使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FDM 管理的独立式 FTDv 设备。要部署高可用性对，请参阅 FDM 配置指南。

关于使用 Firepower 设备管理器管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 设备管理器 (FDM) 管理 FTDv，这是部分 Firepower 威胁防御 型号中包含的基于 Web 的设备设置向导。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。

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 Firepower 管理中心（而不是集成的Firepower设备管理器）来配置您的设备。有关详细信息，请参阅使用Firepower管理中心管理 Firepower Threat Defense Virtual。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 Firepower CLI 连接到 FTD。

默认配置

FTDv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。

因此，默认配置的设计使您可以将 Management0-0 和 GigabitEthernet0-1（内部）两个接口都连接到虚拟交换机上的同一网络。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。

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。

FTDv 首次启动时，必须启用至少四个接口：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机上的第二个接口是诊断接口 (Diagnostic0-0)。
- 虚拟机的第三个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-1) 是内部接口。

您还可以添加最多六个额外的数据流量接口，使数据接口的总数达到八个。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。请参阅“配置 VMware 接口”。

初始配置

您必须完成初始配置，才能使 FTDv 在网络中正常运行，其中包括配置将安全设备插入网络以及将其连接到互联网或其他上游路由器所需的地址。您可以通过以下两种方式来进行系统初始配置：

- 使用 FDM Web 界面（推荐）。FDM 在您的网络浏览器中运行。使用该界面可配置、管理和监控系统。
- 使用命令行界面 (CLI) 设置向导（可选）。可以使用 CLI 设置向导（而不是 FDM）进行初始配置，并可以使用 CLI 执行故障排除。您仍然可以使用 FDM 来配置、管理和监控系统；请参阅（可选）“启动 Firepower 威胁防护 CLI 向导”。

以下主题介绍如何使用这些界面来执行系统初始配置。

启动 Firepower 设备管理器

在首次登录 Firepower 设备管理器 (FDM) 时，系统会通过设备设置向导指导您完成初始系统配置。

过程

步骤 1 打开浏览器并登录 FDM。假定您未在 CLI 中进行初始配置，请在 **https://***ip-address* 中打开 Firepower 设备管理器，其中地址为以下项之一：

- 如果您连接到内部桥组界面：**https://192.168.1.1**。
- 如果连接到管理物理接口，则地址为：**https://192.168.45.45**。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

步骤 3 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。只有完成这些步骤，才能继续。

步骤 4 为外部接口和管理接口配置以下选项，然后单击**下一步**。

注释 单击**下一步**后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。确保您的设置正确。

a) **Outside Interface** - 即连接到网关调制解调器或路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 (Configure IPv4) - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

b) **管理接口**

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请单击**使用 OpenDNS** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

注释 在使用设备设置向导配置 Firepower 威胁防御 设备时，系统会为出站和入站流量提供两个默认访问规则。您可以在完成初始配置后更改这些访问规则。

步骤 5 配置系统时间设置，然后单击**下一步**。

a) **时区** - 选择系统时区。

b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 6 为系统配置智能许可证。

只有具有智能许可证账户，才能获取和应用系统需要的许可证。最初，可以使用为期90天的评估许可证，以后再设置智能许可。

要立即注册设备，请单击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择 **Start 90 day evaluation period without registration**。如需稍后注册设备并获取智能许可证，请单击菜单中的设备名称打开 **Device Dashboard**，然后单击 **Smart Licenses** 组中的链接。

步骤 7 单击 **Finish**。

下一步做什么

- 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 4 页。

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 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。
- 在内部接口或网桥组上运行的 DHCP 服务器。

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

过程

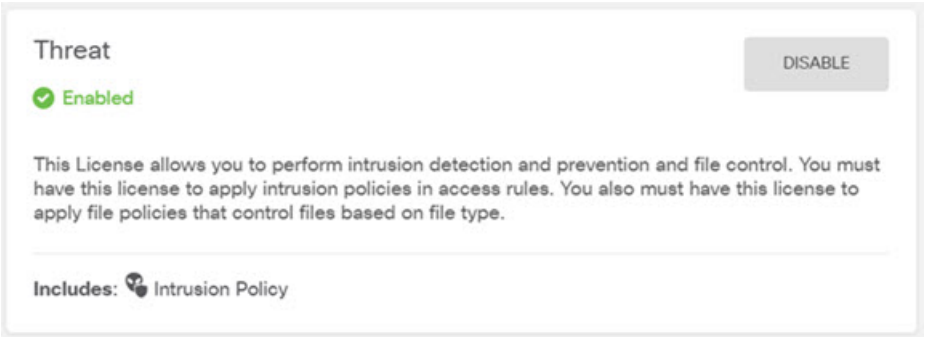
步骤 1 选择 **Device**，然后单击 **Smart License** 组中的 **View Configuration**。

对于您想要使用的可选许可证（威胁、恶意软件、URL），单击**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。单击**Request Register**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的威胁许可证：

