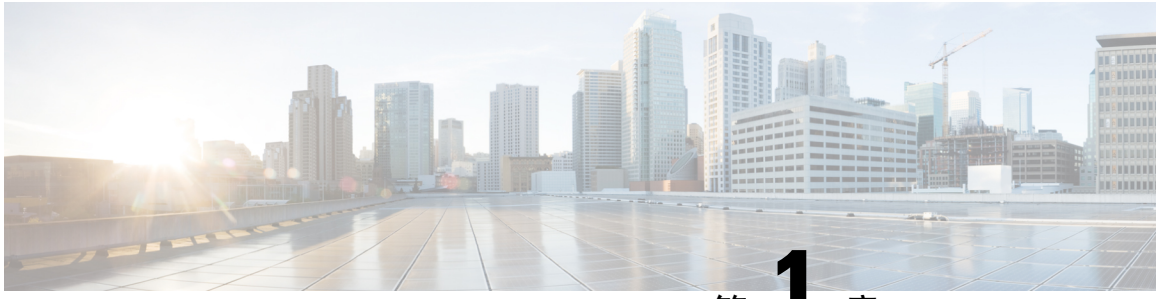
适用于 Microsoft Azure Cloud 的 Cisco Firepower Threat Defense Virtual 快速入门指南

首次发布日期: 2018 年 8 月 23 日

上次修改日期: 2020 年 7 月 13 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

Firepower Threat Defense Virtual 和 Azure 入门

思科 Firepower Threat Defense Virtual（FTDv）将 Cisco Firepower 新一代防火墙功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

本章介绍 Firepower Threat Defense Virtual 如何在 Azure 市场中运行，包括功能支持、系统要求、准则和限制。本章还介绍了管理 FTDv 的选项。

在开始部署之前，了解您的管理选项非常重要。您可以使用 Firepower 管理中心 或 Firepower 设备管理器 管理和监控 FTDv。其他管理选项也可能可用。

关于 FTDv 和 Microsoft Azure 云

FTDv (Firepower Threat Defense Virtual) 集成到 Microsoft Azure 市场中，支持以下实例类型：

- 标准 D3 - 4 个 vCPU，14 GB，4vNIC
- 标准 D3_v2 - 4 个 vCPU，14 GB，4vNIC
- 标准 D4_v2 - 8 个 vCPU，28 GB，8 个 vNIC（**版本 6.5 中新增**）
- 标准 D5_v2 - 16 个 vCPU，56 GB，8 个 vNIC（**版本 6.5 中新增**）

FTDv 和 Azure 的前提条件和要求

前提条件

- Microsoft Azure 帐户。您可以在 https://azure.microsoft.com/en-us/ 创建一个。

  在 Azure 上创建帐户之后，您可以登录、在市场中搜索 Cisco Firepower Threat Defense，然后选择“Cisco Firepower NGFW Virtual (NGFWv)”项。

- 思科智能账户。您可以在 Cisco 软件中心创建一个。

  许可 FTDv；有关 Firepower 系统功能许可的概述，包括有用的链接，请参阅 Cisco Firepower 功能许可证。

- 有关 FTDv 与 Firepower 系统的兼容性，请参阅《Cisco Firepower 威胁防御虚拟兼容性》。

通信路径

- 管理接口 - 用于将 FTDv 连接到 Firepower Management Center。
- 诊断接口 - 用于诊断和报告；不能用于直通流量。
- 内部接口（必需）- 用于将 Firepower 威胁防御虚拟连接到内部主机。
- 外部接口（必需）- 用于将 Firepower 威胁防御虚拟连接到公共网络。

FTDv 和 Azure 的准则和限制

支持的功能

- 仅路由防火墙模式
- Azure 加速网络 (AN)
- 管理模式，两个选择之一：
  - 您可以使用 Firepower 管理中心 来管理您的 FTDv，请参阅使用 Firepower 管理中心管理 Firepower Threat Defense Virtual, on page 51。
  - 您可以使用集成 Firepower 设备管理器 来管理您的 FTDv，请参阅使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual, on page 67。（版本 6.5+）

Note 在 FDM (Firepower Device Manager) 模式下部署的 FTDv 设备上不支持 PAYG 许可。

- 公共 IP 寻址 - 向管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。

  您可以根据需要为其他接口分配公共IP地址；请参阅公共IP地址中Azure关于公共IP的准则，包括如何创建、更改或删除公共 IP 地址。

- Interfaces:
  - FTDv默认情况下随 4 个 vNIC 一起部署。
  - 通过支持较大的实例，您最多可以将 FTDv 随 8 个 vNIC 一起部署。
  - 要为您的 FTDv 部署添加额外的 vNIC，请遵循 Microsoft 向虚拟机添加网络接口或从虚拟机删除网络接口所提供的准则。
  - 您可以使用您的管理器配置 FTDv 接口。有关接口支持和配置的完整信息，请参阅管理平台（Firepower Management Center 或 Firepower Device Manager）对应的配置指南。

- 许可：
  - 使用 Cisco 智能许可证帐户的 BYOL（自带许可证）
  - PAYG（即付即用）许可，一种基于使用的计费模式，允许客户在不购买 Cisco 智能许可的情况下运行 FTDv。对于已注册的 PAYG FTDv 设备，将启用所有许可的功能（恶意软件/威胁/URL 过滤/VPN 等）。许可的功能无法从 FMC 编辑或修改。（版本 6.5+）

Note 在 FDM (Firepower Device Manager) 模式下部署的 FTDv 设备上不支持 PAYG 许可。

不支持的功能

- 许可：
  - PLR（永久许可证预留）。
  - PAYG（即付即用）（版本 6.4 及更低版本）

- 网络（其中很多限制是 Microsoft Azure 限制）：
  - 巨帧
  - IPv6
  - 802.1Q VLAN
  - 透明模式及其他第 2 层功能；无广播、无组播。
  - 从 Azure 的角度不归设备所有的 IP 地址的代理 ARP（影响某些 NAT 功能）。
  - 混合模式（不捕获子网流量）。
  - 内嵌设置模式，被动模式。

Note Azure 策略阻止 FTDv 在透明防火墙或内联模式下运行，因为它不允许接口在混合模式下运行。

- ERSPAN（使用在 Azure 中不会被转发的 GRE）。

- 管理：
  - 控制台访问；使用 Firepower 管理中心经由网络执行管理（SSH 可用于部分设置和维护活动）
  - Azure 门户“重置密码”功能
  - 基于控制台的密码恢复；由于用户没有实时访问控制台的权限，所以无法恢复密码。无法启动密码恢复映像。唯一的办法是部署一个新 Firepower 威胁防御虚拟虚拟机。
- 高可用性（活动/备用）
- 集群
- 虚拟机导入/导出
- FDM (Firepower Device Manager) 用户接口（版本 6.4 及更低版本）

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)。

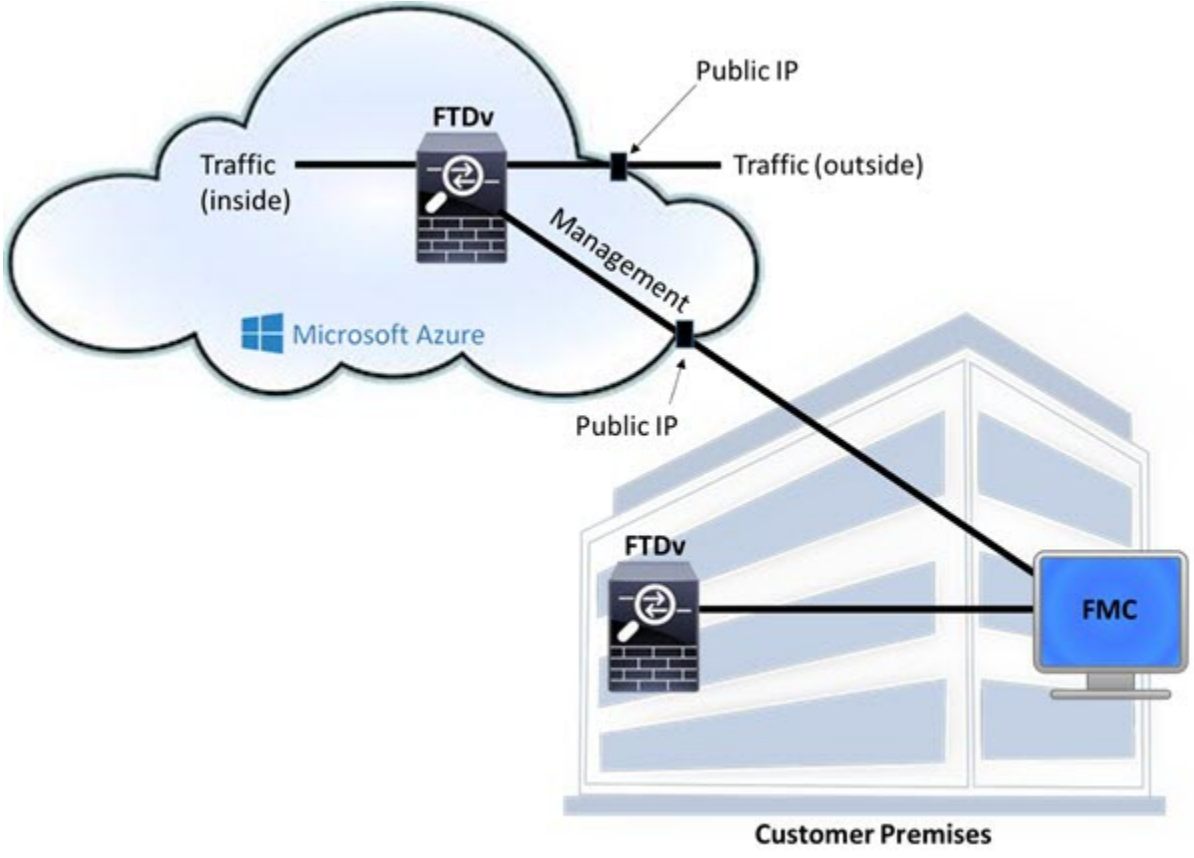
如果要管理大量设备或要使用 Firepower 威胁防御 支持的更复杂的功能和配置，请使用 FMC（而不是集成的 FDM）来配置您的设备。

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。

Azure 上 FTDv 的网络拓扑示例

下图显示了适用于 Azure 内路由防火墙模式下的 Firepower 威胁防御虚拟的典型拓扑。定义的第一个接口始终是管理接口，并且仅可为管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。



在部署期间创建的资源

在 Azure 中部署 Firepower 威胁防御虚拟时，会创建以下资源：

- Firepower 威胁防御虚拟机 (VM)
- 一个资源组
  - Firepower威胁防御虚拟始终部署到新的资源组中。不过，您可以将其附加到另一个资源组的现有虚拟网络。
- 四个 NIC，分别名为 *vm name* -Nic0、*vm name* -Nic1、*vm name* -Nic2 和 *vm name* -Nic3

  这些 NIC 分别映射到 Firepower Threat Defense Virtual 管理、诊断 0/0、GigabitEthernet 0/0 和 GigabitEthernet 0/1 接口。
- 一个名为 *vm name* -mgmt-SecurityGroup 的安全组。

  该安全组将被附加到虚拟机的 Nic0（映射到 Firepower 威胁防御虚拟管理接口）。

  该安全组包括允许 SSH（TCP 端口 22）和 Firepower 管理中心接口（TCP 端口 8305）的管理流量的规则。您可以在部署后修改这些值。
- 公共 IP 地址（根据您在部署期间选择的值命名）。

  您可以为任何接口分配一个公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。
- 如果选择了“新建网络”选项，会创建一个包含四个子网的虚拟网络。
- 每个子网的路由表（如果已存在，则相应更新）

  这些表的名称为“子网名称”-FTDv-RouteTable。

  每个路由表包含通往其他三个子网的路由，以 Firepower 威胁防御虚拟 IP 地址作为下一跳。如果流量需要到达其他子网或互联网，您可以选择添加默认路由。
- 所选存储帐户中的启动诊断文件

  启动诊断文件将在 Blobs（二进制大对象）中。
- 所选存储帐户中位于 Blobs 和容器 VHD 下的两个文件，名为 *vm name* -disk.vhd 和 *vm name* -<uuid>.status
- 一个存储帐户（除非您选择了现有的存储帐户）

Note 在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

加速网络 (AN)

Azure 的加速网络 (AN) 功能对 VM 启用单根 I/O 虚拟化 (SR-IOV)，允许 VM NIC 绕过虚拟机监控程序并直接转至下面的 PCIe 卡，以加速网络连接。AN 显著提高 VM 的吞吐性能，还会随着内核的增加（例如较大的 VM）而扩展。

AN 在默认情况下禁用。Azure 支持在预调配的虚拟机上启用 AN。您只需在 Azure 中停止 VM 并更新网卡属性，即可将 *enableAcceleratedNetworking* 参数设置为 true。请参阅 Microsoft 文档：在现有虚拟机上启用加速网络。然后重新启动 VM。

Azure 路由

Azure 虚拟网络子网中的路由取决于子网的有效路由表。有效路由表由内置系统路由和用户定义路由 (UDR) 表中的路由组合而成。

Note 您可以在 VM NIC 属性下查看有效路由表。

您可以查看和编辑用户定义路由表。如果有效路由表是由系统路由与用户定义路由组合而成，系统会优先使用最具体的路由，并关联至用户定义路由表。系统路由表包括指向 Azure 虚拟网络互联网网关的默认路由 (0.0.0.0/0)。系统路由表还包括通往其他已定义子网的具体路由（下一跳指向 Azure 的虚拟网络基础设施网关）。

要通过 Firepower 威胁防御虚拟传输流量，必须在与每个数据子网关联的用户定义路由表中添加/更新路由。应使用该子网上的 Firepower 威胁防御虚拟 IP 地址作为下一跳来传输相应流量。此外，如果需要，可为 0.0.0.0/0 的默认路由加上 Firepower 威胁防御虚拟 IP 的下一跳。

由于系统路由表中存在现有的具体路由，因此您必须将具体的路由添加到用户定义路由表，以指向 Firepower 威胁防御虚拟作为下一跳。否则，用户定义表中的默认路由将让步于系统路由表中更具体的路由，并且流量将绕过 Firepower 威胁防御虚拟。

虚拟网络中虚拟机的路由配置

Azure 虚拟网络中的路由取决于有效路由表，而非客户端上的特定网关设置。系统可能通过 DHCP 为虚拟网络中运行的客户端提供路由，即各个子网上最后一位为 .1 的地址。这是一个占位符，仅用于将数据包传送到虚拟网络的基础设施虚拟网关。一旦数据包离开虚拟机，系统会根据有效路由表（由用户定义表修改）对数据包进行路由。有效路由表确定下一跳，无论客户端是具有配置为 .1 还是配置为 Firepower 威胁防御虚拟地址的网关。

Azure 虚拟机 ARP 表将为所有已知主机显示相同的 MAC 地址 (1234.5678.9abc)。这可确保所有离开 Azure 虚拟机的数据包都将到达 Azure 网关，其中有效路由表将用于确定数据包的路径。

IP 地址

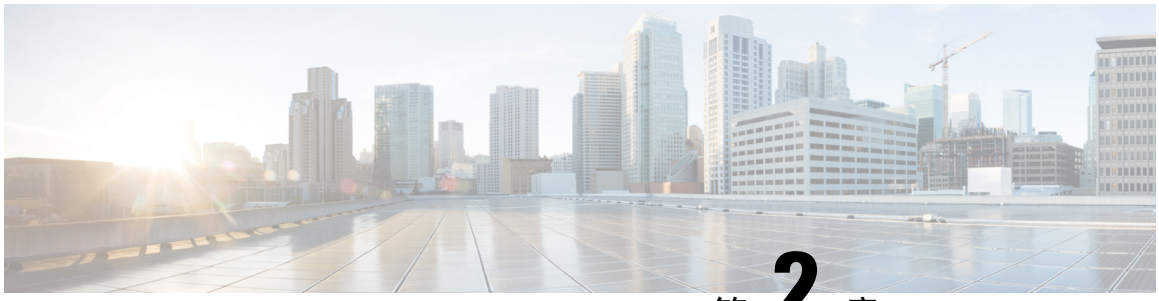
以下信息适用于 Azure 中的 IP 地址：

- 系统会为 Firepower 威胁防御虚拟上的第一个 NIC（映射到管理接口）提供其附加到的子网中的专用 IP 地址。

  公共 IP 地址可能与此专用 IP 地址相关联，Azure 互联网网关将处理 NAT 转换。

  在部署 Firepower Threat Defense Virtual 后，您可以将一个公共 IP 地址与一个数据接口（例如，GigabitEthernet0/0）关联；请参阅公共 IP 地址，了解有关公共 IP 的 Azure 准则，包括如何创建、更改或删除公共 IP 地址。

- 动态的公共 IP 地址在 Azure 停止/启动周期期间可能发生变化。不过，它们在 Azure 重启和 Firepower 威胁防御虚拟重新加载期间是固定不变的。
- 静态的公共 IP 地址不会发生变化，除非您在 Azure 中进行更改。
- Firepower 威胁防御虚拟接口可能使用 DHCP 来设置其 IP 地址。Azure 基础设施可确保为 Firepower 威胁防御虚拟接口分配 Azure 中设置的 IP 地址。



第 2 章

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 9。
- **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 12。

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 12。

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, on page 51。
- 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, on page 67。

