思科 Firepower 威胁防御 强化指南，版本 6.4

首次发布日期: 2019 年 5 月 10 日

思科 Firepower 威胁防御强化指南，版本 6.4

Firepower 可以保护您的网络资产和流量免受网络威胁，但您还应该配置 Firepower 本身以使其更加强大，进一步降低其遭受网络攻击的脆弱性。本指南讨论如何加强 Firepower 部署，主要侧重于 Firepower 威胁防御 (FTD)。有关 Firepower 部署的其他组件的强化信息，请参阅以下文档：

- 《思科 *Firepower* 管理中心强化指南，版本 *6.4*》
- 《思科 *Firepower 4100/9300* 强化指南》

本指南是两种不同的配置FTD设备配置方法，但不是为所涉及的任何接口提供详细的手册。

- 有些 FTD 配置设置可通过 FMC web 界面建立；该产品的交叉引用请参考《 *Firepower* 管理中心配置指南，版本 *6.4* 》。
- 有些 FTD 配置设置可以使用 FTD 命令行界面 (CLI) 建立。有关本文档所述及所有 CLI 命令的完整信息，请参阅《 思科 *Firepower* 威胁防护命令参考 》

本文档中的所有功能描述均参考 Firepower 版本6.4。并非所有 Firepower 版本都提供本手册中讨论的所有配置设置。有关配置 Firepower 部署的详细信息，请参阅您的版本的 Firepower 文档。

安全认证合规性

您的组织只能使用符合由美国国防部和其他政府认证机构制定的安全标准的设备和软件。一旦经过相应认证机构的认证，并且按照认证特定的指导文档进行配置，Firepower 的设计符合以下认证标准：

- 通用标准 (CC)：国际共同标准承认协定建立的全球标准，用于定义对安全产品的要求。
- 国防部信息网络获批产品列表 (DoDIN APL)：符合美国国防信息系统机构 (DISA) 建立的安全要求的产品列表。

注释 美国政府已将统一功能获批产品列表 (UCAPL) 的名称改为 DODIN APL。Firepower 文档和 Firepower 管理中心 Web 界面中对 UCAPL 的引用可以解释为对 DoDIN APL 的引用。

- 联邦信息处理标准 (FIPS) 140：针对加密模块的要求规范。

认证指导文档在产品认证完成后将单独提供；本强化指南的发布并不保证完成任何产品认证。

本文档所述的Firepower配置设置不能保证严格遵守认证实体的所有最新要求。有关必要强化程序的详细信息，请参阅由认证实体提供的关于此产品的相关规定。

本文档提供有助增强 FTD 安全性的指导，但即使使用本文所述的配置设置，部分 FTD 功能也不支持认证合规性。有关详细信息，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“安全证书合规性建议”。我们努力确保此强化指南和《*Firepower* 管理中心配置指南，版本 *6.4*》不会与证书特定指导原则发生冲突。如果发现思科文档和认证指南之间出现冲突，请以认证指南为准或者咨询系统所有者。

监控思科安全公告及对策

思科产品安全事件响应团队 (PSIRT) 负责发布有关思科产品安全相关问题的 PSIRT 建议。对于不太严重的问题，思科还会发布思科安全响应。安全建议和响应将发布在思科安全建议和警报页面上。有关这些沟通工具的更多信息，请参阅思科安全漏洞策略。

要确保网络的安全，必须了解思科安全建议和响应。这些资料提供了评估漏洞对网络构成的威胁所需的信息。如需获取与此评估流程相关的帮助，请参阅安全漏洞公告风险分类。

保持系统更新

思科会定期发布Firepower软件更新以解决问题并做出改进。保持系统软件为最新状态对于维护强化的系统至关重要。要确保您的系统软件正确更新，请使用《*Firepower*管理中心配置指南，版本*6.4*》“系统软件更新”章节以及《*Firepower* 管理中心升级指南》中的信息。

思科还会定期针对 Firepower 用于保护您的网络和资产的数据库发布更新。要在 FMC 管理的 FTD 设备上提供最佳保护，请确保负责管理任务的FMC上的地理位置、入侵规则和漏洞数据库为最新。在更新 Firepower 部署的任何组件之前，您必须阅读更新随附的思科 Firepower 发行说明。这些内容提供版本特定的关键信息，包括兼容性、必备条件、新功能、行为更改和警告。有些更新可能很大，需要一些时间才能完成；您应该在网络使用率较低的时段执行更新，以减少对系统性能的影响。

