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。

- 概述， 第 1 页
- 前提条件， 第 2 页
- 准则和限制， 第 2 页
- 配置策略和设备设置, on page 3
- 配置 Alibaba 环境, on page 8
- 部署 ASA Virtual， 第 8 页
- 性能调优， 第 11 页

概述

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 不支持调整阿里云上安装的 ASA 虚拟的实例类型的大小。只能部署使用不同实例类型的新 ASA 虚拟。

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

前提条件

- 在 https://www.alibabacloud.com/ 上创建账户。
- 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 Virtual。
- 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 SSH 访问以及将 ASA Virtual 连接到 ASDM。
  - 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。

准则和限制

支持的功能

Alibaba 上的 ASA 虚拟支持以下功能：

- 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 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。

配置策略和设备设置

以下各部分提供有关在部署 ASA Virtual之前需要创建和配置的资源的详细信息。

创建 VPC

虚拟私有云 (VPC) 是 Alibaba 账户专用的虚拟网络。该网络逻辑上与阿里云中的其他虚拟网络相隔离。您可以将 Management Center Virtual 和 ASA Virtual 实例等阿里云资源启动到 VPC 中。您可以配置 VPC，选择其 IP 地址范围，创建 VSwitch（子网），并配置路由表、网络网关和安全设置。

Procedure

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

阿里云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 点击**产品 (Products) > VPC**。

步骤 3 点击**VPC 控制面板 (VPC Dashboard) > 您的 VPC (Your VPCs)**。

步骤 4 点击**创建 VPC (Create VPC)**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址的 **IPv4 CIDR 块**。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) 默认的**租户设置**，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**确定 (OK)** 以创建 VPC。

What to do next

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关（NAT 网关）以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

准备工作

- 为 ASA Virtual实例创建 VPC。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard)** > **互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 3 输入用户自定义的**名称标签**以标识网关，然后点击**确定 (OK)** 以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**绑定到 VPC (Bind to VPC)** 并选择之前创建的 VPC。

步骤 6 点击**确定 (OK)** 以将网关绑定到您的 VPC。

默认情况下，在创建 NAT 网关并将其绑定到 VPC 之前，在 VPC 中启动的实例无法与互联网通信。

What to do next

添加 VSwitch（子网）到 VPC 中，详见下一部分。

添加 vSwitch

您可以对 ASA Virtual 实例可连接的 VPC IP 地址范围进行分段。您可以根据安全和运营需要创建 vSwitch（子网），以实现实例的分组。对于 ASA Virtual，您需要创建一个用于管理的 vSwitch 和用于流量的 VSwitch。

准备工作

- 为 ASA Virtual 实例创建四个 VPC。如创建 VPC 部分中所述。
- 为每个 VPC 添加一个 vSwitch（子网）。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击 **VPC 控制面板 (VPC Dashboard)** > **VSwitches**，然后点击**点击 vSwitch (Click vSwitch)**。

步骤 3 在**创建 vSwitch (Create vSwitch)** 对话框中输入以下信息：

a) 用于标识 vSwitch 的用户自定义**名称标签**。

b) 用于此 vSwitch 的 **VPC**。

c) 此 vSwitch 将驻留的**区域**。选择**无首选项 (No Preference)**，由阿里云来选择区域。

d) IP 地址 (IPv4) 的 **CIDR 块**。vSwitch 中的 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。vSwitch 大小可以与 VPC 相等。

步骤 4 点击**确定 (OK)** 以创建 vSwitch。

步骤 5 如需多个 vSwitch，重复以上步骤。为管理流量创建单独的 vSwitch，根据需要为数据流量创建多个 vSwitch。

What to do next

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为VPC配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard)** > **路由表 (Route Tables)**，然后点击**创建路由 (Create Route)**。

步骤 3 输入用于标识路由表的用户自定义**名称标签**。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击**确定 (OK)**以创建路由表。

步骤 6 选择创建的路由表。

步骤 7 点击**路由 (Routes)** 选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击**编辑 (Edit)**，然后点击**添加其他路由 (Add another route)**。

a) 在**目标 (Destination)** 列中，为所有 IPv4 流量输入 **0.0.0.0/0**。

b) 在**目标**列中，选择您的网关。

步骤 9 点击**保存**。

What to do next

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。

Procedure

步骤 1 点击**产品 (Products)** > **ECS**。

步骤 2 点击**ECS 控制面板 (ECS Dashboard)** > **安全组 (Security Groups)**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站规则 (Inbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)**。

