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 *1:* 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

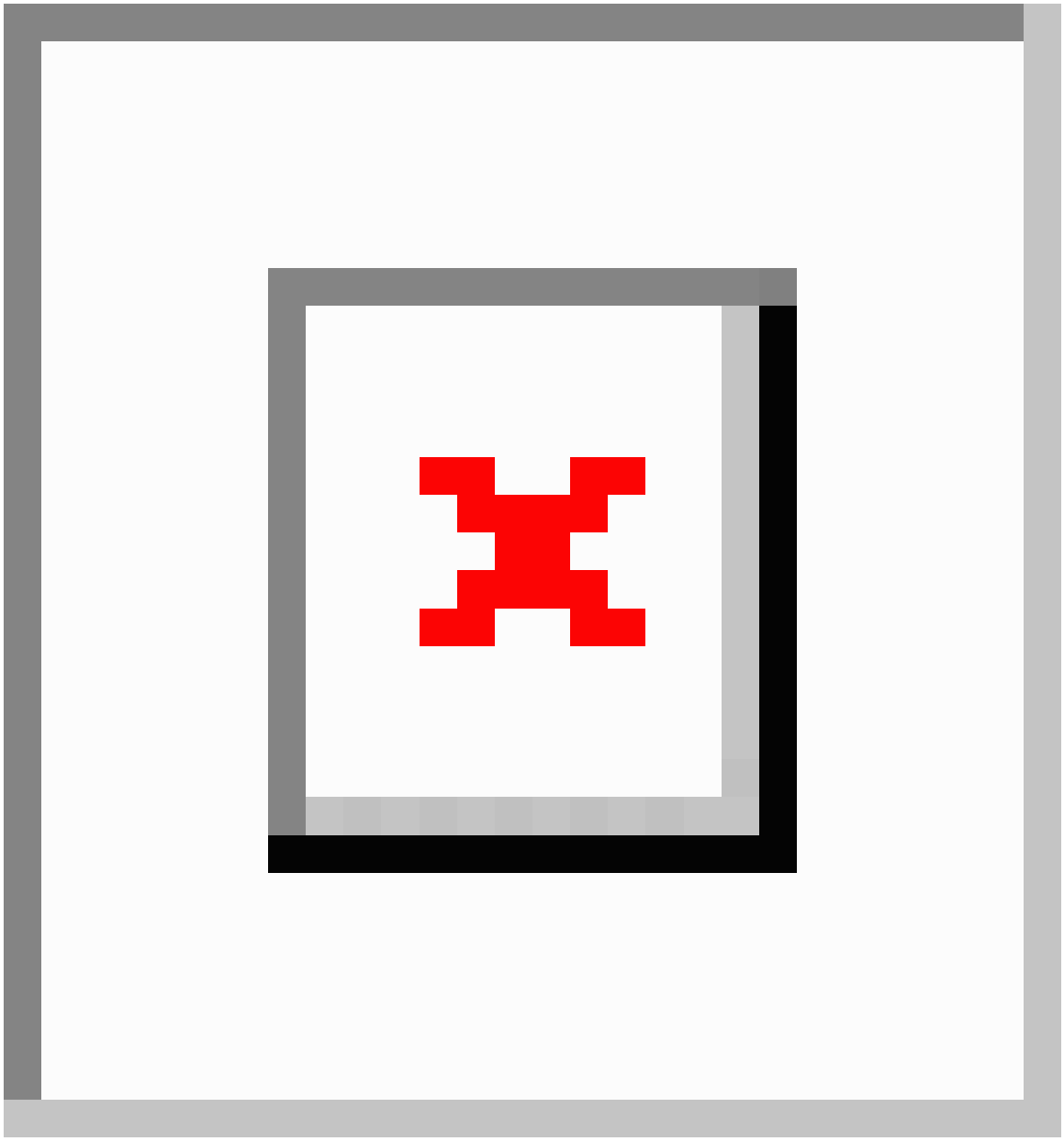
表 *2:* 支持的通用计算机类型

- 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)**）。

	工作空间	步骤
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”。
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 管理中心 来管理 Threat Defense Virtual • 使用 设备管理器 来管理 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 14 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 *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。

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

.

.