地理位置数据库 (GeoDB)

此数据库包含与可路由IP地址关联的地理数据（例如国家/地区、城市坐标）和连接相关数据（例如互联网服务提供商、域名、连接类型）。Firepower 检测与已经检测到的 IP 地址匹配的 GeoDB 信息时，您可以查看与IP地址关联的地理位置信息。要查看除国家/地区或大洲以外的任何地理位置详细信息，必须在系统上安装 GeoDB。要从 FMC Web 界面更新 GeoDB，请使用**系统** > **更新** > **地理位置更新**，然后选择以下方法之一：

- 要在没有 Internet 访问权限的 FMC 上更新 GeoDB，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“手动更新 GeoDB（无 Internet 连接）”中的说明操作。
- 要在具有 Internet 访问权限的 FMC 上更新 GeoDB，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“手动更新 GeoDB（Internet 连接）”中的说明操作。
- 要在具有 Internet 访问权限的 FMC 上安排自动周期性更新 GeoDB，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“安排 GeoDB 更新”中的说明操作。

入侵规则

随着新漏洞的暴露，思科 Talos 安全情报和研究小组 (Talos) 会发布可导入到 FMC 上的入侵规则更新（亦称为 Snort 规则更新，简称 SRU），然后通过将已更改的配置部署到受管设备进行实施。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。FMC Web 界面提供三种方法来更新入侵规则，全部位于**系统** > **更新** > **规则更新**之下：

- 要在没有 Internet 访问权限的 FMC 上更新入侵规则，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“一次性手动更新入侵规则”中的说明操作。
- 要在具有 Internet 访问权限的 FMC 上更新入侵规则，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“一次性自动更新入侵规则”中的说明操作。
- 要在具有 Internet 访问权限的 FMC 上安排自动周期性更新入侵规则，请按照《*Firepower* 管理中心配置指南，版本 *6.4*》“配置周期性入侵规则更新”中的说明操作。

也可以使用**系统** > **更新** > **规则更新**导入本地入侵规则。可以使用 Snort 用户手册（可在 http://www.snort.org 上获取）中的说明创建本地入侵规则。在将其导入到 FMC 之前，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“导入本地入侵规则指引”，确保导入本地入侵规则的过程符合您的安全策略。

漏洞数据库 (VDB)

此数据库包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用程序指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。FMC Web 界面提供两种更新 VDB 的方法：

- 使用 **系统** > **更新** > **产品更新** 并遵照《*Firepower* 管理中心配置指南，版本 *6.4*》“手动更新漏洞数据库 (VDB)”中的说明操作。
- 如《*Firepower* 管理中心配置指南，版本 *6.4*》中的“配置周期性任务”所述，使用 **系统** > **工具** > **计划** 并安排周期性任务以下载和安装 VDB 更新。

启用 CC 或 UCAPL 模式

要通过单个设置应用多个强化的配置更改，请为 FTD 选择 CC 或 UCAPL 模式。将此设置应用到 FMCFTD平台设置策略（位于中找到）thorugh 中的 web 界面**设备** > **平台设置**。在您部署新配置之前，更改不会在 FTD 上生效；有关完整详情，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“启用安全证书合规性”。

选择这些配置选项之一，以使《*Firepower* 管理中心配置指南，版本 *6.4*》“安全证书合规性特征”之下所列的更改生效。请注意，Firepower 部署中的所有设备都应在相同的安全证书合规性模式下运行。

⚠

注意 启用此设置后，您将无法将其禁用。在启用 CC 或 UCAPL 模式之前，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“安全证书合规性”。如果您需要撤消此设置，请与思科 TAC 联系以获取帮助。

注释 启用安全认证合规性不保证严格符合所选安全模式的所有要求。本文档介绍了一些额外设置，这些设置可以强化您的部署，使之比 CC 或 UCAPL 模式提供的部署更加强大。有关确保完全合规所需的强化程序的完整信息，请参阅由认证实体提供的此产品的相关规定。

使用 NetFlow 实现流量的可视性

借助思科的 IOS NetFlow，您可以实时监控网络中的流量。FTD 设备可以与某些 NetFlow 功能配合，例如查看和重置运行时计数器。（请参阅 **show flow-export counters** 和 **clear flow-export counters** CLI 命令。）

