在 Google 云平台上部署虚拟 Firepower 管理中心

Google 云平台 (GCP) 是 Google 提供的公共云服务，允许您构建和托管 Google 的可扩展基础设施应用。Google 的虚拟私有云 (VPC) 可让您灵活地扩展和控制工作负载在区域和全球范围内的连接方式。GCP 允许您在 Google 的公共基础设施之上构建自己的 VPC。

您可以在 GCP 上部署 Firepower Management Center Virtual (FMCv)。

- 关于 FMCv 部署和 GCP，第 1 页
- GCP 上 FMCv 的前提条件，第 2 页
- FMCv 和 GCP 的准则和限制，第 3 页
- GCP 上 FMCv 的网络拓扑，第 3 页
- 在 GCP 上部署 FMCv，第 4 页
- 在 GCP 上访问 FMCv 实例，第 6 页

关于 FMCv 部署和 GCP

Cisco Firepower Management Center Virtual (FMCv) 运行与物理思科 FMC 相同的软件，以虚拟形式提供成熟的安全功能。FMCv 可以部署在公共 GCP 中。然后可以将其配置为管理虚拟和物理 Firepower 设备。

GCP 计算机类型支持

FMCv 支持计算优化和通用计算机高内存计算机类型，以及高 CPU 计算机类型。FMCv 支持以下 GCP 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)
c2-standard-8	8	32 GB
c2-standard-16	16	64 GB

表 *2:* 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)
n1-standard-8	8	30 GB
n1-standard-16	16	60 GB
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-32	32	28.8
n2-highcpu-32	32	32
n1-highmem-8	8	52
n1-highmem-16	16	104
n2-highmem-4	4	32
n2-highmem-8	8	64

GCP 上 FMCv 的前提条件

- 在 https://cloud.google.com 上创建 GCP 帐户。
- 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。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower管理中心配置指南》中的“Firepower系统许可”。

- 接口要求：
  - 管理接口 - 用于将 Firepower 威胁防御设备连接到 Firepower 管理中心。
- 通信路径：
  - 用于管理访问 FMCv 的公共 IP。
- 对于 Firepower Management Center Virtual 和 Firepower 系统的兼容性，请参阅《Cisco Firepower 兼容性》。

FMCv 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 32 个 vCPU（基于 GCP 计算机类型）
- 许可 - 仅支持 BYOL

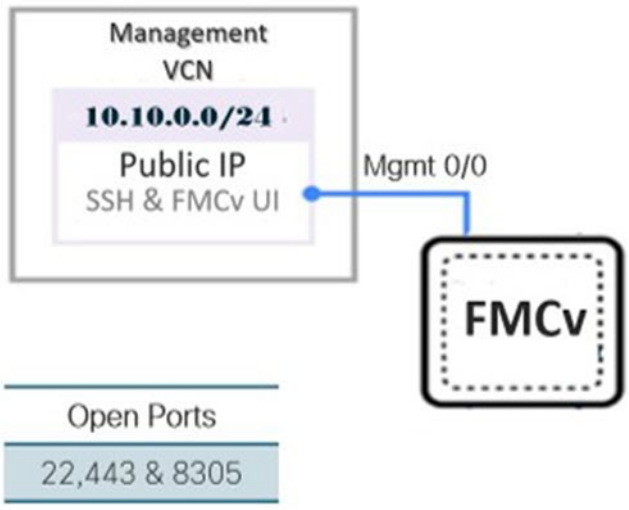
不支持的功能

- IPv6
- FMCv 本地 HA
- 自动缩放
- 透明/内联/被动模式
- 多情景模式

GCP 上 FMCv 的网络拓扑

下图显示了在 GCP 中配置了 1 个子网的 FMCv 的典型拓扑。

图 *1: GCP* 上 *FMCv* 部署的拓扑示例



在 GCP 上部署 FMCv

以下程序介绍了如何准备 GCP 环境并启动 FMCv 实例。

创建 VPC 网络

FMCv 部署需要为管理 FMCv 使用管理 VPC。请参阅第 3 页的图 1 作为指南。

步骤 1 在 GCP 控制台中，选择 **VPC 网络 (VPC networks)**，然后单击**创建 VPC 网络 (Create VPC Network)**。
步骤 2 在**名称 (Name)** 字段中，为 VPC 网络输入描述性名称。
步骤 3 在**子网创建模式 (Subnet creation mode)**，下，单击**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。
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，然后单击**创建 (Create)**。

