入门信息

以下主题介绍如何开始使用 防火墙设备管理器 配置 Firewall Threat Defense 设备。

本指南适用对象

本指南介绍如何使用 Firewall Threat Defense 设备自带的 防火墙设备管理器 基于 Web 的配置界面配置 Firewall Threat Defense。

防火墙设备管理器可以配置小型或中型网络最常用软件的基本功能。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Firewall Threat Defense设备的大型网络。

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 （而不是集成的 防火墙设备管理器）来配置您的设备。

防火墙设备管理器/Firewall Threat Defense 版本 10.5 新功能

下表列出了在使用 防火墙设备管理器进行配置时 Firewall Threat Defense 10.5 中可用的新功能：

表 *1:* 版本 *10.5* 新功能

功能	说明
硬件功能	
支持 Cisco Secure Firewall 220G、240GP 和 260GP。	您可使用 防火墙设备管理器 来配置 Cisco Secure Firewall 220G、240GP 和 260GP。
防火墙和 IPS 功能	
基于 TLS 的 TACACS+ 1.3。	您可将 TACACS+ 服务器配置为使用 TLS 1.3 加密的连接。 添加/编辑 TACACS+ 服务器对话框中新增了相关字段以支持此配置。在**对象** > **身份源**下配置 TACACS+。
VPN 功能	
支持站点间 VPN 的后量子密码学 (PQC) 算法和多重密钥交换。	您可以为站点间 VPN 配置多重密钥交换。通过使用多重密钥交换，结合 Diffie-Hellman、椭圆曲线 Diffie-Hellman 和后量子算法，您可以设置最低安全级别，同时使更高安全级别成为可能。初始密钥交换是 DH/ECDH 密码；后续交换可以包括 PQC 算法。您最多可以定义 7 个额外的后量子密钥交换。 我们添加了向 IKEv2 策略和 IKEv2 IPSec 方案对象添加最多 7 个额外后量子密钥交换的功能，以及添加 DH 模块格组（35、36、37）。您只能在站点间 VPN 中选择使用这些功能定义的对象；不能将它们用于远程访问 VPN。
管理功能	
DHCP 服务器支持 4096 个地址。	您可配置地址池上限为 4096 个的 DHCP 服务器（即 /20 掩码）。以前的限制是 255 个。 我们更新了**系统设置** > **DHCP 服务器**页面，以支持更大的地址范围。
NTPv4 身份验证	您可配置 NTP 服务器启用身份验证。NTPv4 身份验证使用加密密钥验证 NTP 服务器身份，确保时间同步数据来自可信源，并防止系统时钟被未授权篡改。您可使用 MD5、SHA-1、SHA-256、SHA-512 或 AES-128 CMAC。 我们新增了**对象** > **NTP 服务器**页面用于创建 NTP 服务器对象，并更新了**系统设置** > **时间服务**页面以使用这些对象。
防火墙设备管理器的多个本地管理账户。	此前仅有一个本地用户 admin 可登录 防火墙设备管理器。您现在可创建多个本地管理员账户，并为设备管理器分配相应的授权角色。这些账户会与 CLI 用户账户同步，因此在 防火墙设备管理器中创建的用户也可登录 CLI。 我们在**对象** > **用户**页面中新增了创建本地管理用户的功能。

功能	说明
查看 SSH 服务器配置的命令。	您可使用 **show ssh server-config** 命令查看 SSH 服务器的配置。该命令将显示已配置用于保护与防火墙 SSH 连接的密钥交换算法、加密密码及消息认证码。请使用设备管理器修改 SSH 设置。
弱配置警告。	若选择了安全性较弱的项（如 TLS 1.0 或弱加密密码），系统将向您发出警告。启用系统日志后，若发现存在更安全选项的弱配置，系统将每日发送 111012 消息。您可使用 **show weak-config** 命令列出具体问题，或验证所有潜在弱安全配置均已修复。
HTTP/2 Web 服务器支持。	本产品的 Web 服务器用于 防火墙设备管理器 和强制网络门户。这些 Web 服务器现已支持 HTTP/2。无需进行配置。若用户浏览器支持，系统将自动使用 HTTP/2；否则将回退至 HTTP/1.1。

防火墙设备管理器/Firewall Threat Defense 版本 10.1 中的新增功能

下表列出了在使用 防火墙设备管理器进行配置时 Firewall Threat Defense 10.1 中可用的新功能：

功能	说明
平台功能	
Cisco Secure Firewall 240P。	Cisco Secure Firewall 220 是一款经济实惠的安全设备，适用于分支机构和远程位置，兼顾了成本和功能。

防火墙设备管理器/Firewall Threat Defense 版本 10.0 中的新功能

发布日期：2025 年 12 月 3 日

下表列出了在使用 防火墙设备管理器进行配置时 Firewall Threat Defense 10.0 中可用的新功能：

功能	说明
硬件功能	
Cisco Secure Firewall 220。	Cisco Secure Firewall 220 是一款经济实惠的安全设备，适用于分支机构和远程位置，兼顾了成本和功能。
公共云和私有云	

功能	说明
Firewall Threat Defense Virtual适用于 Microsoft Hyper-V 的	Firewall Threat Defense Virtual 现在支持 Microsoft Hyper-V。
停止支持：VMware vSphere/VMware ESXi 6.5、6.7 和 7.0。	**升级影响。在升级软件之前请先升级 VMware**。 我们不再支持 VMware vSphere/VMware ESXi 6.5、6.7 和 7.0 上的虚拟部署。在升级任何虚拟设备之前，请将您的托管环境升级至版本 8.0。 版本限制：版本 7.3.x 和 7.4.1 未经 VMware 8.0 认证。如果您正在运行上述任一版本，请先升级至 VMware 8.0。请尽快进入下一步。为获得最佳效果，请执行多步骤升级：首先将虚拟设备升级至 7.4.2 – 7.7.x，接着升级 VMware，最后再次升级虚拟设备。
更大的默认磁盘大小以及部署后调整 Firewall Threat Defense Virtual 磁盘大小的能力。	虚拟防火墙的默认磁盘大小已更改。
防火墙和 IPS 功能	
能够限制用于设备管理器 Web 服务器和用于防火墙设备管理器主动身份验证身份规则的强制网络门户的密码套件。	您可以限制连接到防火墙设备管理器时或用户被身份规则提示进行主动身份验证时可以使用的密码套件。通过限制允许的密码套件，您可以实施比默认密码套件更强的安全要求。 我们在**系统设置** > **SSL 设置**页面添加了**防火墙设备管理器 Web 服务器**和**身份 Web 服务器**卡片。以前的 SSL 设置仅适用于远程访问 VPN 连接。
VPN 功能	
通过移除智能卡来断开远程访问 VPN 会话。	如果将智能卡用于 RA VPN 连接，您可以配置组策略，以便在移除智能卡时断开连接。升级时，所有组策略上默认启用此功能。您可以禁用此功能，以便在移除智能卡时不会断开连接。 我们在 RA VPN 组策略配置的会话设置中添加了**智能卡移除时断开连接**选项。
管理功能	

功能	说明
更新了安全智能源的互联网访问要求。	**升级影响。系统连接至新源。** 系统现在从与 URL 过滤数据相同的位置获取安全智能源： • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com 系统不再需要访问 intelligence.sourcefire.com。 有关互联网访问要求的更多信息，请参阅访问的互联网资源，第 32 页。
设备管理器 防火墙设备管理器 HTTPS 管理连接的 TACACS+ 服务器身份验证、授权和记账支持。	您可以配置防火墙设备管理器设备管理器使用 TACACS+ 服务器对设备管理器的 HTTPS 连接进行身份验证和授权防火墙设备管理器。您也可以为这些连接启用 TACACS+ 记账。 我们向身份源添加了 TACACS+ 服务器和服务器组对象，并更新了管理系统设置（**系统设置** > **管理访问**，**AAA 配置**选项卡）以允许选择 TACACS+ 服务器组。

