在 Oracle 云基础设施上部署 ASA 虚拟

您可以在 Oracle 云基础设施 (OCI) 上部署 ASA 虚拟。

关于 OCI 上的 ASA 虚拟部署

OCI 是一种公共云计算服务，使您能够在 Oracle 提供的高度可用的托管环境中运行应用。

ASA 虚拟 运行与物理 ASA 虚拟 相同的软件，以虚拟形式提供成熟的安全功能。ASA 虚拟 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。ASA 虚拟支持以下标准 – 通用 OCI 形状类型：

表 *1: ASA* 虚拟 支持的计算资源大小

虚拟机形状	属性		接口
	oCPU	内存 (GB)	
VM.Standard2.4	4	60	最小值 3，最大值 4
VM.Standard2.8	8	120	最小值 3，最大值 8

- ASA 虚拟 至少需要 3 个接口。
- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。

- 支持的最大 vCPU 数量为 16 个（8 个 oCPU）。

您可以在 OCI 上创建帐户，使用 Oracle 云市场上的思科 ASA 虚拟防火墙（ASA 虚拟）产品来启动计算实例，然后选择 OCI 形状。

ASA 虚拟和 OCI 的前提条件

- 在 https://www.oracle.com/cloud/sign-in.html 上创建账户。
- 许可 ASA 虚拟。在您许可 ASA 虚拟之前，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。
- 接口要求：
  - 管理接口
  - 内部和外部接口
  - （可选）其他子网 (DMZ)
- 通信路径：
  - 管理接口 - 用于将 ASA 虚拟连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA 虚拟连接到内部主机。
  - 外部接口（必需）- 用于将 ASA 虚拟连接到公共网络。
  - DMZ 接口（可选） - 用于将 ASA 虚拟连接到 DMZ 网络。
- 有关 ASA 虚拟 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

ASA 虚拟和 OCI 的准则和限制

支持的功能

OCI 上的 ASA 虚拟支持以下功能：

- 在 OCI 虚拟云网络 (VCN) 中部署
- 每个实例最多 16 个 vCPU（8 个 oCPU）
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- 支持单根 I/O 虚拟化 (SR-IOV)

不支持的功能

OCI 上的 ASA 虚拟不支持以下功能：

- ASA 虚拟 本地 HA
- IPv6
- 透明/内联/被动模式
- 多情景模式

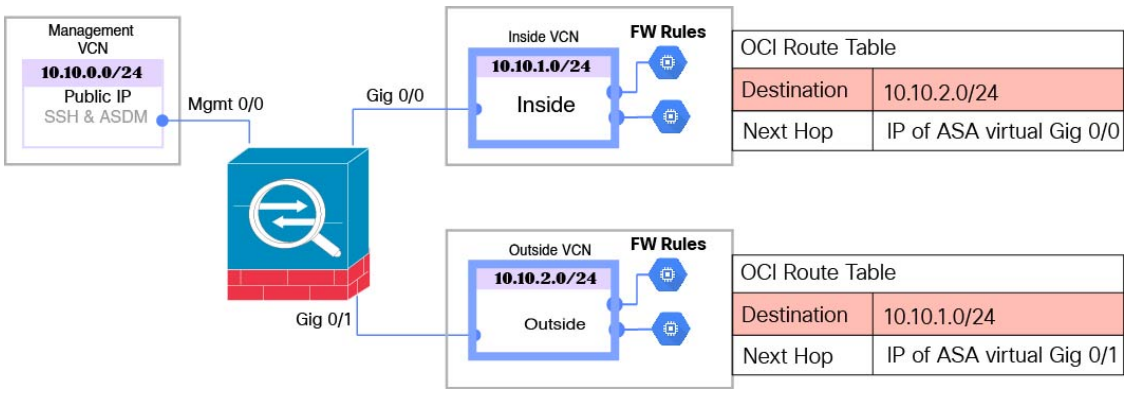
限制

- OCI 上的 ASA 虚拟部署不支持将 Mellanox 5 作为 SR-IOV 模式下的 vNIC。
- ASAv 静态和 DHCP 配置所需的单独路由规则。

OCI 上的 ASA 虚拟网络拓扑示例

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

图 *1: OCI* 上的 *ASA* 虚拟部署示例



在 OCI 上部署 ASA 虚拟

以下程序介绍了如何准备 OCI 环境并启动 ASA 虚拟实例。您可以登录 OCI 门户，在 OCI 市场中搜索思科 ASA 虚拟防火墙（ASA 虚拟）产品，然后启动计算实例。启动 ASA 虚拟后，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。

创建虚拟云网络 (VCN)

您可以为 ASA 虚拟 部署配置虚拟云网络 (VCN)。至少需要三个 VCN，每个 ASA 虚拟接口各一个。

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)**，为内部和外部接口创建 VCN。

开始之前

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”(Managing Compartments)。

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“创建虚拟云网络”(Create Virtual Cloud Networks)。

