# 适用于 Microsoft Azure 云的思科 Firepower 威胁防御虚拟快速入门指南

**发布日期：** 2017 年 1 月 23 日

**更新日期：**2017 年 7 月 13 日

Microsoft Azure 是一个开放而灵活的企业级公共云计算平台，该平台提供一系列云服务，包括用于计算、分析、存储和网络的服务。您可以从中挑选服务来开发和扩展新应用，或在公共云中运行现有的应用。

本文档介绍如何在 Azure 上部署 Firepower 威胁防御虚拟。



## 关于 Microsoft Azure 云上的部署

Firepower 威胁防御虚拟集成在 Microsoft Azure 市场内。在客户场所，客户在 Azure 外部管理 Firepower 管理中心。Microsoft Azure 上的 Firepower 威胁防御虚拟支持两种实例类型：

- 标准 D3 - 4 个 vCPU，14 GB，4vNIC
- 标准 D3_v2 - 4 个 vCPU，14 GB，4vNIC

## Firepower 威胁防御虚拟和 Azure 的先决条件及系统要求

- 在 Azure.com 上创建帐户。

  在 Microsoft Azure 上创建帐户后，您可以登录该市场，搜索“思科 Firepower 威胁防御”，然后选择“思科 Firepower 下一代防火墙 - 虚拟”产品。
- 思科智能帐户。可以在思科软件中心 (https://software.cisco.com/) 创建一个帐户。
- 许可 Firepower 威胁防御虚拟。在您许可 Firepower 威胁防御虚拟之前，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。
  - 所有安全服务的许可证授权均在 Firepower 管理中心中配置。
  - 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”。

- 通信路径：
  - 管理接口 – 用于将 Firepower 威胁防御虚拟连接到 Firepower 管理中心。
  - 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。
- 有关 Firepower 威胁防御虚拟与 Firepower 系统的兼容性，请参阅思科 Firepower 威胁防御虚拟兼容性。

# Firepower 威胁防御虚拟和 Azure 指南和限制

### 支持的功能

- 仅 Firepower 威胁防御虚拟可从 Microsoft Azure 市场获取。Firepower 管理中心在 Azure 外部运行。
- 支持的 Azure 实例 – Standard_D3_V2（默认）和 Standard_D3。两种实例都支持 4vCPU、14GB 内存、4vNIC。
- 许可模式：
  - 仅智能许可证
  - 不支持 PLR
- 网络：
  - 仅路由防火墙模式
- 公共 IP 寻址
  - 仅为管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。
- Interfaces:
  - Firepower 威胁防御虚拟配备四个接口。

### 不支持的功能

- 许可
  - 现收现付 (PAYG) 许可
  - 永久许可证预留 (PLR)
- 网络（其中许多限制都是 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 的角度看，设备不拥有的 IP 地址的代理 ARP（会影响到某些 NAT 功能）
  - 混杂模式（不捕获子网流量）
  - 内联集模式，被动模式

