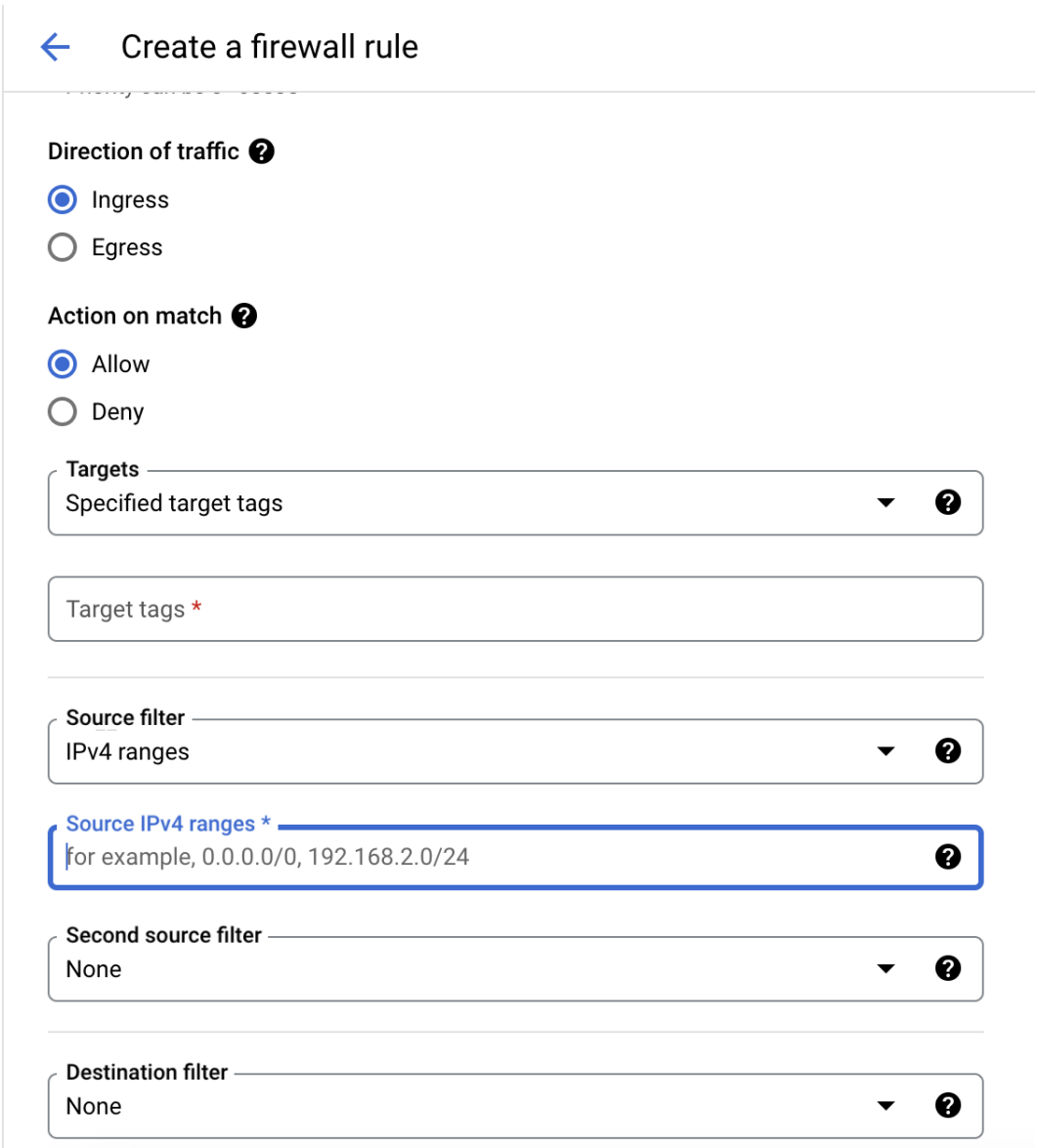


步骤 2 在名称 **(Name)** 字段中，为防火墙规则输入描述性名称，例如：*vpc-asiasouth-inside-fwrule*。

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 **IPv4** 范围字段中，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 Firewall Threat Defense Virtual

