



## 在阿里云上部署 ASA 虚拟

Cisco 自适应安全设备虚拟与物理思科 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。您可以在阿里云中部署和配置虚拟 ASA，以便保护虚拟和物理数据中心工作负载。随着时间的推移，ASA 虚拟可以扩展、收缩或移动位置。



**重要事项** 从 9.13(1) 开始，您可以在任何支持的 ASA 虚拟 vCPU/内存配置上使用任何 ASA 虚拟许可证。ASA 虚拟许可证允许 ASA 虚拟客户在各种各样的 VM 资源占用空间中运行。ASA 虚拟许可证还会增加受支持的阿里云实例类型的数量。

- [关于在阿里云上部署 ASA 虚拟，第 1 页](#)
- [ASA 虚拟和 Alibaba 的前提条件，第 2 页](#)
- [ASA 虚拟和 ASA 的功能支持和限制，第 2 页](#)
- [在 Alibaba 上部署 ASA 虚拟，第 3 页](#)
- [阿里云上的 ASA 虚拟的性能调整，第 5 页](#)

## 关于在阿里云上部署 ASA 虚拟

ASA 虚拟设备支持以下阿里云实例类型。

### 阿里云支持的实例类型



**注释** ASA 虚拟至少需要三个接口 (ENI) 且最多四个接口来支持一个实例。

### 网络要求

- 为基本 ASA 虚拟支持创建一个至少具有一个 Vswitch（子网）的 VPC。
- Vswitch 必须可用于部署实例的同一区域中，否则必须创建实例。

## 相关文档

有关实例类型及其配置的更多信息，请参阅[阿里云](#)

# ASA 虚拟和 Alibaba 的前提条件

- 在 <https://www.alibabacloud.com/> 上创建账户。
- 从 Cisco.com 下载 ASA 虚拟 qcow2 文件并将其放在 Linux 主机上：  
<http://www.cisco.com/go/asa-software>



---

**注释** 需要 Cisco.com 登录信息和思科服务合同。

---

- 许可 ASA 虚拟。在您许可 ASA 虚拟之前，该产品在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅[许可 ASA 虚拟](#)。
- 接口要求：
  - 管理接口
  - 内部和外部接口
- 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。
- 有关 ASA 虚拟的系统要求，请参阅[思科 ASA 兼容性](#)。

# ASA 虚拟和 ASA 的功能支持和限制

## 支持的功能

Alibaba 上的 ASA 虚拟支持以下功能：

- QCOW2 映像包
- 基本产品调配
- Day 0 配置
- 使用公共密钥或密码的 SSH
- Alibaba UI 控制台，用于访问 ASA 虚拟以进行任何调试。

- Alibaba UI 停止/重启
- 支持的实例类型：ecs.g5ne.large、ecs.g5ne.xlarge、ecs.g5ne.2xlarge 和 ecs.g5ne.4xlarge
- BYOL 许可证支持

#### 不支持的功能

ASA 虚拟在 7.2 版本中不支持以下功能：

- 高可用性功能
- Autoscale
- IPv6
- SR-IOV

#### 限制

- Alibaba 不支持同一 VPC 中的东西向流量，因为不允许子网级路由。
- 当前不支持透明、内联和被动模式。
- 建议使用网络增强型实例规范系列 g5ne 来部署 ASA 虚拟应用。
- 不支持巨型帧，因为它仅限于 Alibaba 提供的几种实例类型。

#### 相关文档

有关更多信息，请参阅[阿里云](#)。

## 在 Alibaba 上部署 ASA 虚拟

确保您计划部署的 ASA 虚拟的映像显示在映像配置 (Image Configuration) 上。

**步骤 1** 登录 <https://www.alibabacloud.com/> 并选择您所在的区域。

**注释** Alibaba 会被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** 创建自定义虚拟化映像

Alibaba 仅支持 QCOW2 映像。

a) 转到对象存储服务 (OSS)，然后创建存储桶并执行以下操作：

[存储桶名称](#)在您的 Alibaba 项目中必须是全局唯一的。

1. 将 QCOW2 映像从本地目录上传到 Alibaba 存储桶。

2. 在左侧导航窗格中，点击**存储桶 (Buckets) > ASA 虚拟存储桶 (ASA Virtualbucket) > 上传 (Upload)**
  3. 选择**专用 (Private)** 作为 ACL，并在上传成功完成后复制对象详细信息中提到的 OSS 对象地址。
  4. 粘贴存储桶中的自定义映像的 OSS 对象地址。
  5. 选择 **Linux** 作为操作系统，选择**其他 Linux (Others Linux)** 作为变体类型。
  6. 选择 **x86\_64** 作为系统架构。
  7. 选择 **QCOW2** 作为映像格式。
  8. 选择 **BYOL** 作为许可证类型。
- b) 从上一步中的半虚拟化映像创建实例。
1. 在左侧导航窗格中，点击**映像 (Images) > 自定义映像 (Custom Image) > 操作 (Actions) > 创建实例 (Create Instance)**

### 步骤 3 从自定义映像创建实例

- a) 转至弹性计算服务 (**Elastic Compute Service**) > **创建实例 (Create Instance)**，然后选择以下选项：
1. **计费方法 (Billing Method)**: 即用即付
  2. **区域 (Region)**: 根据要求。
  3. **实例类型 (Instance Type)**: ecs.g5ne.large / ecs.g5ne.xlarge / ecs.g5ne.2xlarge / ecs.g5ne.4xlarge
  4. **数量 (Quantity)**: 根据需要。
  5. **映像 (Image)**: 在上一部分中创建的自定义映像。
  6. **系统磁盘 (System Disk)**: 最小值为 20GB。
- b) 要继续操作，请选择以下选项：
1. **VPC**: 将在其中部署 ASA 虚拟的 VPC。
  2. **Vswitch**: 主接口的子网。
  3. **分配公共 IPv4 地址 (Assign Public IPv4 Address)**: 需要通过 SSH 进行连接（如果未选择，则只能从 UI 中通过 Alibaba 的控制台连接访问虚拟 ASA）。
  4. **安全组 (Security Group)**: 选择适当的安全组。
  5. **接口 (Interfaces)**: 主接口属于在步骤 2 中选择的子网。一个实例可以部署两个接口，其余接口可以在部署后再连接。
- c) 移至下一部分并执行以下操作。
1. **密钥对 (Key-Pair)**: 对于基于密钥的登录，请生成密钥对（如果尚未生成）。您还可以使用密码来访问实例。
  2. **实例名称 (Instance-name)**: 实例的名称。

3. **Day-0 (用户数据) (Day-0 [User Data]):** 根据要求提供 Day0 配置 (不要选择 64 位基本编码)。

**Day 0 配置示例 -**

```
! ASA Version 9.x! required config start
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp
no shut
!
crypto key generate rsa modulus 2048 noconfirm
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
! required config end
```

d) 接受服务条款并创建实例。

**步骤 4** 点击启动实例 (**Launch Instance**) 以部署 ASA 虚拟。

---

## 阿里云上的 ASA 的性能调整

### VPN 优化

Alibaba c5 实例的性能比较老的 c3、c4 和 m4 实例高得多。在 c5 实例系列上，RA VPN 吞吐量 (使用 450B TCP 流量与 AES-CBC 加密的 DTLS) 大约为：

- c5.large 上 0.5Gbps
- c5.xlarge 上 1Gbps
- c5.2xlarge 上 2Gbps
- c5.4xlarge 上为 4Gbps



## 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。