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, on page 4。

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。

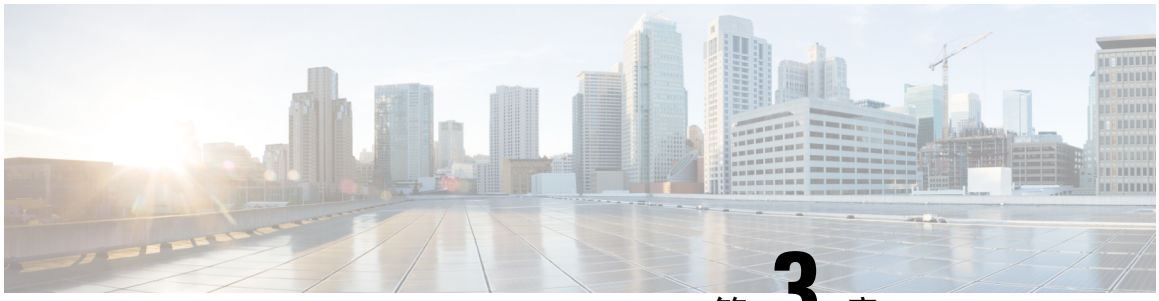
步骤 12 单击**购买**，使用托管映像和自定义模板部署 FTDv 防火墙。

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。



第 3 章

部署适用于 Azure 的 Firepower Threat Defense Virtual Auto Scale

适用于 Azure 上 FTDv 的 Auto Scale 解决方案

关于 Auto Scale 解决方案

FTDv Auto Scale for Azure 是完整的无服务器实现，它利用 Azure 提供的无服务器基础架构（逻辑应用、Azure 函数、负载均衡器、安全组、虚拟机规模集等）。

FTDv Auto Scale for Azure 实现的一些主要功能包括：

- FMC 中完全自动化的 FTDv 实例注册和取消注册。
- （**FP 6.7 新增**）支持基于 CPU 和内存 (RAM) 的扩展指标：
  - 仅 CPU。未改变之前版本中的行为。
  - CPU、内存。对于外向扩展策略，您可以选择将 CPU 或内存指标的扩展阈值分开。内向扩展策略同时考虑 CPU 和内存，将终止 CPU 负载最小的设备。

    有关详细信息，请参阅Auto Scale 逻辑， 第 46 页。

- 自动应用到外向扩展 FTDv 实例的 NAT 策略、访问策略和路由。
- 支持标准负载均衡器。
- 支持 FTDv 部署 om 多可用性区域。
- 对启用和禁用自动扩展功能的支持。
- 基于 Azure Resource Manager (ARM) 模板的部署。
- 仅适用于 FMC；不支持 Firepower Device Manager。
- 支持使用 PAYG 或 BYOL 许可模式部署 FTDv。PAYG 仅适用于 FTDv 软件版本 6.5 和更高版本。请参阅支持的软件平台，第 16 页。

Cisco 提供 Auto Scale for Azure 部署包以方便部署。

支持的软件平台

FTDv Auto Scale 解决方案适用于 FMC 管理的 FTDv，与软件版本无关。《Cisco Firepower 兼容性指南》提供 Cisco Firepower 软件和硬件兼容性，包括操作系统和托管环境要求。

- Firepower Management Center：虚拟表列出 FMCv 的 Firepower 兼容性和虚拟托管环境要求。
- Firepower Threat Defense Virtual 兼容性表列出了 Azure 上 FTDv 的 Firepower 兼容性和虚拟托管环境要求。

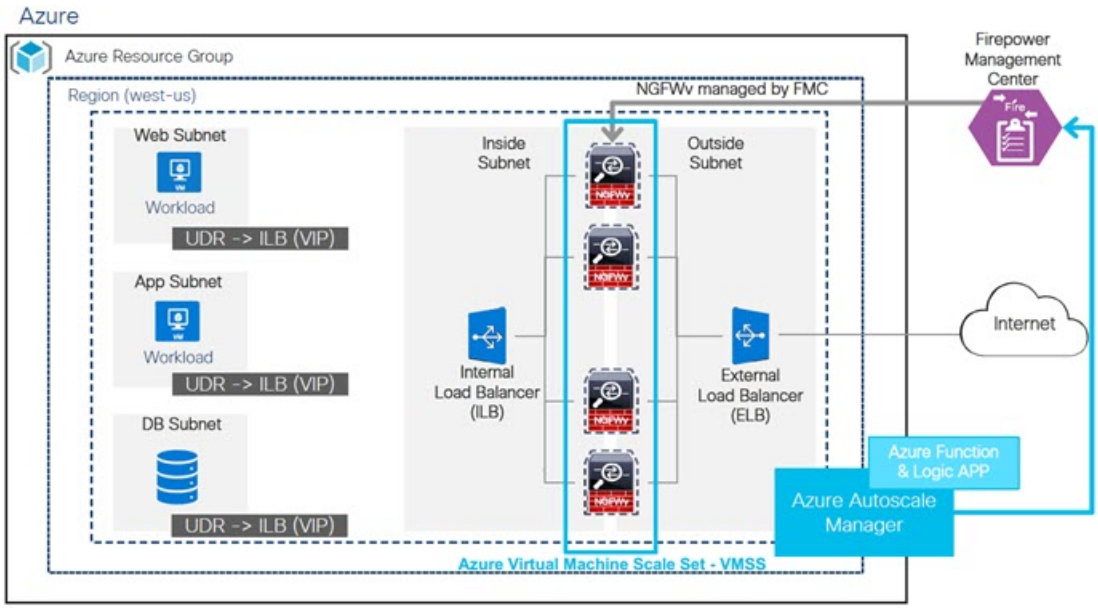
注释 就部署 Azure Auto Scale 解决方案而言，Azure 上的 FTDv 最低支持的 Firepower 版本是版本 6.4。

Auto Scale 使用案例

FTDv Auto Scale for Azure 是一种自动化水平扩展解决方案，它将 FTDv 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到规模集中的 FTDv 实例；然后，防火墙将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到规模集中的 FTDv 实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 FTDv 实例数将根据负载条件自动进行扩展和配置。

图 *1: FTDv Auto Scale* 用例图



适用范围

本文档介绍部署 FTDv Auto Scale for Azure 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

FTDv Auto Scale for Azure 解决方案作为存档文件提供：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。从 GitHub 存储库下载该存档文件，网址为：

- https://github.com/CiscoDevNet/cisco-ftdv/tree/master/deployment-templates/azure

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅附录 - 通过源代码构建 Azure 函数 ，第 49 页。

Auto Scale 解决方案组件

以下组件构成了 FTDv Auto Scale for Azure 解决方案。

Azure Functions（函数应用）

函数应用是一组 Azure 函数。基本功能包括：

- 定期交流/探测 Azure 指标。
- 监控 FTDv 负载和触发内向扩展/外向扩展操作。
- 向 FMC 注册新的 FTDv。
- 通过 FMC 配置新的 FTDv。
- 从 FMC 取消注册（删除）内向扩展的 FTDv。

这些函数以压缩 Zip 包的形式提供（请参阅构建 Azure 函数应用包， 第 20 页）。这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

Orchestrator（逻辑应用）

Auto Scale 逻辑应用是一个工作流，即按照一定序列的步骤集合。Azure 函数是独立的实体，无法彼此通信。此编排器按顺序排列这些函数的执行，并在它们之间交换信息。

- 逻辑应用可用于编排 Auto Scale Azure 函数并在函数之间传递信息。
- 每个步骤代表一个 Auto Scale Azure 函数或内置标准逻辑。
- 逻辑应用作为 JSON 文件交付。
- 可以通过 GUI 或 JSON 文件自定义逻辑应用。

虚拟机规模集 (VMSS)

VMSS 是同构虚拟机（如 FTDv 设备）的集合。

- VMSS 可以向集合中添加新的相同虚拟机。
- 添加到 VMSS 的新虚拟机将自动与负载均衡器、安全组和网络接口连接。
- VMSS 具有内置 Auto Scale 功能，该功能对适用于 Azure 的 FTDv 禁用。
- 您不应在 VMSS 中手动添加或删除 FTDv 实例。

Azure Resource Manager (ARM) 模板

ARM 模板用于部署 FTDv Auto Scale for Azure 解决方案所需的资源。

ARM 模板为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机规模集 (VMSS)
- 内部/外部负载均衡器。
- 部署所需的安全组和其他各种组件。

重要事项 ARM 模板在验证用户输入方面有限制，因此您需要在部署过程中负责验证输入。

Auto Scale 解决方案前提条件

Azure 资源

资源组

部署此解决方案的所有组件需要一个现有的或新创建的资源组。

注释 记录资源组名称、创建它的区域，以及供以后使用的 Azure 订用 ID。

网络

确保在资源组中创建虚拟网络。Auto Scale 部署将不会创建、更改或管理任何网络资源。

FTDv 需要 4 个网络接口，因此您的 Azure 部署需要 4 个子网以用于：

1. 管理流量
2. 诊断流量
3. 内部流量
4. 外部流量

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22)

  负载均衡器与 FTDv 之间的运行状况探测所必需。

  无服务器函数与 FTDv 之间的通信所必需。

- TCP/8305

FTDv 与 FMC 之间的通信所必需。

- HTTPS(TCP/443)

  无服务器组件与 FMC 之间的通信所必需。

- 应用程序特定协议/端口

  任何用户应用程序所必需（例如，TCP/80 等）。

注释 记录虚拟网络名称、虚拟网络 CIDR、所有 4 个子网的名称，以及外部和内部子网的网关 IP 地址。

构建 Azure 函数应用包

FTDv Azure Auto Scale 解决方案要求您构建一个存档文件：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅附录 - 通过源代码构建 Azure 函数 ，第 49 页。

这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

准备 Firepower Management Center

您可以使用功能齐全的多设备管理器 Firepower Management Center (FMC) 来管理 FTDv。FTDv 在您分配给 FTDv 虚拟机的管理接口上向 FMC 注册并与之通信。

创建 FTDv 配置和管理所需的所有对象，包括设备组，以便您能够轻松地在多个设备上部署策略和安装更新。设备组上应用的所有配置都将被推送到 FTDv 实例。

以下各节简要概述准备 FMC 的基本步骤。有关完整信息，应参阅整个《Firepower Management Center 配置指南》。准备 FMC 时，请确保记录以下信息：

- FMC 公共 IP 地址。
- FMC 用户名/密码。
- 安全策略名称。
- 内部和外部安全区域对象名称。
- 设备组名称。

创建新 FMC 用户

在 FMC 中创建具有 Admin 权限的新用户，以便仅供 AutoScale Manager 使用。

重要事项 为了避免与其他 FMC 会话冲突，拥有专用于 FTDv Auto Scale 解决方案的 FMC 用户帐户非常重要。

过程

步骤 1 在 FMC 中创建具有 Admin 权限的新用户。选择**系统** > **用户**，然后单击**创建用户**。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

步骤 2 根据环境需要完成用户选项。有关完整信息，请参阅 FMC 配置指南。

配置访问控制

配置访问控制以允许从内部到外部的流量。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。对规则正确进行配置和排序对于构建有效的部署至关重要。请参阅 FMC 配置指南中的“访问控制最佳实践”。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 单击**新建策略**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 请参阅 FMC 配置指南，以便为您的部署配置安全设置和规则。

配置许可

所有许可证都由 FMC 提供给 FTD。您可以选择购买以下功能许可证：

- **威胁** - 安全情报和 Cisco Firepower 下一代 IPS
- **恶意软件** - 适用于网络的高级恶意软件防护 (AMP)
- **URL** - URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

注释 购买威胁、恶意软件或 URL 许可证时，您还需要匹配的订用许可证以获取 1 年、3 年或 5 年的更新。

开始之前

- 拥有思科智能软件管理器主帐户。

  如果您还没有账户，请单击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主账户。

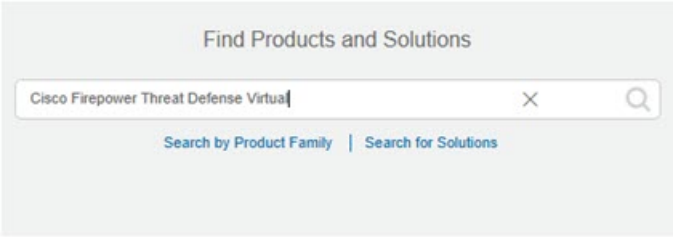
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *2:* 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

步骤 2 如果尚未这样做，请向智能许可服务器注册 FMC。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 FMC 配置指南。

创建安全区域对象

为您的部署创建内部和外部安全区域对象。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**接口**。

步骤 3 单击**添加** > **安全区域**。

步骤 4 输入一个**名称**（例如，*inside*、*outside*）。

步骤 5 选择**已路由**作为**接口类型**。

步骤 6 单击**保存**。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。

过程

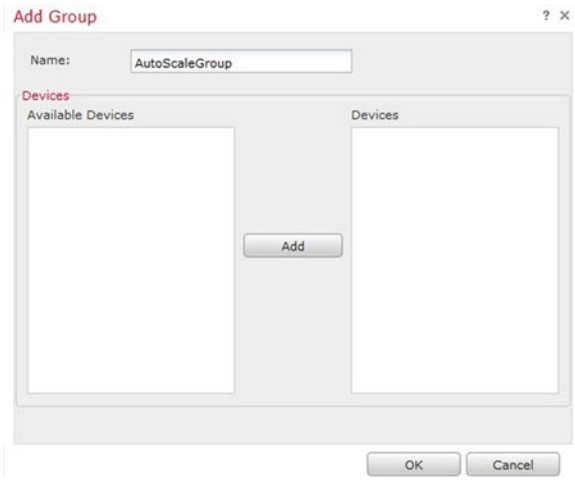
步骤 1 选择**设备** > **设备管理**。

图 ***3:*** 设备管理

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

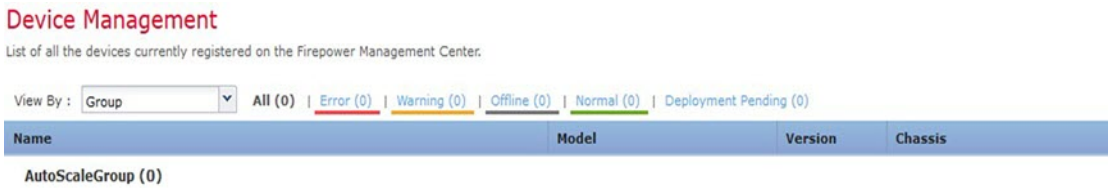
步骤 3 输入 **Name**。例如，*AutoScaleGroup*。

图 ***4:*** 添加设备组



步骤 4 单击**确定 (OK)** 以添加组。

图 *5:* 已添加设备组



配置安全外壳访问

FTD 设备的平台设置会配置一系列不相关的功能，您可能想要在多个设备之间共享它们的值。FTDv Auto Scale for Azure 需要 FTD 平台设置策略，以便允许在内部/外部区域和为 Auto Scale 组创建的设备组上使用 SSH。这是必需的，以便 FTDv 的数据接口可以响应负载均衡器的运行状况探测。

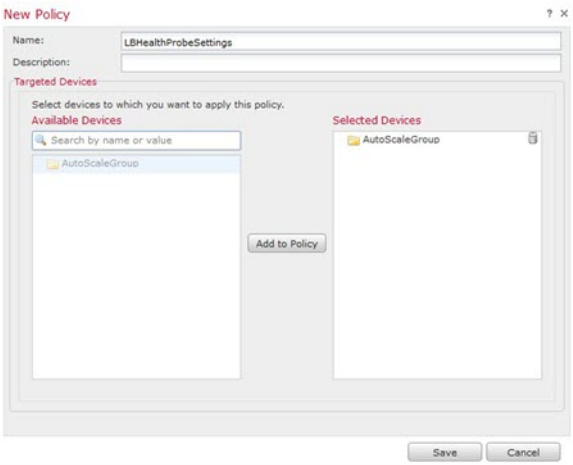
开始之前

- 您需要定义允许与设备建立 SSH 连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。例如，参阅以下步骤中的 *azure-utility-ip (168.63.129.16)* 对象。