Note
要从 Alibaba 外部管理 Management Center Virtual，需要 HTTPS 和 SSH 访问。您应指定相应的源 IP 地址。此外，如果在 Alibaba VPC 内同时配置 Management Center Virtual 和 ASA Virtual，则应允许专用 IP 管理子网访问。

b) 点击**出站规则 (Outbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)** 以添加出站流量规则，或保留**所有流量 (All traffic)**（作为**类型 (Type)**）和**任意位置 (Anywhere)**（作为**目标 (Destination)**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

What to do next

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址（IPv4）或 DHCP 为 ASA Virtual 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

Procedure

步骤 1 点击**服务 (Services)** > **弹性网络接口 (Elastic Network Interface)**。

步骤 2 点击**网络接口 (Network Interfaces)**。

步骤 3 点击**创建网络接口 (Yes, Create)**。

步骤 4 在**创建网络接口**对话框中输入以下信息：

a) 网络接口的用户自定义**说明**（可选）。

b) 从下拉列表中选择一个 **vSwitch**。确保选择要创建 ASA Virtual 实例所在 VPC 的 vSwitch。

c) 输入**专用 IP** 地址。您可以使用静态 IP 地址 (IPv4) 或自动生成 (DHCP)。

d) 选择一个或多个**安全组**。确保安全组已打开所有必需的端口。

步骤 5 点击**创建网络接口 (Create network interface)** 以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键点击并选择**修改源/目的地址检查**。

步骤 8 取消选中**源/目标 (Source/destination check)** 复选框下的**启用 (Enable)** 复选框，然后点击**保存 (Save)**。

What to do next

创建弹性 IP 地址，详见下一部分。

创建弹性 IP 地址

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址 (IPv4) 会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是一个保留的公共 IP 地址，用于远程访问 ASA Virtual 和其他实例。

Procedure

步骤 1 点击**产品 (Products)** > **弹性计算服务 (Elastic Compute Service)**。

步骤 2 在**弹性计算服务 (Elastic Compute Service)** 控制面板中，点击左侧菜单中的**弹性 IP (Elastic IP)**。

步骤 3 点击**分配弹性 IP 地址 (Allocate Elastic IP Address)**。

步骤 4 配置 EIP 设置：

a) 选择要分配 EIP 的**区域**。

b) 为 EIP 选择所需的带宽计划。例如，BYOL 或订用。

c) 指定所需的带宽量。
d) 查看您的选择，然后点击**确定 (OK)** 以分配 EIP。

步骤 5 将 EIP 与实例关联：

a) 分配 EIP 后，转至**弹性计算服务 (Elastic Compute Service)** 控制面板中的**弹性 IP (Elastic IP)** 部分。
b) 找到您创建的 EIP，然后点击**关联 (Associate)**。
c) 选择要与 EIP 关联的 ECS 实例，然后点击**确定 (OK)**。

步骤 6 确保 EIP 现在列在关联的 ECS 实例下，并验证其连接性。

What to do next

部署 ASA Virtual，详见下一部分。

配置 Alibaba 环境

要在 Alibaba 部署 ASA Virtual，需要根据部署的特定要求和设置来配置 Alibaba VPC。在大多数情况下，设置向导将引导您完成设置过程。Alibaba 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关更多信息，请参阅阿里云文档。

ASA Virtual 部署需要四个网络虚拟私有云 (VPC)，您必须在部署 ASA Virtual之前创建这些网络。

这三个网络 VPC 包括：

- 管理子网的管理 VPC。
- 内部子网的内部 VPC。
- 外部子网的外部 VPC。

为更好地控制 Alibaba 设置，以下部分提供有关在启动 ASA Virtual 实例之前如何配置 VPC 和 EC2 的指南：

准备工作

- 创建您的阿里云账户。

部署 ASA Virtual

以下操作程序概要列出了在阿里云上部署 ASA Virtual 的步骤。

过程

步骤 1 转到 https://marketplace.alibabacloud.com/ 并搜索 **Cisco Secure Firewall ASA Virtual (NGFWv) - BYOL** 产品以部署 ASA Virtual。

注释
Alibaba 会被划分为彼此隔离的多个区域。区域显示在窗口的右上角。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 点击产品链接以打开 **Cisco Secure Firewall ASA Virtual - BYOL** 页面。

