Firepower Threat Defense Virtual 和 AWS 入门

Amazon 虚拟私有云 (Amazon VPC) 使您可以在自定义的虚拟网络中启动 Amazon Web 服务 (AWS) 资源。此虚拟网络非常类似于您可能在自有数据中心内运行的传统网络，并且具有使用 AWS 可扩展基础设施所带来的优势。

本文档说明如何在 AWS 上部署 Firepower Threat Defense Virtual。

关于 FTDv 和 AWS 云

AWS 是一种公共云环境。Firepower Threat Defense Virtual 在以下实例类型的 AWS 环境中作为访客运行。

注释 Firepower 版本 6.6 加入了对下表中所示 C5 实例类型的支持。较大的实例类型可为 AWS 虚拟机提供更多 CPU 资源，从而提高性能，有些则提供更多网络接口。

表 *1: AWS* 支持的 *FTDv* 实例

实例类型	vCPU	内存 (RAM)	vNic
C5.xlarge	4	8 GB	4
C5.2xlarge	8	16 GB	4
C5.4xlarge	16	32 GB	8
C4.xlarge	4	7.5 GB	4

实例类型	vCPU	内存 (RAM)	vNic
C3.xlarge	4	7.5 GB	4

如何管理您的 Firepower 设备

您可以通过两种方法来管理您的 Firepower 威胁防御设备。

Firepower 设备管理器

Firepower 设备管理器 (FDM) 板载集成的管理器。

FDM 是一个基于 Web 的配置界面，在部分 Firepower 威胁防御 设备上可用。您可以通过 FDM 配置最常用于小型网络的软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 Firepower 威胁防御 设备的大型网络。

注释 有关支持 FDM 的 Firepower 威胁防御 设备的列表，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》。

Firepower 管理中心

思科 Firepower 管理中心 (FMC)。

如果要管理大量设备或要使用 Firepower 威胁防御 支持的更复杂的功能和配置，请使用 FMC（而不是集成的 FDM）来配置您的设备。

重要事项 您不能同时使用 FDM 和 FMC 管理 Firepower 设备。FDM 集成管理功能启用后，将无法使用 FMC 来管理 Firepower 设备，除非您禁用本地管理功能并重新配置管理功能以使用 FMC。另一方面，当您向 FMC 注册 Firepower 设备时，FDM 板载管理服务会被禁用。

注意 目前，Cisco 不提供将 FDM Firepower 配置迁移到 FMC 的选项，反之亦然。选择为 Firepower 设备配置的管理类型时，请考虑这一点。

AWS 解决方案概述

AWS 是由 Amazon.com 提供并构成云计算平台的一系列远程计算服务（也称为 Web 服务）。这些服务遍布全球 11 个地区。通常，在部署 Firepower Management Center Virtual 和 Firepower Threat Defense Virtual 时，您应该会熟悉以下 AWS 服务：

- Amazon 弹性计算云 (EC2) - 使您能够通过租用虚拟计算机，在 Amazon 数据中心启动和管理自己的应用和服务（例如防火墙）的 Web 服务。
- Amazon 虚拟私有云 (VPC) - 使您能够配置 Amazon 公共云中的隔离专用网络的 Web 服务。您可以在 VPC 内运行自己的 EC2 实例。
- Amazon 简单存储服务 (S3) - 提供数据存储基础设施的 Web 服务。

您可以在 AWS 上创建账户，设置 VPC 和 EC2 组件（使用 AWS 向导或手动配置），并选择 Amazon 系统映像 (AMI) 实例。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

Note AMI 映像在 AWS 环境之外不可下载。

Firepower Threat Defense Virtual 前提条件

- 拥有 Amazon 账户。您可以在 http://aws.amazon.com/ 创建一个。
- 思科智能账户。您可以在 Cisco 软件中心创建一个https://software.cisco.com/
- 许可 Firepower Threat Defense Virtual。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower 管理中心配置指南》中的“Firepower 系统许可”。
- Firepower Threat Defense Virtual 接口要求：
  - 管理接口 (2) - 一个用于将 Firepower Threat Defense Virtual 连接到 Firepower Management Center，另一个用于诊断；无法用于直通流量。
  - 流量接口 (2) - 用于将 Firepower Threat Defense Virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于接入 Firepower Threat Defense Virtual 的公共/弹性 IP。

支持的功能和限制

支持的功能

- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署
- 路由模式（默认）
- ERSPAN 被动模式

Firepower Threat Defense Virtual 限制

- c4.xlarge 是推荐实例；c3.xlarge 实例在不同 AWS 区域的可用性受限。
- 您必须在启动期间配置两个管理接口。
- 必须有两个流量接口和两个管理接口才能启动，总计四个接口。

Note 没有四个接口，Firepower Threat Defense Virtual 将不会启动。

- 在 AWS 中配置流量接口时，必须禁用“更改源/目标检查”选项。
- 通过 CLI 或 Firepower 管理中心完成的任何 IP 地址配置必须与 AWS 控制台中创建的内容一致；在部署期间应注意配置。
- 在注册 Firepower Threat Defense Virtual 后，必须在 Firepower Management Center 编辑并启用这些接口；请注意，IP 地址必须与 AWS 配置的接口匹配。
- 目前不支持 IPv6。
- 目前不支持透明/内联/被动模式。
- 修改接口时需要从 AWS 控制台进行更改：
  - 从 Firepower Management Center 取消注册。
  - 通过 AWS AMI 用户界面停止实例。
  - 通过 AWS AMI 用户界面分离要更改的接口。
  - 连接新接口（请记住，必须有两个流量接口和两个管理接口才能启动）。
  - 通过 AWS AMI 用户界面启动实例。
  - 重新注册到 Firepower Management Center。