过程

步骤 1 选择**设备** > **平台设置**，然后创建或编辑 FTD 策略，例如 *LBHealthProbeSettings*。

图 *6: FTD* 平台设置策略



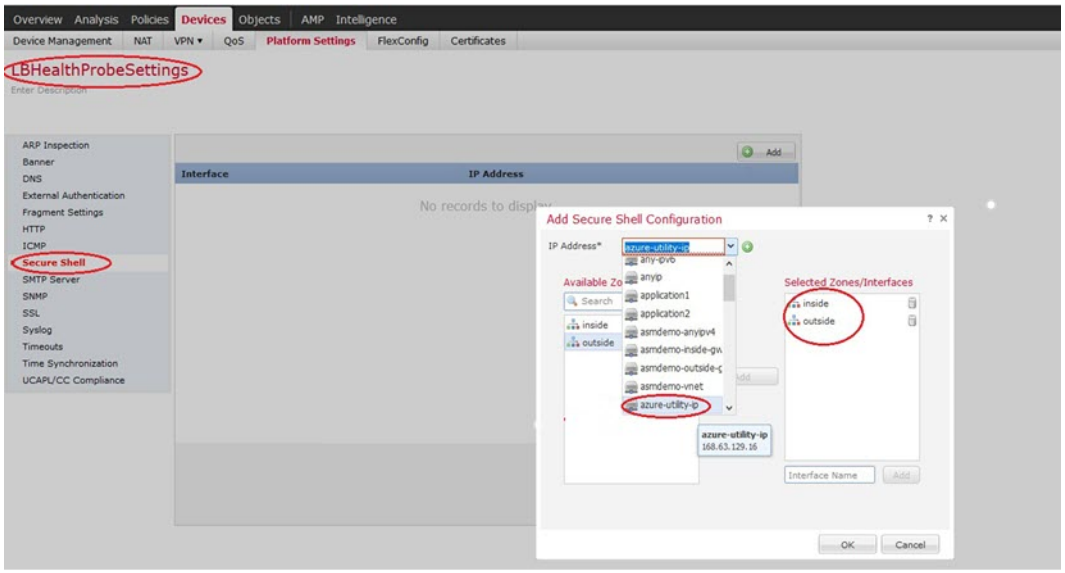
步骤 2 选择**安全外壳**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

a) 单击**添加**以添加新规则，或单击**编辑**以编辑现有规则。
b) 配置规则属性：

- **IP 地址** - 用于标识您允许进行 SSH 连接的主机或网络的网络对象（例如，*azure-utility-ip (168.63.129.16)*）。从下拉列表中选择一个对象，或者单击“+”添加新的网络对象。
- **安全区域** - 添加包含将允许进行 SSH 连接的接口的区域。例如，您可以将内部接口分配到**内部**区域，而将外部接口分配到**外部**区域。您可以从 FMC 的**对象**页创建安全区域。有关安全区域的完整信息，请参阅 FMC 配置指南。
- 单击**确定**。

图 *7: FTDv Auto Scale* 的 *SSH* 访问



步骤 4 单击**保存**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 NAT

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为自动扩展创建的设备组。

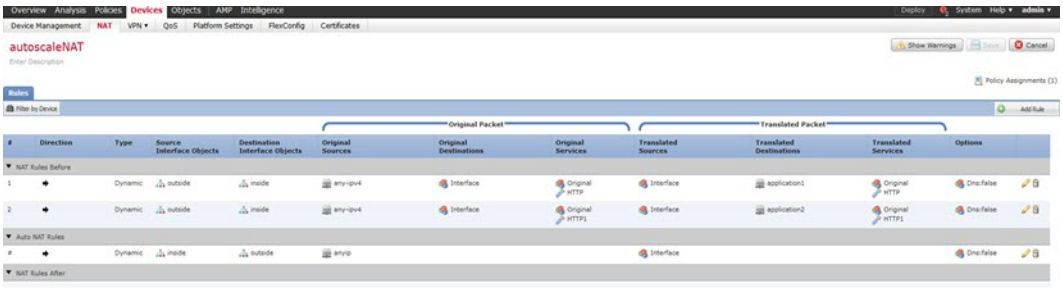
过程

步骤 1 选择**设备** > **NAT**。
步骤 2 从**新策略**下拉列表中，选择**威胁防御 NAT**。
步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 配置您的 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的准则，请参阅 FMC 配置指南中“配置威胁防御 NAT”。下图所示为基本方法。

图 *8: NAT* 策略示例



注释 我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。

步骤 6 单击**保存**。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 ARM 模板部署到 Azure 订用时使用这些参数创建 FTDv 设备。请参阅部署 Auto Scale ARM 模板，第 31 页。

表 *1:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。	New
virtualNetworkRg	字符串	资源组的名称	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）	现有
virtualNetworkCidr	CIDR 格式 x.x.x.x/y	虚拟网络的 CIDR（已创建）	现有
mgmtSubnet	字符串	管理子网名称（已创建）	现有
diagSubnet	字符串	诊断子网名称（已创建）	现有
insideSubnet	字符串	内部子网名称（已创建）	现有

参数名	允许的值/类型	说明	资源创建类型
insideNetworkGatewayIp	字符串	内部子网关 IP（已创建）	现有
outsideSubnet	字符串	外部子网名称（已创建）	现有
outsideNetworkGatewayIp	字符串	外部子网关 IP（已创建）	现有
internalLbIP	字符串 x.x.x.x	要分配给内部负载均衡器的 IP（内部子网）	New
deviceGroupName	字符串	FMC 中的设备组（已创建）	现有
insideZoneName	字符串	FMC 中的内部区域名称（已创建）	现有
outsideZoneName	字符串	FMC 中的外部区域名称（已创建）	现有
softwareVersion	字符串	FTDv 版本（在部署期间从下拉列表中选择）	现有
vmSize	字符串	FTDv 实例的大小（在部署过程中从下拉列表中选择）	不适用
ftdLicensingSku	字符串	FTDv 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
ftdVmManagementUserName	字符串*	FTDv VM 管理管理员用户名。 注：这不能是“admin”。	New
ftdVmManagementUserPassword	字符串*	FTDv VM 管理管理员用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 注：模板中不对此进行合规性检查。	New

参数名	允许的值/类型	说明	资源创建类型
ftdAdminUserPassword	字符串*	FTDv“admin”用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 注：模板中不对此进行合规性检查。	New
fmcIpAddress	字符串 x.x.x.x	FMC 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	FMC用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 FMC 用户名的 FMC 密码（已创建）	现有
policyName	字符串	在 FMC 中创建的安全策略（已创建）	现有
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 FTDv 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 FTDv 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 FTDv 的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	
scaleInThreshold	整数	当所有 FTDv 指标（仅 CPU 利用率、CPU/内存利用率）低于此值时，将触发内向扩展。	不适用
scaleOutThreshold	整数	当任何 FTDv 指标（仅 CPU 利用率、CPU/内存利用率）高于此值时，将触发外向扩展。 “scaleOutThreshold”应始终大于“scaleInThreshold”。	不适用

参数名	允许的值/类型	说明	资源创建类型
minFtdCount	整数	在任何给定时间，规模集中可用的最小 FTDv 实例数。 示例：2	不适用
maxFtdCount	整数	规模集中允许的最大 FTDv 实例数。 示例：10 注 1：此数量受 FMC 容量的限制。 注 2：Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值（仅 CPU 利用率、CPU/内存利用率），并且基于此平均值做出扩展决定。 注：由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用

参数名	允许的值/类型	说明	资源创建类型
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 FTDv 实例时。 BULK：Auto Scale Manager 将尝试一次并行部署“minFtdCount”数量的 FTDv 实例。 注：启动采用并行方式，但由于 FMC 的限制，需要按顺序注册到 FMC。 STEP：Auto Scale Manager 将按照计划间隔逐个部署“minFtdCount”数量的 FTD。 注 1：STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 FMC 进行配置，然后实现运行，但在调试时很有帮助。 注 2：BULK 选项启动所有“minFtdCount”数量的 FTDv 所花费的时间与一次 FTDv 启动相同（因为它是并行运行的），但 FMC 注册是按顺序进行的。 部署“minFtdCount”数量的 FTDv 所花费的总时间 =（启动一个 FTDv 所用的时间 + 注册/配置一个 FTDv 所用的时间 * minFtdCount）。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

Auto Scale 部署

下载部署软件包

FTDv Auto Scale for Azure 解决方案作为存档文件提供：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。从 GitHub 存储库下载该存档文件，网址为：

- https://github.com/CiscoDevNet/cisco-ftdv/tree/master/deployment-templates/azure

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅附录 - 通过源代码构建 Azure 函数 ，第 49 页。

部署 Auto Scale ARM 模板

ARM 模板用于部署 FTDv Auto Scale for Azure 所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机规模集 (VMSS)
- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

开始之前

- 从 GitHub 存储库 (https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure) 下载 ARM 模板 *azure_ftdv_autoscale.json*。

过程

步骤 1 如果您需要在多个 Azure 区域中部署 FTDv 实例，请基于部署区域中可用的区域编辑 ARM 模板。

示例：

```
"zones": [
    "1",
    "2",
    "3"
],
```

本示例显示了包含 3 个区域的“美国中部”区域。

步骤 2 编辑外部负载均衡器中所需的流量规则。您可以通过扩展此“json”数组来添加任意数量的规则。

示例：

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
```

```
        "location": "[resourceGroup().location]",
        "apiVersion": "2018-06-01",
        "sku": {
          "name": "Standard"
        },
        "dependsOn": [
          "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

        ],
        "properties": {
          "frontendIPConfigurations": [
            {
              "name": "LoadBalancerFrontEnd",
                "properties": {
                  "publicIPAddress": {
                    "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
                  }
                }
            }
          ],
          "backendAddressPools": [
            {
              "name": "backendPool"
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/backendAddressPools/BackendPool')]"
                },
                "probe": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

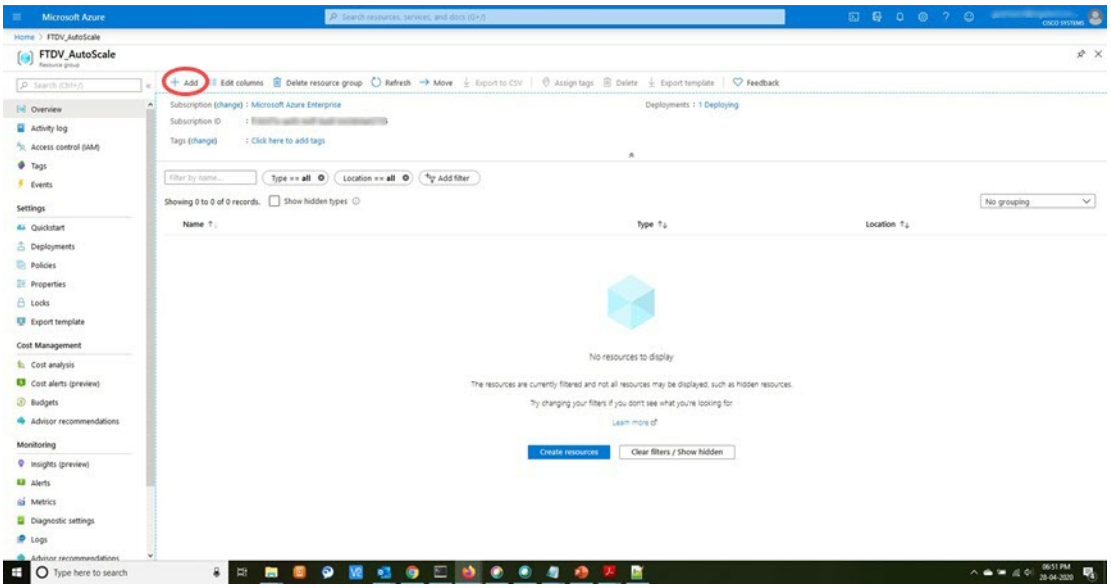
注释 如果您不想编辑此文件，也可以在部署后从 Azure 门户编辑此项。

步骤 3 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户。

步骤 4 单击服务菜单中的**资源组**以访问资源组边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。

创建新资源组或选择现有的空资源组；例如，*FTDV_AutoScale*。

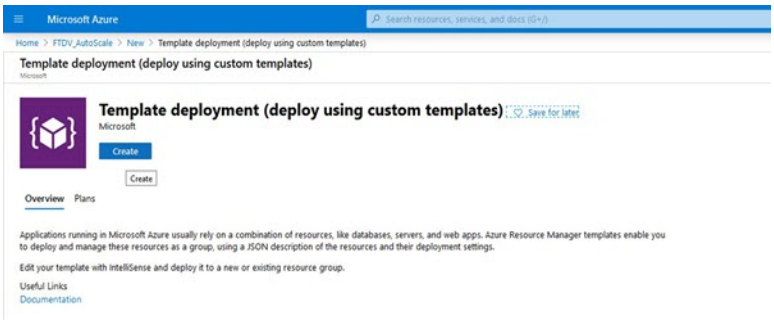
图 ***9: Azure*** 门户



步骤 5 单击**创建资源 (+)**，为模板部署创建新资源。此时将显示“创建资源组”边栏选项卡。

步骤 6 在**搜索市场**中，键入**模板部署（使用自定义模板部署）**，然后按 **Enter**。

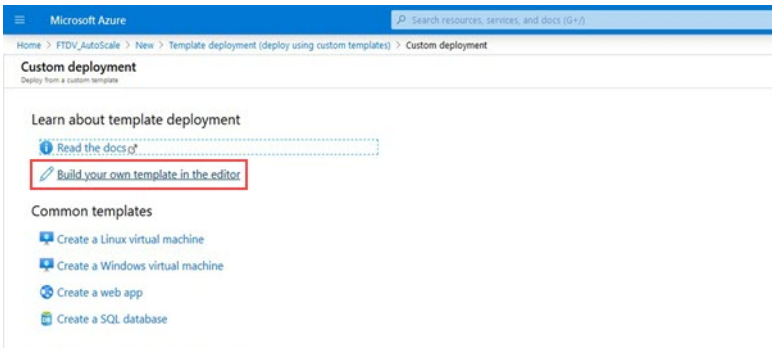
图 ***10:*** 自定义模板部署



步骤 7 单击**创建**。

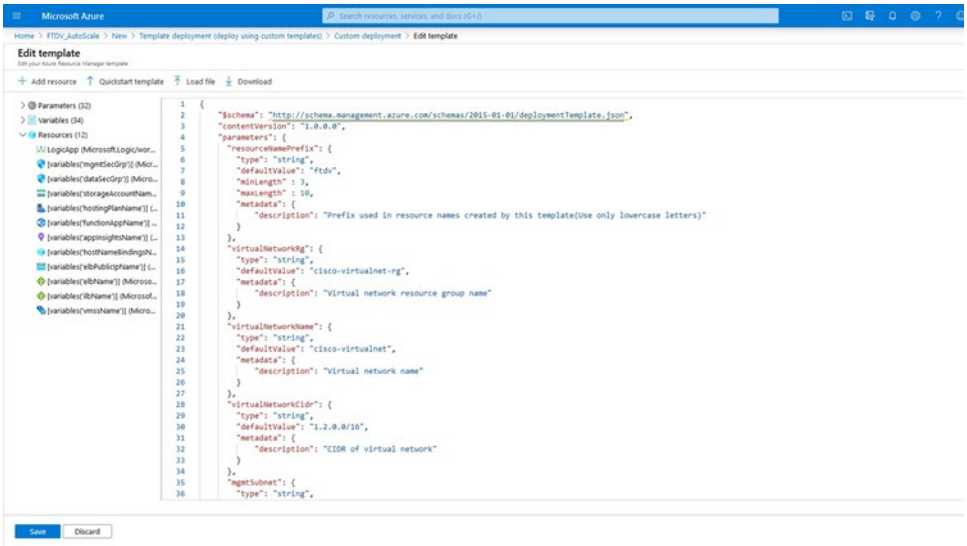
步骤 8 创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板**。

图 *11:* 构建您自己的模板



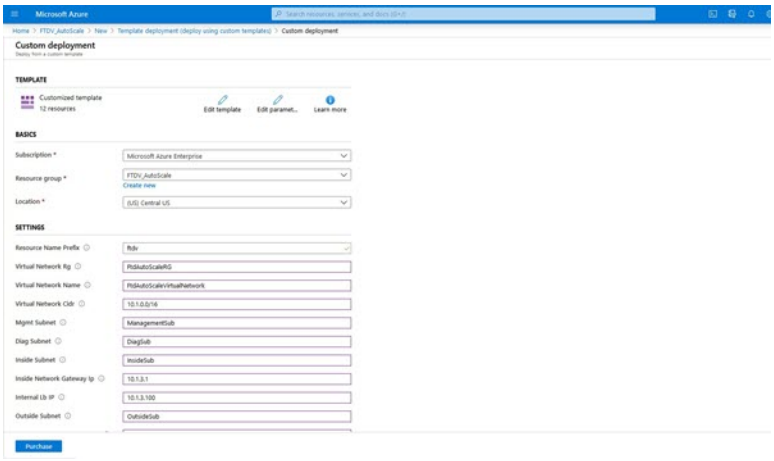
步骤 9 在**编辑模板**窗口中，删除所有默认内容并更新来自 *azure_ftdv_autoscale.json* 的内容，然后单击**保存**。

图 *12:* 编辑模板



步骤 10 在下一部分，填写所有参数。有关每个参数的详细信息，请参阅输入参数，第 26 页，然后单击**购买**。

图 *13: ARM* 模板参数

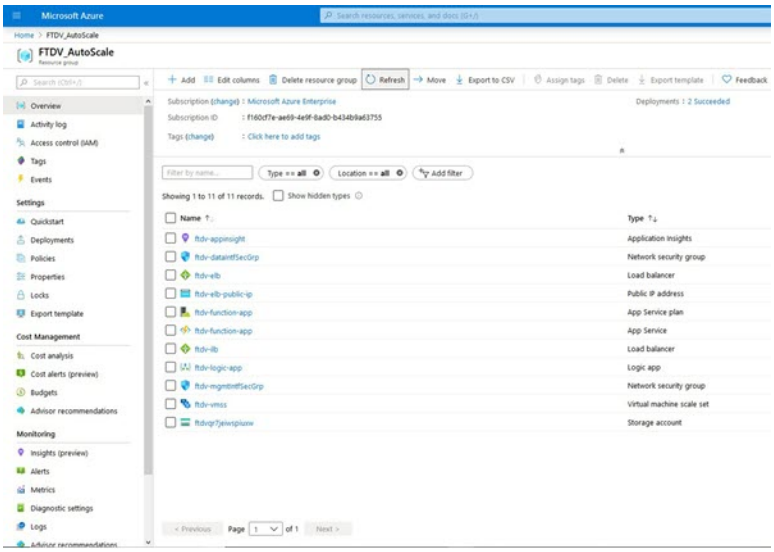


注释　　您也可以单击**编辑参数**，然后编辑 JSON 文件或上传预填的内容。

ARM 模板的输入验证功能有限，因此您需要负责验证输入。

步骤 11　当成功部署模板后，它将为 FTDv Auto Scale for Azure 解决方案创建所有必要的资源。请参阅下图中的资源。“类型”列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

