



使用面向 KVM 的 Firepower 设备管理器部署思科 Firepower 威胁防御虚拟快速入门指南

版本 6.2.3 及更高版本

首次发布日期：2018 年 3 月 29 日

最后更新日期：2018 年 8 月 2 日

您可以使用配备了基于内核的虚拟机 (KVM) 监控程序的 Firepower 设备管理器部署 Firepower 威胁防御虚拟。

- [关于使用 KVM 的部署（第 1 页）](#)
- [Firepower 威胁防御虚拟、Firepower 设备管理器和 KVM 的前提条件（第 2 页）](#)
- [许可证要求（第 3 页）](#)
- [准备 Day 0 配置文件（第 3 页）](#)
- [启动 Firepower 威胁防御虚拟（第 5 页）](#)
- [在没有 Day 0 配置文件的情况下启动（第 10 页）](#)
- [如何在 Firepower 设备管理器中配置设备（第 11 页）](#)

关于使用 KVM 的部署

KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的内核模块 `kvm.ko`（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 `kvm-intel.ko`）。

您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

KVM 上的 Firepower 威胁防御虚拟支持以下硬件：

- 处理器
 - 需要 4 个 vCPU
- 内存
 - 需要 8 GB RAM
- 网络
 - 需要两个管理接口和两个数据接口才能启动

注意：虚拟 Firepower 威胁防御的默认配置将管理接口、诊断接口和内部接口置于同一子网上。

- 支持 `virtio` 驱动程序
- 支持共计 10 个接口

Firepower 威胁防御虚拟、Firepower 设备管理器和 KVM 的前提条件

- 每个虚拟机的主机存储
 - Firepower 威胁防御虚拟需要 50 GB
 - 支持 virtio 块设备
- 控制台
 - 通过 telnet 支持终端服务器

规定和限制

- 虚拟 Firepower 威胁防御的默认配置假定您将管理（管理和诊断）接口和内部接口都置于**同一子网**上，并且管理地址使用内部地址作为其连接互联网的网关（通过外部接口）。
- Firepower 威胁防御虚拟**首次启动时，必须启用至少四个接口**。您的系统必须要有四个接口才能部署。
- KVM 上的 Firepower 威胁防御虚拟支持共计 10 个接口 - 1 个管理接口、1 个诊断接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
 - 1. 管理接口（必需）
 - 2. 诊断接口（必需）
 - 3. 外部接口（必需）
 - 4. 内部接口（必需）
 - 5-10 数据接口（可选）

请查看 Firepower 威胁防御虚拟接口的以下网络适配器、源网络和目标网络的对应关系：

表 1 源网络与目标网络的映射

网络适配器	源网络	目标网络	功能
vnic0 ¹	Management0-0	Management0/0	管理
vnic1 ¹	诊断	诊断	诊断
vnic2	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
vnic3 ¹	GigabitEthernet0-1	GigabitEthernet0/1	内部流量

1. 连接到同一子网。

- 如果在 OpenStack 环境中部署 Firepower 威胁防御虚拟，您需要使用混杂模式运行并禁用端口安全（即数据包过滤）。执行此操作时，请务必记住，如果为某个接口分配了安全组或允许的地址对，则不能禁用端口安全。一旦禁用端口级安全，将会允许所有流量（入口和出口）。
- 不支持克隆虚拟机。

Firepower 威胁防御虚拟、Firepower 设备管理器和 KVM 的前提条件

- 从 Cisco.com 下载 Firepower 威胁防御虚拟 qcow2 文件并将其放在 Linux 主机上：
<https://software.cisco.com/download/navigator.html>

注意：需要 Cisco.com 登录信息和思科服务合同。
- 您必须为虚拟机安装新版映像（版本 6.2.3 或更高版本），才能使其支持 Firepower 设备管理器。不能将现有虚拟机从较低版本升级后切换至 Firepower 设备管理器。