通过 FMC Web 界面，您可以禁用与 NetFlow 捕获的消息冗余的 FTD 系统日志消息。要执行此操作，请在**设备 > 平台设置**下创建一个 FTD 平台设置策略，然后从菜单中选择**系统日志**。在**系统日志设置**选项卡上，选中 **NetFlow 等效系统日志**复选框（使用 **show logging flow-export-syslogs** CLI 命令确定哪些系统日志消息是冗余的。）

如果您使用 NetFlow 配置网络设备，可以充分利用这些功能。无论流信息是否导出到远程收集器，您都可以根据需要应变性地使用 NetFlow。有关详细信息，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“Firepower 系统中的 Netflow 数据”。

保护本地网络基础设施

Firepower 部署可能会出于多种目的与其他网络资源交互。强化这些其他服务可以保护您的 Firepower 系统以及所有网络资产。要确定需要解决的所有问题，请尝试绘制网络及其组件、资产、防火墙配置、端口配置、数据流和桥接点的图表。

建立并遵守网络的操作安全流程，将安全问题考虑在内。

保护网络时间协议服务器

要使 Firepower 成功运行，必须在 FMC 及其受管设备上同步系统时间。我们强烈建议使用安全和值得信赖的网络时间协议 (NTP) 服务器来同步 FMC 及其所管理的设备上的系统时间。

在**设备 > 平台设置**下创建一个 FTD 平台设置策略，然后在策略页面内选择**时间同步**选项卡，从而从 FMC Web 界面为 FTD 设备配置 NTP 时间同步。有关详细信息，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“为威胁防御配置 NTP 时间同步”。

注意 如果 FMC和受管设备之间的时间不同步，可能会导致意外后果。为确保正确同步，请将 FMC 及其管理的所有设备配置为使用相同的 NTP 服务器。

保护域名系统 (DNS)

网络环境中相互通信的计算机依赖于 DNS 协议来提供 IP 地址和主机名之间的映射。如适用于您的型号的快速入门指南中所述，配置 FTD 设备连接本地域名系统以支持通过其管理接口通信是初始配置过程的一部分。

使用数据或诊断接口的某些FTD功能也使用DNS - 示例包括NTP、访问控制策略、FTD提供的VPN服务、ping 或跟踪路由。要为数据或诊断接口配置 DNS，请在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择**DNS**。有关详细信息，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中“适用于 Firepower 威胁防御的平台设置”下的“配置 DNS”。

DNS可能容易受到特定类型的攻击，这些攻击会利用DNS服务器中未配置安全防护措施的薄弱点。确保您的本地 DNS 服务器配置符合行业建议的安全最佳实践；思科在此文档中提供了指导原则：http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html。

保护 SNMP 轮询和陷阱

您可以按照《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“为威胁防御配置 SNMP”所述，配置FTD以支持SNMP轮询和陷阱。如果选择使用SNMP轮询，则应注意SNMP管理信息库(MIB)中包含可用于攻击部署的系统详细信息，例如联系人、管理、位置和服务信息；IP寻址和路由信息；以及传输协议使用统计信息。选择配置选项以保护系统免受基于 SNMP 的威胁。

要为 FTD 设备配置 SNMP 功能，请在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择 **SNMP**。有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“为威胁防御配置 SNMP”。

使用以下选项强化对 FTD 设备的 SNMP 访问：

- 创建 SNMP 主机时，选择仅支持使用 AES128 和只读用户加密的 SNMPv3。（请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“添加 SNMP 主机”。）
- 使用以下选项创建 SNMPv3 用户：
  - 为**安全级别**选择 **Priv**。
  - 为**加密密码类型**选择**已加密**。

  有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“添加 SNMPv3 用户”。

重要事项 虽然您可以从 Firepower 建立与 SNMP 服务器的安全连接，但身份验证模块不符合 FIPS 标准。

保护网络地址转换 (NAT)

网络计算机通常使用网络地址转换(NAT)重新分配网络流量中的来源或目标IP地址。要保护Firepower部署以及整个网络基础架构免受基于 NAT 的攻击，请根据行业最佳实践以及 NAT 提供商的建议在网络中配置 NAT 服务。

有关配置您的Firepower部署以在NAT环境中运行的信息，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“NAT 环境”。建立部署时，请在两个阶段使用以下信息：