图 *14: FTDv Auto Scale* 模板部署



部署 Azure 函数应用

部署 ARM 模板时，Azure 会创建一个主干函数应用，然后您需要为其更新和手动配置 Auto Scale Manager 逻辑所需的函数。

开始之前

- 构建 *ASM_Function.zip* 包。请参阅附录 - 通过源代码构建 Azure 函数 ， 第 49 页。

过程

步骤 1 转至您在部署 ARM 模板时创建的函数应用，然后确认不存在任何函数。在浏览器中，转至以下 URL：

https://<函数应用名称>.scm.azurewebsites.net/DebugConsole

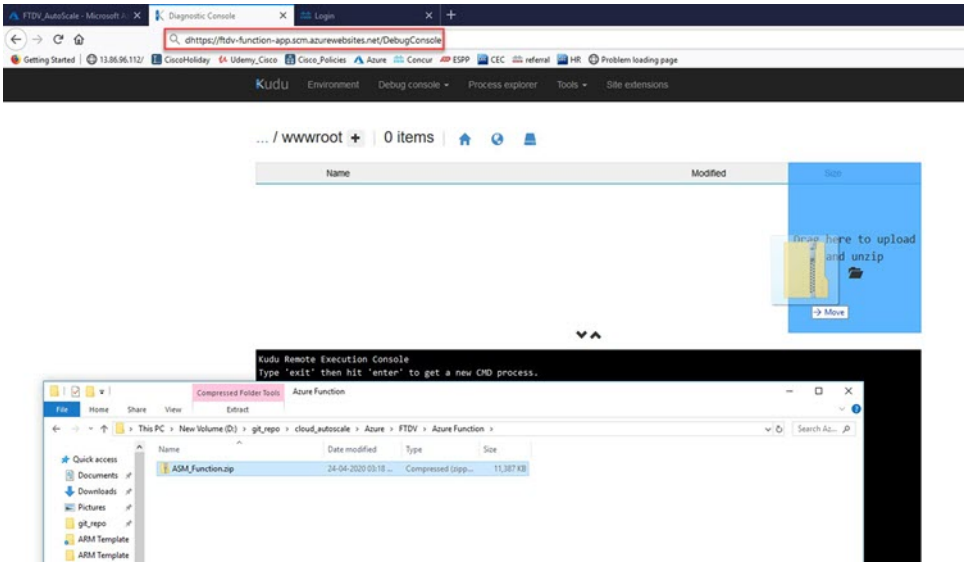
对于部署 Auto Scale ARM 模板 ， 第 31 页中的示例：

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

步骤 2 在文件资源管理器中，导航到 **site/wwwroot**。

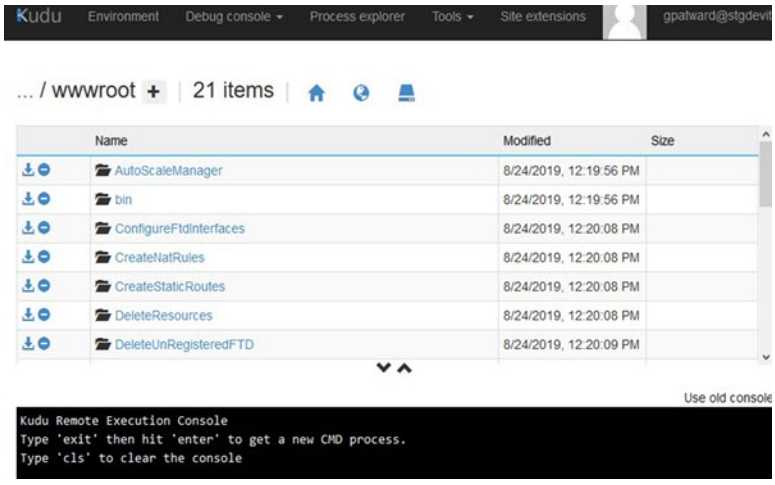
步骤 3 将 **ASM_Function.zip** 拖放到文件资源管理器的右侧。

图 *15:* 上传 ***FTDv Auto Scale*** 函数



步骤 4 成功上传后，应该会显示所有无服务器函数。

图 *16: FTDv* 无服务器函数

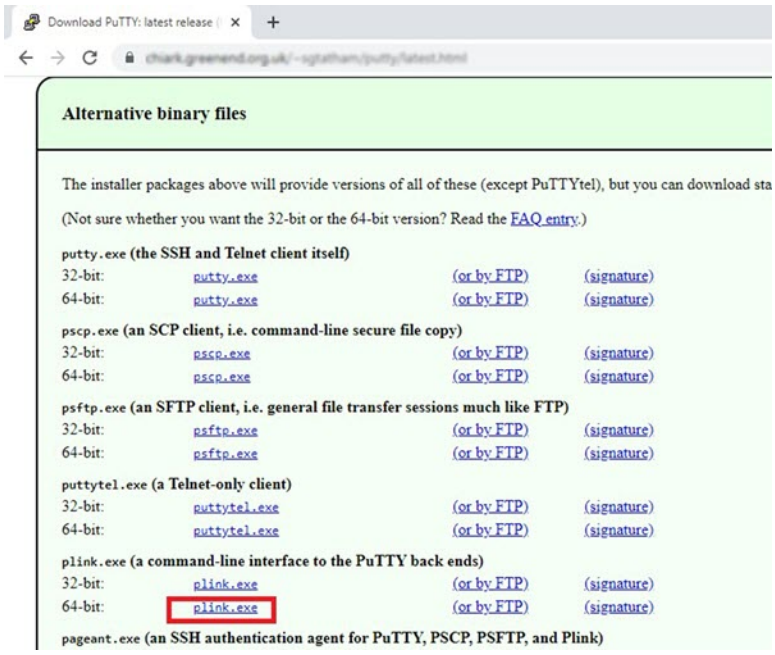


步骤 5 下载 PuTTY SSH 客户端。

Azure 函数需要通过 SSH 连接访问 FTDv。但是，无服务器代码中使用的开源库不支持 FTDv 所用的 SSH 密钥交换算法。因此，您需要下载预构建 SSH 客户端。

从 www.putty.org 将 PuTTY 命令行界面下载到 PuTTY 后端 (*plink.exe*)。

图 *17:* 下载 ***PuTTY***



步骤 6 将 SSH 客户端可执行文件 **plink.exe** 重命名为 **ftdssh.exe**。

步骤 7 将 **ftdssh.exe** 拖放到文件资源管理器的右侧，放到上一步中上传 **ASM_Function.zip** 的位置。

步骤 8 验证 SSH 客户端与函数应用程序一起存在。必要时刷新页面。

微调配置

有一些配置可用于微调 Auto Scale Manager 或在调试中使用。这些选项不会在 ARM 模板中显示，但可以在函数应用下编辑它们。

开始之前

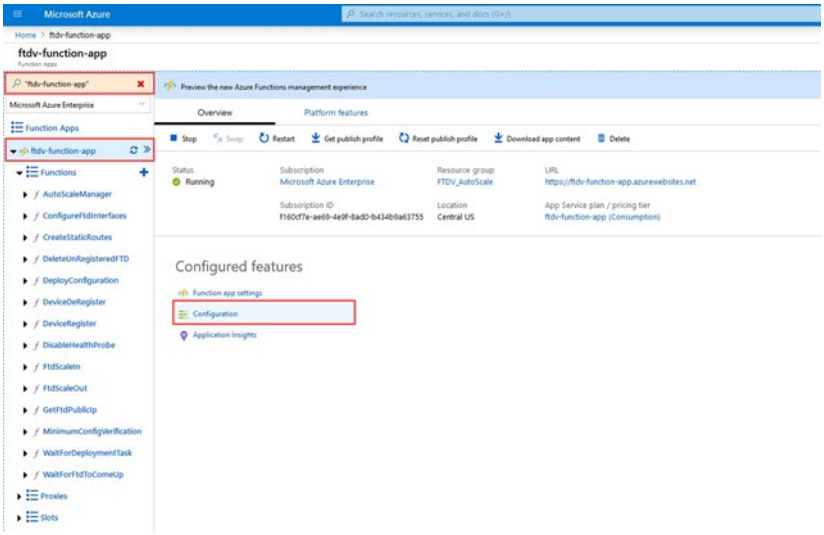
注释 可以随时编辑此项。按照以下顺序编辑配置。

- 禁用函数应用。
- 等待现有的计划任务完成。
- 编辑并保存配置。
- 启用函数应用。

过程

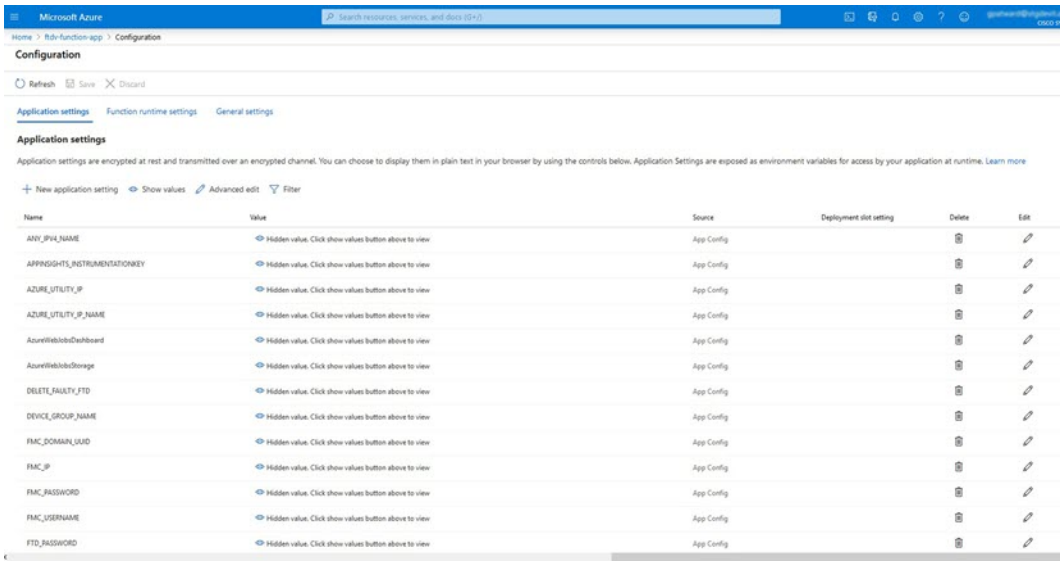
步骤 1 在 Azure 门户中，搜索并选择 FTDv 函数应用。

图 *18: FTDv* 函数应用



步骤 2 也可以在此处编辑通过 ARM 模板传递的配置。变量名称可能与 ARM 模板不同，但您可以轻松地从其名称中确定它们的用途。

图 *19:* 应用设置



大多数选项的名称不言自明。例如：

- 配置名称：”DELETE_FAULTY_FTD“（默认值：YES）

  在外向扩展期间，将会启动新的 FTDv 实例并将其注册到 FMC。如果注册失败，则 Auto Scale Manager 将根据此选项决定保留该 FTD 实例或将其删除。（YES：删除错误的 FTD/NO：保留 FTD 实例，即使未能注册到 FMC）。

- 在函数应用设置中，有权访问 Azure 订用的用户都可以看到明文格式的所有变量（包括含安全字符串的变量，如“密码”）。

  如果用户对此有安全担忧（例如，如果在组织内的低权限用户之间共享 Azure 订用），可以使用 Azure 的 *Key Vault* 服务来保护密码。配置此项后，用户必须提供由存储密码的密钥保管库生成的安全标识符，而不是函数设置中的明文密码。

  注释 搜索 Azure 文档，查找保护应用程序数据的最佳实践。

在虚拟机规模集中配置 IAM 角色

Azure 身份及访问管理 (IAM) 作为 Azure 安全和访问控制的一部分，用于管理和控制用户的身份。Azure 资源的托管身份为 Azure 服务提供 Azure Active Directory 中自动托管的身份。

这将允许函数应用控制虚拟机规模集 (VMSS)，无需显式身份验证凭证。

过程

步骤 1 在 Azure 门户中，转至 VMSS。

步骤 2 单击**访问控制 (IAM)**。

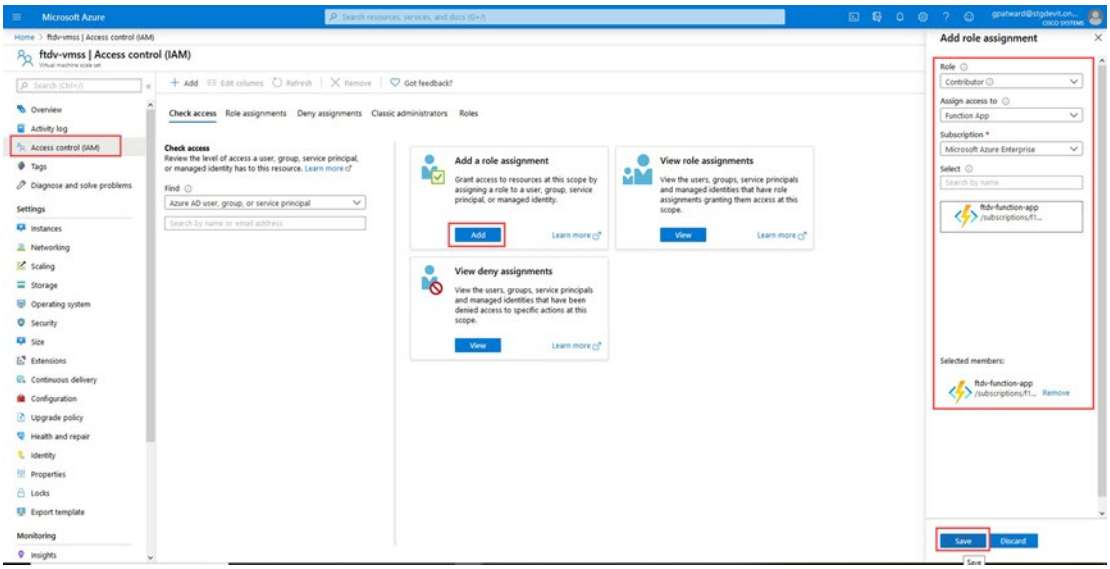
步骤 3 单击**添加**以添加角色分配

步骤 4 从**添加角色分配**下拉列表中选择**参与者**。

步骤 5 从**分配访问**下拉列表中选择**函数应用**。

步骤 6 选择 FTDv 函数应用。

图 ***20: AIM*** 角色分配



步骤 7 单击**保存**。

注释 此外，还应确认尚未启动任何 FTDv 实例。

更新安全组

ARM 模板创建两个安全组，一个用于管理接口，一个用于数据接口。管理安全组将只允许 FTDv 管理活动所需的流量。不过，数据接口安全组将允许所有流量。

过程

根据您的部署的拓扑和应用程序需求，微调安全组规则。

注释 数据接口安全组至少应允许来自负载均衡器的 SSH 流量。

更新 Azure 逻辑应用

逻辑应用充当Autoscale功能的编排器。ARM模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 编排器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项 在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) （可选） 编辑触发间隔，或保留默认值 (5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
        "triggers": {
```

```
"Recurrence": {
    "conditions": [],
    "inputs": {},
    "recurrence": {
        "frequency": "Minute",
        "interval": 5
    },
```

e) （可选）编辑要进行排空的时间，或保留默认值 (5)。这是内向扩展操作期间，在删除设备之前从 FTDv 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

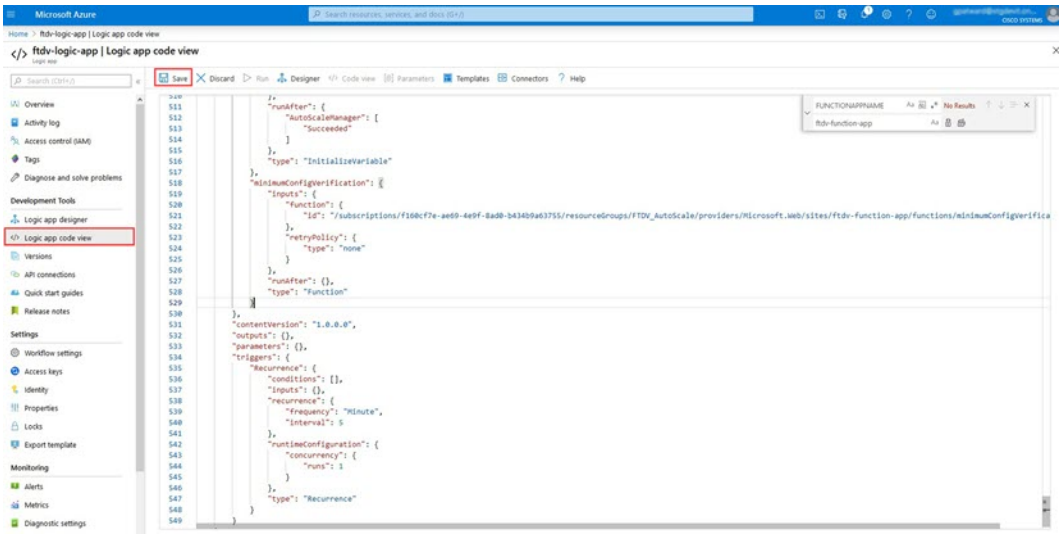
f) （可选）编辑冷却时间，或保留默认值 (10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"actions": {
    "Branch_based_on_Scale-Out_or_Invalid_condition": {
        "actions": {
            "Cooldown_time": {
                "inputs": {
                    "interval": {
                        "count": 10,
                        "unit": "Second"
                    }
```