- Firepower 设备管理器（本地管理器）会默认启用。
注意：当启用本地管理器选项设置为是时，**防火墙模式**会变为**已路由**。这是唯一支持使用 Firepower 设备管理器的模式。
- 为与本文档中的部署示例吻合，我们假定您使用 Ubuntu 14.04 LTS。将以下数据包安装在 Ubuntu 14.04 LTS 主机之上：
 - qemu-kvm
 - libvirt-bin
 - bridge-utils
 - virt-manager
 - virtinst
 - virsh tools
 - genisoimage
- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的 Firepower 威胁防御虚拟吞吐量。有关通用的主机调整概念，请参阅《[网络功能虚拟化：具备 Linux 和 Intel 架构的宽带远程访问服务器的服务质量](#)》。
- Ubuntu 14.04 LTS 的有用优化包括以下内容：
 - macvtap - 高性能 Linux 网桥；您可以使用 macvtap，而不是 Linux 网桥。
注意：您必须配置特定设置才能使用 macvtap，而不是 Linux 网桥。
 - 透明大页面 (Transparent Huge Pages) - 用于增加内存页面大小，在 Ubuntu 14.04 中默认开启。
 - 禁用超线程 (Hyperthread disabled) - 用于将两个 vCPU 减少到一个单核。
 - txqueuelength - 用于将默认 txqueuelength 增加到 4000 个数据包并减少丢包率。
 - 固定 (pinning) - 用于将 qemu 和 vhost 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分发的信息，请参阅《[Red Hat Enterprise Linux6 虚拟化调整和优化指南](#)》。
- 有关 KVM 与 Firepower 系统的兼容性，请参阅《[思科虚拟 Firepower 威胁防御的兼容性](#)》。

许可证要求

购买 Firepower 威胁防御设备或虚拟 Firepower 威胁防御会自动附带基本许可证。所有其他许可证（威胁、恶意软件或 URL 过滤）均为可选。有关 Firepower 威胁防御许可的更多信息，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中的“系统许可”一章。

准备 Day 0 配置文件

在启动 Firepower 威胁防御虚拟之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时装载和读取的 day0.iso 文件。

注意：该 day0.iso 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 Firepower 威胁防御虚拟设备的整个初始设置。可以指定：

- 接受 EULA
- 系统的主机名

准备 Day 0 配置文件

- 管理员帐户的新管理员密码
- 初始防火墙模式
- 允许设备在管理网络通信的网络设置
- 管理思科 FirePOWER 管理中心

如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置 Firepower 系统所需的设置；有关更多信息，请参阅[在没有 Day 0 配置文件的情况下启动（第 10 页）](#)。

注意：我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

程序

1. 在名为“day0-config”的文本文件中输入 Firepower 威胁防御虚拟的 CLI 配置。添加网络设置和关于管理 Firepower 管理中心的信息。

示例：

```
#Firepower Threat Defense on KVM
{
  "EULA": "accept",
  "Hostname": "ftdv-kvm-production",
  "AdminPassword": "Admin123",
  "FirewallMode": "routed",
  "DNS1": "1.1.1.1",
  "DNS2": "1.1.1.2",
  "DNS3": "",
  "IPv4Mode": "manual",
  "IPv4Addr": "10.12.129.44",
  "IPv4Mask": "255.255.0.0",
  "IPv4Gw": "10.12.0.1",
  "IPv6Mode": "disabled",
  "IPv6Addr": "",
  "IPv6Mask": "",
  "IPv6Gw": "",
  "FmcIp": "",
  "FmcRegKey": "",
  "FmcNatId": "",
  "ManageLocally": "Yes"
}
```

注意：在 Day 0 配置文件的 **ManageLocally** 中输入 **Yes**，并将 Firepower 管理中心字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）留白。

2. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

或

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

3. 为每个要部署的 Firepower 威胁防御虚拟重复创建唯一的默认配置文件。

后续操作

- 如果使用 virt-install，请在 virt-install 命令中添加以下行：
`--disk path=/home/user/day0.iso,format=iso,device=cdrom \`
- 如果使用 virt-manager，则可以使用 virt-manager GUI 创建虚拟 CD-ROM；请参阅[使用虚拟机管理器启动（第 6 页）](#)。

启动 Firepower 威胁防御虚拟

使用部署脚本启动

可以使用基于 `virt-install` 的部署脚本启动 Firepower 威胁防御虚拟。

请注意，您可以通过选择适合您环境的最佳访客缓存模式来优化性能。正在使用的缓存模式不仅会影响到是否发生数据丢失，还会影响到磁盘性能。

可以为每个 KVM 访客磁盘接口指定以下缓存模式之一：`writethrough`、`writeback`、`none`、`directsync` 或 `unsafe`。`writethrough` 提供读取缓存。`writeback` 提供读取和写入缓存。`directsync` 绕过主机页面缓存。`unsafe` 可能会缓存所有内容，并忽略来自访客的刷新请求。