默认配置

设备默认配置取决于是否已完成初始设置。

进行初始设置之前的默认配置

在使用本地管理器（防火墙设备管理器）对 Firewall Threat Defense 设备进行初始配置之前，设备包括以下默认配置。

对于许多型号，此配置假定您通过内部接口打开设备管理器，通常是将计算机直接插入接口，并使用内部接口上定义的 DHCP 服务器为计算机提供 IP 地址。或者，也可以将计算机插入管理接口，并通过 DHCP 获取地址。但是，某些型号具有不同的默认配置和管理要求。有关详细信息，请参阅下表。

注释 在使用向导执行设置操作之前，可以使用 CLI 设置（（可选）在 CLI 中更改管理网络设置，第 17 页）预配置其中的许多设置。

默认配置设置

设置	默认	是否可在初始配置期间更改？
管理员用户的密码。	Admin123 Firepower 4100/9300：部署逻辑设备时设置密码。 AWS：除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则默认值为 AWS 实例 ID。	是。必须更改默认密码。
管理 IP 地址。	通过 DHCP 获取。 Firewall Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300：部署逻辑设备时设置管理 IP 地址。	否。 Firepower 4100/9300：是。
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。此网关仅适用于关联设备流量。如果设备收到来自 DHCP 服务器的默认网关，则使用该网关。 Firepower 4100/9300：部署逻辑设备时设置网关 IP 地址。 ISA 3000：192.168.45.1。 Firewall Threat Defense Virtual：192.168.45.1	否。 Firepower 4100/9300：是。
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35。系统从不使用从 DHCP 获取的 DNS 服务器。 Firepower 4100/9300：部署逻辑设备时设置 DNS 服务器。	是
内部接口 IP 地址。	192.168.95.1/24 Firepower 4100/9300：未预配置数据接口。 ISA 3000：BVI1 IP 地址未预配置。BVI1 包括所有内部和外部接口。 Firewall Threat Defense Virtual: 192.168.45.1/24	否。

设置	默认	是否可在初始配置期间更改？
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.95.5 - 192.168.95.254。 Firepower 4100/9300：未启用 DHCP 服务器。 ISA 3000：未启用 DHCP 服务器。 Firewall Threat Defense Virtual：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	否。
内部客户端的DHCP自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	在外部接口上启用。	是的，但属于间接更改。如果为外部接口配置的是静态 IPv4 地址，则禁用 DHCP 服务器自动配置。
外部接口 IP 地址。	IPv4：通过 DHCP 从互联网服务提供商 (ISP) 或上游路由器获取。 IPv6：自动配置。 Firepower 4100/9300：未预配置数据接口。 ISA 3000：BVI1 IP 地址未预配置。BVI1 包括所有内部和外部接口。	是。

各个设备型号的默认接口

在初始配置期间不能选择不同的内部接口和外部接口。若要在配置后更改接口分配，请编辑接口和 DHCP 设置。您必须从网桥组中删除一个接口，然后才能将其配置为非交换接口。

设备型号	外部接口	内部接口
Cisco Secure Firewall 200	以太网接口 1/1	VLAN1（包括除外部接口外的所有其他交换机端口）是个物理防火墙接口。
Firepower 1010	以太网接口 1/1	VLAN1（包括除外部接口外的所有其他交换机端口）是个物理防火墙接口。
Firepower 1120、1140 和 1150	以太网接口 1/1	以太网接口 1/2
Cisco Secure Firewall 1210/1220	以太网接口 1/1	VLAN1（包括除外部接口外的所有其他交换机端口）是个物理防火墙接口。
Cisco Secure Firewall 1230/1240/1250	以太网接口 1/1	以太网接口 1/2
Cisco Secure Firewall 3100	以太网接口 1/1	以太网接口 1/2

设备型号	外部接口	内部接口
Firepower 4100	未预配置数据接口。	未预配置数据接口。
Firepower 9300	未预配置数据接口。	未预配置数据接口。
Firewall Threat Defense Virtual	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 和 GigabitEthernet1/3 GigabitEthernet1/1 (outside1) 和 1/2 (inside1) 以及 GigabitEthernet1/3 (outside2) 和 1/4 (inside2)（仅非光纤型号）配置为硬件旁路对。 所有内部和外部接口均是 BVI1 的一部分。	GigabitEthernet1/2 和 GigabitEthernet1/4

初始设置之后的配置

在完成安装向导后，设备配置将包括以下设置。下表显示某项特定设置是否为您显式选择的项目，或者它们是否基于您的其他选项而定义。请验证任何“隐式”配置，如果它们不符合您的需求，对其进行编辑。

注释 Firepower 4100/9300 和 ISA 3000 不支持设置向导。对于 Firepower 4100/9300，从机箱部署逻辑设备时即完成所有初始配置。对于 ISA 3000，在发货前应用特殊默认配置。

设置	配置	显式、隐式或默认配置
管理员用户的密码。	您输入的任何信息。	显式。
管理 IP 地址。	通过 DHCP 获取。 Firewall Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300：部署逻辑设备时设置的管理 IP 地址。	默认值。
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。管理网关仅适用于关联设备流量。如果设备收到来自 DHCP 服务器的默认网关，则使用该网关。 Firepower 4100/9300：部署逻辑设备时设置的网关 IP 地址。 ISA 3000：192.168.45.1 Firewall Threat Defense Virtual：192.168.45.1	默认值。

设置	配置	显式、隐式或默认配置
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35，或您输入的任何内容。系统从不使用从 DHCP 获取的 DNS 服务器。 Firepower 4100/9300：部署逻辑设备时设置的 DNS 服务器。	显式。
管理主机名。	**firepower** 或您输入的任何信息。 Firepower 4100/9300：部署逻辑设备时设置的主机名。	显式。
通过数据接口进行管理访问。	数据接口管理访问列表规则允许通过内部接口进行 HTTPS 访问。不允许 SSH 连接。允许 IPv4 和 IPv6 连接。 Firepower 4100/9300：任何数据接口均无默认管理访问规则。 ISA 3000：任何数据接口均无默认管理访问规则。 Firewall Threat Defense Virtual：任何数据接口均无默认管理访问规则。	隐式。
系统时间。	您所选的时区和 NTP 服务器。 Firepower 4100/9300：系统时间继承自机箱。 ISA 3000：思科 NTP 服务器：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。	显式。
智能许可证。	注册的基本许可证或激活的评估期，以您的选择为准。 未启用订阅许可证。如需启用它们，请转到智能许可页面。	显式。
内部接口 IP 地址。	192.168.95.1/24 Firepower 4100/9300：未预配置数据接口。 ISA 3000：无。必须手动设置 BVI1 IP 地址。 Firewall Threat Defense Virtual: 192.168.45.1/24	默认值。
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.95.5 - 192.168.95.254。 Firepower 4100/9300：未启用 DHCP 服务器。 ISA 3000：未启用 DHCP 服务器。 Firewall Threat Defense Virtual：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	默认值。
内部客户端的 DHCP 自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	如果使用 DHCP 来获取外部接口 IPv4 地址，则在外部接口上启用。 如果使用静态寻址，则禁用 DHCP 自动配置。	显式，但属于间接配置。

