思科 FirePOWER 管理中心

思科 FirePOWER™ 管理中心通过一体式的集中简化管理，提高思科® 网络安全解决方案的效力。

产品概述

思科 Firepower 管理中心（前身为 FireSIGHT 管理中心）是运行在许多不同平台上的特定思科安全产品的管理中枢。它可以对防火墙、应用控制、入侵防御、URL 过滤和高级恶意软件保护进行全面、统一的管理。管理中心是面向以下解决方案集中管理事件和策略的地方：

- 思科 Firepower 下一代防火墙 (NGFW)
- 具备 FirePOWER 服务的 Cisco ASA
- 思科 Firepower 下一代 IPS (NGIPS)
- 面向 ISR 的思科 Firepower 威胁防御
- 思科高级恶意软件防护 (AMP)

思科 Firepower 管理中心提供有关您的网络中存在的用户、应用、设备、威胁和漏洞的丰富情报。它也使用这些信息分析网络的漏洞。然后它会根据具体情况，就应该要部署的安全策略以及应该要调查的安全事件，为您提供量身定制的建议。

管理中心提供易于使用的策略界面来控制访问和防范已知攻击。它集成了高级恶意软件保护和沙盒技术，可以提供工具来跟踪整个网络中的恶意软件感染。它将所有这些功能整合到单一管理界面中。从防火墙管理到应用控制，乃至恶意软件爆发调查与补救，都能在这个单一平台上轻松实现。

图 1. 集中管理策略、事件和设备

企业级管理

思科 Firepower 管理中心发现不断变化的网络资源和操作的实时信息。您可以在全面掌握情况的前提下作出明智的决策（见图 1）。除了提供广泛的情报外，管理中心还可提供深入的详细信息，包括：

- **趋势和高级统计。**帮助您及时了解某个时间点的安全状况及变化情况（改善或恶化）。
- **事件详细信息、合规性和调查分析。**提供安全事件期间发生的事件的详细信息。帮助您改善防御，支持漏洞遏制工作并协助法律执行行动。
- **工作流程数据。**您可以将此数据轻松导出到其他解决方案，以改善事件响应管理。

功能和优点

特性	优点
统一管理多个解决方案中的多项安全功能	便于集中管理思科安全环境，包括： • 思科 Firepower 下一代防火墙 (NGFW) • 具备 FirePOWER 服务的 Cisco ASA • 思科 Firepower NGIPS • 面向 ISR 的思科 Firepower 威胁防御 • 思科 AMP
对多个安全功能进行集中策略管理	在单一策略中配置防火墙访问、应用控制、威胁防御、URL 过滤和高级恶意软件保护设置 方便策略管理，减少错误，并促进一致性 支持将单一策略部署到多个安全解决方案中
集成访问策略控制与思科身份服务引擎	基于 ISE 安全组标记、设备类型和位置 IP 以及快速遏制威胁控制访问 帮助您强制实现合规性、增强基础设施安全性并简化服务操作
一流的威胁情报	集成思科 Talos 团队的安全、威胁和漏洞情报进行最新的威胁防范 利用基于 IP 和基于 URL 的安全情报，应对新攻击方法 利用思科 Umbrella，实现网络边界外的威胁可视性 支持从第三方威胁订阅源和威胁情报平台注入和关联 STIX/TAXII 或平面文件格式的威胁情报
应用可视性与可控性	通过精准控制 4000 多个商业应用，进一步降低对网络的威胁 使用开源标准开放式应用 ID 获取自定义应用的详细标识和控制信息
多租户管理和策略继承性	创建多达 50 个管理域并提供独立的事件数据、报告和网络映射，通过基于角色的访问控制进行管理 通过每一级都继承上一级策略的策略层次结构，实施一致且高效的管理
报告和控制面板	通过可自定义的控制面板，提供自定义的基于模板的报告，实现所需的可视性 针对一般信息和焦点信息提供综合报警和报告 在超链接表格、图形和图表中显示事件和情景信息，方便分析使用 监控网络行为和性能来识别异常并维护系统运行状况
安全启动	安全启动是在系统启动时验证 FMC 硬件上运行的思科软件完整性的一种机制。如果签名缺失或软件无效，它将不会加载，启动将失败。（仅限 FMC 1000、FMC 2500、FMC 4500）