- 按照《思科 Firepower 管理中心入门指南》中关于您的硬件型号的说明，执行 FMC 的初始设置。

- 如《*Firepower* 管理中心配置指南，版本 *6.4*》中的“向 Firepower 管理中心添加设备”所述，向 FMC 注册受管设备时。

在您的部署中保护 FMC 和其他设备

您的 Firepower 部署包括 FMC 以及由 FMC 管理的安全设备，每个提供不同的访问方式。受管设备会与 FMC 交换信息，其安全性对于整个部署的安全非常重要。在部署中分析设备并根据需要应用强化配置，例如保护用户访问权限以及关闭不需要的通信端口。

强化网络协议设置

FTD 设备可使用多个协议与其他网络设备交互；选择网络通信的配置设置，以保护 FTD 设备及其发送和接收的数据。

- 默认情况下，FTD 设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但是，零碎的数据包通常被用于拒绝服务 (DoS) 攻击，因此我们建议您不要允许分段。要为 FTD 设备配置分段设置，请在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择**分段**。要禁止 FTD 设备处理的网络流量中的片段，请将**链**（**片段**）选项设置为 1。有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“配置片段处理”。
- FTD 可以配置为提供两种虚拟专用网络 (VPN) 服务：
  - 远程访问虚拟专用网络 (RA VPN) - 要通过 RA VPN 连接保护与远程客户端之间的消息传输，FTD 可以使用传输层安全 (TLS) 或 IPsec_IKEv2。除非达到《思科 *Firepower* 管理中心配置指南，版本 *6.4*》“AnyConnect 许可证”中所述的标准，否则 FMC 不会允许您将 RA VPN 配置部署到 FTD。
  - 站点到站点虚拟专用网络 - 要通过站点到站点 VPN 连接保护与远程网络之间的消息传输，FTD 可以使用 IPSEC_IKEv1 或 IPSEC_IKEv2。根据您的设备许可证，您可能可以对站点到站点 VPN 传输应用强加密。请注意，具有强加密功能的站点到站点 VPN 需要特殊许可；请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“出口控制功能的许可”。

  要配置这些服务，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“Firepower 威胁防御 VPN”。Firepower 支持各种加密和哈希算法，以及可供选择的 Diffie-Hellman 组。但是，选择强加密可能会导致系统性能降低，因此必须在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。有关可用选项和待考虑因素的讨论，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4* 》中的“VPN 连接应有多高的安全性？”。
- 对于 Firepower 管理中心管理的 FTD 设备，涉及 FTD 的 HTTPS 连接只能用于下载数据包捕获文件以进行故障排除。配置 FTD 设备以仅允许对允许下载数据包捕获的 IP 地址进行 HTTPS 访问；在 FMC Web 界面的**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择 **HTTP**。有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“配置 HTTP”。
- 默认情况下， FTD 可以使用 IPv4 或 IPv6 在任何接口上接收 ICMP 数据包，不过有两种情况例外：
  - FTD 不响应定向至广播地址的 ICMP 回显请求。

- FTD 仅响应发送至流量进入的接口的 ICMP 流量；不能通过 FTD 接口将 ICMP 流量发送至远端接口。

为了保护 FTD 设备免受基于 ICMP 的攻击，您可以使用 ICMP 规则将 ICMP 访问限制为选定主机、网络或 ICMP 类型。在 FMC Web 界面的**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择 **ICMP**。有关详细信息，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“配置 ICMP 访问规则”。

- FTD 可以配置为提供 DHCP 和 DDNS 服务（请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“用于威胁防御的 DHCP 和 DDNS 服务”）。根据其性质，这些协议容易受到攻击。如果您选择将 FTD 设备配置为 DHCP 或 DDNS，则务必应用行业最佳实践来确保安全性、为您的网络资产提供物理保护，并强化用户对 FTD 设备的访问。

强化 FTD 用户访问

FTD 支持两种类型的用户：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

您可以考虑通过外部身份验证机制（如 LDAP 或 RADIUS）建立用户访问权限，以将用户管理与网络环境中的现有基础设施集成，或利用双因素身份验证等功能。建立外部身份验证需要在 FMC Web 界面中创建外部身份验证对象；可以共享外部身份验证对象，以便为 FMC 和 FTD 验证外部用户。

请注意，如果使用外部身份验证，您必须为部署配置域名服务器。确保遵循适用于 DNS 的强化建议。（请参阅保护域名系统 (DNS)）

有关用户管理的讨论指 Firepower 版本 6.4 中可用的功能；并非本部分谈及的所有用户帐户配置功能都适用于所有 Firepower 版本。有关您系统的特定信息，请参阅您的版本的 Firepower 文档。