步骤 3 点击**选择您的计划 (Choose Your Plan)**。您将被重定向到**弹性计算服务 (Elastic Compute Service)** 页面。

步骤 4 在**自定义启动 (Custom Launch)** 部分中输入以下详细信息：

- **计费方法 (Billing Method)**：根据要求。

  注释
  计费方式适用于阿里云上的基础设施，您可以根据需要选择。

- **区域 (Region)**：根据要求。
- **网络和区域 (Network and Zone)**：从下拉列表中选择 VPC 和您之前创建的管理 vSwitch，或者使用**创建 VPC (Create VPC)** 和**创建 vSwitch (Create vSwitch)** 链接重新创建。

步骤 5 移至**实例和映像 (Instances and Images)** 页面。

在**所有实例类型 (All Instance Types)** 部分下，执行以下操作：

- **实例 (Instance)**：选择以下任何受支持的实例类型 - **ecs.g5ne.large**、**ecs.g5ne.xlarge**、 **ecs.g5ne.2xlarge** 或 **ecs.g5ne.4xlarge**。
- **映像 (Image)**：最新的 ASA Virtual 市场版本显示在**市场映像 REC** 部分中。
  1. 点击**重新选择映像 (Reselect Image)**。系统将显示“阿里云市场映像”对话框，其中包含您正在部署的 ASA Virtual 映像详细信息。
  2. 从下拉列表中选择 ASA Virtual 设备并点击**选择 (Select)**。

步骤 6 转到**存储 (Storage)** 部分。保留默认值并继续。

步骤 7 转到**带宽和安全组 (Bandwidth and Security Groups)** 部分并执行以下操作：

- **ENI**
  - **安全组 (Security Group)**：选择适当的安全组。
  - **主 ENI (Primary ENI)**：输入在**网络和区域 (Network and Zone)** 字段中选择的主接口，即管理 vSwitch。
  - **辅助 ENI (Secondary ENI)**：从**现有辅助接口 (Existing Secondary Interface)** 下拉列表中选择辅助接口，或通过选择所需的 vSwitch 创建新的辅助接口。

注释
在实例启动阶段，可以使用一个或两个（主要或主要和次要ENI）接口来部署实例，并且可以在从ECS控制台部署后连接其他接口。

- **密钥对 (Key Pair)**：从下拉列表中选择现有的密钥对或创建新的密钥对。

步骤 8 转到**高级设置 (Advance Settings)** 并执行以下操作：

- **实例名称 (Instance Name)**：合适的实例名称。
- **用户数据 (User Data)**：根据要求提供 Day-0 配置（不要选中**输入 Base64 编码的信息 (Enter Base64 Encoded iInformation)** 复选框）。

  使用管理中心来管理 ASA Virtual 的 Day-0 配置示例：

```
{
"ASA Version
!
interface management0/0
nameif management
security-level 100
no shut

interface gigabitethernet0/0
nameif inside
security-level 100
no shut

interface gigabitethernet1/0
nameif outside
security-level 100
no shut

crypto key generate rsa general-keys modulus 4096
ssh ::/0 inside
ssh timeout 60
ssh version 2
aaa authentication ssh console LOCAL

dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
}
```

步骤 9 接受 **ECS 服务条款**，然后点击**创建订单 (Create Order)**。
ASA Virtual 使用两个接口来启动，您可以在 ECS 控制台上查看接口。

步骤 10 要使用其他两个接口来配置 ASA Virtual ，请执行以下操作：

a) 在阿里云上，转到**弹性计算服务 (Elastic Compute Service)**。
b) 点击左侧窗格中**网络和安全 (Network & Security)** 下的 **弹性网络接口 (Elastic Network Interface)**。
c) 搜索之前创建的流量接口。
d) 选中与流量接口对应的复选框，然后点击**绑定到实例 (Bind to Instance)**。系统将显示**绑定到实例 (Bind to Instance)** 对话框。
e) 在**实例 (Instance)** 字段中输入 ASA Virtual 名称。
f) 点击**确认 (Confirm)**，将其配置为实例的 **eth2** 接口。

步骤 11　点击 **EC 控制面板 (EC Dashboard)** > **实例 (Instances)**。

下一步做什么

继续使用可通过 SSH 输入的 CLI 命令进行配置，或使用 ASDM。有关访问 ASDM 的说明，请参阅启动 ASDM。

性能调优

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。