图 2. 面向多个安全功能的单一策略

出色的可视性和见解

如果看不到威胁，就无法进行防护。思科 Firepower 管理中心自动收集、整理并显示有关您的环境中所运行的一切事务的情景信息。表 1 展示了对传统安全技术所无法检测到的威胁途径的情景感知程度。这可让您深入了解您的网络，所获信息可用于您的保护策略，达到其他解决方案无法企及的保护级别。

表 1. 全堆栈可视性

类别	思科 Firepower 管理中心	典型的 IPS	典型的下一代防火墙
威胁	支持	支持	支持
用户	支持	支持	支持
Web 应用	支持	不支持	支持
应用协议	支持	不支持	支持
文件传输	支持	不支持	支持
恶意软件	支持	不支持	不支持
命令和控制服务器	支持	不支持	不支持
客户端应用	支持	不支持	不支持
网络服务器	支持	不支持	不支持
操作系统	支持	不支持	不支持
路由器和交换机	支持	不支持	不支持
移动设备	支持	不支持	不支持
打印机	支持	不支持	不支持
VoIP 电话	支持	不支持	不支持
虚拟机	支持	不支持	不支持
漏洞信息	支持	不支持	不支持

攻击前中后的管理

思科 Firepower 管理中心可在“整个攻击过程”（攻击前、攻击中和攻击后）提供统一管理。

攻击前

- 提供卓越的可视性，可洞见网络中所运行的一切事务，因此，您可以看到需要保护的对象
- 创建防火墙规则并控制 4000 多个商业及自定义应用在您的环境中的使用方式

攻击中

- 定义要部署的入侵防御级别、URL 信誉规则以及高级恶意软件保护组件
- 应用各种策略，例如：“当网络流量来自使用此特定应用的这个国家/地区，且含有文件附件，我将应用这个级别的入侵检测并分析文件是否含有恶意软件，如有必要，甚至将其发送至集成沙盒”

攻击后

- 生成受攻击感染的所有设备的图形表示
- 能够轻松创建自定义规则来阻止攻击进一步发展
- 提供对恶意软件的详细分析，以妥当地进行补救

安全管理自动化，实现动态防御

思科 Firepower 管理中心可持续监控您网络中的变化。它简化了操作并提高了安全性：

- 自动关联新的攻击事件与您的网络漏洞，警示您可能已经得手的攻击。让安全团队可以专注于最重要的事件。
- 分析网络漏洞并自动建议落实适当的安全策略您可以根据不断变化的情况调整您的防御，并实施针对您的网络量身定制的安全措施。
- 关联来自网络、终端、入侵和安全情报源的具体事件。如果个别主机出现已被未知攻击损害的迹象，您将收到警报。
- 应用文件策略条件。如果符合，它会自动分析文件来识别已知的恶意软件和/或发送该文件到集成沙盒以确定未知的恶意软件。

利用开放式 API 轻松集成

思科 Firepower 管理中心通过四个强大、功能丰富的应用编程接口，集成可行的第三方技术。API 提供以下功能的连接点：

- 将事件数据从管理中心移动到另一个平台，例如安全信息和事件管理 (SIEM) 解决方案。
- 使用第三方数据增强思科 Firepower 数据库包含的信息。这类数据可能包括来自活动扫描程序的漏洞管理数据或操作系统信息。
- 启动由用户定义的关联规则激活的工作流程和补救步骤。例如，您可以集成您的工作流程与网络访问控制 (NAC) 解决方案，来隔离受感染的终端或启动全数字化调查流程。
- 通过允许那些解决方案来查询管理中心数据库，支持第三方报告和分析。

这些 API 也用于集成许多思科安全产品和工作流程。其中包括思科 AMP Threat Grid 沙盒；用于识别数据和网络分段的思科身份服务引擎；以及互联网域名可视性的思科 Umbrella。