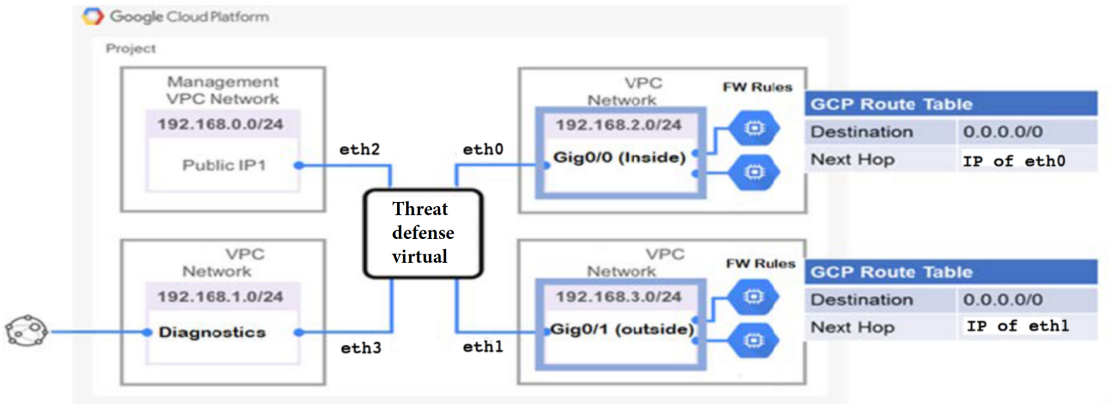
.

- 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 *1: GCP* 上的 *Threat Defense Virtual*部署示例



如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您可以使用以下选项来管理 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（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。

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 在**子网创建模式 (Subnet creation mode)**下，点击**自定义 (Custom)**。

步骤 4 在**新子网 (New subnet)** 下的**名称 (Name)** 字段中输入所需的名称。

步骤 5 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 6 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 7 接受所有其他设置的默认设置，然后点击**创建 (Create)**。

步骤 8 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 11 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 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 6 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 7 添加安全规则。

步骤 8 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 2 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**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。

3. 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。

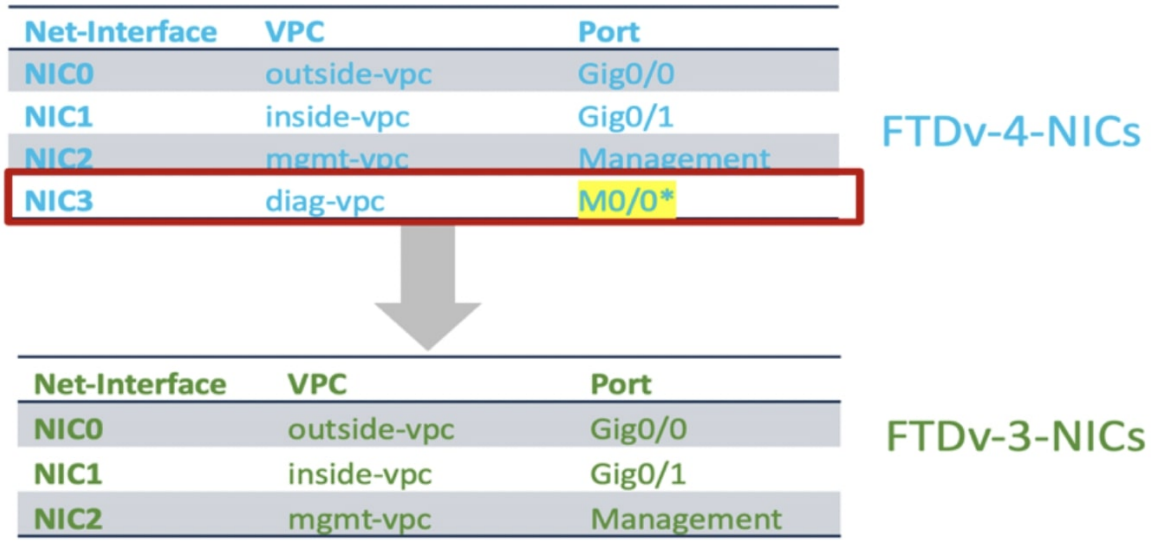
- 不支持将具有诊断接口端口的 Threat Defense Virtual 实例和不具有诊断接口端口的 Threat Defense Virtual 实例分组。