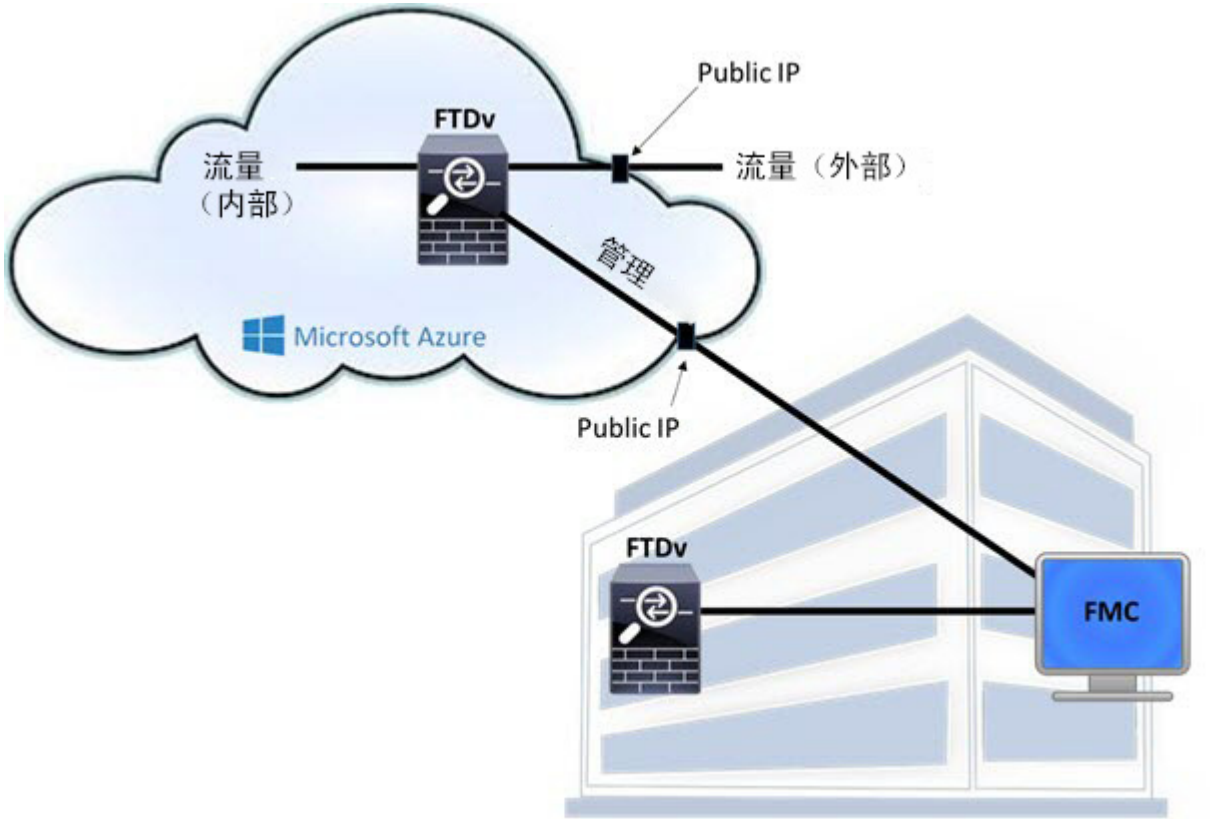
  **注意：** Azure 策略会阻止 Firepower 威胁防御虚拟在透明防火墙或内嵌模式下运行，因为它不允许接口在混杂模式下工作。
  - ERSPAN（使用 GRE，不在 Azure 中转发）

- 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
- Firepower 设备管理器用户界面

# 适用于 Azure 中 Firepower 威胁防御虚拟的示例网络拓扑

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。

**图 1** Azure 部署中的示例 Firepower 威胁防御虚拟



# 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 威胁防御虚拟接口：管理、诊断 0/0、GigabitEthernet 0/0 和 GigabitEthernet 0/1。
- 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）。

  该公共 IP 地址与虚拟机 Nic0 相关联，后者映射到管理接口。

  **注意：** 您必须选择公共 IP 地址（新地址或现有地址）；不支持“无”(NONE) 选项。
- 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）

  表命名为 *“subnet name”*-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）

  **注意：** 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）。

# 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。

**注意：**您可以在虚拟机 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 威胁防御虚拟后，您可以将公共 IP 地址与数据接口（例如 GigabitEthernet0/0）相关联。
- 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。

# 部署 Firepower 威胁防御虚拟

以下程序概要列出在 Microsoft Azure 环境中设置 Firepower 威胁防御虚拟的步骤。如需了解详细的 Azure 设置步骤，请参阅 Azure 入门。

在 Azure 中部署 Firepower 威胁防御虚拟时，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”(Idle Timeout) 默认值。

### 程序

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。
2. 依次选择 **Azure 市场** > **虚拟机**。
3. 搜索“思科 Firepower 下一代防火墙 - 虚拟”市场，选择产品，并点击**创建**。
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。