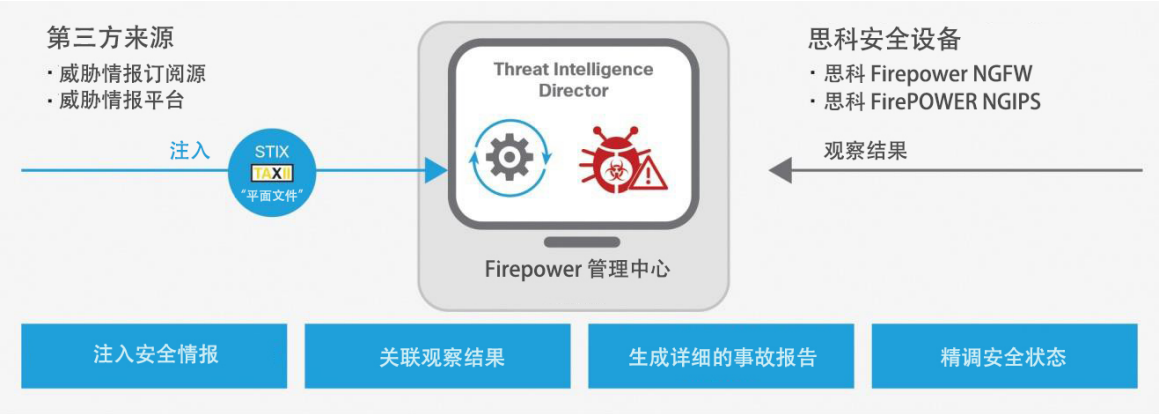
Threat Intelligence Director

Threat Intelligence Director 现可用于思科 Firepower 管理中心 (v6.2.1)。使用开放式 API，便于注入来自威胁订阅源和威胁情报平台 (TIP) 的第三方威胁情报。它支持结构化威胁信息表达式 (STIX) 和可信指标信息的自动交换 (TAXII) 或特定平面（未编排）文件格式。Threat Intelligence Director 将注入的情报解构到被观察对象 (IoC)，包括 IP (IPv4，IPv6)、域、URL 和 SHA-256。这些会被发布到思科安全设备，因而可以自动阻止内嵌恶意活动或监控网络以快速响应。

Threat Intelligence Director 通过以下思科安全设备利用可用的威胁情报：

- 思科 Firepower NGFW
- 思科 Firepower NGIPS

图 3. Threat Intelligence Director 集成第三方安全情报



要查看第三方网络威胁情报和 TIP 合作伙伴的最新列表，请访问思科技术联盟合作伙伴名单。

部署选项

思科 Firepower 管理中心可以部署为物理或虚拟设备，亦或从云部署（表 2）。您可以根据您的环境选择最适合的选项。相比同等条件的虚拟设备，物理设备一般管理的传感器数量更多，并且提供的事件存储能力更强。虚拟设备则更为便利，能够使用现有的 VM 基础设施。您还可以使用云计算服务来托管管理中心。这些服务让您不必在计算能力和数据库存储方面进行投资，就能管理安全性。它们将让您能够随着需求的变化，灵活地进行快速扩展。

在 NGFWv 上使用 Threat Intelligence Director 时，我们建议在主机硬件上安装 15 GB 内存，以实现最佳性能。

表 2. 部署选项

部署平台	最低版本级别
VMware ESX 和 ESXi 虚拟机监控程序	Version 5.x
KVM 虚拟机监控程序	版本 6.1
Amazon Web Services 云平台	版本 6.0

平台规格

思科 Firepower 管理中心有多种型号。您可以根据所要监控的传感器设备（物理设备和虚拟设备）数量、您的环境中的主机数量，以及预期的安全事件率，选择适合您组织的型号（参见表 3）。所有型号都具有相同的管理功能，包括：

- 集中的设备、许可证、事件和策略管理
- 基于角色的管理（基于管理员角色或用户组的分段或单独视图及职责）
- 带有定制和基于模板的报告的可定制控制面板
- 针对一般信息和焦点信息的综合报告和报警
- 在超链接表格、图形和图表中显示事件和情景信息
- 网络行为和性能监控
- 强大的高可用性选项，可帮助确保避免出现单点故障
- 关联和补救功能，可实现实时威胁响应
- 可与第三方解决方案和客户工作流（如防火墙、网络基础设施、日志管理、SIEM、故障通知单和补丁管理）集成的开放式 API