设置	配置	显式、隐式或默认配置
数据接口配置。	• 200/1010/1210/1220 — 外部接口 Ethernet1/1 为物理防火墙接口。所有其他接口均是已启用的交换机端口，且是内部接口 VLAN1 的一部分。可以将终端或交换机插入这些端口，并从内部接口的 DHCP 服务器获取地址。 • Firepower 4100/9300 — 所有数据接口均禁用。 • ISA 3000 - 所有数据接口均已启用，且是同一网桥组 BVI1 的一部分。GigabitEthernet1/1 和1/3 是外部接口，GigabitEthernet1/2 和1/4 都是内部接口。GigabitEthernet1/1 (outside1) 和 1/2 (inside1) 以及 GigabitEthernet1/3 (outside2) 和 1/4 (inside2)（仅非光纤型号）配置为硬件旁路对。 • 所有其他型号 - 外部和内部接口是唯一配置和启用的接口。所有其他数据接口均已禁用。	默认值。
外部物理接口和 IP 地址。	基于设备型号的默认外部端口。请参阅进行初始设置之前的默认配置，第 5 页。 通过 DHCP 和 IPv6 自动配置获取 IP 地址，或者是输入的静态地址 (IPv4、IPv6 或两者)。 Firepower 4100/9300：未预配置数据接口。 ISA 3000：无。必须手动设置 BVI1 IP 地址。	接口是默认值。 寻址是显式值。
静态路由。	如果为外部接口配置的是静态 IPv4 或 IPv6 地址，则会为 IPv4/IPv6 配置相应的静态默认路由，指向您为该地址类型定义的网关。如果选择 DHCP，则从 DHCP 服务器获取默认路由。 另外，也会为网关和“任何”地址创建网络对象，即为 IPv4 创建 0.0.0.0/0，为 IPv6 创建 ::/0。	隐式。
安全区。	**inside_zone**，包含内部接口。对于 Firepower 4100/9300，需手动将接口添加至此安全区。 **outside_zone**，包含外部接口。对于 Firepower 4100/9300，您需要手动将接口添加至此区域。 （您可以编辑这些区域以添加其他接口，也可以自己创建区域）。	隐式。

设置	配置	显式、隐式或默认配置
访问控制策略。	信任从 inside_zone 到 outside_zone 之间所有流量的规则。此规则允许用户的所有流量从网络内部传至外部，并允许这些连接返回所有流量，无需进行检查。 对于任何其他流量，默认操作是阻止。这样可防止外部发起的任何流量进入网络。 Firepower 4100/9300：无预配置访问规则。 ISA 3000：信任从 inside_zone 到 outside_zone 的所有流量的规则，以及信任从 outside_zone 到 inside_zone 的所有流量的规则。流量受阻止。设备还具有信任 inside_zone 和 outside_zone 中的接口之间所有流量的规则。这使得无需检查内部用户和外部用户之间的所有流量。	隐式。
NAT	接口动态 PAT 规则可将发往外部接口的任何 IPv4 流量的源地址转换为外部接口 IP 地址上的唯一端口。 还有一些隐藏的 PAT 规则，允许通过内部接口进行 HTTPS 访问，并通过管理地址的数据接口进行路由。这些不会显示在 NAT 表中，但如果您在 CLI 中使用 **show nat** 命令，就会看到它们。 Firepower 4100/9300：未预配置 NAT。 ISA 3000：未预配置 NAT。	隐式。

登录系统

Firewall Threat Defense设备有两个界面：

防火墙设备管理器 网络接口

防火墙设备管理器 在 Web 浏览器中运行。使用该界面可配置、管理和监控系统。

命令行界面（CLI、控制台）

可以使用 CLI 进行故障排除。您也可以将其用于初始设置，而不是 防火墙设备管理器。

以下主题介绍如何登录这些界面和管理您的用户账户。

用户角色决定用户的访问及操作权限

用户名分配了角色，而角色决定用户能够在 防火墙设备管理器中查看哪些内容，或执行哪些操作。本地定义的 **admin** 用户拥有所有权限，但如果使用不同的账户登录，享有的权限可能会减少。

防火墙设备管理器 窗口的右上角将显示您的用户名和权限级别。

权限：

- **管理员** - 可以查看和使用所有功能。
- **读写用户**-可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止其他 防火墙设备管理器 用户的会话。
- **只读用户** - 可以查看控制面板和配置，但不能进行任何更改。如果尝试进行更改，错误消息会解释由于缺乏权限出错。
- **加密管理员** - 您可以配置与加密相关的功能（例如证书、解密策略和密钥）。对其他功能的只读权限。
- **审核管理员** - 您可以查看用户登录历史记录和审计日志并执行审核相关操作。对配置功能的只读权限。

这些权限与 CLI 用户可享受的权限不相关。

登录至防火墙设备管理器

防火墙设备管理器可用于配置、管理和监控系统。配置功能可通过浏览器实现，但无法通过命令行界面 (CLI) 执行，即：必须使用 Web 界面实施安全策略。

使用以下浏览器的最新版本：Firefox、Chrome、Safari、Edge。

注释 如果输入错误的密码且连续 3 次尝试登录失败，账户将锁定 5 分钟。必须待锁定时间结束后方可尝试重新登录。

开始之前

最初，您只能使用 **管理员** 用户名登录 防火墙设备管理器 。但是，您可以稍后为外部 AAA 服务器中定义的其他用户配置授权，如管理防火墙设备管理器和Firewall Threat Defense用户访问中所述。

一次最多可以有 5 个活动登录用户。这包括登录到设备管理器和活动 API 会话（以未过期的 API 令牌表示）的用户。如果超过此限制，则最早的会话（设备管理器登录或 API 令牌）将过期以允许建立新会话。这些限制不适用于 SSH 会话。

过程

步骤 1 使用浏览器打开系统主页，例如 https://ftd.example.com。

您可以使用以下地址中的任何一个。如果配置了 Ipv4 或 IPv6 地址或 DNS 名称，则可以直接使用。

- 管理地址。默认情况下（大多数平台），管理接口为 DHCP 客户端，具体 IP 地址取决于您的 DHCP 服务器。
- 您为 HTTPS 访问打开的数据接口的地址。默认情况下（大多数平台），“内部”接口允许 HTTPS 访问，因此可连接至默认内部地址 192.168.95.1。有关适用于您型号的内部 IP 地址的详细信息，请参阅进行初始设置之前的默认配置，第 5 页。

  如果更改了 HTTPS 数据端口，则必须在 URL 中包含该自定义端口。例如，如果您已将端口更改为 4443，则 URL 应为：https://ftd.example.com:4443

提示

如果浏览器未配置为识别服务器证书，系统会显示一条有关证书不受信任的警告。将证书作为一种例外接受，或者将证书放到受信任的根证书存储库中。

步骤 2 如果登录屏幕包含警告或免责声明等文字，请阅读相关信息，然后选中复选框以确认同意。

步骤 3 （仅限本地用户和 RADIUS。）输入为设备定义的用户名和密码，然后点击 **登录**。

您可以使用“**admin**”用户名，这是预定义的用户。默认管理员密码为 Admin123。在 AWS 上，除非您在初始部署期间通过用户数据（**高级详细信息** > **用户数据**）定义了默认密码，否则默认管理员密码为 AWS 实例 ID。

如果会话连续30分钟处于非活动状态，就会过期，系统将提示您重新登录。从页面右上角的用户图标下拉菜单中选择**注销 (Log Out)**。

步骤 4 （仅限 SAML 服务器。）点击 **登录** 按钮旁边的 **单点登录 (SSO)** 链接。

这会将您引导至 SAML 服务器进行登录。请勿输入凭证，只需点击链接即可。如果输入本地凭证并点击登录，则会使用本地数据库登录。

在 SAML 服务器的登录页面上，像往常一样登录。如果您使用通用访问卡 (CAC) 登录，请点击链接以使用证书登录。设备管理器不直接处理 CAC 身份验证。

登录命令行界面 (CLI)

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。

要登录到 CLI，请执行以下一项操作：

- 使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特率、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。