步骤 3 输入 VCN 的描述性**名称**，例如 *ASAvManagement*。

步骤 4 输入 VCN 的 **CIDR 块**。

步骤 5 点击**创建 VCN (Create VCN)**。

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。

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 *ASAv-Mgmt-Allow-22-443*。

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 SSH 通过 TCP 端口 22 访问 ASA 虚拟控制台。

b) 添加规则以允许 HTTPS 通过 TCP 端口 443 访问 ASDM。

可以通过 ASDM 来管理 ASA 虚拟，这需要为 HTTPS 连接打开端口 443。

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。

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 *ASAv-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) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。

g) 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。对于内部 VCN，您还需要一个内部子网，而对于外部 VCN，您需要一个外部子网。

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。

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)**。

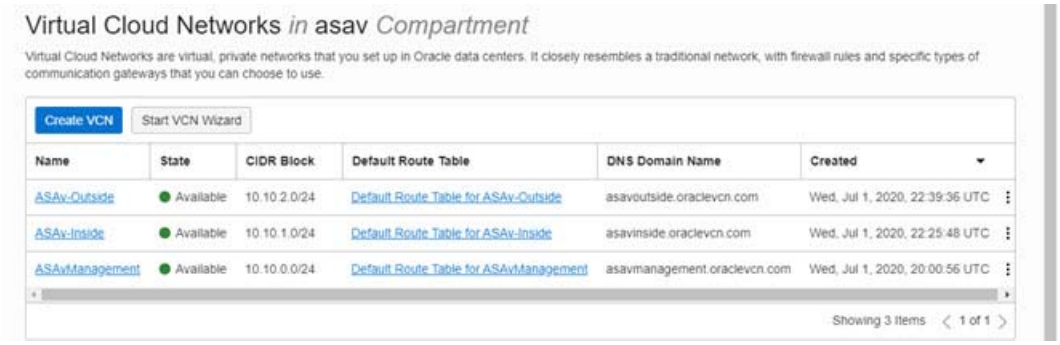
步骤 8 选择您之前创建的**安全列表**。

步骤 9 点击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN（管理、内部、外部）后，您便可以启动 ASA 虚拟。有关 ASA 虚拟 VCN 配置的示例，请参见下图。

图 *2: ASA* 虚拟 云网络



在 OCI 上创建 ASA 虚拟实例

您可以使用 Oracle 云市场中的思科 ASA 虚拟防火墙（ASA 虚拟）产品通过计算实例在 OCI 上部署 ASA 虚拟。您可以根据 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。

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 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 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 *ASAv-9-15*。

步骤 7 点击**更改形状 (Change Shape)**，然后选择包含 ASA 虚拟所需 oCPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅表 1: ASA 虚拟 支持的计算资源大小，第 1 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 ASA 虚拟提供 day0 配置。当 ASA 虚拟启动时，将应用 day0 配置。

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：

有关 ASA 命令的完整信息，请参阅《ASA 配置指南》和《ASA 命令参考》。

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 9.18.1
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 managementssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

步骤 15 点击**创建 (Create)**。

下一步做什么

监控 ASA 虚拟 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 ASA 虚拟实例从调配变为运行状态，您需要在 ASA 虚拟启动完成之前根据需要连接 VNIC。

连接接口

ASA 虚拟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 ASA 虚拟完成首次启动之前，您需要为之前创建的其他 VCN 子网（内部、外部）连接 VNIC，以便在 ASA 虚拟上正确检测 VNIC。

步骤 1 选择新启动的 ASA 虚拟实例。

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内部和外部路由表。

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 IPv4 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)**。

步骤 8 对部署所需的每个 VNIC 重复此程序。

注释 ASA 虚拟（静态和 DHCP）配置所需的单独路由规则。

在 OCI 上访问 ASA 虚拟 实例

您可以使用安全外壳 (SSH) 连接来连接到正在运行的实例。

- 大多数 UNIX 风格的系统均默认包含 SSH 客户端。
- Windows 10 和 Windows Server 2019 系统应包含 OpenSSH 客户端，如果使用 Oracle 云基础设施生成的 SSH 密钥来创建实例，则需要使用此客户端。
- 对于其他 Windows 版本，您可以从 http://www.putty.org 下载免费的 SSH 客户端 PuTTY。

前提条件

您需要以下信息才能连接到实例：

- 产品实例的公共 IP 地址。您可以从控制台的“实例详细信息”(Instance Details) 页面获取地址。打开导航菜单。在**核心基础设施 (Core Infrastructure)**，转到**计算 (Compute)** 并点击**实例 (Instances)**。然后，选择您的实例。或者，您可以使用核心服务 ListVnicAttachments 和 GetVnic 操作。
- 实例的用户名和密码。
- 启动实例时使用的 SSH 密钥对的私钥部分的完整路径。有关密钥对的详细信息，请参阅关于 Linux 实例的管理密钥对。

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 ASA 虚拟实例。

使用 SSH 连接到 ASA 虚拟实例

要从 Unix 风格的系统连接到 ASA 虚拟 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 ASA 虚拟 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 ASA 虚拟实例

要从 Windows 系统连接到 ASA 虚拟 实例，请使用 OpenSSH 登录实例。

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 ASA 虚拟 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 ASA 虚拟实例

要使用 PuTTY 从 Windows 系统连接到 ASA 虚拟 实例，请执行以下操作：

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 ASA 虚拟 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。

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。