# 在 Google 云平台上部署 ASAv

您可以在 Google 云平台 (GCP) 上部署 ASAv。



# 关于 GCP 上的 ASAv 部署

GCP 允许您在与 Google 相同的基础设施上构建、部署和扩展应用、网站及服务。

Cisco 自适应安全虚拟设备（ASAv）与物理 Cisco Asa 运行相同的软件，以虚拟外形规格提供经验证的安全功能。ASAv 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。

### GCP 计算机类型支持

选择 Google 虚拟机类型和大小以满足 ASAv 需求。

ASAv支持以下通用 *N1*、*N2* 和计算优化 *C2* GCP 计算机类型：

**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** | **内存 (GB)** |
| c2-standard-4 | 4 | 16 |
| c2-standard-8 | 8 | 32 |
| c2-standard-16 | 16 | 64 |

表 2: 支持的通用计算机类型

| 计算机类型 | 属性 | |
|---|---|---|
| | vCPU | 内存 (GB) |
| n1-standard-4 | 4 | 15 |
| n1-standard-8 | 8 | 30 |
| n1-standard-16 | 16 | 60 |
| n2-standard-4 | 4 | 16 |
| n2-standard-8 | 8 | 32 |
| n2-standard-16 | 16 | 64 |
| n1-highcpu-8 | 8 | 7.2 |
| n1-highcpu-16 | 16 | 14.4 |
| n2-highcpu-8 | 8 | 8 |
| n2-highcpu-16 | 16 | 16 |
| n2-highmem-4 | 4 | 32 |
| n2-highmem-8 | 8 | 64 |
| n2-highmem-16 | 16 | 128 |

- ASAv 至少需要 3 个接口。
- 支持的最大 vCPU 数量为 16 个。
- 不支持内存优化计算机类型

您可以在 GCP 上创建帐户、使用 GCP 市场上的思科 ASA 虚拟防火墙 (ASAv) 产品来启动 ASAv 实例，以及选择 GCP 计算机类型。

### C2 计算优化计算机的类型限制

计算优化 C2 计算机类型具有以下限制：

- 不能将区域持久性磁盘用于计算优化的计算机类型。有关详细信息，请参阅 Google 文档添加或调整区域持久性磁盘大小 (Adding or resizing regional persistent disks)。
- 受与通用和内存优化计算机类型不同的磁盘限制。有关详细信息，请参阅 Google 文档块存储性能 (Block storage performance)。
- 仅在所选区域和地区中可用。有关详细信息，请参阅 Google 文档可用地区和区域 (Available regions and zones)。
- 仅在选定的 CPU 平台上可用。有关详细信息，请参阅 Google 文档 CPU 平台 (CPU platforms)。

# ASAv 和 GCP 的前提条件

- 在 https://cloud.google.com 创建一个 GCP 账户。
- 创建 GCP 项目。请参阅 Google 文档创建项目 (Creating Your Project)。
- 许可 ASAv。在您许可 ASAv 之前，ASAv 将在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅许可证：智能软件许可（Firepower 上的 ASAv、ASA）。
- 接口要求：
  - 管理接口 - 用于将 ASAv 连接到 ASDM；不能用于直通流量。
  - 内部接口 - 用于将 ASAv 连接到内部主机。
  - 外部接口 - 用于将 ASAv 连接到公共网络。
- 通信路径：
  - 用于访问 ASAv 的公共 IP。
- 有关 ASAv 的系统要求，请参阅思科 ASA 兼容性矩阵。