缓存模式指导原则

- 当主机遇到突然断电时，`cache=writethrough` 有助于降低 KVM 访客计算机上的文件损坏。我们建议使用 `writethrough` 模式。
- 但是，由于 `cache=writethrough` 的磁盘 I/O 写入次数高于 `cache=none`，所以该模式也会影响磁盘性能。
- 如果删除了 `--disk` 选项上的 `cache` 参数，则默认值为 `writethrough`。
- 未指定缓存选项还有可能大幅减少创建虚拟机所需的时间。这是因为，一些较旧的 RAID 控制器的磁盘缓存能力较差。因此，禁用磁盘缓存 (`cache=none`)，从而使用默认值 `writethrough`，有助于确保数据完整性。

程序

1. 创建名为“`virt_install_ftdv.sh`”的 `virt-install` 脚本。

Firepower 威胁防御虚拟虚拟机 (VM) 的名称在此 KVM 主机上的所有其他虚拟机中必须是唯一的。

注意：虚拟 Firepower 威胁防御的默认配置假定您将管理接口、诊断接口和内部接口置于同一子网上。系统至少需要 4 个接口才能成功启动。虚拟 NIC 必须是 Virtio。接口到网络分配必须遵循以下顺序：

- 1. 管理接口（必需）
- 2. 诊断接口（必需）
- 3. 外部接口（必需）
- 4. 内部接口（必需）
- 5-10 数据接口（可选）

```
virt-install \
  --connect=qemu:///system \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --name=ftdv \
  --arch=x86_64 \
  --cpu host \
  --vcpus=4 \
  --ram=8192 \
  --os-type=linux \
  --os-variant=virtio26 \
  --virt-type=kvm \
  --import \
  --watchdog i6300esb,action=reset \
```

启动 Firepower 威胁防御虚拟

```
--disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,  
  cache=writethrough \  
--disk path==<day0_filename>.iso,format=iso,device=cdrom \  
--console pty,target_type=serial \  
--serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \  
--force
```

2. 运行 virt_install 脚本：

```
/usr/bin/virt_install_ftdv.sh
```

```
Starting install...  
Creating domain...
```

系统将显示窗口，其中显示 VM 的控制台。您可以看到 VM 正在启动。VM 需要几分钟进行启动。一旦虚拟机停止启动，您便可以从控制台屏幕发出 CLI 命令。

后续操作

- 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 11 页）](#)。

使用虚拟机管理器启动

使用 virt-manager（也称为虚拟机管理器）启动 Firepower 威胁防御虚拟。Virt-manager 是用于创建和管理访客虚拟机的图形化工具。

1. 启动 virt-manager（应用 > 系统工具 > 虚拟机管理器）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