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。

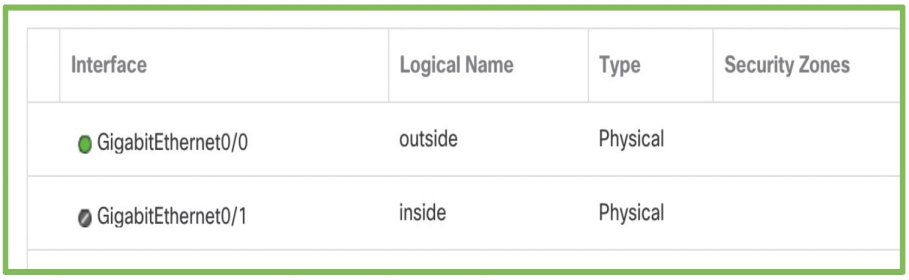
有关在 GCP 上部署 Threat Defense Virtual 的详细程序，请参阅在 Google 云平台上部署 Threat Defense Virtual。

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 25 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。

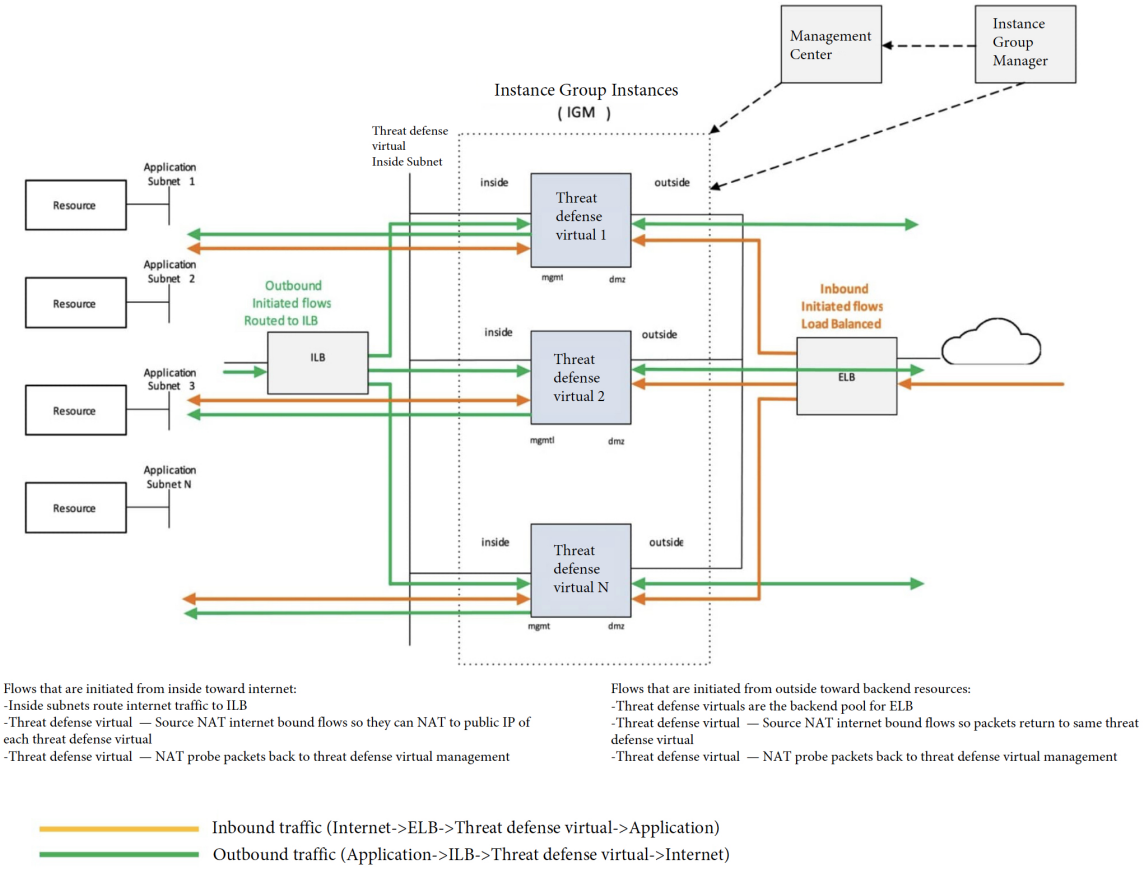
- 必须在 management center virtual 中创建设备组、NAT 规则和网络对象，然后才能启动自动扩展。请注意，ILB 和 ELB IP 仅在部署解决方案后才可用。因此，您可以创建虚拟对象，并在获取实际 IP 后更新对象。