Firepower 威胁防御 管理的 FMC设备提供单一的用户访问方式：对于物理设备，可以通过 SSH、串行或键盘和显示器连接访问的命令行界面。使用某些配置设置时，这些用户还可以访问 Linux 外壳程序。

限制配置权限

默认情况下，FTD 设备会向单个 **admin** 用户提供对所有 FTD CLI 命令的完全管理员权限。该用户可以使用 **configure user access** CLI 命令创建其他帐户并为其授予两个访问权限级别之一：

- 基本：用户可以使用 FTD CLI 命令而不会影响系统配置
- 配置：用户可以使用所有 FTD CLI 命令，包括提供重要系统配置功能的命令。

在为帐户分配配置访问权限时，以及在选择向具有配置访问权限的帐户授予访问权限的用户时，请仔细考虑。

限制 Linux 外壳程序访问

由 FMC 管理的 FTD 仅支持通过其管理接口的 CLI 访问（使用 SSH、串行或键盘和显示器连接）。此功能可用于 **admin** 帐户和内部用户，并且可供外部用户使用。

具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。

⚠

注意 在所有设备上，具有 CLI 层级访问权限或 Linux 外壳程序访问权限的用户可以在 Linux 外壳程序中获取 sudoers 权限，这可能构成安全风险。为提高系统安全性，我们建议：

- 在允许用户访问 FTD 设备上经过外部验证的帐户时，请记住，FTD 设备上的所有外部验证帐户都有 CLI 配置级访问权限。
- 请勿直接在 Linux 外壳程序中添加新帐户；在 FTD 设备上，仅使用 **configure user add** CLI 命令创建新帐户。
- 使用 FTD CLI 命令 **configure ssh-access-list** 限制 FTD 设备在其管理接口上接受 SSH 连接的 IP 地址。

管理员还可以使用 **system lockdown-sensor** CLI 命令配置 FTD 阻止对 Linux 外壳程序的所有访问。系统锁定完成后，任何登录 FTD 的用户都只能访问 FTD CLI 命令。这可能是一个重要的强化操作，但请仔细考虑使用，因为只能通过思科 TAC 的热补丁才能撤消此操作。

强化内部用户帐户

配置单个内部用户角色时，用户可以使用 **configure user** FTD CLI 命令通过 Web 界面登录机制强化系统以抵御攻击。以下设置可用：

- 限制用户锁定并必须由管理员重新激活的登录最大失败次数 (**configure user maxfailedlogins**)。
- 强制使用最短密码长度 (**configure user minpasswdlen**)。
- 设置密码的有效天数 (**configure user aging**)。
- 需要强密码 (**configure user strengthcheck**)。
- 分配仅适用于用户所需访问类型的用户访问权限 (**configure user access**)。
- 强制用户在下次登录时重置帐户密码 (**configure user forcereset**)。

如果您的 Firepower 部署使用了多租户，则在向用户授予该设备的访问权限时，请考虑 FTD 设备所属的域。有关完整讨论，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“域管理”。

强化外部用户帐户

如果您选择使用外部服务器进行 FTD 用户验证，请记住，外部用户始终拥有配置权限；其他用户角色不受支持。在**设备>平台设置**下创建一个 FTD 平台设置，然后自目录中选择**外部身份验证**，从而从 FMC Web 界面为 FTD 用户配置外部身份验证。配置外部用户帐户需要通过外部身份验证对象与 LDAP 或 RADIUS 服务器建立连接。有关详细信息，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“为 SSH 配置外部身份验证”。

重要事项 尽管可以从 Firepower 设置与 LDAP 或 RADIUS 服务器的安全连接，但身份验证模块不符合 FIPS 标准。

- 请注意，所有 FTD 外部用户都有配置访问权限，除非您通过 **system lockdown-sensor** 命令阻止对 Linux 外壳程序的访问，否则这些用户可以访问 linux 外壳程序。外壳程序用户可以获得 root 权限，带来安全风险。
- 如果使用 LDAP 进行外部验证，请在**高级选项**下配置 TLS 或 SSL 加密。

建立会话超时

限制与 FTD 的连接时长可以减少未经授权的用户利用无人参与会话的机会。

要在 FTD 设备上设置会话超时，请在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择**超时**。有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“配置全局超时”。

