部署 Firepower Threat Defense Virtual

本章介绍如何从 AWS 门户部署 Firepower Threat Defense Virtual。

- 部署 Firepower Threat Defense Virtual 实例, on page 1

部署 Firepower Threat Defense Virtual 实例

Before you begin

Cisco 建议以下操作：

- 如配置 AWS 环境中所述，配置 AW VPC 和 EC2 元素。
- 确认 AMI 可用于 Firepower Threat Defense Virtual 实例。

Procedure

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 登录 Amazon Marketplace 后，单击所提供的 Firepower Threat Defense Virtual 链接 (Cisco Firepower NGFW Virtual (NGFWv) - BYOL)。

Note 如果之前已登录 AWS，您可能需要注销并重新登录，以确保链接有效。

步骤 3 单击**继续**，然后单击**手动启动**选项卡。

步骤 4 单击**接受条款**。

步骤 5 在期望的区域单击**使用 EC2 控制台启动**。

步骤 6 选择 Firepower Threat Defense Virtual 支持的**实例类型**，建议 c4.xlarge。

步骤 7 单击屏幕底部的**下一步：配置实例详细信息**按钮：

- 更改**网络**，以匹配先前创建的 VPC。
- 更改**子网**，以匹配先前创建的管理子网。您可以指定 IP 地址或使用自动生成。
- 在网络接口下单击**添加设备**按钮以添加 eth1 网络接口。

- 更改**子网**，使其与之前创建的用于 eth0 的管理子网匹配。

Note Firepower Threat Defense Virtual 需要两个管理接口。

- 在**高级详细信息**下方，添加默认的登录信息。修改以下示例，以满足设备名称和密码要求。

小心：在**高级详细信息**字段中输入数据时，请仅使用纯文本。如果从文本编辑器复制此信息，请确保仅以纯文本形式复制。如果将任何 Unicode 数据（包括空格）复制到**高级详细信息**字段，可能会造成实例损坏，然后您必须终止此实例并重新创建实例。

使用 Firepower Management Center 管理 FTDv 的登录配置示例：

```
#Sensor { "AdminPassword": "<your_password>", "主机名": "<Your_hostname>", "ManageLocally":
"No", "FmcIp": "<FMC 的 IP 地址>", "FmcRegKey":"<registration_passkey>",
"FmcNatId":"<NAT_ID_if_required>", }
```

使用 Firepower Device Manager 管理 FTDv 的登录配置示例：

```
#Sensor { "AdminPassword": "<your_password>", "主机名": "<Your_hostname>", "ManageLocally":
"Yes", }
```

步骤 8 单击**下一步：添加存储**。

您可以接受默认值或更改卷。

步骤 9 单击**下一步：标记实例**。

标签由区分大小写的键值对组成。例如，您可以按照“**Key = 名称**”和“**Value = 防火墙**”的格式定义标签。

步骤 10 选择**下一步：配置安全组**。

步骤 11 单击**选择现有安全组**并选择先前配置的安全组，或创建新的安全组；有关创建安全组的详细信息，请参阅 AWS 文档。

步骤 12 单击**检查和启动**。

步骤 13 单击**启动**。

步骤 14 选择现有的密钥对或创建新的密钥对。

Note 您可以选择现有的密钥对或者创建新的密钥对。密钥对由 AWS 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 15 单击**启动实例**。

步骤 16 单击**查看启动**，然后按照提示进行操作。

步骤 17 单击 **EC2 控制面板 > 网络接口**。

步骤 18 查找之前在配置 AWS 环境中创建的流量接口，然后单击**连接**。这将成为 Firepower Threat Defense Virtual 实例上的 **eth2** 接口。

步骤 19 查找之前在配置 AWS 环境中创建的流量接口，然后单击**连接**。这将成为 Firepower Threat Defense Virtual 实例上的 **eth3** 接口。

Note 您必须配置四个接口，否则 Firepower Threat Defense Virtual 将不会完成启动过程。

步骤 20 单击 **EC2 控制面板 > 实例**。

步骤 21 右键单击实例，然后选择**实例设置 > 获取系统日志**以查看状态。

Note 系统可能会显示连接问题的警告。这在预料之内，因为 eth0 接口在 EULA 完成之前不会激活。

步骤 22 20 分钟后，您应该能够将 Firepower Threat Defense Virtual 注册到 Firepower Management Center。

What to do next

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器**选择**否**，您将使用 Firepower 管理中心 管理 FTDv；请参阅使用 Firepower 管理中心管理 Firepower Threat Defense Virtual。
- 如果为**启用本地管理器**选择**是**，您将使用集成的 Firepower 设备管理器 管理 FTDv；请参阅使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual。

有关如何选择管理选项的概述，请参阅如何管理您的 Firepower 设备。