# ASAv 和 GCP 的准则和限制

### 支持的功能

GCP 上的 ASAv 支持以下功能：

- GCP 虚拟私有云 (VPC) 中的部署
- 每个实例最多 16 个 vCPU
- 路由模式（默认）
- 许可 - 仅支持 BYOL

### 不支持的功能

GCP 上的 ASAv 不支持以下功能：

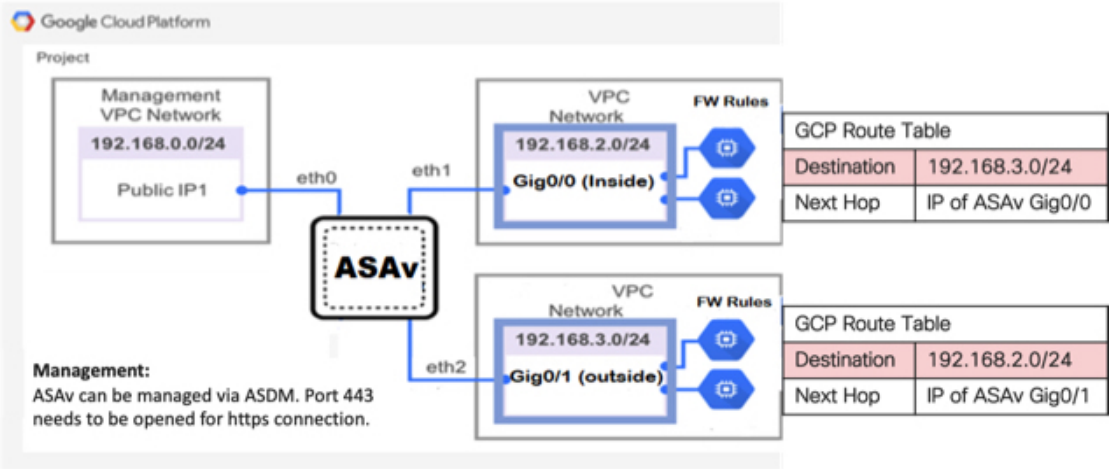
- IPv6
  - GCP 上不支持实例级 IPv6 设置
  - 只有负载均衡器可以接受 IPv6 连接，并将它们通过 IPv4 代理到 GCP 实例
- 巨型帧

- ASAv 本地高可用性
- Autoscale
- 透明/内联/被动模式

# GCP 上的 ASAv 网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASAv 的网络拓扑，在 GCP 中为 ASAv 配置了 3 个子网（管理、内部和外部）。

**图 *1: GCP* 上的 *ASAv* 部署示例**




# 在 GCP 上部署 ASAv

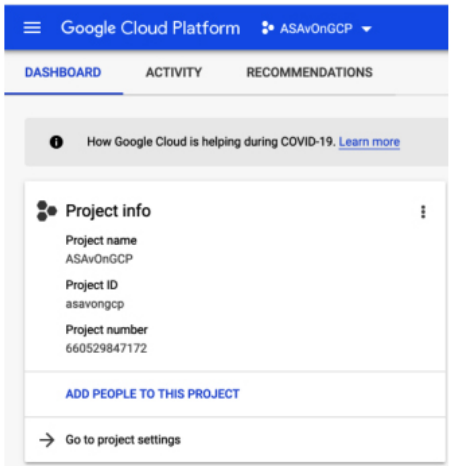
您可以在 Google 云平台 (GCP) 上部署 ASAv，这是一种公共云计算服务，让您能够在 Google 提供的高度可用的托管环境中运行应用。

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，请单击导航菜单 > 主页 (Home) > 控制面板 (Dashboard)。

图 2: 示例 GCP 控制面板




您可以登录 GCP 控制台，在 GCP 市场中搜索思科 ASA 虚拟防火墙 (ASAv) 产品，然后启动 ASAv 实例。以下程序介绍了如何准备 GCP 环境并启动 ASAv 实例，以便部署 ASAv。

# 创建 VPC 网络

### 开始之前

ASAv 部署需要三个网络，您必须在部署 ASAv 之前创建这些网络。网络如下：

- 管理子网的管理 VPC。
- 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 ASAv。路由表和防火墙规则与在 ASAv 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 上的 ASAv 网络拓扑示例，第 4 页。

**步骤 1** 在 GCP 控制台中，依次选择网络 (Networking) > VPC 网络 (VPC network) > 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，输入您的 VPC 网络的描述性名称，例如，*vpc-asiasouth-mgmt*。