注释 这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

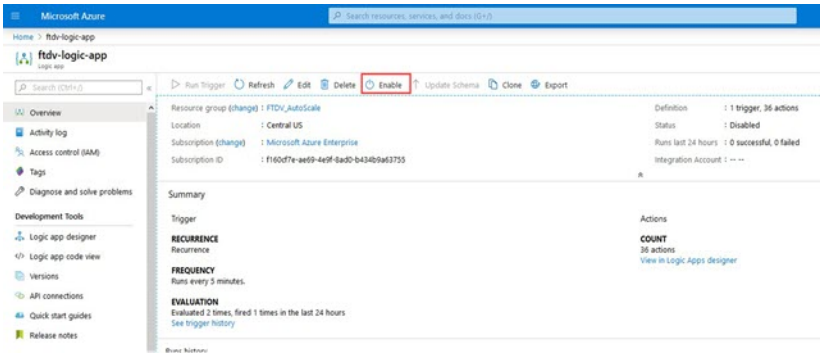
步骤 2 转至**逻辑应用代码视图**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后单击**保存**。

图 *21:* 逻辑应用代码视图



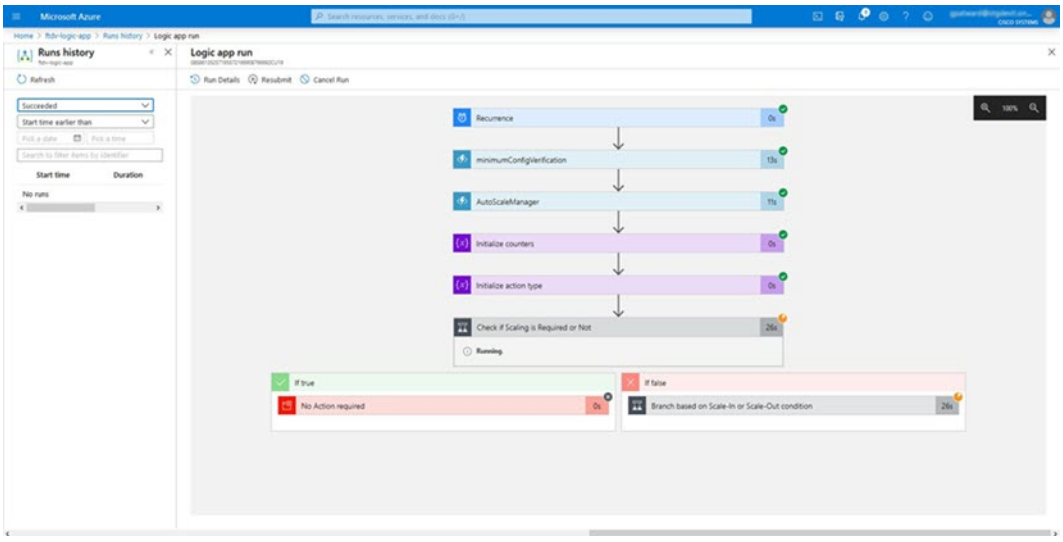
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请单击**启用**。

图 *22:* 启用逻辑应用



步骤 4 启用后，任务就会开始运行。单击“正在运行”状态可查看活动。

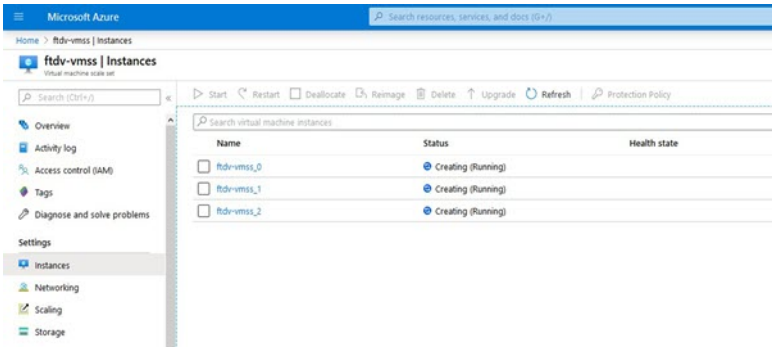
图 *23:* 逻辑应用运行状态



步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 FTDv 实例。

图 *24:* 正在运行的 *FTDv* 实例



在此示例中，由于在 ARM 模板部署中将“minFtdCount”设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 FTDv 实例。

升级 FTDv

FTDv 升级仅支持采用虚拟机规模集 (VMSS) 映像升级的形式。因此，您需要通过 Azure REST API 接口升级 FTDv。

注释 您可以使用任何 REST 客户端来升级 FTDv。以下是一个简单的示例。

开始之前

- 获取市场中提供的新 FTDv 映像版本（例如：650.32.0）。
- 获取用于部署原始规模集的 SKU（例如：ftdv-azure-byol）。
- 获取资源组和虚拟机规模集名称