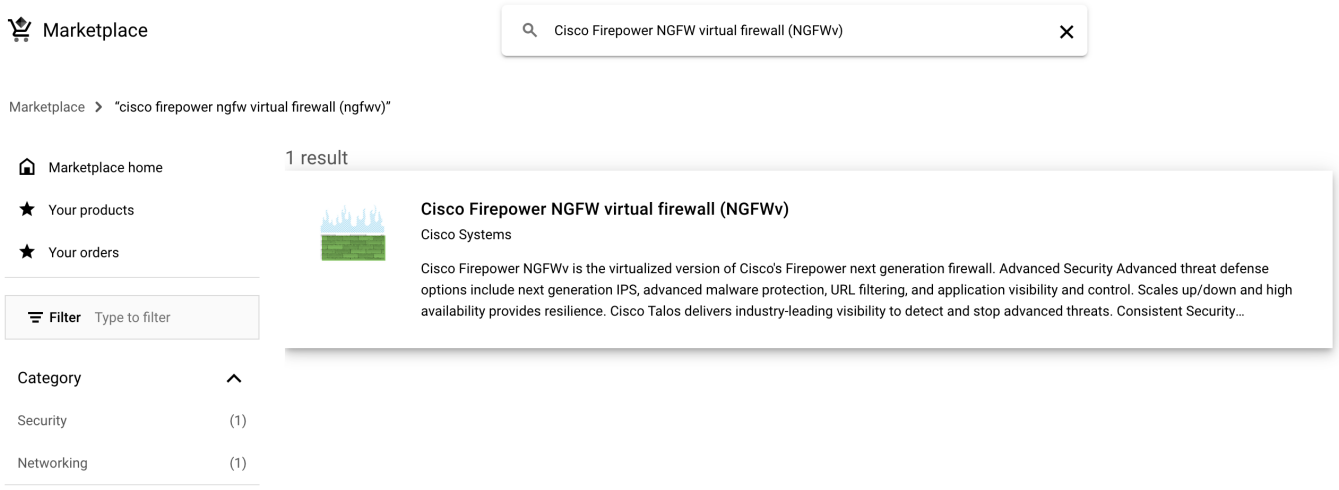
您可以按照以下步骤，使用 GCP 市场提供的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 部署 Firewall Threat Defense Virtual 实例。

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) **角色** - 选择具有部署和管理 Threat Defense Virtual 实例所需权限的服务帐户。
c) **映像版本** - 选择要部署的 Threat Defense Virtual 映像的软件版本。
d) **区域 (Zone)** - 选择要部署 Firewall Threat Defense Virtual 的区域。
e) **计算机类型 (Machine type)** - 根据 系统要求，第 2 页 选择正确的计算机类型。
f) **SSH 密钥（可选）** - 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。

g) 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。
h) **启动脚本 (Startup script)** - 您可以为 Firewall 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**字段的示例：

示例 1：

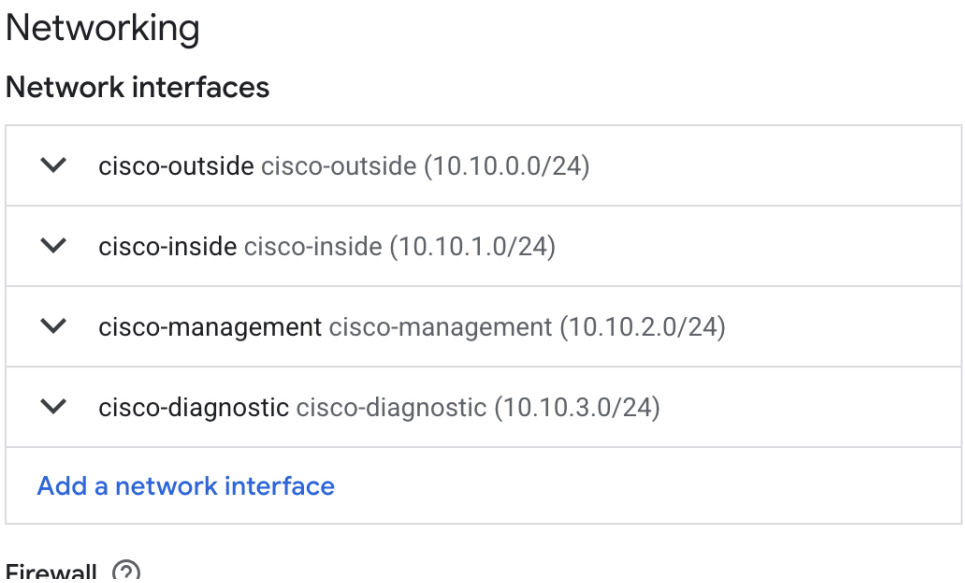
```
{
"AdminPassword": "<your_password>",
"Hostname": "cisco-sf-gcp",
"ManageLocally": "No",
"FmcIp":  "<FMC_IP>",
"FmcRegKey":"<FMC_regkey>",
"FmcNatId":"<FMC_natid>"
}
```