2. 点击左上角的按钮，打开新建虚拟机向导。

3. 输入虚拟机的详细信息：

a. 指定名称。

b. 对于操作系统，选择导入现有的磁盘映像。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

c. 点击继续继续操作。

4. 加载磁盘映像：

a. 点击浏览...，选择映像文件。

b. 对于操作系统类型，选择 Linux。

c. 对于版本，选择通用 2.6.25 或更高版本 virtio 内核。

d. 点击继续继续操作。

5. 配置内存和 CPU 选项：

a. 将内存 (RAM) 设为 8192。

b. 将 CPUs 设为 4。

c. 点击继续继续操作。

6. 选中安装前自定义配置复选框，然后点击完成。

执行此操作将会打开另一个向导，您可以在其中添加、删除和配置虚拟机的硬件设置。

7. 修改 CPU 配置：

从左侧面板中，选择**处理器**，然后选择**配置 > 复制主机 CPU 配置**。

这会将物理主机的 CPU 型号和配置应用于您的虚拟机。

8. 配置虚拟磁盘：

a. 从左侧面板中，选择**磁盘 1**。

b. 选择**高级选项**。

c. 将**磁盘总线**设为 *Virtio*。

d. 将**存储格式**设为 *qcow2*。

9. 配置串行控制台：

a. 从左侧面板中，选择**控制台**。

b. 选择**删除**，删除默认的控制台。

c. 点击**添加硬件**，添加一个串行设备。

d. 对于**设备类型**，选择 *TCP net 控制台 (tcp)*。

e. 对于“模式”，选择“服务器”模式（绑定）。

f. 对于**主机**，输入 IP 地址和端口号。

g. 选中**使用 Telnet** 框。

h. 配置设备参数。

10. 配置看门狗设备，在 KVM 访客挂起或崩溃时自动触发某项操作：

a. 点击**添加硬件**，添加一个看门狗设备。

b. 对于**型号**，选择**默认值**。

c. 对于**操作**，选择**强制重置访客**。

11. 配置至少 4 个虚拟网络接口：

a. 点击**添加硬件**，添加一个接口。

b. 对于**源设备**，选择 *macvtap*。

c. 对于**设备型号**，选择 *virtio*。

d. 对于**源模式**，选择**网桥**。

注意：虚拟 Firepower 威胁防御的默认配置假定您将管理接口、诊断接口和内部接口置于**同一子网**上。系统至少需要 4 个接口才能成功启动。虚拟 NIC 必须是 Virtio。接口到网络分配必须遵循以下顺序：

- vnic0 - 管理接口（必需）
- vnic1 - 诊断接口（必需）
- vnic2 - 外部接口（必需）
- vnic3 - 内部接口（必需）
- vnic4-9 - 数据接口（可选）

注意：请确保将 vnic0、vnic1 和 vnic3 映射到同一子网。

启动 Firepower 威胁防御虚拟

12. 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：
 - a. 单击**添加硬件(Add Hardware)**。
 - b. 选择**存储**。
 - c. 点击**选择托管或其他现有存储**，然后浏览到 ISO 文件的位置。
 - d. 对于**设备类型**，选择 *IDE CDROM*。
13. 配置虚拟机的硬件后，点击**应用**。
14. 点击**开始安装**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

后续操作

- 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 11 页）](#)。

使用 OpenStack 启动

您可以在 OpenStack 环境中部署 Firepower 威胁防御虚拟。OpenStack 是一套用于构建和管理适用于公共云和私有云的云计算平台的软件工具，并且与 KVM 虚拟机监控程序紧密集成。

注意：如果在 OpenStack 环境中部署 Firepower 威胁防御虚拟，您需要使用混杂模式运行并禁用端口安全（即数据包过滤）。执行此操作时，请务必记住，如果为某个接口分配了安全组或允许的地址对，则不能禁用端口安全。一旦禁用端口级安全，将会允许所有流量（入口和出口）。

关于 OpenStack 上的 Day 0 配置文件

OpenStack 支持通过特殊的配置驱动器 (config-drive) 提供配置数据，该驱动器在 OpenStack 启动时连接到实例。要使用 nova boot 命令和 Day 0 配置部署 Firepower 威胁防御虚拟实例，请包括以下行：

```
--config-drive true --file day0-config=/home/user/day0-config \
```

启用 `--config-drive` 命令后，在调用 nova 客户端的 Linux 文件系统上找到的文件 `=/home/user/day0-config`，将被传递到虚拟 CDROM 上的虚拟机。

注意：虚拟机可能看到此文件名为 `day0-config`，而 OpenStack 通常将文件内容存储为 `/openstack/content/xxxx`，其中 `xxxx` 是分配的四位数编号（例如 `/openstack/content/0000`）。这可能因 OpenStack 的发行版本而异。

使用命令行启动

使用 **nova boot** 命令创建和启动 Firepower 威胁防御虚拟实例。

程序

1. 使用映像、风格、接口和 Day 0 配置信息启动 Firepower 威胁防御虚拟实例。

Firepower 威胁防御虚拟可支持多达 10 个网络接口。此示例使用了四个接口。

注意：虚拟 Firepower 威胁防御的默认配置将管理接口、诊断接口和内部接口置于同一子网上。系统至少需要 4 个接口才能成功启动：管理接口、诊断接口、外部接口和内部接口。

```
local@maas:~$ nova boot \
  --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \
  --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \
  --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \
  --nic net-id=ae638375-d0d1-4f1e-a93d-6e621e5fabd2 \
  --nic net-id=e9cedefd-178e-41a8-9c47-4e1feaa48477 \
  --nic net-id=f8b8dd2d-c8cc-452e-98f3-9542dddc7965 \
  --config-drive true --file day0-config=/home/local/day0-config \
```


使用 OpenStack 控制面板启动

Horizon 是一个为 OpenStack 服务（包括 Nova、Swift、Keystone 等等）提供基于 Web 的用户界面的 OpenStack 控制面板。