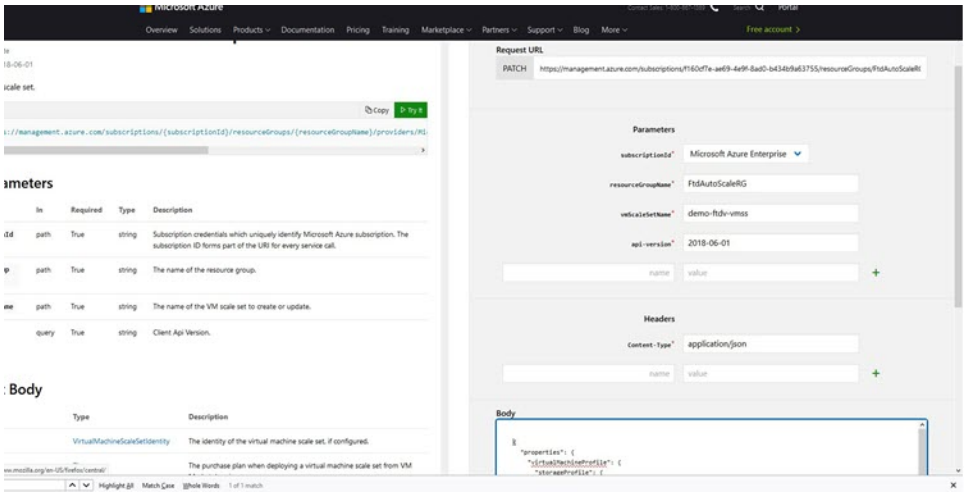
过程

步骤 1 在浏览器中，转至以下 URL：

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

步骤 2 在参数部分输入详细信息。

图 *25:* 升级 *FTDv*



步骤 3 在**主体**部分输入包含新 FTD 映像版本、SKU 和触发器运行的 JSON 输入。

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                     "imageReference": {
                          "publisher": "cisco",
                          "offer": "cisco-ftdv",
                          "sku": "ftdv-azure-byol",
                           "version": "650.32.0"
                     }
                },
            }
      }
}
```

步骤 4 Azure 成功响应意味着 VMSS 已接受更改。

新映像将在新的 FTDv 实例中使用，而这些新实例将在外向扩展操作过程中启动。

- 虽然位于同一规模集中，但现有的 FTDv 实例将继续使用旧软件映像。
- 您可以覆盖上述行为，手动升级现有的 FTDv 实例。要执行此操作，请单击 VMSS 中的**升级**按钮。它将重新启动并升级选定的FTDv实例。您必须手动重新注册并重新配置这些升级后的FTD实例。**请注意，不建议使用此方法**。

Auto Scale 逻辑

扩展指标

您可以使用 ARM 模板部署 FTDv Auto Scale 解决方案所需的资源。在 ARM 模板部署期间，您有以下选项可用于扩展指标：

- CPU（版本 6.6 及更低版本）。CPU 指标是从 Azure 收集的。
- CPU、内存（版本 6.7+）。内存指标是从 FMC 收集的。

外向扩展逻辑

- **POLICY-1**：当**任何** FTDv 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中任何 FTDv 的平均 CPU 或内存利用率。
- **POLICY-2**：当**所有** FTDv 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中所有 FTDv 设备的平均 CPU 或内存利用率。

内向扩展逻辑

- 如果**所有** FTDv 设备的 CPU 利用率在所配置的持续时间内低于配置的内向扩展阈值。使用“CPU、内存”扩展指标时，如果规模集中所有 FTDv 设备的 CPU **和**内存利用率在所配置的持续时间内低于配置内向扩展阈值，则将选择终止 CPU 负载最小的 FTDv。

说明

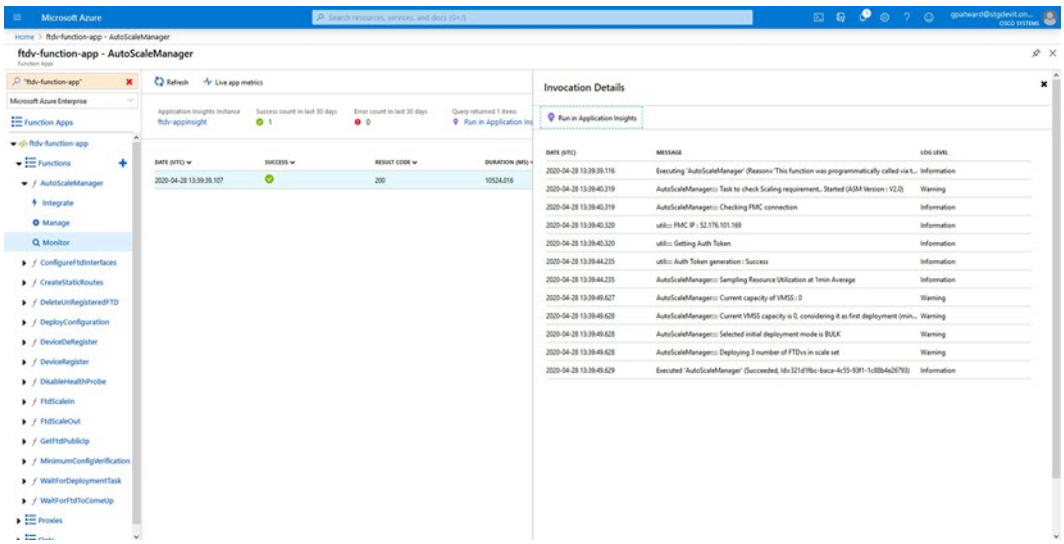
- 内向扩展/外向扩展以 1 为单位发生（即一次仅内向扩展/外向扩展 1 个 FTDv）。
- 从 FMC 收到的内存消耗指标不是按时间计算的平均值，而是瞬时快照/示例值。因此，在做出扩展决定时不能单独考虑内存指标。在部署过程中，您无法选择使用仅内存指标。

Auto Scale 日志记录和调试

无服务器代码的每个组件都有自己的日志记录机制。此外，还会将日志发布到应用程序洞察。

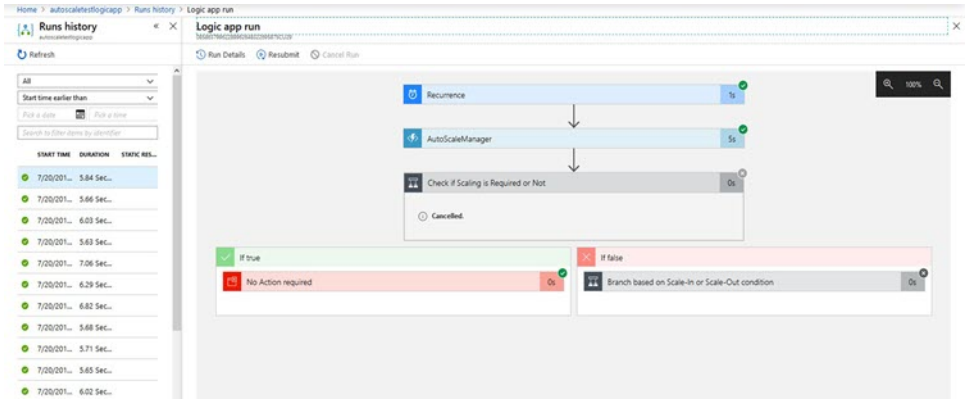
- 可以查看个别 Azure 函数的日志。

图 *26: Azure* 函数日志



- 可以查看每个逻辑应用及其各个组件每次运行的类似日志。

图 *27:* 逻辑应用运行日志



- 如果需要，可以随时停止/终止逻辑应用中任何正在运行的任务。但是，被启动/终止的当前运行 FTDv 设备将处于不一致状态。
- 在逻辑应用中可以看到每个运行/个别任务所花费的时间。
- 通过上传新的 zip，可以随时升级函数应用。在升级函数应用之前，先停止逻辑应用并等待所有任务完成。

Auto Scale 准则和限制

部署 FTDv Auto Scale for Azure 时，请注意以下准则和限制：

- （版本 6.6 及更低版本）扩展决定基于 CPU 使用率。
- （版本 6.7+）扩展决定可以使用仅 CPU 利用率，或者同时使用 CPU 及内存利用率。
- FMC 管理是必需的。不支持 FDM。
- FMC 应具有公共 IP 地址。
- FTDv 管理接口配置为具有公共 IP 地址。
- 仅支持 IPv4。
- FTDv Auto Scale for Azure 仅支持访问策略、NAT 策略、平台设置等配置，它们将应用到设备组并传播到外向扩展 FTDv 实例。您只能使用 FMC 来修改设备组配置。不支持设备特定的配置。
- ARM 模板的输入验证功能有限，因此您需要负责提供正确的输入验证。
- Azure 管理员可以在函数应用环境中看到明文形式的敏感数据（如 FTD/FMC 凭证）。您可以使用 *Azure Key Vault* 服务保护敏感数据。

Auto Scale 故障排除

以下是 FTDv Auto Scale for Azure 的常见错误情况和调试提示：

- 连接到 FMC 失败：检查 FMC IP/凭证；检查 FMC 是否故障/无法访问。
- 无法通过 SSH 连接到 FTDv：检查是否通过模板将复杂密码传递到 FTDv；检查安全组是否允许 SSH 连接。
- 负载平衡器运行状况检查失败：检查 FTDv 是否在数据接口上响应 SSH；检查安全组设置。
- 流量问题：检查负载均衡器规则、FTDv 中配置的 NAT 规则/静态路由；检查模板和安全组规则中提供的 Azure 虚拟网络/子网/网关详细信息。
- FTDv 无法注册到 FMC：检查 FMC 容量以容纳新的 FTDv 设备；检查许可；检查 FTDv 版本兼容性。
- 逻辑应用无法访问 VMSS：检查 VMSS 中的 IAM 角色配置是否正确。
- 逻辑应用运行很长时间：在外向扩展 FTDv 设备上检查 SSH 访问；检查 FMC 中是否有任何设备注册问题；检查 Azure VMSS 中 FTDv 设备的状态。
- 与订用 ID 相关的 Azure 函数抛出错误：验证您的帐户中是否选择了默认预订。
- 内向扩展操作失败：有时 Azure 会花费很长时间删除实例，在这种情况下，内向扩展操作可能会超时并报告错误，但最终实例将被删除。

- 在做出任何配置更改之前，请确保禁用逻辑应用程序，并等待所有正在运行的任务完成。

附录 - 通过源代码构建 Azure 函数

系统要求

- Microsoft Windows 桌面/笔记本电脑。
- Visual Studio（使用 Visual Studio 2019 版本 16.1.3 进行测试）

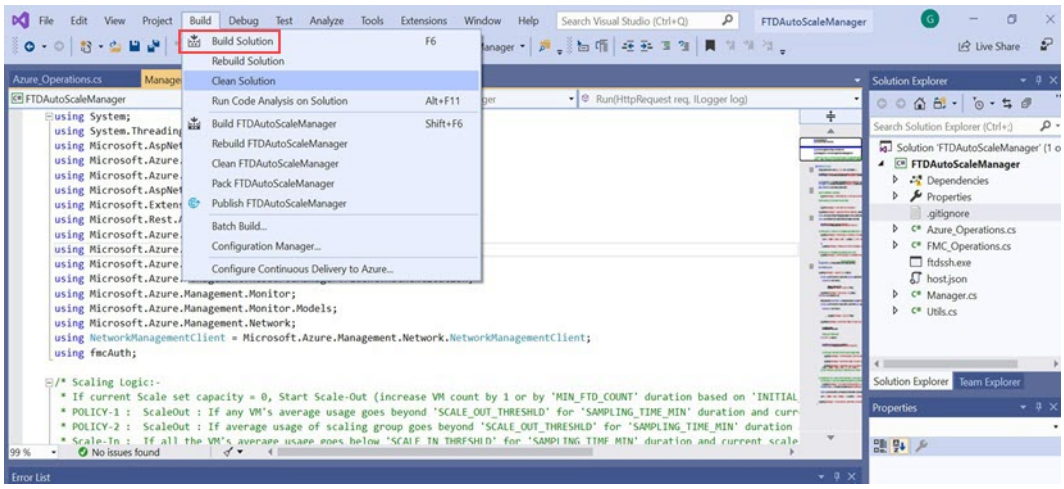
注释 Azure 函数是使用 C# 编写的。

- “Azure Development”工作负载需要安装在 Visual Studio 中。

使用 Visual Studio 构建

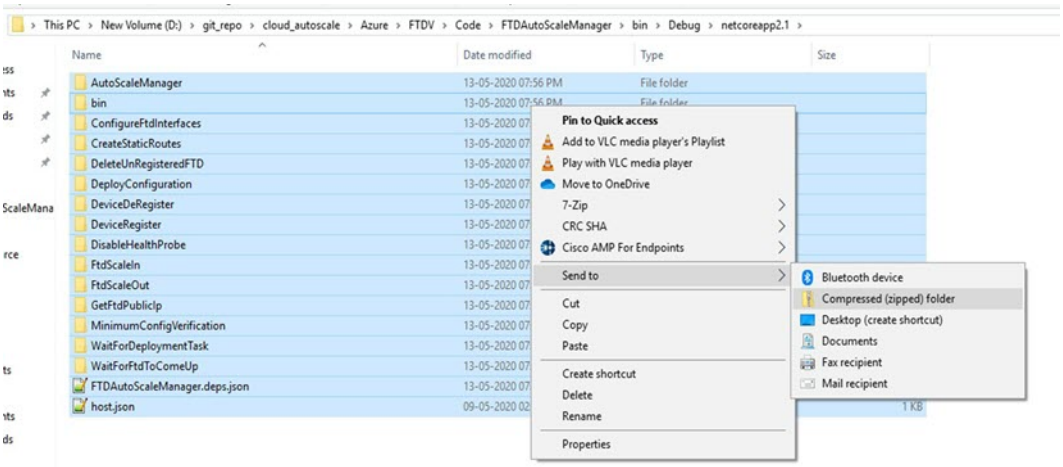
1. 将“code”文件夹下载到本地计算机。
2. 导航到文件夹“FTDAutoScaleManager”。
3. 在 Visual Studio 中打开项目文件“FTDAutoScaleManager.csproj”。
4. 使用 Visual Studio 标准程序进行清理和构建。

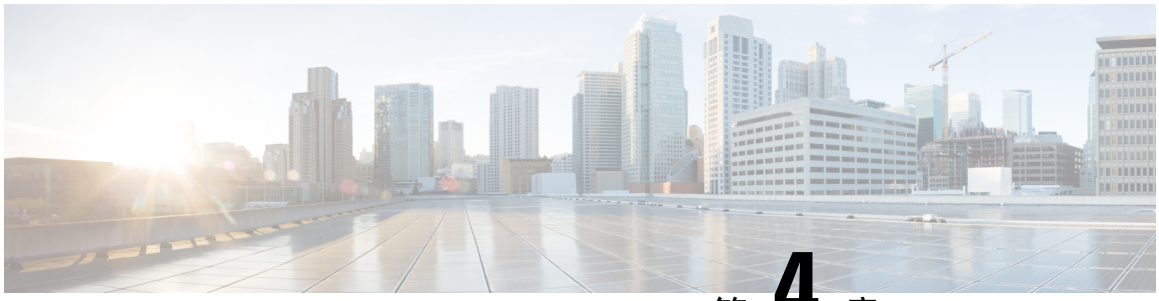
图 *28: Visual Studio* 内部版本



5. 成功编译内部版本后，导航到 **\bin\Debug\netcoreapp2.1** 文件夹。
6. 选择所有内容，单击 **发送到** > **压缩(zipped)文件夹**，然后将 ZIP 文件保存为 *ASM_Function.zip*。

图 ***29:*** 生成 ***ASM_Function.zip***





第 4 章

使用 Firepower 管理中心管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FMC 管理的独立式 FTDv 设备。

注释 本文档涵盖最新的 FTDv 版本功能；有关功能更改的详细信息，请参阅使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史 ， 第 65 页。如果您使用的是旧版本的软件，请参考您的版本的《FMC 配置指南》中的步骤。

关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 管理中心 (FMC) 管理 FTDv，这是一个功能齐全的多设备管理器，位于单独的服务器上。有关安装 FMC 的详细信息，请参阅 FMC 入门指南。

FTDv 向您分配给 FTDv 虚拟机的管理接口上的 FMC 注册并与之通信。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 Firepower CLI 连接到 FTD。

登录到 Firepower 管理中心

使用 FMC配置并监控 FTD。

开始之前

有关受支持浏览器的信息，请参阅您所用版本的发行说明（参阅https://www.cisco.com/go/firepower-notes）。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://*fmc_ip_address*

- *fmc_ip_address* - 标识 FMC 的 IP 地址或主机名。

步骤 2 输入您的用户名和密码。

步骤 3 单击 **Log In**。

向 Firepower 管理中心注册设备

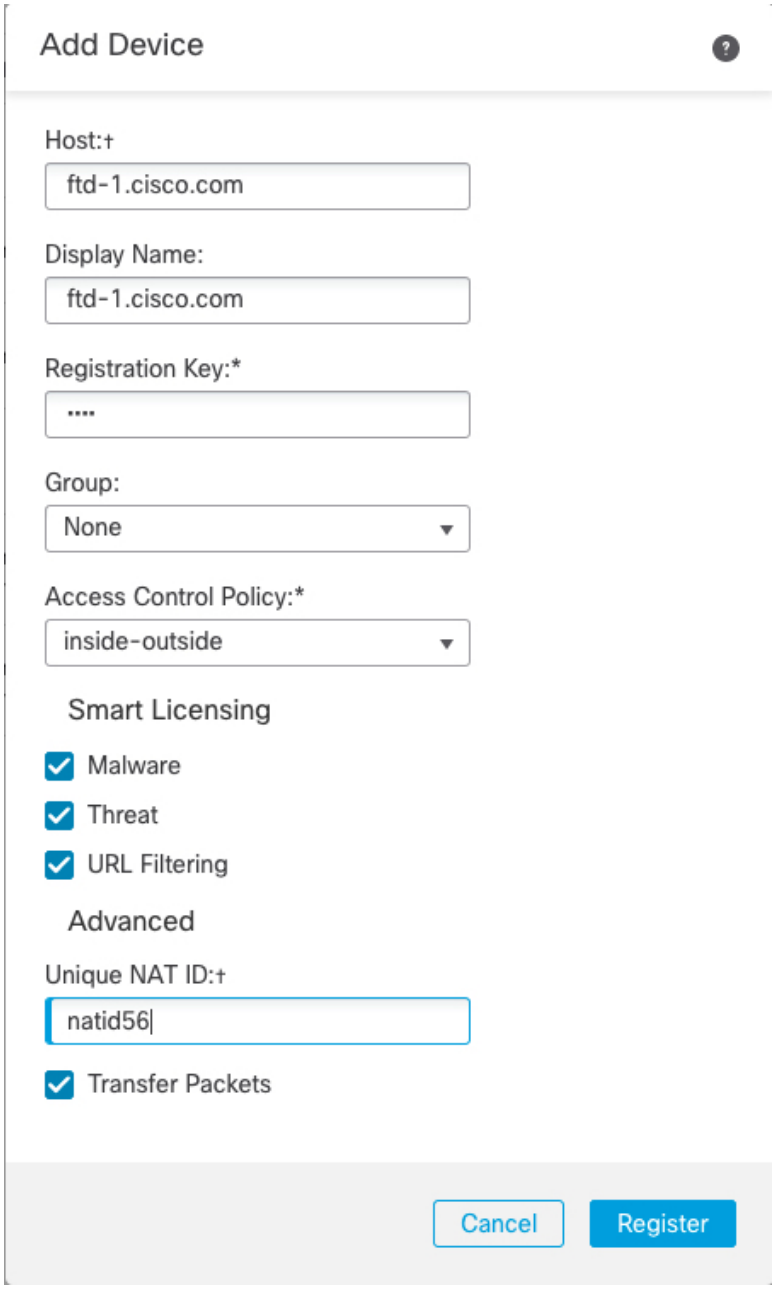
开始之前

确保 FTDv 虚拟机已部署成功、已接通电源并且已首次完成其启动程序。

过程

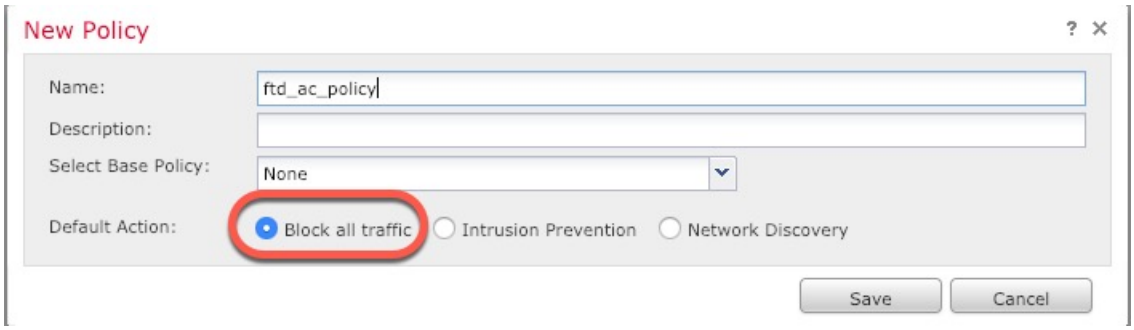
步骤 1 选择 **设备** > **设备管理**.

步骤 2 从**添加**下拉列表选择**添加设备**，然后输入以下参数。



- **主机** - 输入要添加的逻辑设备的 IP 地址。如果您在 FTD 引导程序配置中指定了 FMC IP 地址和 NAT ID，则可以将此字段留空。
- **显示名称** - 输入要在 FMC 中显示的逻辑设备的名称。
- **注册密钥** - 输入您在 FTDv 引导程序配置中指定的注册密钥。
- **Domain** - 如果有多域环境，请将设备分配给分叶域。
- **Group** - 如果在使用组，则将其分配给设备组。

- **Access Control Policy** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择 **Create new policy**，然后选择 **Block all traffic**。之后您可以更改此设置以允许流量通过；请参阅配置访问控制，第 63 页。



- **Smart Licensing** - 为要部署的功能分配所需的智能许可证：**Malware**（如果您打算使用 AMP 恶意软件检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。
- **唯一 NAT ID** - 指定您在 FTDv 启动程序配置中指定的 NAT ID。