      **注意：**确保不要使用现有的名称，否则部署将失败。

   b. 输入 Firepower 威胁防御虚拟管理员的用户名。

      **注意：**“admin”是 Azure 中的预留名称，不能使用。

c. 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。

d. 在登录配置 Firepower 威胁防御虚拟时，创建一个用于 **Admin** 用户帐户的密码。

e. 选择订用类型。

f. 创建一个新资源组。

应将 Firepower 威胁防御虚拟部署到新资源组中。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。

g. 选择地理位置。此项应与此次部署中使用的所有资源（例如：ASAv、网络、存储帐户）相同。

h. 点击 **确定**。

5. 完成 Firepower 威胁防御虚拟初始配置。

a. 选择虚拟机大小。

b. 选择一个存储帐户。

**注意：**您可以使用现有的存储帐户，或创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

c. 请求一个公共 IP 地址，方法是在**名称**字段中输入该 IP 地址的标签，然后点击**确定**。

**注意：**Azure 会创建一个动态公共 IP 地址，无论此步骤中选择的是动态还是静态。当虚拟机停止和重启时，该公共 IP 可能会变化。如果您更喜欢固定的 IP 地址，可以在部署后打开创建的公共 IP，将其从动态地址更改为静态地址。

d. 根据需要添加 DNS 标签。

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

e. 选择现有的虚拟网络，或创建新的虚拟网络。

f. 为 Firepower 威胁防御虚拟网络接口配置四个子网：

- **FTDv 管理**接口，连接到“第一个子网”
- **FTDv 诊断**接口，连接到“第二个子网”
- **FTDv Gig0/0** 接口，连接到“第三个子网”
- **FTDv Gig0/1** 接口，连接到“第四个子网”

g. 点击 **确定**。

6. 查看配置摘要，然后点击**确定**。

7. 查看使用条款，然后点击**购买**。

部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 Firepower 威胁防御虚拟虚拟机正在运行。

## 后续操作

- 在 Azure 中更新 Firepower 威胁防御虚拟的 IP 配置。

# 更新公共 IP 地址配置

### 程序

1. 从**虚拟机**列表中，选择“Firepower 威胁防御虚拟虚拟机”。
2. 点击**概述**。
3. 点击**公共 IP 地址/DNS 名称标签**下的蓝色 IP 和 DNS 名称。
4. 点击**配置**：
   - 要按 IP 地址进行连接，请选择**静态**分配。
   - 要按 DNS 名称进行连接，请输入 DNS 名称标签。
   - （可选）为方便起见，您可以将**空闲超时**增加到最大范围（30 分钟）。这样可防止管理 SSH 会话过快超时。
5. 点击**保存**。

### 后续操作

- （可选）将公共 IP 地址添加到数据接口。
- 通过 Firepower 管理中心配置要管理的 Firepower 威胁防御虚拟。

# （可选）将公共 IP 地址添加到数据接口

### 程序

1. 从**虚拟机**列表中，选择“Firepower 威胁防御虚拟虚拟机”。
2. 点击**网络接口**。
3. 选择要将该 IP 地址添加到的数据接口：
   - 从 Firepower 管理中心查看时，Nic2（第三个 NIC）映射到 GigabitEthernet 0/0。这是第一个数据 NIC。
   - 从 Firepower 管理中心查看时，Nic3（第四个 NIC）映射到 GigabitEthernet 0/1。这是第二个数据 NIC。
4. 点击 **IP 配置**。
5. 点击 **添加**。
6. 从右侧的列表中选择 **IPConfig-1**。
7. 在 **IPConfig-1** 配置刀片中，将**公共 IP 地址**切换为**已启用**。
8. 使用**新建**对话框创建一个新的公共 IP 地址。

   **注意：**可以创建静态或动态 IP 地址。如果创建动态 IP 地址，则必须始终通过 DNS 名称（而不是 IP 地址）访问此接口。
9. 点击 **确定**。

   等待系统处理配置更改，然后检查**网络接口**列表，以确保已将公共 IP 地址添加到数据接口。

   **注意：**当 Internet 流量在与数据接口关联的公共 IP 地址定向时，该流量将通过 Azure 网关传输到目标 NAT，而数据包的新目标 IP 将为与公共 IP 关联的 Firepower 威胁防御虚拟接口的专用 IP。必须为 Firepower 威胁防御虚拟配置 NAT，以便将目标 IP 转换为内部子网中某个资源的 IP。
10. 点击**保存**。