注释 在 Firepower 和 Cisco Secure Firewall 设备型号上，控制台端口上的 CLI 是 Cisco Secure Firewall 可扩展操作系统 (FXOS)。对于某些设备型号，您可以使用 **connect ftd** 命令进入 Firewall Threat Defense CLI。对于 Firepower 4100/9300，请参阅连接到应用控制台。仅将 FXOS CLI 用于机箱级故障排除。使用 Firewall Threat Defense CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

- 对于 Firewall Threat Defense Virtual，请打开虚拟控制台。
- 使用 SSH 客户端连接到管理 IP 地址。如果您为 SSH 连接打开某个数据接口，也可以连接到该接口上的地址（请参阅配置管理访问列表）。默认情况下，禁用 SSH 数据接口访问。使用 **admin** 用户名或其他 CLI 用户账户登录。默认管理员密码为 Admin123。在 AWS 上，除非您在初始部署期间使用用户数据（**(高级详细信息 > 用户数据**）定义默认密码，否则 Firewall Threat Defense Virtual 的默认管理员密码为 AWS 实例 ID。

提示

- 如果管理员在登录过程中添加了文本（例如警告或免责声明），您需要确认您已阅读并同意该声明。
- 登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html 中的Cisco Firepower Threat Defense 命令参考。
- 您可以使用 **configure user add** 命令创建可登录 CLI 的本地用户账户。但这些用户只能登录 CLI，他们无法登录防火墙设备管理器 Web 界面。
- 您可以在外部服务器中创建可访问 SSH 的用户账户。有关配置 SSH 访问外部身份验证的信息，请参阅配置 Firewall Threat Defense CLI (SSH) 用户外部授权 (AAA)。

更改密码

密码应定期更改。以下步骤程序介绍了登录到 防火墙设备管理器时如何更改密码。

注释 如果已登录到 CLI，可使用 **configure password** 命令更改密码。您可以使用 **configure user password** *username* 命令为不同的 CLI 用户更改密码。

开始之前

此步骤仅适用于本地用户。如果用户账户是在外部 AAA 服务器上定义的，必须通过该服务器更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。

步骤 2 点击**密码**选项卡。

步骤 3 输入您当前的密码。

步骤 4 输入新密码，然后进行确认。

您可以点击**生成**，为您生成随机的 16 个字符密码。点击“显示密码”() 按钮可查看无掩蔽的密码。然后，点击**复制到剪贴板**链接，以便将密码粘贴到确认字段中。

该页面包括密码的最低要求。您无法更改这些最低要求。密码必须：

- 介于 8 至 128 个字符之间
- 至少有一个小写和一个大写字母
- 至少有一个数字
- 至少有一个特殊字符
- 不包含重复的字母

步骤 5 点击**更改**。

设置用户配置文件首选项

您可以设置用户界面的首选项并更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。

步骤 2 在**配置文件**选项卡中配置以下选项，然后点击**保存**。

- **安排任务的时区** - 选择安排备份和更新等任务要使用的时区。如果此处设置了不同的时区，将对控制面板和事件使用浏览器时区。
- **颜色主题** - 选择用户界面中要使用的颜色主题。

步骤 3 在**密码**选项卡中，可以输入新密码并点击**更改**。

查看英语之外语言的页面

您可以查看以下语言的 GUI 和联机帮助。

- 加拿大法语
- 中文
- 英语（默认）
- 日语
- 韩语

要使用这些语言，您必须在浏览器设置中选择该语言。产品本身没有语言设置。

如果您的浏览器不支持特定语言，则产品不会以该语言显示。例如，仅当您将浏览器配置为使用加拿大法语时，才会显示法语版本。选择其他类型的法语会使产品显示英语。

设置系统

只有完成初始配置，系统才能在网络中正常运行。成功部署包括正确连接电缆和配置将设备插入网络所需的地址，以及将设备连接到互联网或其他上游路由器。以下程序介绍了相关过程。

开始之前

在开始初始设置之前，设备中包括了一些默认设置。有关详细信息，请参阅进行初始设置之前的默认配置，第 5 页。

过程

步骤 1 连接接口，第 16 页

步骤 2 使用设置向导完成初始配置，第 18 页

有关生成的配置的详细信息，请参阅初始设置之后的配置，第 8 页。

连接接口

默认配置假定某些接口用于内部和外部网络。如果基于上述预期将网线连接至接口，初始配置将变得更易于完成。

大多数型号的默认配置旨在让您将管理计算机连接至内部接口。或者，您也可以直接将工作站连接到管理端口。接口位于不同的网络上，因此不要尝试将任何内部接口和管理端口连接到同一网络。

不要将任何内部接口连接至存在活动 DHCP 服务器的网络。这将与已在内部接口上运行的 DHCP 服务器冲突。如果要为网络使用不同的 DHCP 服务器，请在初始设置后禁用不需要的 DHCP 服务器。

有关接线图，请参阅您型号的入门指南。

（可选）在 CLI 中更改管理网络设置

如果您无法使用默认管理 IP 地址，可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。您只能配置管理接口设置；而无法配置内部或外部接口，稍后可在 GUI 中配置它们。

注释 Firepower 4100/9300 无需使用此流程，因部署时已手动设置 IP 地址。

注释 除非清除配置，否则无法重复 CLI 设置脚本（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 *Cisco Secure Firewall Threat Defense 命令参考*。

过程

步骤 1 连接到 Firewall Threat Defense 控制台端口。有关详细信息，请参阅登录命令行界面 (CLI)，第 13 页。

步骤 2 使用用户名 **admin** 登录。

默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（(**高级详细信息** > **用户数据**）定义默认密码，否则 Firewall Threat Defense Virtual 的默认管理员密码为 AWS 实例 ID。

步骤 3 首次登录 Firewall Threat Defense 时，系统会提示您接受“最终用户许可协议” (EULA) 并 更改管理员密码。然后，系统将显示 CLI 设置脚本。

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。

请参阅以下准则：

- **输入管理接口的 IPv4 默认网关** - 如果您设置手动 IP 地址，则可以输入网关路由器的**数据接口**或 IP 地址。**data-interfaces** 设置将通过背板发送出站管理流量，以退出数据接口。如果您没有可以访问互联网的单独管理网络，则此设置非常有用。源自管理接口的流量包括需要访问互联网的许可证注册和数据库更新。如果您使用 **data-interfaces**，在直接连接到管理网络的情况下，您仍可以在管理接口上使用 防火墙设备管理器（或SSH）但是，要对特定网络或主机进行远程管理，则应该使用 **configure network static-routes** 命令添加静态路由。请注意，数据接口上的

防火墙设备管理器 管理不受此设置的影响。如果使用 DHCP，则系统使用 DHCP 提供的网关，如果 DHCP 不提供网关，则使用**数据接口**作为回退方法。

- **如果网络信息已更改则需要重新连接** - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **在本地管理设备？** - 输入**是** 以使用 防火墙设备管理器。回答**否**表示您打算使用本地部署或云端交付来管理设备。

示例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

步骤 4 在新的管理 IP 地址上登录防火墙设备管理器 。

使用设置向导完成初始配置

在首次登录防火墙设备管理器时，系统会通过设备设置向导指导您完成初始系统配置。

如果您计划在高可用性配置中使用设备，请阅读准备两台用于高可用性的设备。

注释 Firepower 4100/9300 和 ISA 3000 不支持设置向导，因此本流程不适用于这些型号。对于 Firepower 4100/9300，从机箱部署逻辑设备时即完成所有初始配置。对于 ISA 3000，在发货前应用特殊默认配置。

开始之前

确保将数据接口连接到网关设备（例如电缆调制解调器或路由器）。对于边缘部署，网关设备可能是面向互联网的网关。对于数据中心部署，可能是主干路由器。使用您的设备型号的默认“外部”接口（请参阅连接接口，第 16 页和进行初始设置之前的默认配置，第 5 页）。