**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，例如 *vpc-asiasouth-mgmt*。

**步骤 5** 从区域 (Region) 下拉列表中，选择适合您的部署的区域。所有三个网络都必须位于同一区域。

**步骤 6** 在 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)。

**步骤 8** 重复步骤 1-7，在您的 VPC 中创建其余两个网络。

# 创建防火墙规则

在部署 ASAv 实例时，请为管理接口应用防火墙规则（以允许 SSH 和 HTTPS 连接），请参阅在 GCP 上创建 ASAv 实例，第 6 页。根据您的要求，您还可以为内部和外部接口创建防火墙规则。

**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-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 *asav-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** 单击**创建 (Create)**。

# 在 GCP 上创建 ASAv 实例

完成以下步骤，使用来自 GCP Marketplace 的 Cisco ASA 虚拟防火墙 (ASAv) 产品部署 ASAv 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 Marketplace 中搜索“Cisco ASA 虚拟防火墙 (ASAv)”(Cisco ASA virtual firewall [ASAv])并选择该产品。

**步骤 4** 单击**启动 (Launch)**。

**步骤 5** 为该实例添加唯一的**部署名称**。

**步骤 6** 选择要部署 ASAv 的**区域 (Zone)**。

**步骤 7** 选择适当的**计算机类型 (Machine type)**。有关支持的计算机类型的列表，请参阅关于 GCP 上的 ASAv 部署，第 1 页。

**步骤 8** （可选）将 SSH 密钥对中的公钥粘贴到 **SSH 密钥**（**可选**）下。

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。

**步骤 9** 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。

**步骤 10** （可选）在**启动脚本 (Startup script)** 下，提供 ASAv 的 day0 配置。day0 配置在 ASAv 首次启动期间应用。

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：

有关 ASA 命令的完整信息，请参阅《ASA 配置指南》和《ASA 命令参考》。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.htmlhttps://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

**重要事项** 从此示例复制文本时，应在第三方文本编辑器或验证引擎中验证脚本，以避免格式错误并删除无效的 Unicode 字符。

```
!ASA Version 9.15.1

interface management0/0

management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

**步骤 11** 为调配的磁盘空间保留默认**启动磁盘类型**和**启动磁盘大小 (GB)**。

**步骤 12** 在**网络接口**下配置以下接口。

- 管理
- 内部
- 外部

**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。

a) 从**网络 (Network)** 下拉列表中，选择一个 VPC 网络，例如 *vpc-assoso-mgmt*。
b) 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。

c) 单击**完成 (Done)**。

**步骤 13** 在**防火墙 (Firewall)** 下应用防火墙规则。

- 选中**允许来自 Internet（SSH 访问）的 TCP 端口 22 流量**复选框以允许 SSH。
- 选中**允许来自 Internet（ASDM 访问） 的 HTTPS 流量**复选框以允许 HTTPS 连接。

**步骤 14** 单击**更多 (More)** 展开视图并确保 **IP 转发 (IP Forwarding)** 设置为**开 (On)**。

**步骤 15** 单击**部署 (Deploy)**。

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 ASAv 实例

确保您已在部署期间启用防火墙规则以允许 SSH（通过端口 22 的 TCP 连接）。有关详细信息，请参阅在 GCP 上创建 ASAv 实例 ， 第 6 页。

此防火墙规则允许访问 ASAv 实例，并允许您使用以下方法连接到实例。

- 外部 IP
  - 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** 您可以使用 day0 配置中指定的凭证或在实例启动期间创建的 SSH 密钥对来登录 ASAv 实例。

# 使用外部 IP 连接到 ASAv 实例

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

注释　您可以使用 day0 配置中指定的凭证或在实例启动期间创建的 SSH 密钥对来登录 ASAv 实例。

## 使用 SSH 连接到 ASAv 实例

要从 Unix 风格的系统连接到 ASAv 实例，请使用 SSH 登录实例。

**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>
```

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 ASAv 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到 ASAv 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 ASAv 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 Gcloud 连接到 ASAv 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 ASAv 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。