FTD REST API 注意事项

Firepower 威胁防御 REST API 提供轻量级接口，以供第三方应用使用 REST 客户端和标准 HTTP 方法查看和管理设备配置。《思科 *Firepower* 威胁防御 *REST API* 指南》对 API 进行了详细介绍。

重要事项 虽然可以使用 TLS 在 FTD 与 REST API 客户端之间建立安全连接，但验证模块不符合 FIPS 标准。

保护备份

要保护系统数据及其可用性，请定期备份您的 FTD 设备。备份功能显示在 FMC Web 界面的**系统** > **工具** > **备份/恢复**之下，《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“远程备份设备”对此功能进行了介绍。要恢复保存的 FTD 配置，请使用 FTD CLI **restore** 命令。

FMC 提供在远程设备上自动存储备份的功能。不建议对强化的系统使用此功能，因为无法保护 FMC 与远程存储设备之间的连接。

保护数据导出

FTD CLI 可用于将特定文件从 FTD 下载到本地计算机。此功能旨在帮助您收集信息以便在排除系统故障时提供给思科 TAC，平时不应随便使用。请采取预防措施保护从 FTD 下载的任何文件；下载时选择最安全的选项、保护存储数据的本地计算机的安全，并且在将文件传输到 TAC 时使用最安全的协议。尤为重要的是，使用以下命令时，请注意可能存在的风险：

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  export 选项仅支持 TFTP。

- **file copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

此命令会使用不安全 FTP 将文件传输到远程主机。

- **copy [/noverify] /noconfirm** {**/pcap capture:/**[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

  src_url 和 *dest_url* 的以下选项提供保护复制数据安全的方法：

  - 内部闪存
  - 系统内存
  - 可选的外置闪存驱动器
  - 使用密码保护的 HTTPS
  - 使用密码保护的 SCP，在 SCP 服务器上指定目标接口
  - 使用密码保护的 FTP
  - 使用密码保护的 TFTP，在 TFTP 服务器上指定目标接口

  我们建议您不要在强化的系统中使用 *src_url* 和 *dest_url* 选项：

  - SMB UNIX 服务器本地文件系统
  - 群集跟踪文件系统。（启用了安全认证合规性的系统不支持群集。）

- **cpu profile dump** *dest_url*

  dest_url 的以下选项提供保护转储数据安全的方法：

  - 内部闪存
  - 可选的外置闪存驱动器
  - 使用密码保护的 HTTPS
  - SMB UNIX 服务器本地文件系统
  - 使用密码保护的 SCP，在 SCP 服务器上指定目标接口
  - 使用密码保护的 FTP
  - 使用密码保护的 TFTP，在 TFTP 服务器上指定目标接口

  我们建议您不要在强化的系统中将群集文件系统用于 *src_url* 和 *dest_url* 选项：

- **file secure-copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  使用 SCP 将文件复制到远程主机。

保护系统日志

FTD 可以将系统日志消息发送到外部系统日志服务器；配置系统日志功能时选择安全选项：

1. 在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择**系统日志**。在**系统日志服务器**选项卡下添加系统日志服务器时，确保选择 TCP 协议并选中**启用安全系统日志**复选框。这些选项适用于 FTD 生成的系统日志消息（如果您未在设备配置中的其他位置覆盖它们）。

注释 默认情况下，启用安全系统日志时，如果使用TCP的系统日志服务器关闭，则FTD不会前转流量。要覆盖此行为，选中**TCP 系统日志服务器关闭时，允许用户流量通过**复选框。

2. 配置访问控制策略中的日志记录，以从平台设置策略继承日志记录设置。（在**策略** > **访问控制** <每个策略> **>日志记录**下选中 **FTD 6.3 及更高版本：使用在设备上部署的 FTD 平台设置策略中配置的系统日志设置**复选框。）

使用这两个配置设置时，FTD 系统日志的行为如下：

- 平台设置策略中的系统日志设置适用于与设备和系统运行状况以及网络配置相关的系统日志消息。
- 平台设置中的系统日志设置适用于连接和安全智能事件，除非您在《思科 *Firepower* 管理中心配置指南，版本 *6.4*》的“配置和安全情报事件系统日志的配置位置（所有设备）”中列出的任何位置，覆盖访问控制策略的设置。这些覆盖不提供安全的系统日志选项，因此我们建议您不要在安全的环境中使用它们。
- 平台设置策略中的系统日志设置适用于入侵事件系统日志，除非您在《思科 *Firepower* 管理中心配置指南，版本 *6.4*》的“入侵事件系统日志的配置位置（FTD 6.3 设备）”中列出的任何位置，覆盖访问控制策略的设置。这些覆盖不提供安全的系统日志选项，因此我们建议您不要在安全的环境中使用它们。