然后，将管理计算机连接到适用于您的硬件型号的“内部”接口。或者，可以连接到管理接口。对于 Firewall Threat Defense Virtual，只需确保能连接至管理 IP 地址。

（Firewall Threat Defense Virtual 除外，该型号需从管理 IP 地址连接互联网。）管理接口不需要连接到网络。默认情况下，系统通过连接到互联网的数据接口（通常为外部接口），获取系统许可授权和数据库以及其他更新。如果想使用单独的管理网络，则可以在完成初始设置后，将管理接口连接到网络并配置单独的管理网关。

要在无法访问默认 IP 地址的情况下更改管理接口网络设置，请参阅（可选）在 CLI 中更改管理网络设置，第 17 页。

过程

步骤 1 登录防火墙设备管理器。

a) 假定您未在 CLI 中进行初始配置，请在 **https://***ip-address*中打开 防火墙设备管理器，其中地址为以下项之一。

- 如果连接到内部接口，则地址为：**https://192.168.95.1**。
- (Firewall Threat Defense Virtual) 若连接至管理物理接口，地址为：**https://192.168.45.45**。
- （所有其他型号）如果您已连接到管理接口： **https://***dhcp_client_ip*

b) 使用用户名 **admin** 登录。默认管理员密码为 Admin123。在 AWS上，除非您在初始部署期间使用用户数据（**高级详细信息** > **用户数据**）定义默认密码，否则 Firewall Threat Defense Virtual 的默认管理员密码为 AWS 实例 ID。

步骤 2 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 3 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

注意
点击**下一步 (Next)** 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。请确保您的设置准确无误。

外部接口

- **配置 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。不管是通过静态方式还是通过 DHCP，都不要在与默认内部地址相同的子网上配置 IP 地址（请参阅进行初始设置之前的默认配置，第 5 页）。您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他

连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。请参阅配置物理接口。

- **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。

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 服务器或您从 DHCP 服务器获取的 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。您的 ISP 可能会要求您使用特定的 DNS 服务器。如果您在完成向导后发现无法进行 DNS 解析，请参阅为管理接口排除 DNS 故障。
- **防火墙主机名** - 系统管理地址的主机名。

步骤 4 配置系统时间设置，然后点击**下一步 (Next)**。

- **时区** - 选择系统时区。
- **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 5 为系统配置智能许可证。

只有具有智能许可证帐户，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，请选择注册设备的选项，点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。还必须选择服务区域，并决定是否将使用数据发送至 Cisco Success Network。屏幕上的文本更详细地解释了这些设置。

如果您还不想注册设备，请选择评估模式选项。评估期长达90天。若要在之后注册设备并获取智能许可证，请点击**设备**，然后点击**智能许可证**组中的链接。

步骤 6 点击**完成 (Finish)**。

下一步做什么

- 如果要使用可选许可证涵盖的功能（例如基于类别的URL过滤、入侵检测或恶意软件防御），请启用所需的许可证。请参阅启用或禁用可选许可证。
- 将其他数据接口连接到不同的网络并配置这些接口。有关配置接口的信息，请参阅如何添加子网和接口。
- 如果通过内部接口管理设备，并且想通过内部接口打开 CLI 会话，请打开用于 SSH 连接的内部接口。请参阅配置管理访问列表。
- 查看使用案例以了解如何使用产品。请参阅最佳实践： Firewall Threat Defense的使用案例。

如果未获取外部接口的 IP 地址该怎么办

默认设备配置包括一个用于内部接口的静态 Ipv4 地址。此时无法通过初始设备设置向导更改该地址，但随后可以进行更改。

默认的内部 IP 地址可能与连接到设备的其他网络冲突。如果在外部接口上使用 DHCP 从互联网服务提供商 (ISP) 处获取地址，尤其如此。有些 ISP 使用与内部网络相同的子网作为地址池。由于两个数据接口不能使用位于同一子网上的地址，因此无法在外部接口上配置来自 ISP 的冲突地址。

如果内部静态 IP 地址与外部接口上 DHCP 提供的地址存在冲突，则连接图应将外部接口显示为管理 UP，但没有 IPv4 地址。

在这种情况下，设置向导将会成功完成，并且系统将配置所有默认 NAT、访问以及其他策略和设置。只需按照下列程序消除冲突即可。

开始之前

验证ISP连接是否正常。尽管子网冲突会阻碍您获取外部接口上的地址，但如果根本没有连接ISP，也将无法获取地址。

过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

步骤 2 将鼠标悬停在内部接口中的**操作**列中，然后点击编辑图标 ( )。

步骤 3 在 **IPv4 地址**选项卡中，输入唯一子网上的静态地址，例如 192.168.2.1/24 或 192.168.46.1/24。请注意，默认管理地址是 192.168.45.45/24，因此不使用该子网。

如果已有 DHCP 服务器在内部网络上运行，那么您还可以选择使用 DHCP。但是，首先必须在**为此接口定义 DHCP 服务器**组中点击**删除**，从接口中删除 DHCP 服务器。

步骤 4 在**为此接口定义 DHCP 服务器**区域中，点击**编辑**并将 DHCP 池更改为新子网上的某个范围（例如 192.168.2.5-192.168.2.254）。

步骤 5 点击**确定**，保存接口更改。

步骤 6 点击菜单中的**部署**按钮以部署更改。

步骤 7 点击**立即部署**。

部署完成后，连接图应显示外部接口此时已有一个 IP 地址。使用内部网络中的客户端验证是否已连接到互联网或其他上游网络。

配置基本方法

以下主题介绍配置设备的基本方法。

配置设备

首次登录 防火墙设备管理器时，系统将通过安装向导来帮助您配置基本设置。完成该向导后，请使用以下方法来配置其他功能和管理设备配置。

如果难以从视觉上区分项目，请在用户配置文件中选择不同的配色方案。从页面右上角的用户图标下拉菜单中选择**配置文件 (Profile)**。

过程

步骤 1 点击**设备**进入**设备摘要**。

该控制面板直观地显示了设备的状态，包括所启用的接口以及关键设置（绿色）已配置或还需继续配置。有关详细信息，请参阅查看接口状态和管理状态，第 27 页。

状态图像的上方是设备型号、软件版本、VDB（系统和漏洞数据库）版本及入侵规则最后更新时间的摘要。此区域还显示高可用性状态，包括配置该功能的链接；请参阅高可用性（故障转移）。它还显示云注册状态，如果您使用云管理，则可以看到设备注册使用的账户；请参阅配置云服务。

图像下方是您可以配置的各种功能分组、每组的配置摘要以及管理系统配置可执行的操作。

步骤 2 点击每组中的链接可配置设置或执行操作。

下面是各组的摘要：

- **接口** - 除了管理接口外，至少应配置两个数据接口。请参阅接口。
- **路由** - 路由配置。必须定义默认路由。根据您的配置，也可能需要其他路由。请参阅路由。
- **更新**—地理位置、入侵规则和漏洞数据库更新，以及系统软件升级。如果使用这些功能，请设置定期更新计划，以确保您拥有最新的数据库更新。另外，如需在执行定期计划更新之前下载更新，也可以访问此页面。请参阅更新系统数据库和源。
- **系统设置** - 此组包括多种设置。有些设置是在初始设置设备时配置的基本设置，很少更改。请参阅系统设置。
- **智能许可证** - 显示系统许可证的当前状态。必须安装适当的许可证，才能使用该系统。某些功能需要额外的许可证。请参阅为系统授权许可。
- **备份和恢复** - 备份系统配置或恢复先前的备份。请参阅备份和恢复系统。
- **故障排除** - 应思科技术支持中心的要求生成故障排除文件。请参阅创建故障排除文件。

