部署 Firepower Threat Defense Virtual

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

关于 Azure 部署

您可以使用模板在 Azure 中部署 FTDv。Cisco 提供两种类型的模板：

- **Azure 市场中的解决方案模板**-使用 Azure 市场中提供的解决方案模板， FTDv使用 Azure 门户部署。您可以使用现有资源组和存储帐户（或创建新的资源组和存储帐户）来部署虚拟设备。要使用解决方案模板，请参阅从 Azure 市场使用解决方案模板部署, on page 1。
- **使用来自 VHD**（可从 https://software.cisco.com/download/home 获取）的托管映像的自定义模板 - 除了基于市场的部署，Cisco 还提供一个压缩虚拟硬盘 (VHD)，您可以将其上传到 Azure 以简化 Azure 中的 FTDv 部署过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以通过一次协调操作部署并调配 FTDv 的所有资源。要使用该自定义模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 4。

从 Azure 市场使用解决方案模板部署

以下说明为您展示如何部署 Azure 市场中提供的 FTDv 解决方案模板。这是在 Microsoft Azure 环境中设置 FTDv 所需的顶级步骤列表。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

在 Azure 中部署 FTDv 时，会自动生成各种配置，例如资源、公共 IP 地址和路由表。您可以在部署后进一步管理这些配置。例如，您可能需要更改超时值较低的“空闲超时”默认值。

Note 要使用 GitHub 存储库中提供的自定义 ARM 模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 4。

Procedure

步骤 1 登录到 Azure 资源管理器 (ARM) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 依次选择 **Azure 市场** > **虚拟机**。

步骤 3 在市场中搜索“Cisco Firepower NGFW Virtual (FTDv)”，选择提供的产品，然后单击**创建**。

步骤 4 配置基本设置。

a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

Important 如果使用现有的名称，部署将失败。

b) 选择您的许可方法，可以是 **BYOL** 或 **PAYG**。

选择 **BYOL**（自带许可证）以使用 Cisco 智能许可证帐户。

选择 **PAYG**（即付即用）许可以使用基于使用的计费模式，无需购买 Cisco 智能许可。

Important 您只能在通过 Firepower Management Center 管理 FTDv 时使用 **PAYG**。

c) 输入 FTDv 管理员的用户名。

Note 名称“admin”是 Azure 中的预留名称，不能使用。

d) 选择身份验证类型：密码或 SSH 密钥。

如果您选择密码，请输入密码并确认。

如果选择 SSH 密钥，请指定远程对等体的 RSA 公共密钥。

e) 创建密码，以便搭配**管理员**用户帐户登录以配置 FTDv。

f) 选择您的订用。

g) 创建一个新资源组。

FTDv 始终会部署到新的资源组中。仅当现有资源组为空时，部署到现有资源组的选项才有效。

不过，您可以在后续步骤中配置网络选项时将 FTDv 附加到另一个资源组的现有虚拟网络。

h) 选择地理位置。对于此部署中使用的所有资源，此值应相同（例如：FTDv、网络、存储帐户）。

i) 单击**确定**。

步骤 5 配置 FTDv 设置。

a) 选择虚拟机大小。

b) 选择一个存储帐户。

Note 您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

c) 选择公共 IP 地址。

您可以为所选的订用和位置选择可用的公共 IP 地址，也可以单击**新建**。

当创建新的公共 IP 地址时，将从 Microsoft 拥有的 IP 地址块中得到一个，因此无法选择特定地址。您可以分配给接口的最大公共 IP 地址数量取决于您的 Azure 订用。

Important 默认情况下，Azure 会创建动态公共 IP 地址。当虚拟机停止和重启时，该公共 IP 可能会变化。如果您首选固定 IP 地址，则应创建静态地址。您也可以在部署后修改公共 IP 地址，将其从动态地址更改为静态地址。

d) 添加 DNS 标签。

Note 完全限定域名等于 DNS 标签加上 Azure URL：<dnslabel>.<location>.cloudapp.azure.com

e) 选择虚拟网络。

您可以选择一个现有 Azure 虚拟网络 (VNet)，或创建一个新的 VNet，然后为其输入 IP 地址空间。默认情况下，无类别域际路由 (CIDR) IP 地址为 10.0.0.0/16。

f) 为 FTDv 网络接口配置四个子网：

- **FTDv 管理**接口，连接到 Azure 中的 Nic0，是“第一子网”
- **FTDv 诊断**接口，连接到 Azure 中的 Nic1，是“第二子网”
- **FTDv 外部**接口，连接到 Azure 中的 Nic2，是“第三子网”
- **FTDv 内部**接口，连接到 Azure 中的 Nic3，是“第四子网”

g) 单击**OK**。

步骤 6 查看配置摘要，然后单击**OK**。

步骤 7 查看使用条款，然后单击**购买**。

部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 FTDv 虚拟机正在运行。

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。

从 Azure 使用 VHD 和资源模板部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 FTDv 映像。要使用 VHD 映像进行部署，您必须将 VHD 映像上传到您的 Azure 存储帐户。然后，您可以使用上传的磁盘映像和 Azure 资源管理器模板创建托管映像。Azure 模板是包含资源说明和参数定义的 JSON 文件。