示例 2：

```
{
"AdminPassword": "<your_password>",
"Hostname": "ftdv-gcp",
"ManageLocally": "Yes"
}
```

提示
为防止执行错误，您应使用 JSON 验证器来验证 Day0 配置。

i) **网络接口** — 配置接口：1) 外部、2) 内部、3) 管理、4) 诊断。

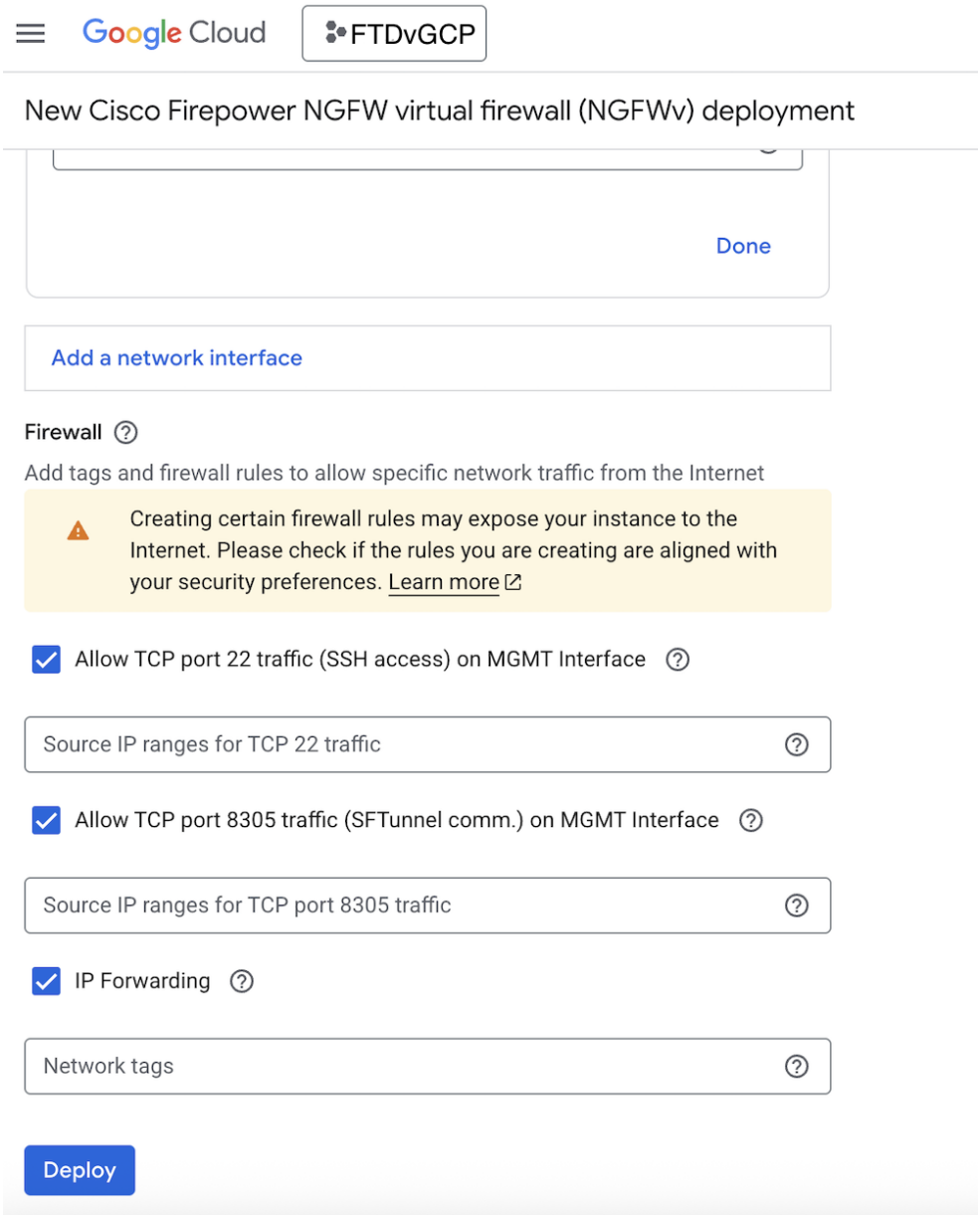


注释
创建实例后，将无法向实例中添加端口。如果使用不正确的接口配置创建实例，则必须删除该实例并使用正确的接口配置重新创建实例。

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)**。

j) **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 防火墙管理中心 和托管设备使用双向 SSL 加密通信通道 (SFTunnel) 进行通信。
- 选中 **IP 转发**复选框。

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 Firewall Threat Defense Virtual实例

Firewall 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 Firewall 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 Firewall Threat Defense Virtual 实例名称以打开 VM 实例详细信息页面。

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 Firewall 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 Firewall Threat Defense Virtual实例

要从 Unix 风格的系统连接到 Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall 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， Firewall 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 Firewall 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 Firewall 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 Firewall 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