准备工作

- 从 Cisco.com 下载 Firepower 威胁防御虚拟 qcow2 文件并将其放在本地的 MAAS 服务器上：

<https://software.cisco.com/download/navigator.html>

注意：需要 Cisco.com 登录信息和思科服务合同。

程序

1. 在登录页面上，输入您的用户名和密码，然后点击**登录**。
控制面板中显示的选项卡和功能取决于已登录用户的访问权限或角色。
2. 从菜单中选择**管理员 > 系统面板 > 风格**。
在 OpenStack 中，虚拟硬件模板被称为**风格**，定义了 RAM 和磁盘大小、核心数量，等等。此过程将为您的 Firepower 部署创建风格。
3. 在**风格信息**窗口中输入需要的信息：
 - a. **名称** - 输入可轻松标识该实例的描述性名称。例如，*FTD-FMC-4vCPU-8GB*。
 - b. **VCPU** - 将 VCPU 数量设为 4 个。
 - c. **RAM MB** - 将 RAM 量设为 8192 MB。
4. 选择**创建风格**。
5. 从菜单中选择**管理员 > 系统面板 > 映像**。
6. 在**创建映像**窗口中输入需要的信息：
 - a. **名称** - 输入可轻松标识该映像的名称。例如，*FTD-Version-Build*。
 - b. **说明** - （可选）输入此映像文件的说明。
 - c. **浏览** - 选择之前从 Cisco.com 下载的 Firepower 威胁防御虚拟 qcow2 文件。
 - d. **格式** - 选择 *QCOW2-QEMU 仿真器* 作为格式类型。
 - e. 选中**公共**复选框。
7. 选择**创建映像**。
查看新创建的映像。
8. 从菜单中选择**项目 > 计算 > 实例**。
9. 点击**启动实例**。
10. 在**启动实例 > 详细信息**选项卡中输入需要的信息：
 - a. **实例名称** - 输入可轻松标识该实例的名称。例如，*FTD-Version-Build*。
 - b. **风格** - 选择先前在第 3. 步中创建的风格。输入此映像文件的说明。
 - c. **实例启动源** - 选择**从映像启动**。
 - d. **映像名称** - 选择先前在第 6. 步中创建的映像。

在没有 Day 0 配置文件的情况下启动

11. 从**启动实例 > 网络**选项卡中，选择 Firepower 威胁防御虚拟实例的管理网络和数据网络。

注意： Firepower 威胁防御虚拟至少需要四个接口才能启动：两个管理接口和两个流量接口。

12. 点击**启动**。

在云计算节点上启动实例。从**实例**窗口中查看新创建的实例。

13. 选择 Firepower 威胁防御虚拟实例。

14. 选择**控制台**选项卡。

15. 在控制台上登录到虚拟设备。

后续操作

- 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 11 页）](#)。

在没有 Day 0 配置文件的情况下启动

由于 Firepower 威胁防御虚拟设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

首次登录新部署的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

在遵循设置提示的情况下，对于多选问题，选项会列在括号内，例如 *(y/n)*。默认值会列在方括号内，例如 *[y]*。按 **Enter** 键确认选择。

注意：要在完成初始设置后更改虚拟设备的上述任何设置，必须使用 CLI；

程序

1. 打开 Firepower 威胁防御虚拟的控制台。
2. 在 **firepower login** 提示符下，使用默认凭据 (*username admin, password Admin123*) 登录。
3. 当 Firepower 威胁防御系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：
 - 接受 EULA
 - 新管理员密码
 - IPv4 或 IPv6 配置
 - IPv4 或 IPv6 DHCP 设置
 - 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
 - 系统名称
 - 默认网关
 - DNS 设置
 - HTTP 代理
 - 管理模式（需要进行本地管理）
4. 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。
5. 根据提示完成系统配置。
6. 当控制台返回到 **firepower #** 提示符时，确认设置是否成功。
7. 关闭 CLI：
 - > **exit**

后续操作

- 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 11 页）](#)。

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应正常工作，并已部署下列基本策略：

- 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。
- 在内部接口或桥接组上运行的 DHCP 服务器。