### 后续操作

- 通过 Firepower 管理中心配置要管理的 Firepower 威胁防御虚拟。

# 配置用于 Firepower 管理的 Firepower 威胁防御虚拟

Firepower 威胁防御虚拟需要配备将设备注册到 Firepower 管理中心所需的网络信息。

要配置 Firepower 威胁防御虚拟以使 FMC 可将其作为设备进行添加，请使用 **configure manager add** 命令。将设备注册至 Firepower 管理中心，始终需要唯一的自身生成的字母数字注册密钥。这是由您指定的简单密钥，不同于许可密钥。

如果您使用“快速路由”(Express Route) 从您的场所连接到 Azure 虚拟网络，可以提供 Firepower 管理中心的 IP 地址以及注册密钥，例如：

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

其中，*XXX.XXX.XXX.XXX* 是管理 Firepower 管理中心的 IP 地址，*my_reg_key* 是用户定义的虚拟设备注册密钥。

不过，如果要使用公共 IP 地址注册 Firepower 威胁防御虚拟，还需要输入唯一的 NAT ID 以及注册密钥，并指定 DONTRESOLVE（而不是 IP 地址）。例如：

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

其中， *my_reg_key* 是用户定义的注册密钥， *my_nat_id* 是用户定义的虚拟设备 NAT ID。

### 程序

1. 使用 Azure 提供的公共 IP 地址通过 SSH 连接到 Firepower 威胁防御虚拟。
2. 使用用户名 **admin** 和密码 **Admin123** 登录。
3. 根据提示完成系统配置。

   必须先阅读并接受最终用户许可协议 (EULA)。然后更改管理员密码，再根据提示配置管理地址、DNS 设置和防火墙模式（路由）。
4. 等待默认系统配置进行处理。此过程可能需要几分钟。
5. 使用 **configure manager add** 命令确定将管理此设备的 Firepower 管理中心设备。

   > **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

   **注意：** 注册密钥是由用户定义的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字字符（A-Z、a-z、0-9）和连字符 (-)。当您将设备添加到 Firepower 管理中心时，需要记住此注册密钥。

   如果 Firepower 管理中心不可直接寻址，请使用 DONTRESOLVE。

   **注意：** NAT ID 为可选的用户定义字母数字字符串，它与以上所述的注册密钥遵循相同的约定。如果主机名设置为 DONTRESOLVE，此项为必填项。当您将设备添加到 Firepower 管理中心时，需要记住此 NAT ID。

   由于 Firepower 管理中心的 IP 地址可能会通过 NAT 连接到 Azure，所以 NAT ID 为必填项。例如：

   **configure manager add DONTRESOLVE 1234 ABCD**

### 后续操作

- 更新 Azure 安全组。

# 更新安全组

安全组控制 Azure 允许/拒绝特定接口连接到哪些端口/目标。要获得 SSH 访问 Firepower 威胁防御虚拟以及 Firepower 管理中心允许 SSH 访问的权限，需要向虚拟机主接口上的安全组中添加规则。SSH 需要使用 TCP 端口 22，而注册和诊断需要使用 TCP 端口 8305。

### 程序

1. 打开新部署的 Firepower 威胁防御虚拟的虚拟机信息页面。
2. 选择**网络接口**。
3. 选择 **Nic0**。
4. 在**基础**窗格中，查找网络安全组。点击蓝色的网络安全组名称。该名称应遵循类似于 *<vmname>-SSH-SecurityGroup* 的约定。
5. 点击**入站安全规则**。
6. 验证其中是否存在允许“服务 = SSH”的 SSH 规则；如果没有，则添加一个相应的规则。

   我们建议您将源地址范围限制为通过 SSH 连接到 Firepower 威胁防御虚拟时希望使用的 IP 地址，否则 SSH 将面向互联网开放。
7. 为诊断接口添加一个安全组规则：
   a. 名称 - 为入站规则命名，例如 *sf-tunnel*。
   b. 优先级 - 保留默认值
   c. 源 - 更改为 CIDR，然后输入 Firepower 管理中心从中发送信息的子网。
   d. 服务 - 自定义
   e. 协议 - TCP
   f. 端口范围 - 8305
   g. 操作 - 允许
8. 点击 **确定**。

### 后续操作

- 将 Firepower 威胁防御虚拟注册到 Firepower 管理中心。

## 注册到 Firepower 管理中心

确保第一个接口和管理子网上的安全组允许来自 Firepower 管理中心源地址的所有流量。源地址通常是面向互联网的防火墙的池中的地址。您可以临时允许所有流量。但在发现 Firepower 管理中心要从中连接的 IP 地址块后，应将安全组限制为仅允许来自这些已知安全块的流量。