- 从 Firepower Management Center 编辑设备接口，然后修改 IP 地址和其他参数，以便与通过 AWS 控制台所做的更改匹配。

- 在启动后无法添加接口。
- 目前不支持克隆/快照。

配置 AWS 环境

要在 AWS 上部署 Firepower Threat Defense Virtual，您需要使用部署特定的要求和设置配置 Amazon VPC。在大多数情况下，设置向导将引导您完成设置过程。AWS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。有关详细信息，请参阅https://aws.amazon.com/documentation/gettingstarted/。

为更好地控制 AWS 设置，以下各节为启动 Firepower Threat Defense Virtual 之前的 VPC 和 EC2 提供了指导：

- 创建 VPC, on page 5
- 添加互联网网关, on page 6
- 添加子网, on page 7
- 添加路由表, on page 7
- 创建安全组, on page 8
- 创建网络接口, on page 9
- 创建弹性 IP, on page 9

准备工作

- 创建 AWS 账户。
- 确认 AMI 可用于您的 Firepower Threat Defense Virtual 实例。

创建 VPC

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

Procedure

步骤 1 登录 http://aws.amazon.com/ 并选择您所在的区域。

AWS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 单击**服务 > VPC**。

步骤 3 单击 **VPC 控制面板 > 我的 VPC**。

步骤 4 单击**创建 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 **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 单击**是，创建**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 Firepower Threat Defense Virtual 实例创建 VPC。

Procedure

步骤 1 单击**服务 > VPC**。

步骤 2 单击 **VPC 控制面板 > 互联网网关**，然后单击**创建互联网网关**。

步骤 3 输入用户自定义的**名称标签**以标识网关，然后单击**是，创建**以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 单击**连接到 VPC** 并选择之前创建的 VPC。

步骤 6 单击**是，连接**，以将网关连接到 VPC。

默认情况下，在创建网关并将其连接到 VPC 之前，在 VPC 上启动的实例无法与互联网通信。

What to do next

添加子网到 VPC 中，详见下一部分。

添加子网

您可以对 Firepower Threat Defense 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子网，以实现实例的分组。对于虚拟 Firepower 协议防御，您需要创建一个管理子网和一个流量子网。

准备工作

- 为 Firepower Threat Defense Virtual 实例创建 VPC。

Procedure

步骤 1 单击**服务** > **VPC**。

步骤 2 单击 **VPC 控制面板** > **子网**，然后单击**创建子网**。

步骤 3 在**创建子网**对话框中输入以下信息：

a) 用于标识子网的用户自定义**名称标签**。

b) 子网所在的 **VPC**。

c) 此子网将驻留的**可用区域**。选择**无首选项**，由 Amazon 来选择区域。

d) IP 地址 **CIDR 块**。子网 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。子网大小可以与 VPC 相等。

步骤 4 单击**是，创建**以创建子网。

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

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 单击**服务** > **VPC**。

步骤 2 单击 **VPC 控制面板** > **路由表**，然后单击**创建路由表**。

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 单击**是，创建**以创建路由表。

步骤 6 选择刚创建的路由表。

步骤 7 单击**路由**选项卡，以在详细信息窗格中显示路由信息。

步骤 8 单击**编辑**，然后单击**添加其他路由**。

a) 在**目的地址**列中，输入**0.0.0.0/0**。

b) 在**目标**列中，选择您的网关。

步骤 9 单击**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 单击**服务** > **EC2**。

步骤 2 单击 **EC2 控制面板** > **安全组**。

步骤 3 单击**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) 单击**入站**选项卡，然后单击**添加规则**。

Note 要从 AWS 外部管理 Firepower 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 AWS VPC 内同时配置 Firepower Management Center Virtual 和 Firepower Threat Defense Virtual，则应允许专用 IP 管理子网访问。

b) 单击**出站**选项卡，然后单击**添加规则**以添加出站流量规则，或保留**所有流量**（作为**类型**）和**任意位置**（作为**目标**） 的默认设置。

步骤 6 单击**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 地址为 Firepower Threat Defense 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 单击**服务** > **EC2**。

步骤 2 单击 **EC2 控制面板** > **网络接口**。

步骤 3 单击**创建网络接口**。

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**子网**。确保选择要创建 Firepower Threat Defense Virtual 实例的 VPC 子网。

c) 输入**专用 IP** 地址。建议使用静态 IP 地址，而不是选择**自动分配**。

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 单击**是，创建**以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键单击并选择**更改源/目的地址检查**。

步骤 8 单击**编辑**，然后单击**添加其他路由**。

步骤 9 选择**禁用**。对于创建的任何网络接口，都要重复此操作。

What to do next

创建弹性 IP 地址，详见下一部分。

创建弹性 IP

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 是预留公共 IP，用于远程访问 Firepower Threat Defense Virtual 以及其他实例。

Note 至少，您要为 Firepower Threat Defense Virtual 管理和诊断接口创建两个弹性 IP 地址。

Procedure

步骤 1 单击**服务** > **EC2**。

步骤 2 单击 **EC2 控制面板** > **弹性 IP**。

步骤 3 单击**分配新地址**。

步骤 4 根据弹性/公共 IP 地址分配需要，重复此步骤。

步骤 5 单击**是，分配**以创建弹性 IP 地址。

步骤 6 根据部署需要，重复上述步骤以创建其他弹性 IP 地址。

What to do next

按照下一节中所述，部署 Firepower Threat Defense Virtual。