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 *2: 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 25 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

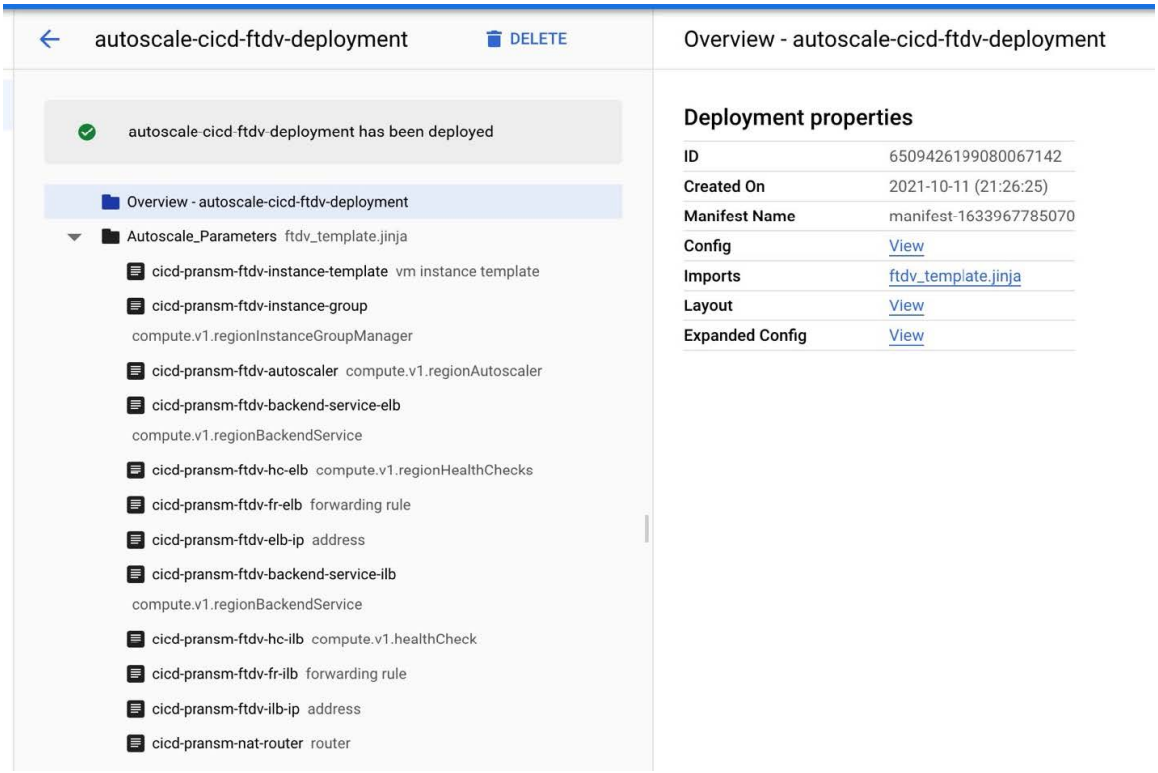
以下组件构成了适用于 GCP 的 Threat Defense Virtual Auto Scale 解决方案。