- **站点间 VPN** - 本设备与远程设备之间的站点间虚拟专用网络 (VPN) 连接。请参阅管理站点间 VPN。
- **远程访问 VPN** - 允许外部客户端连接到内部网络的远程访问虚拟专用网 (VPN) 配置。请参阅配置远程访问 VPN。
- **高级配置** - 使用 FlexConfig 和 Smart CLI 配置使用 防火墙设备管理器无法配置的功能。请参阅高级配置。
- **设备管理** - 查看审核日志或导出配置副本。请参阅审核与变更管理。

步骤 3 点击菜单中的**部署**按钮以部署更改。

只有将更改部署至设备，更改才会生效。请参阅部署更改，第 24 页。

下一步做什么

在主菜单中点击**策略**，并为系统配置安全策略。另外，也可以点击**对象**配置这些策略中所需的对象。

配置安全策略

使用安全策略实施组织可接受的使用策略并保护网络免受入侵或其他威胁。

过程

步骤 1 点击**策略 (Policies)**。

“安全策略”(Security Policies) 页面显示通过系统实现连接的常规流程以及安全策略的应用顺序。

步骤 2 点击策略的名称并对其进行配置。

虽然必须始终拥有访问控制策略，但可能不需要配置每个策略类型。以下是策略摘要：

- **SSL 解密 (SSL Decryption)** - 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。请参阅配置 SSL 解密策略。
- **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。请参阅配置身份策略。
- **安全智能** - 使用安全智能策略快速丢弃进出选定 IP 地址或 URL 的连接。阻止已知恶意站点后，在访问控制策略中便无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全智能阻止列表实现动态更新。使用智能源，无需通过编辑策略来添加或删除阻止列表中的项目。请参阅配置安全智能。

- **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。请参阅配置 NAT。
- **访问控制 (Access Control)** - 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。请参阅配置访问控制策略。
- **入侵 (Intrusion)** - 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。请参阅入侵策略。

步骤 3 点击菜单中的**部署**按钮以部署更改。

只有将更改部署至设备，更改才会生效。请参阅部署更改，第 24 页。

搜索规则或对象

您可以在策略规则或对象列表中使用全文本搜索，帮助您找到要编辑的项目。当策略中包含成百上千条规则或数目繁多的对象时，此功能尤为有用。

在任何类型的策略（除入侵策略外）或对象中搜索规则和对象的方法都是相同的：在**搜索**字段中，输入要查找的字符串，然后按 Enter。

此字符串可以位于规则或对象的任何部分，且可以是部分字符串。您可以使用星号 * 作为通配符，匹配零个或多个字符。请勿输入以下字符，因为搜索字符串不支持这些字符：?~!{}<>:%。以下字符将被忽略：;#&。

字符串可以出现在组中的对象内。例如，可以输入 IP 地址并找到具体指定该地址的网络对象或组。

完成后，点击搜索框右侧的 **x** 清空过滤器。

部署更改

在更新策略或设置时，更改不会立即应用到设备中。更改配置的过程分为两步：

1. 进行更改。
2. 部署更改。

通过此过程，您可以执行一组相关的更改，而不必在进行“部分配置”的情况下运行设备。在大多数情况下，仅会部署您做出的更改。但是，如有必要，系统将重新应用整个配置，这可能会造成您的网络中断。此外，有些更改需要重新启动检测引擎，在重启过程中会丢弃流量。因此，当系统中断带来的影响很小时，可以考虑部署更改。

注释 如果部署作业失败，则系统必须回滚对先前配置的任何部分更改。回滚进程包括清除数据平面配置和重新部署以前的版本。这将中断流量，直至回滚进程完成。

完成要进行的更改后，请按照以下程序将它们部署到设备中。

注意 如果检测引擎由于软件资源问题而处于繁忙状态，或由于某个配置要求引擎在配置部署期间重新启动而出现故障， Firewall Threat Defense 设备将丢弃流量。有关需要重新启动的更改的详细信息，请参阅引发检测引擎重启的配置更改，第 26 页。

过程

步骤 1 点击网页右上角的**部署更改 (Deploy Changes)** 图标。

若有未部署的更改，系统会用圆点高亮显示。

“待处理更改”窗口显示配置的部署版本与待处理更改之间的对比信息。这些更改进行了颜色编码，表示出删除、添加或编辑的元素。有关每种颜色的解释，请参阅窗口中的说明。

如果部署要求重新启动检测引擎，则该页面包含一条消息，其中提供要求重新启动的更改的详细信息。如果此时无法接受瞬时流量丢失，请关闭该对话框，等待更好的更改部署时机。

如果图标未高亮显示，仍可以点击图标查看上一个成功部署作业的日期和时间。窗口中还包含显示部署历史记录的链接，点击此链接可访问已经过过滤仅显示部署作业的审核页面。

步骤 2 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。

窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。如果您在部署过程中关闭窗口，作业不会停止。您可以在任务列表或审核日志中查看结果。如果将窗口保持打开状态，请点击**部署历史记录 (Deployment History)** 链接查看结果。

或者，您现在可以执行以下操作：

- **为作业命名 (Name the Job)** - 要对部署作业命名，请点击**立即部署 (Deploy Now)** 按钮上的下拉箭头，然后选择**为部署作业命名 (Name the Deployment Job)**。输入一个名称，然后点击**部署 (Deploy)**。名称将会连同作业一块显示在审核和部署历史记录中，更便于您查找作业。

  例如，如果将作业命名为“DMZ Interface Configuration”，成功的部署将被命名为“Deployment Completed: DMZ Interface Configuration”。此外，在与部署作业相关的“任务已开始”和“任务已结束”事件中，作业名称将用作事件名称。

- **强制完整部署 (Force a full deployment)** - 如果遇到问题并希望强制系统部署完整配置，而不仅仅是更改，可以点击 **立即部署 (Deploy Now)** 按钮上的下拉箭头，然后选择**应用完整部署 (Apply Full Deployment)**。完整部署会导致流量中断，因此您必须确认要执行此操作，然后才能点击**部署 (Deploy)**。
- **放弃更改** - 要放弃所有待处理更改，请依次点击**更多选项** > **全部放弃**。系统将要求您进行确认。
- **复制更改** - 要将更改列表复制到剪贴板，请依次点击**更多选项** > **复制到剪贴板**。仅当更改不超过 500 项时，选项才可用。
- **下载更改** - 要以文件形式下载更改列表，请依次点击**更多选项** > **以文本形式下载**。系统将提示将文件保存到工作站。文件采用 YAML 格式。如果您没有专门支持 YAML 格式的编辑器，可以使用文本编辑器查看。

引发检测引擎重启的配置更改

在部署配置更改时，以下任意配置或操作都会重新启动检测引擎。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。另外，部署某些配置需要检测引擎重新启动，这样会中断流量检测并丢弃流量。

部署

部分更改需要重新启动检测引擎，这将导致瞬时流量丢失。以下更改需要重新启动检测引擎：

- 启用或禁用 SSL 解密策略。
- 更改一个或多个物理接口（但不是子接口）上的 MTU。
- 在访问控制规则上添加或删除文件策略。
- VDB 已更新。
- 创建或中断高可用性配置。

此外，如果 Snort 进程繁忙、总 CPU 使用率超过 60%，部署期间可能会丢弃部分数据包。可以使用 **show asp inspect-dp snort** 命令，检查 Snort 当前的 CPU 使用率。

系统数据库更新

如要将更新下载到规则数据库或VDB，则必须部署该更新，使其处于活动状态。此部署可能会重新启动检测引擎。手动下载更新或计划更新时，可以指明下载完成后是否应自动部署更改。如果没有将系统设置为自动部署更新，则系统将在下一次部署更改时应用更新，此时检测引擎可能会重新启动。

