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。
  - 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。（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)。

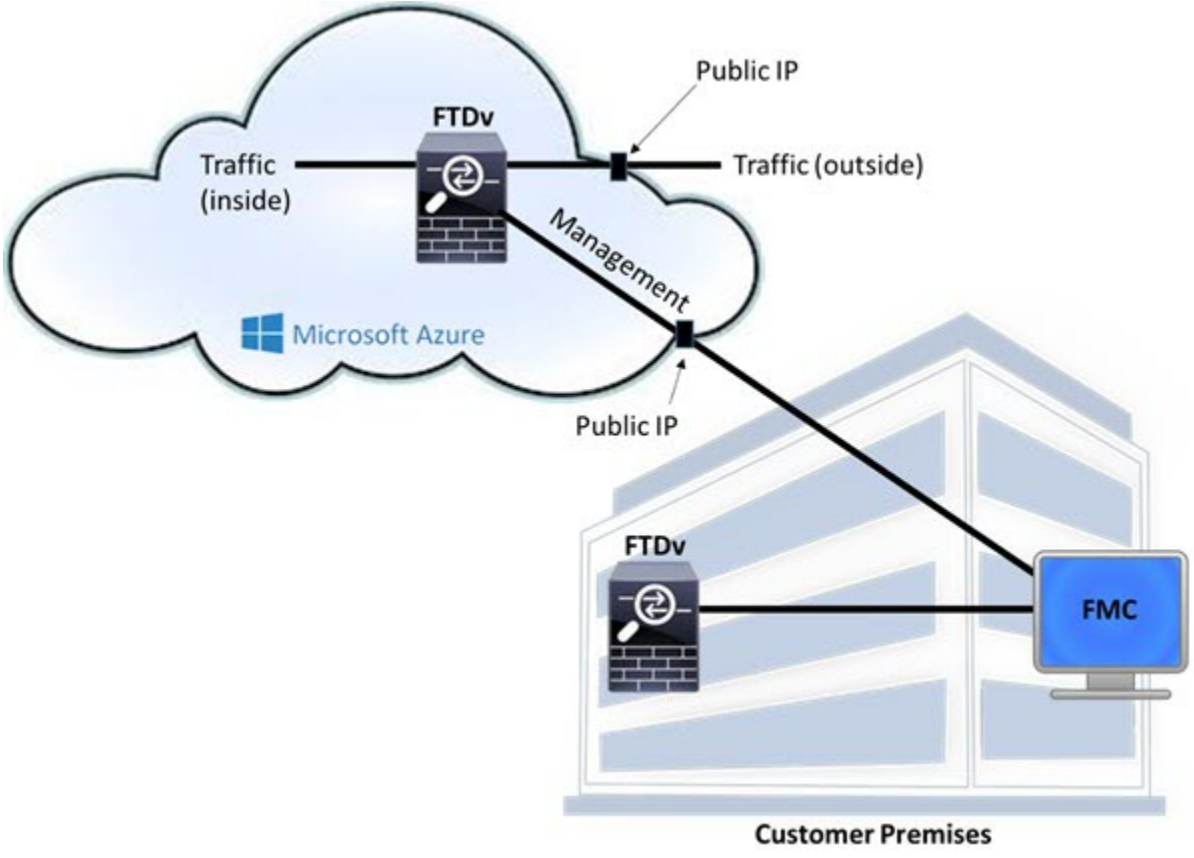
如果要管理大量设备或要使用 Firepower 威胁防御 支持的更复杂的功能和配置，请使用 FMC（而不是集成的 FDM）来配置您的设备。

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。