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。

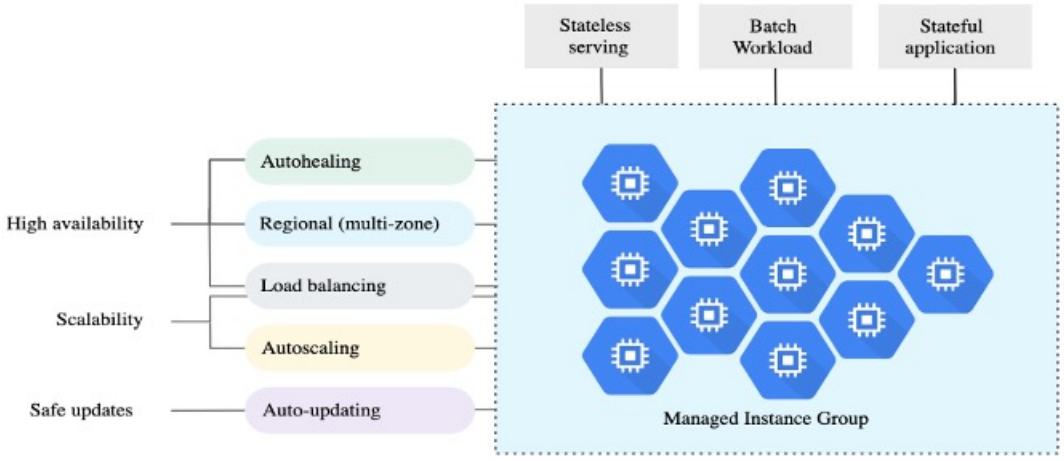
图 *3:* 部署管理器视图



GCP 中的托管实例组

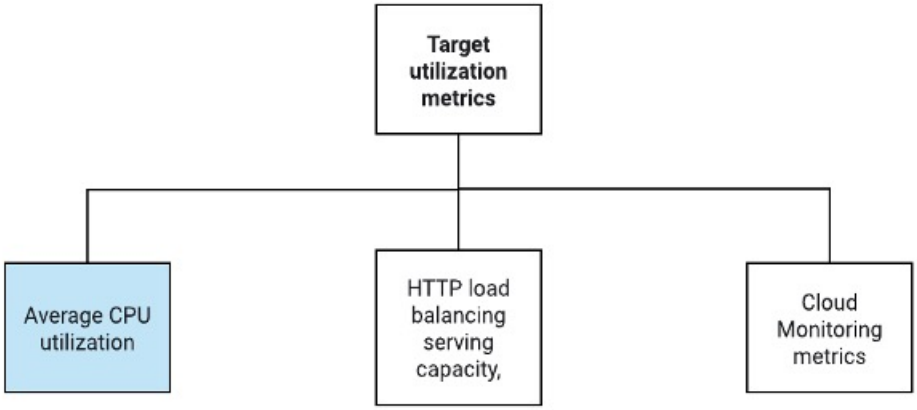
托管实例组 (MIG) 会根据您指定的实例模板和可选状态配置来创建其每个托管实例。有关详细信息，请参阅 https://cloud.google.com/compute/docs/instance-groups。

图 4: 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。

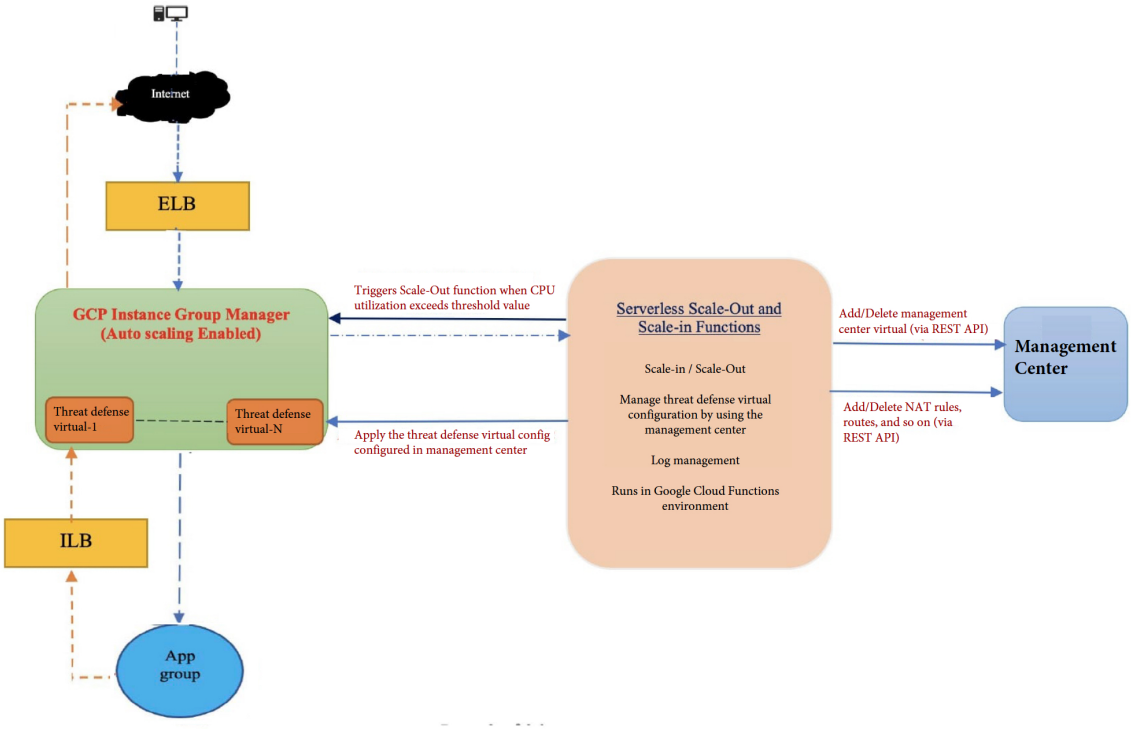
- 当在外向扩展期间实例组中出现新的 threat defense virtual 实例时，您需要执行诸如更改 SSH 密码、配置管理器、在 management center virtual 上注册 threat defense virtual 以及从 management center virtual取消注册 threat defense virtual 等任务。
- 在外向扩展过程中，云功能会通过云发布/订阅主题触发。您还有一个带有过滤器的日志接收器，专门用于在外向扩展时添加实例。

