部署 Firepower Threat Defense Virtual

本章介绍将 Firepower Threat Defense Virtual 部署到 KVM 环境的程序。

使用 KVM 进行部署的前提条件

- 从 Cisco.com 下载 Firepower Threat Defense Virtual qcow2 文件并将其放在 Linux 主机上：

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

  注释 需要 Cisco.com 登录信息和思科服务合同。

- 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 Threat Defense Virtual 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。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 - 用于增加内存页面大小，在 Ubuntu 14.04 中默认开启。
  - 禁用超线程 - 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 - 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 Firepower Threat Defense Virtual 的兼容性》。

准备 Day 0 配置文件

在启动 FTDv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。

重要事项 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 FTDv设备的整个初始设置。可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。
- 管理模式；请参阅如何管理您的 Firepower 设备。

  您可以将**本地管理**设置为**是**，或者输入 Firepower 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。对于您未使用的管理模式，保留字段为空。
- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地 Firepower 设备管理器 (FDM) 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 FDM 配置透明防火墙模式接口。
- 使设备可以在管理网络上进行通信的网络设置。

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 8 页。

注释 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。

SUMMARY STEPS

1. 在名为“day0-config”的文本文件中输入 Firepower Threat Defense Virtual 的 CLI 配置。添加网络设置和关于管理 Firepower 管理中心的信息。
2. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：
3. 为每个要部署的 FTDv重复创建唯一的默认配置文件。

DETAILED STEPS

步骤 1 在名为“day0-config”的文本文件中输入 Firepower Threat Defense Virtual 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
{
    "EULA": "accept",
    "Hostname": "ftdv-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"

}
```

在 Day 0 配置文件的**本地管理**中输入**是**以使用本地 Firepower 设备管理器 (FDM)；输入 Firepower 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的值。对于您未使用的管理选项，将这些字段留空。

步骤 2 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

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

或

示例：

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

步骤 3 为每个要部署的 FTDv重复创建唯一的默认配置文件。

下一步做什么

- 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 Threat Defense Virtual

组织主题

-

使用部署脚本启动

使用基于 virt-install 的部署脚本启动 FTDv。

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。

每个 KVM 访客磁盘接口都可以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* 会绕过主机页面缓存。*unsafe* 可能会缓存所有内容，并忽略来自访客的刷新请求。

- 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。
- 从 6.4 版开始，FTDv 具有可调的 vCPU 和内存资源。在 6.4 版之前，FTDv 部署为固定配置 4vCPU/8GB 设备。请参阅下表，了解每个 FTDv 平台大小的 --vcpus 和 --ram 参数所支持的值。

表 *1: virt-install* 支持的 *vCPU* 和内存参数

--vcpus	--ram	FTDv 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

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

FTDv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。FTDv可支持多达 10 个网络接口。此示例使用了四个接口。虚拟 NIC 必须是 Virtio。

注释 FTDv 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. （可选）数据接口 - 最多 6 个

示例：

```
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=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --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
```

步骤 2 运行 virt_install 脚本：

示例：

```
/usr/bin/virt_install_ftdv.sh

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

此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。一旦虚拟机停止启动，您便可以从控制台屏幕发出 CLI 命令。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理**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**本地管理**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。

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FTDv。Virt-manager是用于创建和管理访客虚拟机的图形化工具。

步骤 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。

步骤 2 单击左上角的按钮，打开**新建虚拟机**向导。

步骤 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) 单击**继续**继续操作。

步骤 4 加载磁盘映像：

a) 单击**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) 单击**继续**继续操作。

步骤 5 配置内存和 CPU 选项：

从 6.4 版开始，FTDv 具有可调的 vCPU 和内存资源。在 6.4 版之前，FTDv 部署为固定配置 4vCPU/8GB 设备。请参阅下表，了解每个 FTDv 平台大小的 --vcpus 和 --ram 参数所支持的值。

表 *2:* 虚拟机管理器支持的 ***vCPU*** 和内存参数

CPU	内存	**FTDv** 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) 针对 FTDv 平台大小设置**内存 (RAM)** 参数。
b) 针对 FTDv 平台大小设置对应的 **CPU** 参数。
c) 单击**继续**继续操作。

步骤 6 选中**安装前自定义配置**复选框，然后单击**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。

步骤 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。

步骤 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*。

步骤 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) 单击**添加硬件**，添加一台串行设备。
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。

步骤 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) 单击**添加硬件**，添加一台看门狗设备。
b) 对于**型号**，选择默认值。
c) 对于**操作**，选择强制重置访客。

步骤 11 配置至少 4 个虚拟网络接口：

a) 单击**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。

注释 KVM 上的 FTDv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：

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）

重要事项 请确保将 vnic0、vnic1 和 vnic3 映射到同一子网。

步骤 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**。
b) 选择**存储**。
c) 单击**选择托管或其他现有存储**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，单击**应用**。

步骤 14 单击**开始安装**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理**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**本地管理**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。

在没有 Day 0 配置文件的情况下启动

由于 FTDv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。

按照设置提示操作时，如遇单选问题，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。

注释 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

开始之前

-

SUMMARY STEPS

1. 打开 FTDv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：
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：

DETAILED STEPS

	命令或操作	目的
步骤 1	打开 FTDv的控制台。	
步骤 2	在 **firepower login** 提示符下，使用默认凭据（**username** *admin*，**password** *Admin123*）登录。	
步骤 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）

	命令或操作	目的
步骤 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。	
步骤 5	根据提示完成系统配置。	
步骤 6	当控制台返回到 firepower # 提示符时，确认设置是否成功。	
步骤 7	关闭 CLI：	

下一步做什么

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。