创建防火墙规则

每个 VPC 网络都需要防火墙规则来允许 SSH 和流量。为每个 VPC 网络创建防火墙规则。

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)**，然后单击**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-mgmt-ssh*。

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 *fmcv-south-mgmt*。

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**。

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：

a) 添加规则以允许 SSH (TCP/22)。

b) 添加规则以允许 TCP 端口 443。

您访问的 FMCv UI 需要为 HTTPS 连接打开端口 443。

步骤 8 单击**创建 (Create)**。

在 GCP 上创建 FMCv 实例

您可以按照以下步骤从 GCP 控制台部署 FMCv 实例。

步骤 1 登录到 GCP 控制台。

步骤 2 单击**导航菜单** > **市场 (Marketplace)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center (FMCv) BYOL”并选择产品。

步骤 4 单击**启动 (Launch)**。

a) **部署名称 (Deployment name)** - 为实例指定唯一的名称。

b) **映像版本 (Image version)** - 从下拉列表中选择版本。

c) **区域 (Zone)** - 选择要部署 FMCv 的区域。

d) **计算机类型 (Machine type)** - 根据 GCP 计算机类型支持， 第 1 页 选择正确的计算机类型。

e) **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。

f) 选择是允许还是**阻止使用项目级别的 SSH 密钥 (Block project-wide SSH keys)** 来访问此实例。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。

g) **启动脚本 (Startup script)** - 为 FMCv 提供 day0 配置。

以下示例显示可以在**启动脚本 (Startup script)** 字段中复制和粘贴的 day0 配置示例：

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

提示 为防止执行错误，您应使用 JSON 验证器来验证 day0 配置。

h) 从下拉列表中选择**启动磁盘类型 (Boot disk type)**。

默认情况下会选中**标准持久磁盘 (Standard Persistent Disk)**。思科建议您使用默认启动磁盘类型。

i) **启动磁盘大小 (GB) (Boot disk size in GB)** 默认值为 250 GB。思科建议您保留默认启动磁盘大小。它不能小于 250 GB。

j) 单击**添加网络接口 (Add network interface)** 以配置管理接口。

注释 创建实例后，无法将接口添加到实例。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。

- 从**网络 (Network)** 下拉列表中，选择一个 VPC 网络，例如 *vpc-branch-mgmt*。
- 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)**。
- 单击**完成 (Done)**。

k) **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 Internet (FMC GUI) 的 HTTPS 流量 (Allow HTTPS traffic from the Internet [FMC GUI])** 复选框以允许 HTTPS 连接。
- 选中**允许来自 Internet (SFTunnel comm) TCP 端口 8305 流量 (Allow TCP port 8305 traffic from the Internet [SFTunnel comm])** 复选框以允许 FMCv 和受管设备使用双向 SSL 加密通信通道进行通信。

l) 单击**更多 (More)** 展开视图并确保 **IP 转发 (IP Forwarding)** 设置为**开 (On)**。

步骤 5 单击**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 35 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。

在 GCP 上访问 FMCv 实例

确保您已创建防火墙规则以允许 SSH（通过端口 22 的 TCP 连接）；有关详细信息，请参阅创建防火墙规则，第 4 页。

此防火墙规则允许访问 FMCv 实例，并允许您使用以下方法连接到实例。

- 外部 IP
  - 浏览器窗口
  - 任何其他 SSH 客户端或第三方工具
- 串行控制台
  - Gcloud 命令行

有关详细信息，请参阅 Google 文档连接到实例 (Connecting to instances)。

注释 如果选择不添加 Day0 配置，则可以使用默认凭证登录到 FMCv 实例。系统会提示您在首次登录时设置密码。

使用串行控制台连接至 FMCv 实例

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 单击 FMCv 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，单击**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)。

使用外部 IP 连接至 FMCv 实例

FMCv 实例分配有内部 IP 和外部 IP。您可以使用外部 IP 来访问 FMCv 实例。

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 单击 FMCv 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，单击 **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 FMCv 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 Gcloud 连接至 FMCv 实例

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 单击 FMCv 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，单击 **SSH** 字段的下拉菜单。

步骤 4 单击**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。