- **Transfer Packets** - 可让设备将数据包传输至 FMC。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到FMC进行检测。如果禁用此选项，只有事件信息会发送到 FMC，数据包数据不发送。

步骤 3 单击 **Register**，并确认注册成功。

如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果 FTDv注册失败，请检查以下项：

- Ping - 访问 FTD CLI (访问 Firepower 威胁防御 CLI，第 65 页)，然后使用以下命令 ping FMC IP 地址：

  ping system *ip_address*

  如果 ping 不成功，请使用 **show network** 命令检查您的网络设置。如果需要更改 FTD IP 地址，请使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令。

- NTP - 确保 NTP 服务器与以下页面上设置的 FMC 服务器相符： **系统** > **配置** > **时间同步**页面。
- 注册密钥、NAT ID 和 FMCIP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。您可以在 FTDv 上使用 **configure manager add** 命令设置注册密钥和 NAT ID。也可以使用此命令更改 FMCIP 地址。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

过程

步骤 1 配置接口，第 55 页
步骤 2 配置 DHCP 服务器，第 58 页
步骤 3 添加默认路由，第 59 页
步骤 4 配置 NAT，第 60 页
步骤 5 配置访问控制，第 63 页
步骤 6 部署配置，第 64 页

配置接口

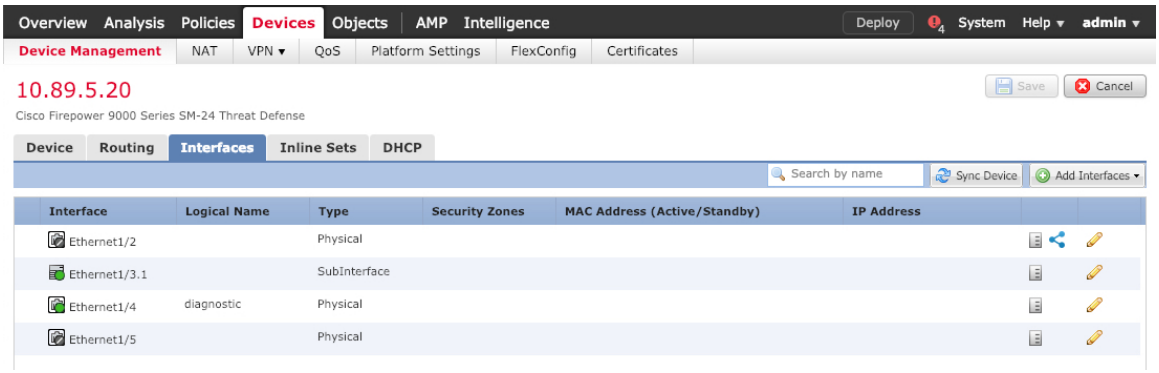
启用 FTDv接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”(DMZ)，您可以在其中放置可公开访问的资产，例如 Web 服务器。

典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

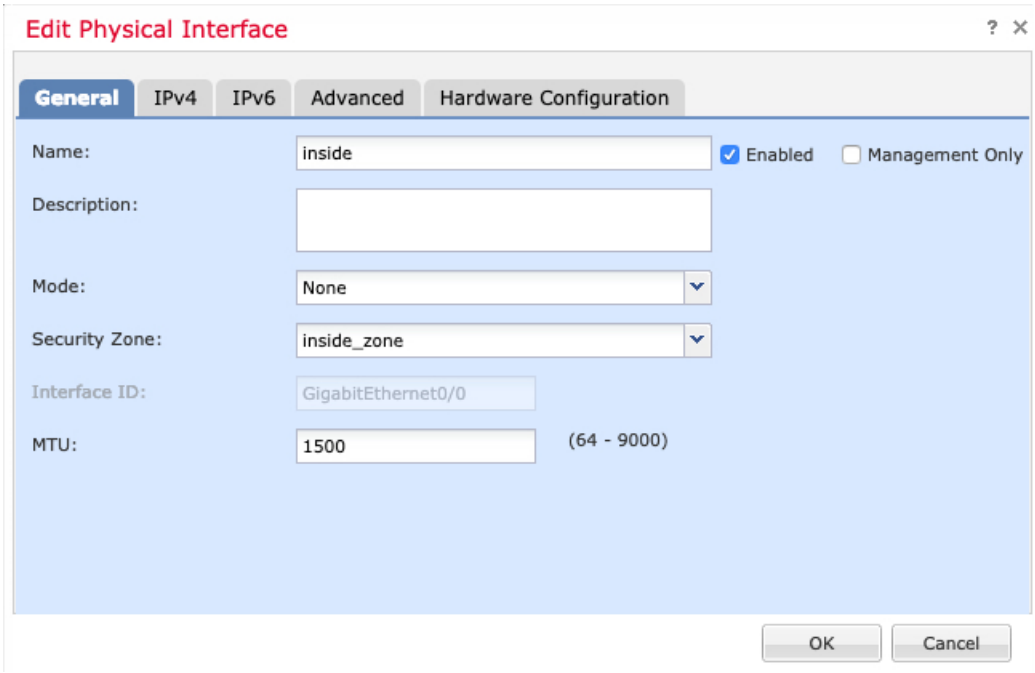
过程

步骤 1 选择 **设备** > **设备管理**，然后单击该设备的 **编辑**（ ）。
步骤 2 单击 **Interfaces**。



步骤 3 单击要用于内部的接口的**编辑**（ ）。

General 选项卡将显示。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **inside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

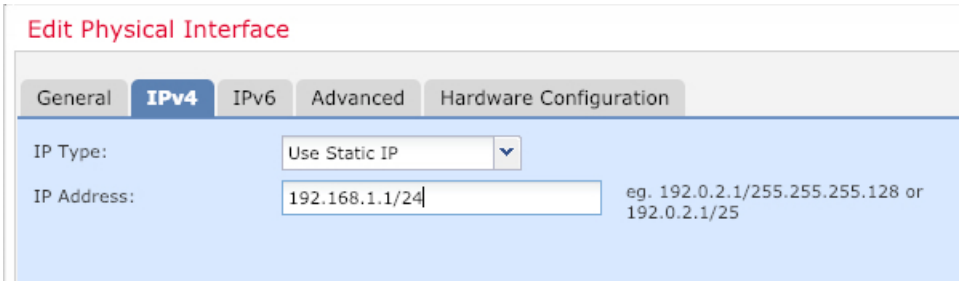
d) 从 **Security Zone** 下拉列表中选择一个现有的内部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择 **Use Static IP**，然后以斜杠表示法输入 IP 地址和子网掩码。

  例如，输入 **192.168.1.1/24**

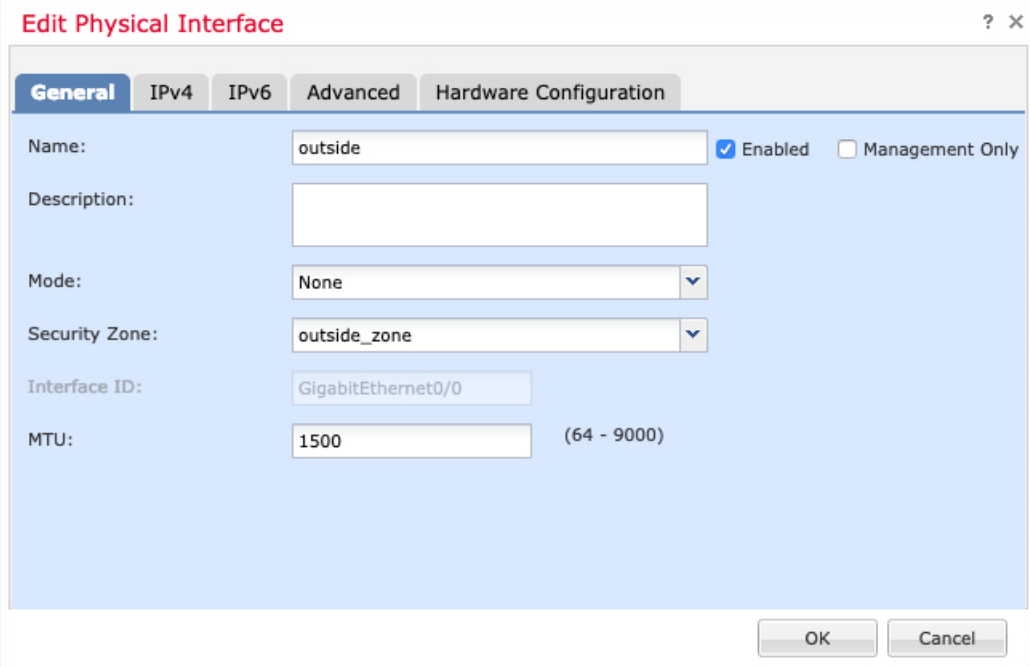


- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 单击**确定**。

步骤 4 单击要用于外部的接口的 **编辑**（ ）。

General 选项卡将显示。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

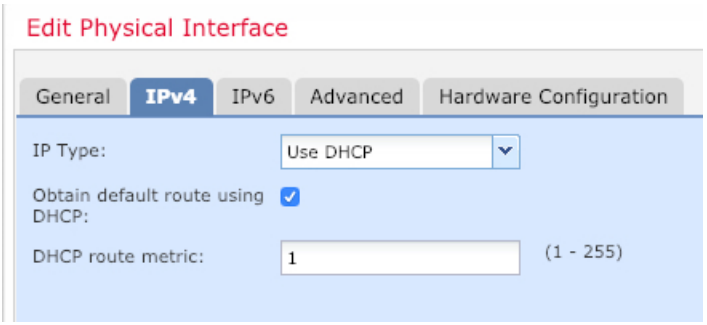
c) 将 **Mode** 保留为 **None**。

d) 从 **Security Zone** 下拉列表中选择一个现有的外部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择 **Use DHCP**，然后配置以下选填参数：
  - **Obtain default route using DHCP** - 从 DHCP 服务器获取默认路由。
  - **DHCP route metric** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。



- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 单击**确定**。

步骤 5 单击**保存**。

配置 DHCP 服务器

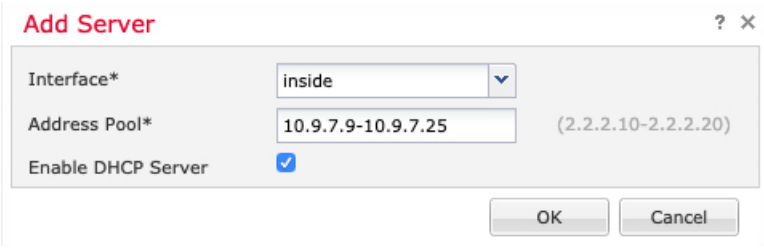
如果希望客户端使用 DHCP 从 FTDv处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择 **设备** > **设备管理**，然后单击该设备的 **编辑**（ ）。

步骤 2 选择 **DHCP** > **DHCP 服务器**.

步骤 3 在 **Server** 页面上单击 **Add**，然后配置以下选项：



- **Interface** -- 从下拉列表中选择接口。

- **Address Pool** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **Enable DHCP Server** - 在所选接口上启用 DHCP 服务器。

步骤 4 单击**确定**。

步骤 5 单击**保存**。

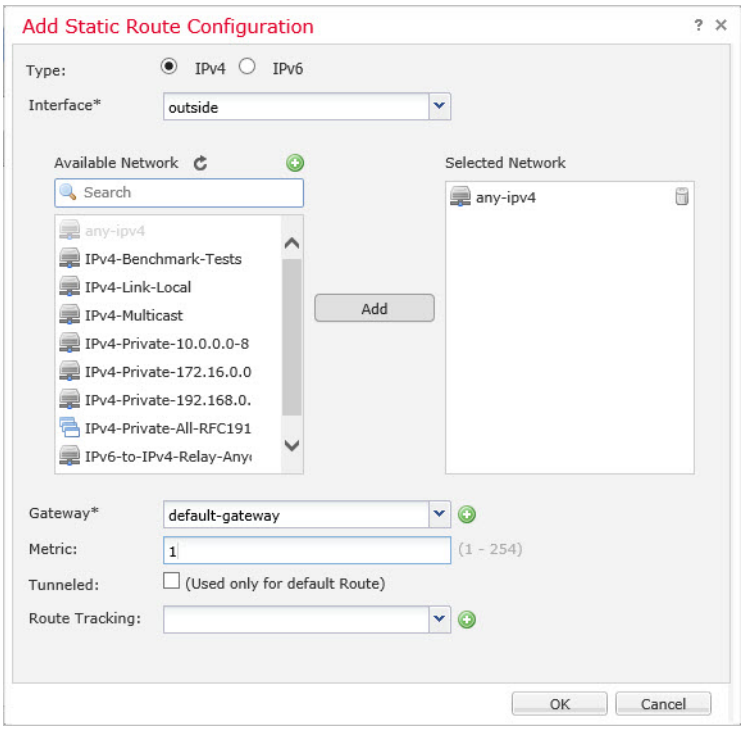
添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果从 DHCP 服务器收到默认路由，它将显示在 **IPv4 路由**或 **IPv6 路由**表中，该表位于 **设备** > **设备管理** > **路由** > **静态路由**页面。

过程

步骤 1 选择 **设备** > **设备管理**，然后单击该设备的 **编辑**（ ）。

步骤 2 选择 **路由** > **静态路由**，单击**添加路由**，然后设置以下参数：

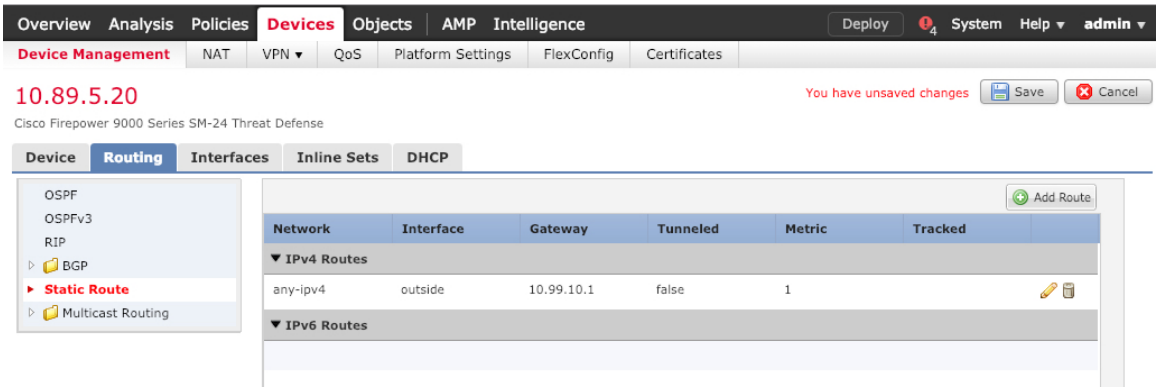


- **Type** - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- **Interface** - 选择出口接口；通常是外部接口。

- **可用网络** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**。
- **Gateway** 或 **IPv6 Gateway** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **Metric** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 单击 **OK**。

路由即已添加至静态路由表。



步骤 4 单击保存。

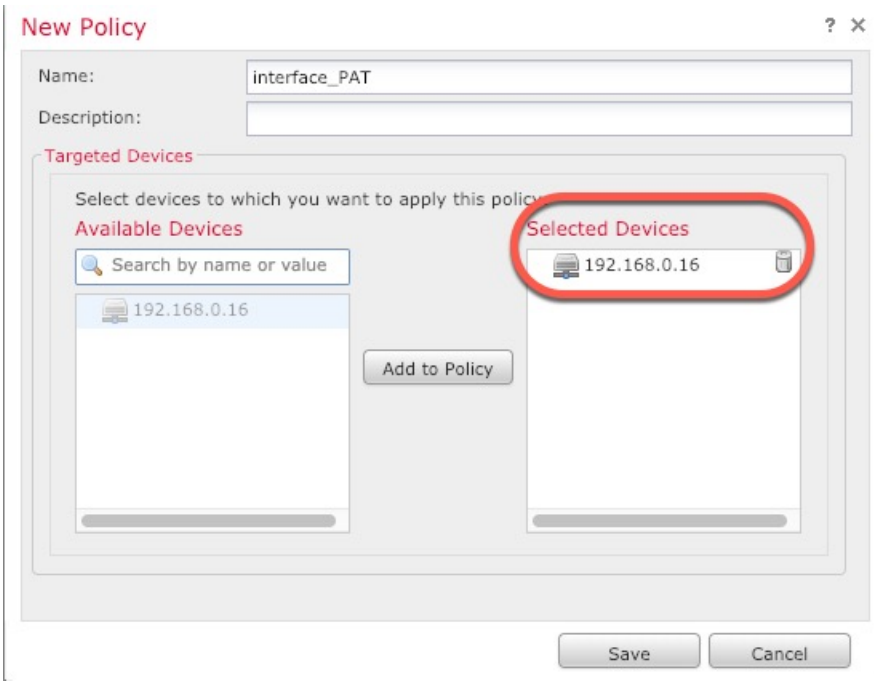
配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

步骤 1 选择 **设备** > **NAT**，然后单击 **新策略** > **Threat Defense NAT**.

步骤 2 为策略命名，选择要使用策略的设备，然后单击 **Save**。



策略即已添加 FMC。您仍然需要为策略添加规则。

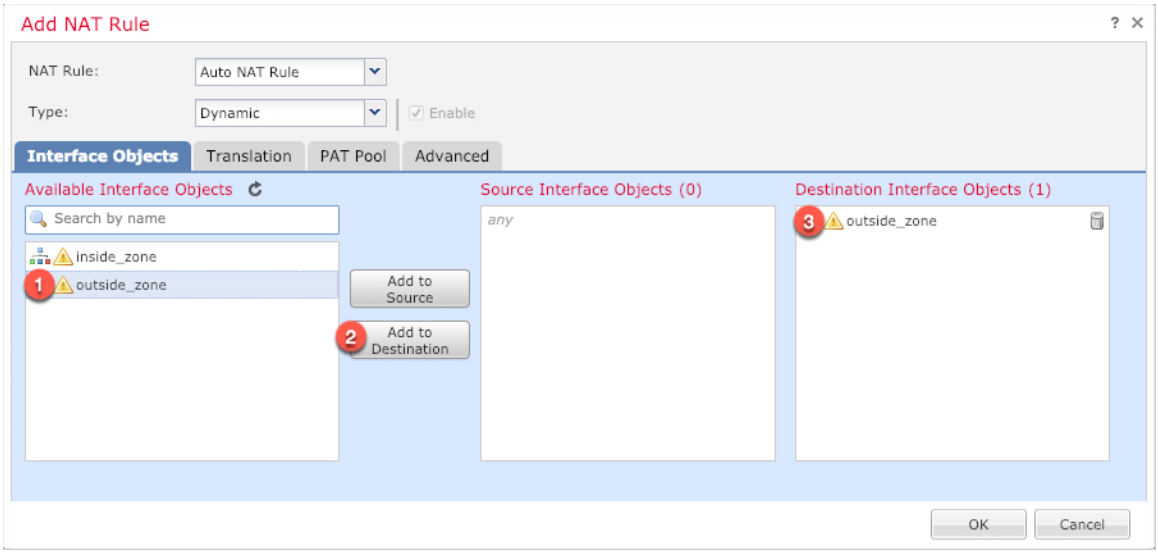
步骤 3 单击 **Add Rule**。

Add NAT Rule 对话框将显示。

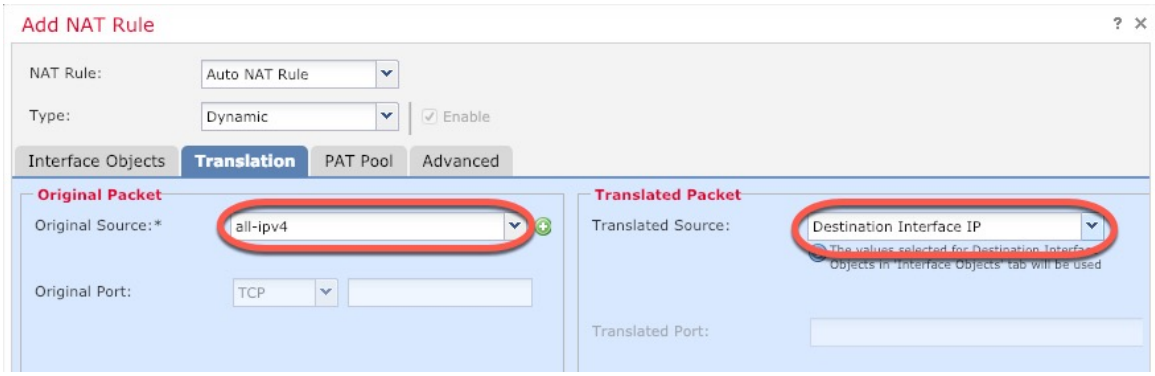
步骤 4 配置基本规则选项：

- **NAT Rule** - 选择 **Auto NAT Rule**。
- **Type** - 选择 **Dynamic**。

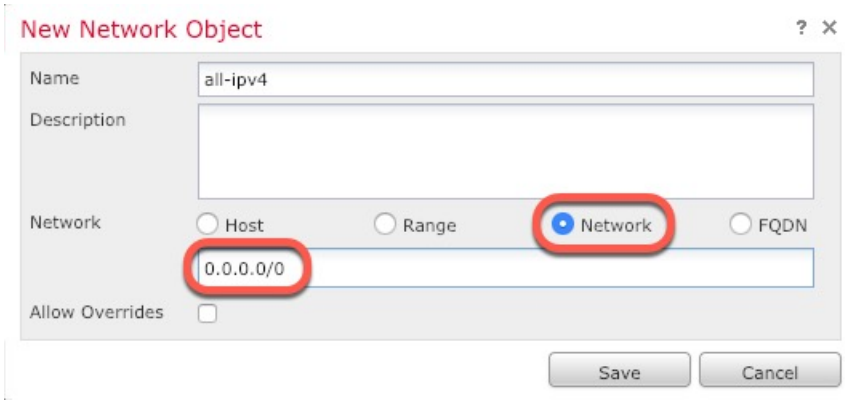
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在 **Translation** 页面上配置以下选项：



- **原始源** - 单击**添加**（+）为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

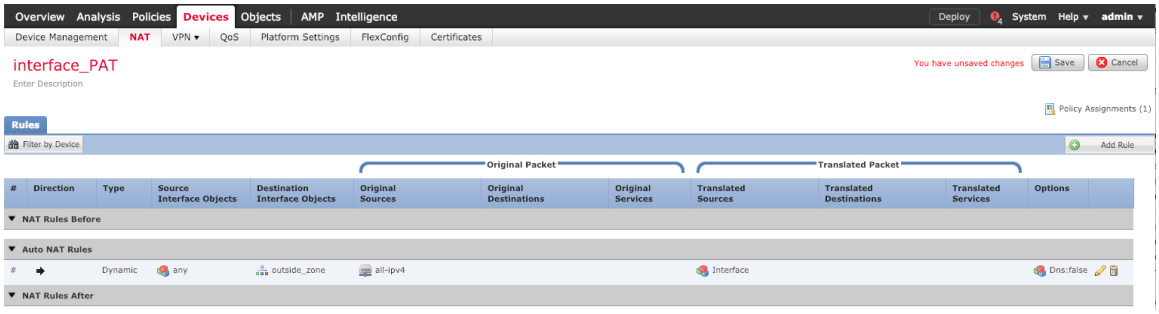


注释　您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- **Translated Source** - 选择 **Destination Interface IP**。

步骤 7 单击 **Save** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 单击 **NAT** 页面上的 **Save** 以保存更改。

配置访问控制

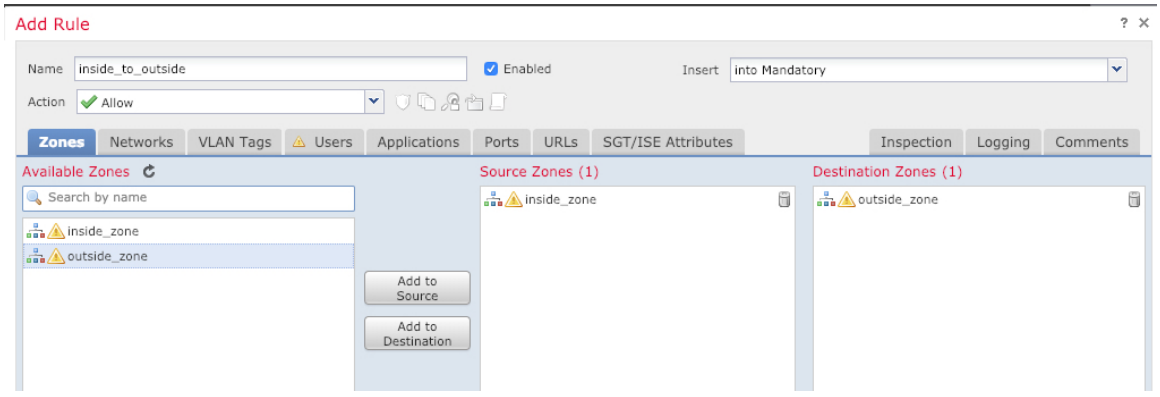
如果您在使用 FMC注册 FTDv 时创建了基本的**封锁所有流量**访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅 FMC 配置指南以配置更高级的安全设置和规则。

过程

步骤 1 选择 **策略** > **访问策略** > **访问策略**，然后单击分配给 FTD 的访问控制策略对应的**编辑**（ ）。

步骤 2 单击 **Add Rule** 并设置以下参数：

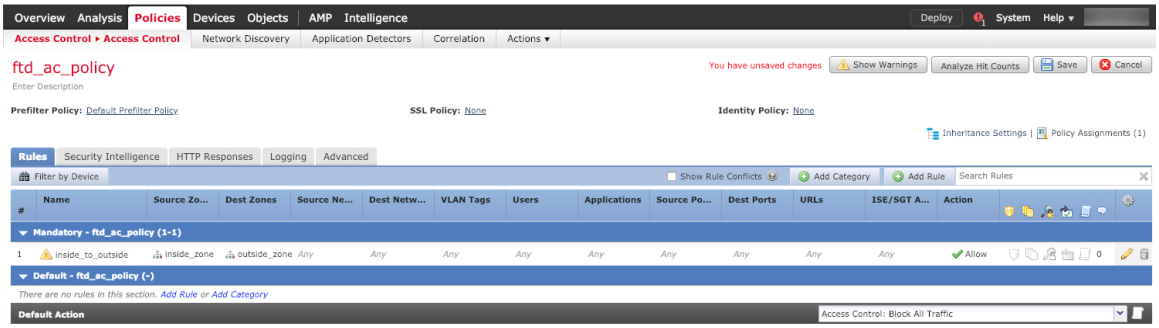


- **Name** - 为此规则命名，例如 **inside_to_outside**。
- **Source Zones** - 从 **Available Zones** 中选择内部区域，然后单击 **Add to Source**。
- **Destination Zones** - 从 **Available Zones** 中选择外部区域，然后单击 **Add to Destination**。

其他设置保留原样。

步骤 3 单击 **Add**。

规则即已添加至 **Rules** 表。



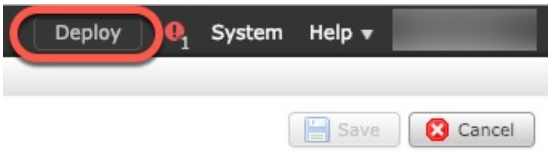
步骤 4 单击**保存**。

部署配置

将配置更改部署到 FTDv；在部署之前，您的所有更改都不会在设备上生效。

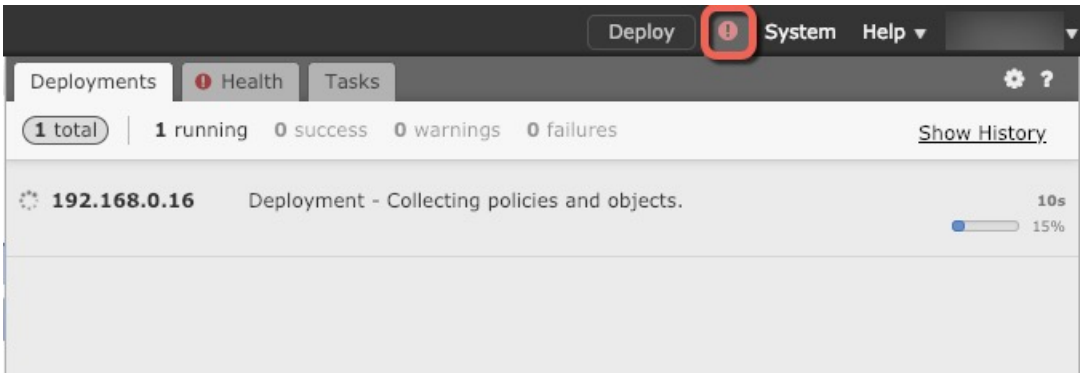
过程

步骤 1 单击右上方的 **Deploy**。



步骤 2 选择 **Deploy Policies** 对话框中的设备，然后单击 **Deploy**。

步骤 3 确保部署成功。单击菜单栏中 **Deploy** 按钮右侧的图标可以查看部署状态。



访问 Firepower 威胁防御 CLI

您可以使用FTDvCLI更改管理接口参数并进行故障排除。要访问CLI，可以使用管理接口上的SSH，也可以从 VMware 控制台连接。

过程

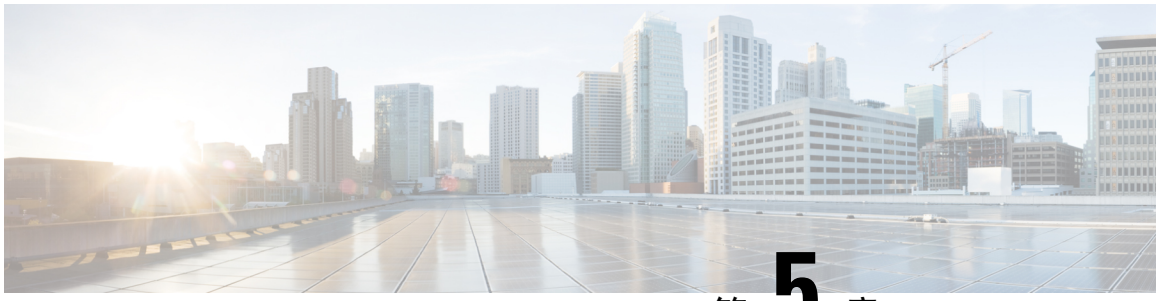
步骤 1 （选项 1）通过 SSH 直接连接到 FTDv 管理接口的 IP 地址。