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

程序

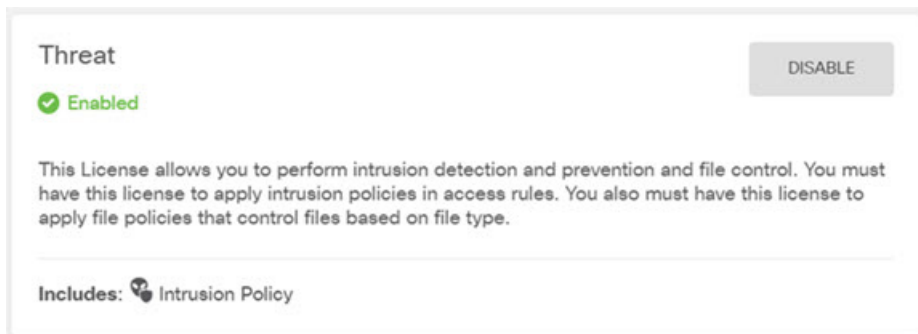
1. 选择**设备**，然后点击**智能许可证组**中的**查看配置**。

虚拟 Firepower 威胁防御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。

对于您想要使用的可选许可证（威胁、恶意软件、URL），点击**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。点击**申请注册**，并按照指示执行操作。请在评估版许可证到期前进行注册。

例如，如果启用了威胁许可证，则应显示如下内容：



2. 虚拟 Firepower 威胁防御的默认配置使您可以将管理、诊断和内部接口连接到虚拟交换机上的同一网络。选择**设备**，然后点击**接口组**中的**查看配置**，以配置其他接口。

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。

注意：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。

请注意，管理接口 IP 配置在**设备 > 系统设置 > 管理接口**中定义。它与**设备 > 接口 > 查看配置**中列出的 Management0/0（诊断）接口的 IP 地址不同。


点击每个接口的编辑图标 (ⓘ)，定义 IP 地址和其他设置。完成后点击**保存**。

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**。

如何在 Firepower 设备管理器中配置设备

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。



4. 如果要让内部客户端使用 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。点击 +，为每个内部接口配置服务器和地址池。

此外，您还可以在**配置**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。



5. 选择**设备**，然后点击**路由组**中的**查看配置**（或**创建第一个静态路由**），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。

注意：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。您可以在**设备 > 系统设置 > 管理接口**下设置管理网关。

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）。可以通过点击**网关**下拉菜单底部的**创建新网络**，来创建该对象。

Add Static Route

Protocol

IPv4 IPv6

Gateway

isp-gateway

Interface

outside

Metric

1

Networks

6. 选择策略，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。

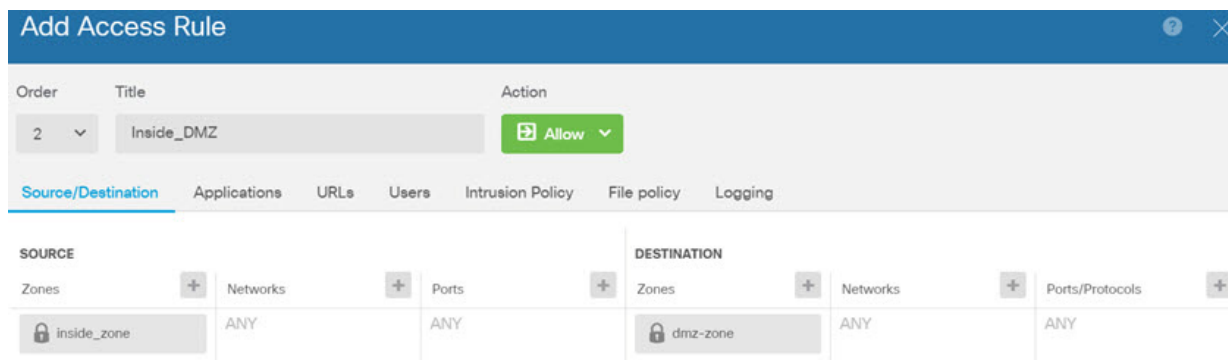
但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

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。
- **安全情报** - 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。通过使用情报源，您将无需编辑策略来添加或删除黑名单中的项目。
- **NAT**（网络地址转换）- 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。使用此策略可实施 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，除**日志记录**中的**在连接结束时**选项外，任何其他选项卡上均未设置任何选项。

如何在 Firepower 设备管理器中配置设备



7. 选择设备，然后单击更新组中的查看配置，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。

8. 单击菜单中的部署按钮，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。

后续操作

- 有关使用 Firepower 设备管理器管理 Firepower 威胁防御虚拟设备的完整信息，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》或 Firepower 设备管理器在线帮助。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1721R)

© 2018 年 Cisco Systems, Inc. 保留所有权利。