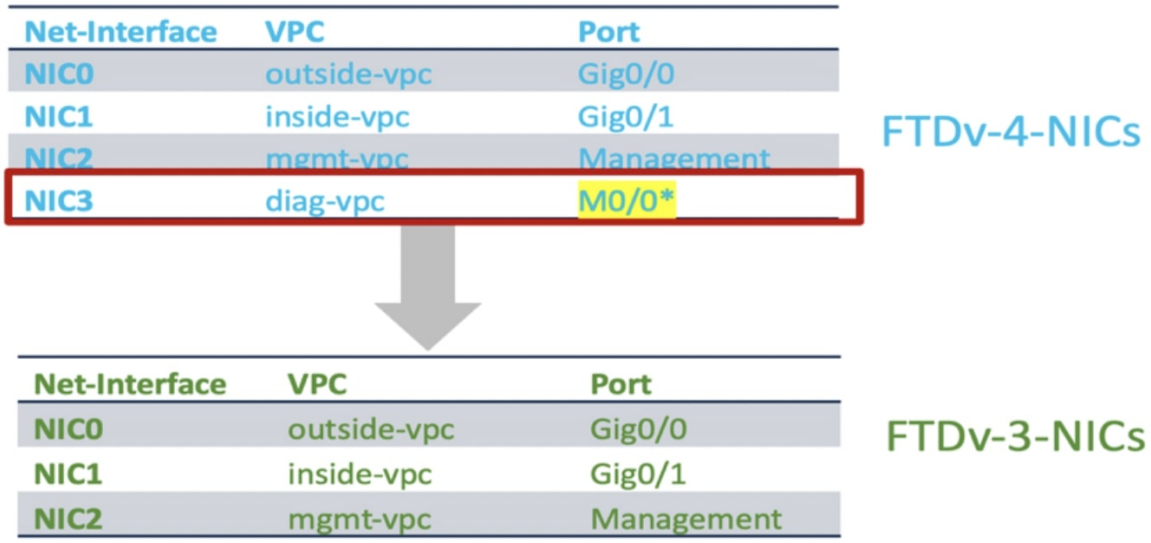
- 当诊断接口被删除时，系统日志和 SNMP 支持使用 Firewall Threat Defense Virtual 管理或数据接口，而不是使用诊断接口。
- 此部署支持集群和自动扩展。
- 不支持将具有诊断接口端口的 Firewall Threat Defense Virtual 实例和不具有诊断接口端口的 Firewall Threat Defense Virtual 实例分组。

注释 此处的 Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense Virtual 的详细程序，请参阅在 GCP 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 Firewall Threat Defense Virtual 实例。

- 所有 Cisco Secure Firewall 版本 – 您可以将部署了诊断接口的 Firewall Threat Defense Virtual 实例升级为具有诊断接口的 Firewall 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 Firewall Threat Defense Virtual 部署实例升级为没有诊断接口的 Firewall 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 Firewall Threat Defense Virtual 实例升级到没有诊断接口的 Firewall 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 Firewall Threat Defense Virtual 部署实例升级为具有诊断接口的 Firewall 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 Firewall Threat Defense Virtual 集群或由 Firewall 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 Firewall 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**。

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。

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。

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。