在部署虚拟机时，您需要设置管理IP地址。使用**admin**帐户和初始部署期间设定的密码登录FTDv。

步骤 2 （选项 2）打开 VMware 控制台并使用默认用户名 **admin** 帐户和初始部署期间设定的密码登录。

使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史

功能名称	平台版本	功能信息
FMC 管理	6.0	初始支持。



第 5 章

使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FDM 管理的独立式 FTDv 设备。要部署高可用性对，请参阅 FDM 配置指南。

关于使用 Firepower 设备管理器管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 设备管理器 (FDM) 管理 FTDv，这是部分 Firepower 威胁防御 型号中包含的基于 Web 的设备设置向导。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。

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 Firepower 管理中心（而不是集成的Firepower设备管理器）来配置您的设备。有关详细信息，请参阅使用Firepower管理中心管理 Firepower Threat Defense Virtual，第 51 页。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 Firepower CLI 连接到 FTD。

默认配置

FTDv默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0-0 和 GigabitEthernet0-1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0-0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

FTDv 首次启动时，必须启用至少四个接口：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机上的第二个接口是诊断接口 (Diagnostic0-0)。
- 虚拟机的第三个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-1) 是内部接口。

您还可以添加最多六个额外的数据流量接口，使数据接口的总数达到八个。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。请参阅“配置 VMware 接口”。

初始配置

您必须完成初始配置，才能使 FTDv 在网络中正常运行，其中包括配置将安全设备插入网络以及将其连接到互联网或其他上游路由器所需的地址。您可以通过以下两种方式来进行系统初始配置：

- 使用 FDM Web 界面（推荐）。FDM 在您的网络浏览器中运行。使用该界面可配置、管理和监控系统。
- 使用命令行界面 (CLI) 设置向导（可选）。可以使用 CLI 设置向导（而不是 FDM）进行初始配置，并可以使用 CLI 执行故障排除。您仍然可以使用 FDM 来配置、管理和监控系统；请参阅（可选）“启动 Firepower 威胁防护 CLI 向导”。

以下主题介绍如何使用这些界面来执行系统初始配置。

启动 Firepower 设备管理器

在首次登录 Firepower 设备管理器 (FDM) 时，系统会通过设备设置向导指导您完成初始系统配置。

过程

步骤 1 打开浏览器并登录 FDM。假定您未在 CLI 中进行初始配置，请在 **https://***ip-address* 中打开 Firepower 设备管理器，其中地址为以下项之一：

- 如果您连接到内部桥组界面：**https://192.168.1.1**。
- 如果连接到管理物理接口，则地址为：**https://192.168.45.45**。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

步骤 3 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。只有完成这些步骤，才能继续。

步骤 4 为外部接口和管理接口配置以下选项，然后单击**下一步**。

注释 单击**下一步**后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。确保您的设置正确。

a) **Outside Interface** - 即连接到网关调制解调器或路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 (Configure IPv4) - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

b) **管理接口**

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请单击**使用 OpenDNS** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

注释 在使用设备设置向导配置 Firepower 威胁防御 设备时，系统会为出站和入站流量提供两个默认访问规则。您可以在完成初始配置后更改这些访问规则。

步骤 5 配置系统时间设置，然后单击**下一步**。

a) **时区** - 选择系统时区。

b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 6 为系统配置智能许可证。

只有具有智能许可证账户，才能获取和应用系统需要的许可证。最初，可以使用为期90天的评估许可证，以后再设置智能许可。

要立即注册设备，请单击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择 **Start 90 day evaluation period without registration**。如需稍后注册设备并获取智能许可证，请单击菜单中的设备名称打开 **Device Dashboard**，然后单击 **Smart Licenses** 组中的链接。

步骤 7 单击 **Finish**。

下一步做什么

- 使用 Firepower 设备管理器配置设备；请参阅如何在 Firepower 设备管理器中配置设备，第 70 页。

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口或网桥组上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请单击页面上的帮助按钮 (**?**)，获取有关每个步骤的详细信息。

过程

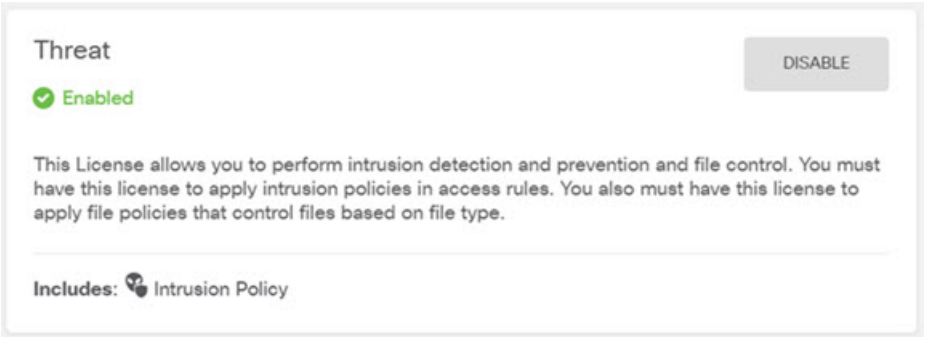
步骤 1 选择 **Device**，然后单击 **Smart License** 组中的 **View Configuration**。

对于您想要使用的可选许可证（威胁、恶意软件、URL），单击**启用**。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。单击**Request Register**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的威胁许可证：

图 *30:* 已启用的威胁许可证

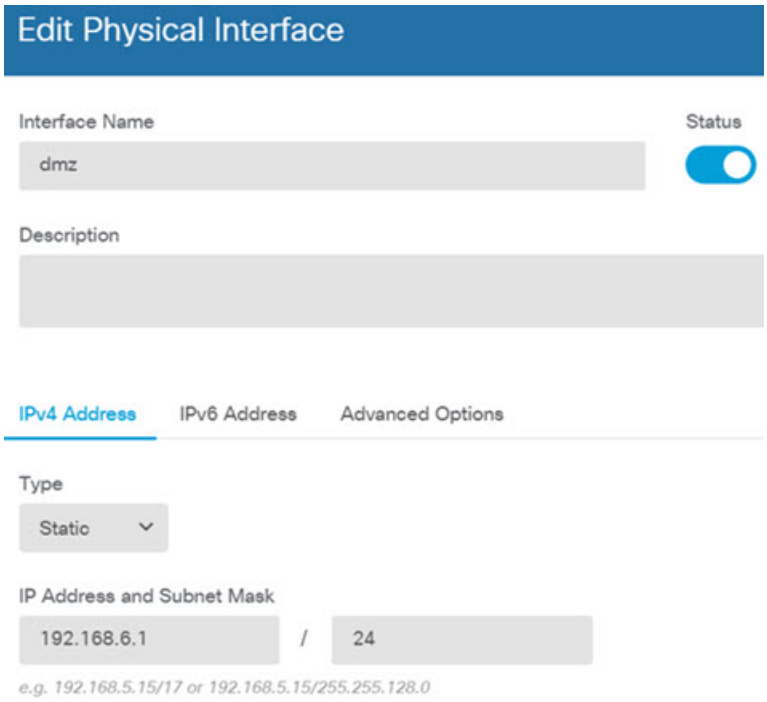


步骤 2 如果配置了其他接口，请选择**设备**，然后单击**接口**组中的**查看配置**并配置每个接口。

可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。单击每个接口的编辑图标 ( )，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后单击**保存**。

图 *31:* 编辑接口



步骤 3 如果已配置新接口，请选择**对象**，然后从目录中选择**安全区域**。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

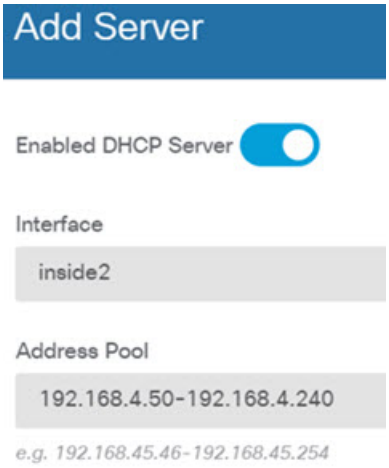
图 *32:* 安全区域对象

步骤 4 如果希望内部客户端使用 DHCP 从设备获取 IP 地址，请选择 **设备** > **系统设置** > **DHCP 服务器**，然后选择 **DHCP 服务器**选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。单击 +，为每个内部接口配置服务器和地址池。

此外，您也可以在 **Configuration** 选项卡中对为客户端提供的 WINS 和 DNS 列表进行精细调整。以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

图 *33: DHCP* 服务器



步骤 5 选择 **Device**，然后单击 **Routing** 组中的 **View Configuration**（或 **Create First Static Route**），配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

注释　此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**设备** > **系统设置** > **管理接口**上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过单击**网关**下拉菜单底部的**创建新网络**，来创建该对象。

图 *34:* 默认路由

步骤 6 选择**策略**，并为网络配置安全策略。

设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

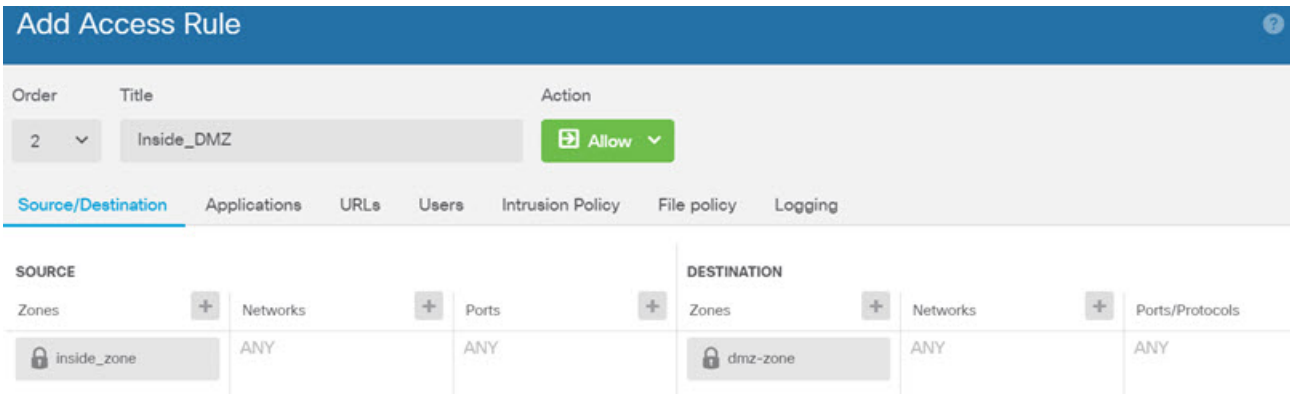
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。

- **Security Intelligence** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和URL源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录**除外，其中**在连接结束时**选项已被选中。

图 *35:* 访问控制策略



步骤 7 选择 **Device**，然后单击 **Updates** 组中的 **View Configuration**，为系统数据库配置更新计划。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全情报源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

步骤 8 单击菜单中的 **Deploy** 按钮，然后单击立即部署按钮 ()，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

下一步做什么

有关使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual 的详细信息，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》或 Firepower 设备管理器联机帮助。