自定义登录横幅

您可以配置 FTD 设备，使其在用户登录到 CLI 时向他们传递必要的信息。从安全角度来看，登录横幅应阻止未经授权的访问；请考虑下例所示的文本：

> 您已登录到安全设备。如果您无权访问此设备，请立即注销，否则可能面临刑事指控。

要为 FTD 设备配置登录横幅，请在**设备** > **平台设置**下创建一个 FTD 平台设置策略，然后从目录中选择**横幅**。有关完整说明，请参阅《思科 *Firepower* 管理中心配置指南，版本 *6.4*》中的“配置横幅”。

保护到支持网络用户权威登录、意识和控制的服务器的连接

Firepower身份策略使用身份源对网络用户进行身份验证，并收集用户数据以便提高用户意识和控制能力。要建立用户身份源，需要在 FMC 或受管设备与以下服务器类型之一之间建立连接：

- Microsoft Active Directory
- Linux Open LDAP
- RADIUS

重要事项 尽管可以从 Firepower 设置到 LDAP、Microsoft AD 或 RADIUS 服务器的安全连接，但身份验证模块不符合 FIPS 标准。

注释 如果选择将 LDAP 或 Microsoft AD 用于外部身份验证，请查看强化外部用户帐户，第 8 页中的信息。

注释 Firepower 使用这些服务器中的每一个来支持可能的用户身份功能的不同组合。有关完整信息，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“关于用户身份源”。

使用 Active Directory 和 LDAP 服务器保护连接的安全：

被称为领域的 Firepower 对象描述与 Active Directory 或 LDAP 服务器上的域关联的连接设置。有关配置领域的完整信息，请参阅《*Firepower* 管理中心配置指南，版本 *6.4*》中的“创建和管理领域”。

当您创建领域（在 FMC web 界面的**系统** > **集成** > **领域**中）时，请记住以下几点，以确保与 AD 或 LDAP 服务器的连接安全：

对于与 Active Directory 服务器关联的领域：

- 为 **AD 加入密码**和**目录密码**选择强密码。
- 将目录添加到 Active Directory 领域时：
  - 为**加密**模式选择 **STARTTLS** 或 **LDAPS**（不要选择**无**）。
  - 指定用于对 Active Directory 域控制器进行身份验证的 **SSL 证书**。我们建议使用由全球知名且值得信赖的证书颁发机构生成的证书。

对于与 LDAP 服务器关联的领域：

- 为**目录密码**选择强密码。
- 将目录添加到 LDAP 领域时：
  - 为**加密**模式选择 **STARTTLS** 或 **LDAPS**（不要选择**无**）。
  - 指定用于对 LDAP 服务器进行身份验证的 **SSL 证书**。我们建议使用由全球知名且值得信赖的证书颁发机构生成的证书。

保护与 RADIUS 服务器的连接：

要配置与 RADIUS 服务器的连接，请创建 RADIUS 服务器组对象（在 FMC web 界面的**对象** > **对象管理** > **RADIUS 服务器组**），然后将 RADIUS 服务器添加到组。要保护与 RADIUS 服务器的连接，请在**新建 RADIUS 服务器**对话框中选择以下选项：

- 提供**密钥**和**确认密钥**以加密受管设备与 RADIUS 服务器之间的数据。
- 为可以支持安全数据传输的连接指定一个接口。

注释 仅当部署中的受管 FTD 设备配置为提供远程访问 VPN（将用作用户身份源）时，Firepower 才会连接到用于用户身份的 RADIUS 服务器。有关配置和保护远程访问 VPN 安全的信息，请参阅强化网络协议设置。

强化支持组件

FTD 软件依赖于复杂的底层固件和操作系统软件。这些底层软件组件自带有必须解决的安全风险：

- 为网络建立操作安全流程，将安全问题考虑在内。
- 对于 FTD 型号 2100、4100 和 9300 设备，确保运行 FTD 的 Firepower 可扩展操作系统的安全。请参阅《思科 *FIREPOWER 4100/9300 FXOS* 强化指南》。