开始之前

- FTDv 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。请参阅 Github 上使用 VHD 和 ARM 模板的 Azure FTDv 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50 G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

  如果您需要创建虚拟机，请使用以下方法之一：

  - 使用 Azure CLI 创建 Linux 虚拟机
  - 通过 Azure 门户创建 Linux 虚拟机

- 在 Azure 订用中，您应该在要部署 FTDv 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面下载 FTDv 压缩 VHD 映像：

a) 导航到**产品** > **安全** > **防火墙** > **下一代防火墙 (NGFW)** > **Firepower NGFW Virtual**。

b) 单击 **Firepower Threat Defense 软件**。

按照说明下载映像。

例如，Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2

步骤 2 将压缩 VHD 映像复制到您在 Azure 中的 Linux 虚拟机。

用于将文件上传到 Azure 和从 Azure 下载文件的选择很多。此示例显示的是 SCP，即安全复制：

```
# scp /username@remotehost.com/dir/Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd. bz2
 <linux-ip>
```

步骤 3 登录到 Azure 中的 Linux 虚拟机，并导航至复制了压缩 VHD 映像的目录。

步骤 4 解压缩 FTDv VHD 映像。

用于解压文件的选择很多。此示例显示的是 Bzip2 实用程序，但也可以使用一些基于 Windows 的实用程序。

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2
```

步骤 5 将 VHD 上传到您的 Azure 存储帐户中的容器。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

用于将 VHD 上传到您的存储帐户的选择很多，包括 AzCopy、Azure 存储复制 Blob API、Azure 存储资源管理器、Azure CLI 或 Azure 门户。对于像 FTDv 这样大的文件，我们不建议使用 Azure 门户。

下例显示了使用 Azure CLI 的语法：

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

步骤 6 从 VHD 创建托管映像：

a) 在 Azure 门户中，选择 **Images**。
b) 单击 **Add** 创建新映像。
c) 提供以下信息：

- **名称** - 为托管映像输入用户定义的名称。
- **订用** - 从下拉列表中选择订用。
- **资源组** - 选择现有资源组或创建一个新资源组。
- **操作系统磁盘** - 选择 Linux 作为操作系统类型。
- **存储 Blob** - 浏览到存储帐户以选择上传的 VHD。
- **帐户类型** - 从下拉列表中选择“标准 (HDD)”。
- **主机缓存** - 从下拉列表中选择“读/写”。
- **数据磁盘** - 保留默认设置；请勿添加数据磁盘。

d) 单击 **Create**。

等待 **Notifications** 选项卡下显示 **Successfully created image** 消息。

注释 创建托管映像之后，可以删除上传的 VHD 和上传存储帐户。

步骤 7 获取新创建的托管映像的资源 ID。

在内部，Azure 将每个资源与一个资源 ID 相关联。从该托管映像部署新 FTDv 防火墙时，将需要资源 ID。

a) 在 Azure 门户中，选择 **Images**。
b) 选择上一步中创建的托管映像。
c) 单击 **Overview** 查看映像属性。
d) 将 **Resource ID** 复制到剪贴板。

Resource ID 采用以下形式：

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

步骤 8 使用托管映像和资源模板构建 FTDv 防火墙：

a) 选择 **New**，然后搜索 **Template Deployment**，直至可从选项中选择它。
b) 选择 **Create**。
c) 选择 **Build your own template in the editor**。

您有一个可供自定义的空模板。请参阅 Github 上使用 VHD 和 ARM 模板的 Azure FTDv 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。

d) 将您的自定义 JSON 模板代码粘贴到窗口中，然后单击 **Save**。
e) 从下拉列表中选择 **Subscription**。
f) 选择现有 **Resource group** 或创建一个新资源组。
g) 从下拉列表中选择 **Location**。
h) 将上一步中的托管映像 **Resource ID** 粘贴到 **Vm Managed Image Id** 字段中。

步骤 9 单击 **Custom deployment** 页面顶部的 **Edit parameters**。您有一个可供自定义的参数模板。

a) 单击**加载文件**，然后浏览到自定义 FTDv 参数文件。请参阅 Github 上使用 VHD 和 ARM 模板的 Azure FTDv 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。
b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后单击 **Save**。

步骤 10 检查自定义部署详细信息。请确保 **Basics** 和 **Settings** 中的信息与您预期的部署配置（包括 **Resource ID**）相符。

步骤 11 仔细阅读条款和条件，然后选中 **I agree to the terms and conditions stated above** 复选框。

步骤 12 单击**购买**，使用托管映像和自定义模板部署 FTDv 防火墙。

如果您的模板和参数文件中不存在冲突，则部署应该会成功。

托管映像可用于同一个订用和区域内的多个部署。

下一步做什么

- 在 Azure 中更新 FTDv 的 IP 配置。