### 程序

### 准备工作

- Firepower 威胁防御虚拟需要智能软件许可，通过 Firepower 管理中心可对此进行配置。
- 确定对您的虚拟设备的时间同步要求。我们建议您将设备同步到物理 NTP 服务器。不要将受管设备与虚拟 Firepower 管理中心同步。有关时间同步要求，请参阅《Firepower 管理中心配置指南》。

### 程序

1. 在浏览器中，使用已配置的 Firepower 管理中心的主机名或地址通过 HTTPS 连接登录 Firepower 管理中心。例如，https://MC.example.com。
2. 在管理中心的 Web 界面上，依次选择**设备 > 设备管理**。
3. 从**添加**下拉列表中，选择**添加设备**。

4. 在**主机**字段中：
   a. 要使用公共 IP 地址通过互联网进行连接，请输入与 Firepower 威胁防御虚拟管理接口相关联的公共 IP 地址。
   b. 要通过 Azure ExpressRoute 进行连接，请输入与 Firepower 威胁防御虚拟管理接口相关联的专用 IP。
5. 在**显示名称**字段中，输入要在管理中心显示的安全模块名称。
6. 在**注册密钥**字段中，输入您为 Firepower 管理配置 Firepower 威胁防御虚拟时所用的相同注册密钥。
7. 如果要在多域环境中添加设备，请从**域 (Domain)** 下拉列表中选择一个值，将设备分配到枝叶域。

   如果当前域是叶域，设备会自动添加到当前域。
8. 或者，也可将设备添加到设备**组 (Group)**。
9. 从**访问控制策略**下拉列表中，选择要部署到安全模块的初始策略：
   - **Default Access Control** 策略阻止所有流量进入网络。
   - **Default Intrusion Prevention** 策略允许也通过 Balanced Security 和 Connectivity 入侵策略传递的所有流量。
   - **Default Network Discovery** 策略允许仅通过网络发现进行检查的所有流量。
   - 您可以选择用户定义的任何现有的访问控制策略。有关详细信息，请参阅《*Firepower 管理中心配置指南*》中的“管理访问控制策略”一节。
10. 选择要应用到设备的许可证。

    **注意：**控制、恶意软件和 URL 过滤许可证需要保护许可证；有关详细信息，请参阅《Firepower 管理中心配置指南》。
11. 如果在将设备配置为由 Firepower 管理中心管理时使用 NAT ID 识别设备，请展开**高级**部分并在“唯一 NAT ID”字段中输入同一 NAT ID。

    **注意：**如果使用管理接口的公共 IP 通过互联网连接到 Firepower 威胁防御虚拟，则需要使用 NAT ID。如果通过 Azure ExpressRoute 进行连接，则不需要使用 NAT ID。
12. 点击**注册**，并确认注册成功。

    Firepower 管理中心可能需要长达两分钟来验证设备的心跳并建立通信。

### 后续操作

- 启用和配置两个数据接口。

# 配置设备设置

在将 Firepower 威胁防御虚拟注册到管理其的 Firepower 管理中心之后，需要启用和配置两个数据接口。

### 程序

1. 依次选择**设备 > 设备管理**。
2. 点击要配置接口的 Firepower 威胁防御虚拟设备旁边的编辑图标。

   在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。
3. 点击 GigabitEthernet0/0 接口旁边的编辑图标。
   a. 从**模式**下拉列表中，选择**无**以使该接口处于路由模式下。
   b. 点击 **IPv4** 选项卡，并验证 **IP 地址**是否与在 Azure 中部署时提供给该接口的地址匹配。
   c. 点击 **确定**。
4. 针对 GigabitEthernet0/1 接口重复相同的步骤。
5. 点击**保存**。

## 后续操作

- 您可以使用 Firepower 管理中心用户界面来配置和应用访问控制策略及其他相关策略，以管理使用 Firepower 威胁防御虚拟实例的流量；请参阅《*Firepower 管理中心配置指南*》或联机帮助。

部署 Firepower 威胁防御虚拟