Firepower Threat Defense Virtual 和 KVM 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。

本章介绍这些 FTDv 功能如何使用基于内核的虚拟机 (KVM) 虚拟机监控程序环境，包括功能支持、系统要求、指导原则和限制。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

关于使用 KVM 的 FTDv 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。

如何管理您的 Firepower 设备

您可以通过两种方法来管理您的 Firepower Threat Defense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 Threat Defense 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 Threat Defense 设备的大型网络。

注释 有关支持 FDM 的 Firepower Threat Defense 设备的列表，请参阅《适用于 Firepower 设备管理器的思科 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 Threat Defense 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。

系统要求

有关 Firepower Threat Defense Virtual 支持的虚拟机管理程序的最新信息，请参阅思科 Firepower 兼容性指南。

根据所需部署的实例数量和使用要求，Firepower Threat Defense Virtual部署所使用的具体硬件可能会有所不同。每个 FTDv 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

表 *1: FTDv* 设备资源要求

设置	值
核心和内存数	**6.4 及更高版本** FTDv 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种： • 4vCPU/8GB（默认） • 8vCPU/16GB • 12vCPU/24GB 注释 要更改 vCPU/内存值，必须先断开 FTDv 设备的电源。仅支持上述三种组合。
	6.3 及更低版本 FTDv 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个： • 4vCPU/8GB 注释 不允许调整 vCPU 和内存。
硬盘调配容量	• 50 GB • 可调节设置。支持 virtio 块设备
vNIC	KVM 上的 FTDv 支持以下虚拟网络适配器： • **VIRTIO** - Virtio 是 KVM 中 IO 虚拟化的主要平台，为 IO 虚拟化的虚拟机监控程序提供通用框架。主机实施是在用户空间 qemu 中，因此主机中不需要驱动程序。 • **IXGBE-VF** - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”。

网络准则和最佳实践

- 需要两个管理接口和两个数据接口来启动。

注释 FTDv 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 SR-IOV 的 ixgbe-vf 驱动程序。
- 支持共计 10 个接口

- FTDv 的默认配置假设您将管理接口（管理和诊断）和内部接口置于**同一子网**，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
- FTDv 首次启动时，必须启用至少四个接口。如果没有四个接口，您的系统将无法部署
- 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：
  - 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 FTDv接口的以下网络适配器、源网络和目标网络的对应关系：

表 *2:* 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*	Management0-0	Management0/0	管理
vnic1	Diagnostic0-0	Diagnostic0/0	Diagnostic
vnic2*	GigabitEthernet0-0	GigabitEthernet0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	内部
*重要信息。连接到同一子网。			

- 不支持克隆虚拟机。
- 对于控制台访问，通过 telnet 支持终端服务器。

CPU 模式

KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - 英特尔以太网服务器适配器 X710
  - Intel 以太网服务器适配器 X520 - DA2
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86_64 多核 CPU - Intel 沙桥或更高版本（推荐）。

  注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 FTDv 进行了测试。

- 核心
  - 每个 CPU 插槽至少 8 个物理核心
  - 8 个核心必须位于一个插槽中。

    注释 建议通过 CPU 固定来实现完整的吞吐量。

- 请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。对于 KVM，您可以验证 SR-IOV 支持方面的 CPU 兼容性。请注意，对于 KVM 上的 FTDv，我们仅支持 x86 硬件。