系统更新

安装不重新启动系统和包括二进制更改的系统更新或补丁，需要检测引擎重新启动。二进制更改可能包括对检测引擎、预处理器、漏洞数据库 (VDB) 或共享对象规则的更改。另请注意，不包括二进制更改的补丁有时需要 Snort 重新启动。

强制执行完整部署的配置更改

在大多数情况下，仅会部署您做出的更改。但是，如有必要，系统将重新应用整个配置，这可能会造成您的网络中断。以下是强制执行完整部署的一些更改。

- 最初启用安全情报或身份策略。
- 安全情报和身份策略均已禁用。
- 重复使用数据时创建 EtherChannel。
- 删除以太网通道。
- 修改 EtherChannel 的成员接口关联。
- 删除配置中使用的任何接口。例如，删除属于访问控制规则使用的安全区域的子接口。
- 更改属于 FlexConfig 策略的 FlexConfig 对象，或从策略中删除不包含取消行的对象。省略取消行会强制系统执行完全部署，因为没有特定方法可以删除 FlexConfig 对象生成的配置。您可以通过始终在每个 FlexConfig 对象中包含适当的否定行来避免此问题。

查看接口状态和管理状态

“设备摘要”包括设备的图形视图和管理地址的选定设置。要打开“设备摘要”，请点击**设备**。

此图中要素的颜色根据该要素的状态而变化。将鼠标悬停在要素的上方，有时会显示更多信息。使用此图可监控以下项目。

注释 此图的接口部分（包括接口状态信息）也会显示于**接口 (Interfaces)** 页面和**监控 (Monitoring)** > **系统 (System)** 控制面板中。

接口状态

将鼠标悬停在端口上方可查看其 IP 地址、启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。将鼠标悬停于网桥虚拟接口 (BVI) 的上方也会显示成员接口列表。

接口端口使用以下颜色代码：

- 绿色 - 接口已配置和启用，链路为运行状态。
- 灰色 - 接口未启用。
- 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。

内部、外部网络连接

图中指出了在以下条件下连接到外部（或上游）和内部网络的端口。

- 内部网络 - 仅对名为“内部”的接口显示内部网络的端口。如有其他内部网络，则不显示它们。如果未命名任何接口为“内部”，则不会将任何端口标记为内部端口。
- 外部网络 - 仅对名为“外部”的接口显示外部网络的端口。同内部网络一样，此名称是必需的，否则不会将任何端口标记为外部端口。

管理设置状态

图中显示是否为管理地址配置了网关、DNS 服务器、NTP 服务器和智能许可，以及这些设置是否正常运行。

绿色表示该功能已配置且运行正常，灰色表示未配置或无法正常运行。例如，如果无法连接服务器，则 DNS 框显示灰色。将鼠标悬停在各个要素上可查看详细信息。

如果发现问题，请按以下步骤更正它们：

- 管理端口和网关 — 依次选择**系统设置** > **管理接口**。
- DNS 服务器 - 依次选择**系统设置** > **DNS 服务器**。
- NTP 服务器 - 依次选择**系统设置** > **NTP**。另请参阅NTP 故障排除。
- 智能许可证 - 点击“智能许可证”组下的**查看配置**链接。

查看系统任务状态

系统任务包括无需直接参与而进行的各种操作，例如检索和应用各种数据库更新。您可以查看这些任务的列表及其状态，以确认系统任务是否成功完成。

任务列表将显示系统任务和部署作业的综合状态。审核日志位于**设备** > **设备管理** > **审核日志**下方，其中包含更多详细信息。例如，审核日志将任务开始和任务结束显示为单独的事件，而任务列表将这些事件合并为一个条目。此外，部署作业的审核日志条目包括有关已部署变更的详细信息。

过程

步骤 1 点击主菜单中的**任务列表 (Task List)** 按钮。

此时将打开任务列表，其中显示系统任务的状态和详细信息。

步骤 2 评估任务状态。

如果发现持续性的问题，可能需要修复设备配置。例如，如果一直无法获取数据库更新，则可能是设备的管理 IP 地址无法访问互联网造成。对于任务说明中指出的某些问题，您可能需要联系思科技术支持中心 (TAC)。

针对任务列表可以执行以下操作：

- 点击**成功 (Success)** 或**失败 (Failures)** 按钮，可依据这些状态过滤列表。
- 点击任务的删除图标 ( )，可将其从列表中移除。
- 点击**删除所有完成的任务 (Remove All Completed Tasks)** 可清空已结束的所有任务的列表。

使用 CLI 控制台监控和测试配置

Firewall Threat Defense 设备包括一个可用于监控和故障排除的命令行界面 (CLI)。虽然可以打开 SSH 会话访问所有系统命令，但也可以在 防火墙设备管理器 中打开 CLI 控制台使用只读命令，例如各种 **show** 命令以及 **ping**、**traceroute** 和 **packet-tracer**。如果您具有管理员权限，还可以输入 **failover**、**reboot** 和 **shutdown** 命令。

从一个页面移动到另一个页面时，可以使 CLI 控制台保持打开状态，并配置和部署功能。例如，在部署新的静态路由之后，可以在 CLI 控制台中使用 **ping** 验证是否可以访问目标网络。

CLI 控制台使用基本的 Firewall Threat Defense CLI。不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

有关命令的详细信息，请参阅Cisco Firepower Threat Defense 命令参考，https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html。

注：

- 尽管 CLI 控制台支持 **ping**，但不支持 **ping system** 命令。
- 系统最多可以处理 2 个并发命令。因此，如果其他用户发出命令（例如，使用 REST API），您可能需要等待其他命令完成后才能输入命令。如果此问题持续存在，请使用 SSH 会话，而非 CLI 控制台。
- 命令会根据已部署的配置来返回信息。如果在 防火墙设备管理器中更改配置而不进行部署，则不会在命令输出中看到所做更改的结果。例如，如果创建一个新静态路由，但不部署该路由，则该路由不会显示在 **show route** 输出中。

过程

步骤 1 点击网页右上角的 **CLI 控制台**图标。

步骤 2 在出现提示时键入命令，然后按 **Enter** 键。

有些命令需要更长时间生成输出，请耐心等待。如果收到命令执行超时的消息，请重试。如果输入需要交互响应的命令（例如 **show perfstats**），也会出现超时错误。如果问题仍然存在，您可能需要使用 SSH 客户端而不是 CLI 控制台。

以下是有关如何使用该窗口的一些提示。

- 按 **Tab** 键，在键入部分命令时系统会自动补全。此外，此时按 Tab 键，系统还会列出命令中可用的参数。Tab 可列出三级关键字。三级之后，需要使用命令参考来获取更多信息。
- 按 Ctrl+C 可以停止命令执行。
- 要移动窗口，请点击并按住标题中的任意位置，然后将窗口拖到所需位置。
- 点击**展开**（  ）或**收起**（  ）按钮放大或缩小窗口。
- 点击**取消停靠，以独立窗口显示**（  ）按钮，将窗口从网页分离出去，在独立的浏览器窗口中显示。要再次停靠，请点击**停靠到主窗口**（  ）按钮。
- 点击并拖动以突出显示文本，然后按 Ctrl+C 将输出复制到剪贴板。
- 点击**清除 CLI**（  ）按钮，清除所有输出。
- 点击**复制最后一个输出**（  ）按钮，将您输入的最后一个命令的输出内容复制到剪贴板上。

步骤 3 完成后，只需关闭控制台窗口即可。请勿使用 **exit** 命令。

尽管用于登录 防火墙设备管理器 的凭证可验证您对 CLI 的访问权限，但使用控制台时，实际上从来无需登录 CLI。

同时使用防火墙设备管理器和 REST API

在本地管理模式下设置设备时，您可以使用 防火墙设备管理器 和 Firewall Threat Defense REST API 配置设备。实际上， 防火墙设备管理器 使用 REST API 配置设备。