图 *1:* 已启用的威胁许可证

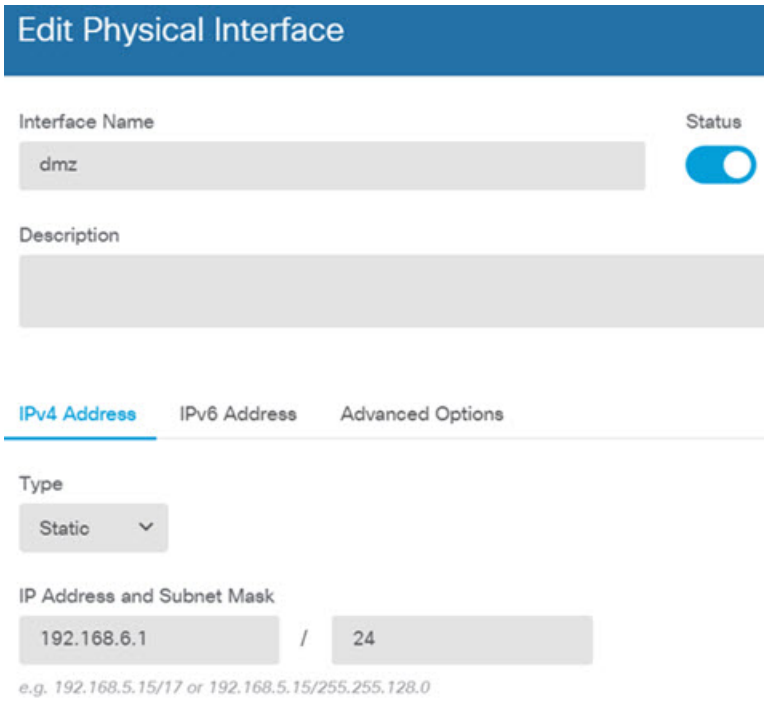


步骤 2 如果配置了其他接口，请选择**设备**，然后单击**接口**组中的**查看配置**并配置每个接口。

可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。单击每个接口的编辑图标 ( )，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后单击**保存**。

图 *2:* 编辑接口



步骤 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**。

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。

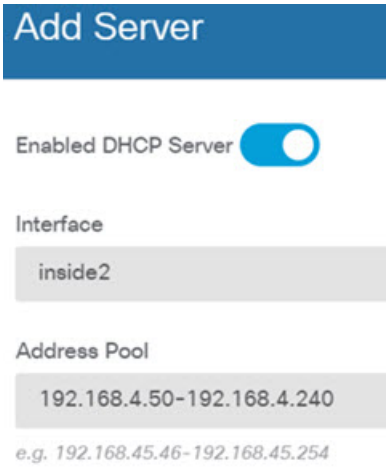
图 *3:* 安全区域对象

步骤 4 如果希望内部客户端使用 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。单击 +，为每个内部接口配置服务器和地址池。

此外，您也可以在 **Configuration** 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。

图 *4: DHCP* 服务器



步骤 5 选择 **Device**，然后单击 **Routing** 组中的 **View Configuration**（或 **Create First Static Route**），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。

注释　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。在**设备** > **系统设置** > **管理接口**上设置管理网关。

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

图 *5:* 默认路由

步骤 6 选择**策略**，并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。

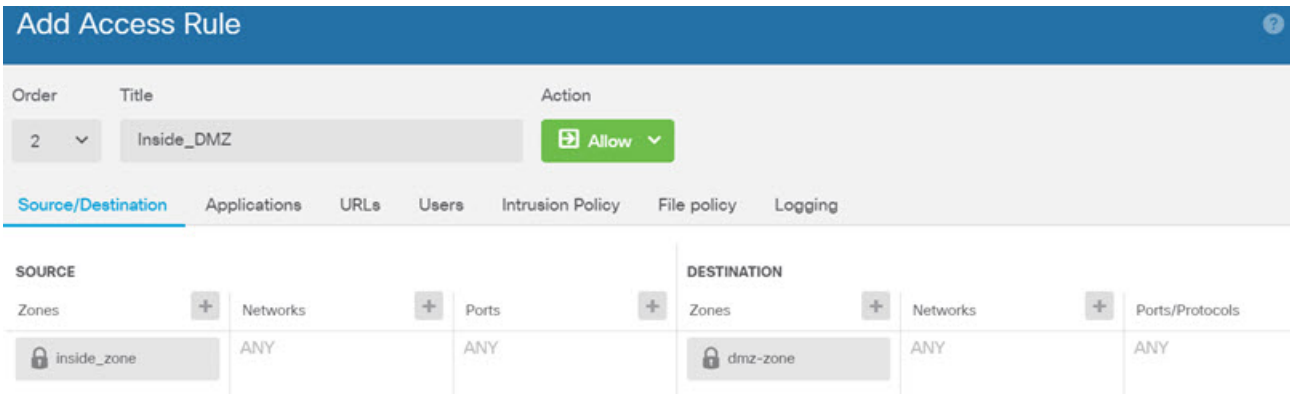
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **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。

- **Security Intelligence** - 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。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 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，任何其他选项卡上均未设置任何选项，**日志记录**除外，其中**在连接结束时**选项已被选中。

图 *6:* 访问控制策略



步骤 7 选择 **Device**，然后单击 **Updates** 组中的 **View Configuration**，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。

步骤 8 单击菜单中的 **Deploy** 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。

下一步做什么

有关使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual 的详细信息，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》或 Firepower 设备管理器联机帮助。