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 *5: 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 *4:* 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

参数名	允许的值/类型	说明
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。
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

参数名	允许的值/类型	说明
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
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

参数名	允许的值/类型	说明
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
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

参数名	允许的值/类型	说明
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
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

参数名	允许的值/类型	说明
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
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

参数名	允许的值/类型	说明
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。
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

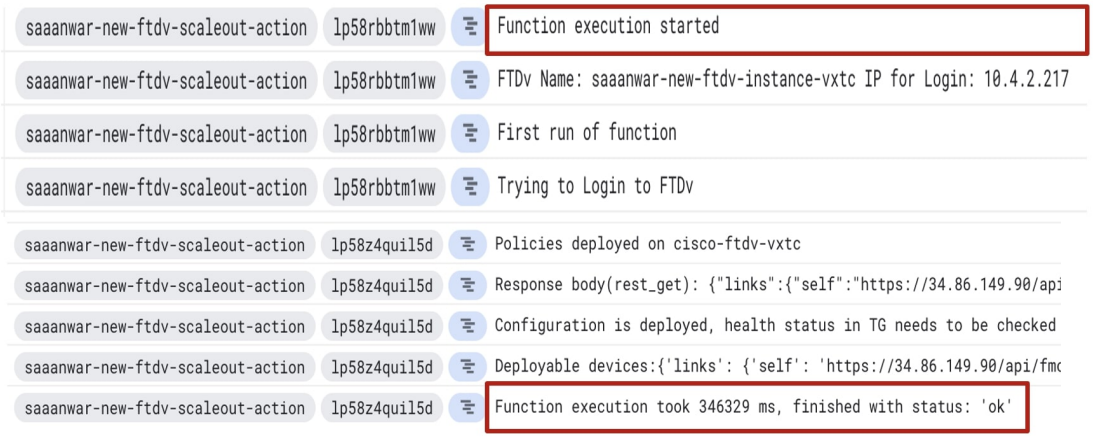
- 自动调节程序将目标 CPU 利用率水平视为实例组中一段时间内所有 vCPU 的平均使用量的一部分。
- 如果总 vCPU 的平均利用率超过目标利用率，则自动扩展程序会添加更多 VM 实例。如果总 vCPU 的平均利用率低于目标利用率，则自动扩展程序会删除实例。
- 例如，设置 0.75 的目标利用率会告知自动扩展程序将实例组中所有 vCPU 的平均利用率保持在 75%。
- 扩展决策中只会使用 CPU 利用率指标。
- 该逻辑基于以下假设：负载均衡器将尝试在所有 threat defense virtual 之间平均分配连接，一般来说，所有 threat defense virtual 应平均加载。

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 *6:* 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。

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。