但请注意，REST API 可提供除通过 防火墙设备管理器提供的功能之外的其他功能。因此，对于任何给定的功能，您可以使用 REST API 配置通过 防火墙设备管理器查看配置时不能显示的设置。

如果配置了在 REST API 中可用、但在 防火墙设备管理器中不可用的功能设置，使用 防火墙设备管理器更改全局功能（例如远程访问 VPN）时，该设置可能会被撤消。是否保留仅 API 设置可能视情况有所不同，并且在许多情况下，通过 防火墙设备管理器 编辑会保留对 防火墙设备管理器 中不可用设置的 API 更改。对于任何给定功能，应验证所作更改是否已保留。

一般而言，应避免对任何给定功能同时使用防火墙设备管理器和 REST API。相反，配置设备时，应从两者中选择一种方法，逐一配置每项功能。

可以使用 API Explorer 查看和尝试 API 方法。点击“更多选项”按钮 (⋮) 并选择 **API Explorer**。

通信端口和互联网访问要求

以下主题介绍了为运行设备上所有可用功能而需要在设备上打开的端口，以及需要访问的互联网站点。如果您以受限方式或气隙方式运行，可以阻止部分或全部端口和互联网站点以满足您的要求。否则，请确保这些端口和站点处于打开状态且可访问。

设备使用的通信端口

下表列出了各项服务需开放的端口。使用访问控制规则确保这些端口在面向服务的接口上开放，或在面向需通过相关协议访问设备的用户接口上开放。若不使用某项功能，可保持对应端口关闭。

表 *2:* 入站端口

入站端口	协议/功能	详细信息
TCP/22	SSH	与设备命令行界面的安全远程连接。 **注释** 若您使用 **copy** 命令或其他需进行外部通信的命令，需开放对应的出站端口。例如，若需使用 FTP，则需开放 TCP/20 和 21。
UDP/161	SNMP	允许通过 SNMP 轮询访问 MIB。
TCP/443	HTTPS	用于以下服务： • 管理到 防火墙设备管理器 的连接。 • Firewall Threat Defense REST API。 • 远程访问 VPN SSL 连接。若为 RA VPN 配置了自定义端口，请开放该端口。
TCP/885	强制网络门户	与强制网络门户身份源通信。此为默认端口。若配置了其他端口，请开放自定义端口。有关详细信息，请参阅配置身份策略设置。
TCP/8989	思科支持诊断结果	接受授权的请求。也会在此端口上发起连接。

表 *3:* 出站端口

出站端口	协议/功能	详细信息
TCP/49 TCP/300	TACACS+	与 RADIUS 服务器通信以进行外部身份验证和记账。 使用 TLS 加密与服务器连接时，建议使用 TCP/300 端口，但非强制要求。 若配置了自定义端口，请开放这些端口。请参阅配置 TACACS+ 服务器。

出站端口	协议/功能	详细信息
UDP/53 （若使用。）TCP/53	DNS	DNS。通常使用 UDP/53 进行 DNS。若使用基于 TCP 的 DNS，也需开放 TCP/53。
UDP/67 UDP/68	DHCP	DHCP 获取地址时。
UDP/123	NTP	同步时间。
UDP/162	SNMP	发送 SNMP 警报至远程陷阱服务器。
TCP/389 TCP/636	LDAP、LDAPS	与 LDAP 服务器通信以进行外部身份验证。 若配置了自定义端口，请开放这些端口。请参阅配置 AD 身份领域。
TCP/443	HTTPS	从互联网收发数据，如下载数据库更新。
UDP/514	系统日志	将系统日志消息发送至远程系统日志服务器。
UDP/1812 UDP/1813	RADIUS	与 RADIUS 服务器通信以进行外部身份验证和记账。 若配置了自定义端口，请开放这些端口。请参阅配置RADIUS服务器。
UDP/8514	Cisco Secure Network Analytics 管理器	将系统日志消息发送至云端。
TCP/8989	思科支持诊断结果	传输使用信息和统计信息。也会在此端口上接受连接。

访问的互联网资源

以下功能必须访问关联的互联网资源才能正常运行。设备会根据需要使用端口 TCP/80 和 TCP/443。

表 *4:* 访问的互联网资源

功能	原因	高可用性	Resource
CA 证书捆绑包	每天在系统定义的时间查询新的 CA 证书。本地 CA 捆绑包包含用于访问多项思科服务的证书。 在 CLI 中，可以使用 **configure cert-update auto-update** 命令配置此功能。 适用于版本 7.0(5)、7.1(0.3)、7.2(4)、7.3 及更高版本。	每个对等体都会下载其自己的证书。	cisco.com/security/pki

功能	原因	高可用性	Resource
恶意软件防御 1	Cisco Secure Malware Analytics 云 查找。	两个对等体均执行查找。	正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址
	下载签名更新以进行文件预分类和本地恶意软件分析。	活动对等体执行下载，并同步到备用对等体。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	提交文件以供动态分析。 查询动态分析结果。	两个对等体均查询动态分析报告。	fmc.api.threatgrid.com fmc.api.threatgrid.eu fmc.api.threatgrid.ca fmc.api.threatgrid.com.au fmc.api.threatgrid.in
安全智能	下载安全智能源。	活动对等体执行下载，并同步到备用对等体。	est.sco.cisco.com updates-talos.sco.cisco.com updates.ironport.com (http) updates-dyn-talos.sco.cisco.com

功能	原因	高可用性	Resource
URL 过滤	下载 URL 类别和信誉数据。 手动查询（查找）URL 类别和信誉数据。 查询未分类的 URL。	活动对等体执行下载，并同步到备用对等体。	URL： • *.talos.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com • 思科区域云：Cisco Security Cloud/Security Services Exchange IPv4 块： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPV6 块： • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
思科 智能软件管理器	与 智能软件管理器通信。	活动对等体执行通信。	www.cisco.com smartreceiver.cisco.com
Cisco Success Network	传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
思科支持诊断结果	接受授权请求并传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989
一般云服务	—	—	api-sse.cisco.com
思科 XDR 集成	配置设备将事件发送到 Security Cloud Control。	活动对等体执行通信。	Cisco Secure Firewall Threat Defense 和 Cisco XDR 集成指南

功能	原因	高可用性	Resource
时间同步	同步部署中的时间。 代理服务器不支持。	两个对等体都与 NTP 服务器通信。	用户已配置。 默认服务器： • 0.sourcefire.pool.ntp.org • 1.sourcefire.pool.ntp.org • 2.sourcefire.pool.ntp.org
入侵规则	下载入侵规则 (SRU/LSP)。	活动对等体执行下载，并同步到备用对等体。	est.sco.cisco.com updates-talos.sco.cisco.com updates-dyn-talos.sco.cisco.com updates.ironport.com 思科区域云：Cisco Security Cloud/Security Services Exchange
Cisco Security Cloud/Security Services Exchange	Cisco Success Network 思科支持诊断结果 下载与 Talos 通信的证书，获取威胁情报更新。请参阅下载具有永久许可证预留的威胁情报。	两个对等体进行通信。	api-sse.cisco.com api.eu.sse.itd.cisco.com api.apj.sse.itd.cisco.com api.au.sse.itd.cisco.com api.in.sse.itd.cisco.com
漏洞数据库	下载 VDB 更新。	活动对等体执行下载，并同步到备用对等体。	support.sourcefire.com
地理位置数据库	下载 GeoDB 更新。	活动对等体执行下载，并同步到备用对等体。	support.sourcefire.com

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。