表 3 对比了可用的思科 Firepower 管理中心物理设备和虚拟设备的功能和吞吐量。

表 3. 思科 Firepower 管理中心型号

性能和功能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
受管理传感器的最大数量	10	50	250	300	500	750	25 10 2
MaxIPS 事件	2000 万	6000 万	6000 万	6000 万	3 亿	3 亿	1000 万
管理界面	100/100/1000 RJ-45						
网络接口	2 个 1 Gbps	2 个 1 Gbps	2 个 1Gbps 2 个 10Gbps SFP+	2 个 1Gbps 2 个 10Gbps SFP+	2 个 1Gbps 2 个 10Gbps SFP+	2 个 1Gbps 2 个 10Gbps SFP+	-
内存	8 GB（目前在售）	32 GB	64 GB	64 GB	128 GB	128 GB	-
CPU	4 核 Xeon	8 核 Xeon	6 核 Xeon	2 x 8 核 Xeon	2 x 10 核 Xeon	2 x 10 核 Xeon	-
事件存储空间	100 GB	900 GB	1.8 TB	1.8 TB	3.2 TB	3.2 TB	250 GB
最大网络映射大小（主机/用户）	2,000/2,000	50,000/50,000	150,000/150,000	150,000/150,000	600,000/600,000	600,000/600,000	50,000/50,000
最大流量（每秒流量）	2,000 fps	5,000 fps	12,000 fps	12000 fps	20,000 fps	20,000 fps	视情况而定*
网络接口	2 个 1 Gbps	2 个 10 Gbps 2 个端口	2 个 1 Gbps 2 个 10 Gbps（在思科商务中提供可选 SFP）	1 个 10 Gbps 2 个端口 1 个双端口 10Gbps SFP+	2 个 1 Gbps 2 个 10 Gbps（在思科商务中提供可选 SFP）	1 个 10 Gbps 2 个端口 1 个双端口 10Gbps SFP+	1 个 1 Gbps
安全启动	-	是	-	是	-	是	-

性能和功能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
冗余功能							
支持高可用性	无	支持	是	是	是	支持	否
双电源	无	支持	是	是	是	是	-
RAID 支持	否	HDD RAID 1	HDD RAID 5	HDD RAID 1	SSD RAID 6	SSD RAID 6	-
物理尺寸和环境参数							
外形	1RU	1RU	1RU	1RU	1RU	1RU	-
尺寸 深 x 宽 x 高（英寸）	27.19 x 16.9 x 1.7 英寸（69 x43 x 4.3 厘米）	29.8 x 16.9 x 1.7 英寸（75.7 x 43 x 4.3 厘米）	28.5 x 16.9 x 1.7 英寸（72.3 x 43 x 4.3 厘米）	29.8 x 16.9 x 1.7 英寸（75.7 x 43 x 4.3 厘米）	28.5 x 16.9 x 1.7 英寸（72.3 x 43 x 4.3 厘米）	29.8 x 16.9 x 1.7 英寸（75.7 x 43 x 4.3 厘米）	-
运输重量	33 磅（15 千克）	39 磅（17.7 千克）	35.6 磅（16.2 千克）	39 磅（17.7 千克）	35.6 磅（16.2 千克）	39 磅（17.7 千克）	-
功率（最大）	350W	770W	650W	770W	650W	770W	-
电源	110V、50/60 Hz 时电流最大为 9.5 A 220V、50/60 Hz 时电流最大为 4.75 A	100-240 VAC（额定） 90-264 VAC（最小/最大） 100 VAC 时最大 9.5 A 208 VAC 时最大 4.5 A	90 至 264 VAC 自适应范围 100-120 VAC（额定） 200-240 VAC（额定） 100VAC 时峰值 7.6 A 208VAC 时峰值 3.65 A	100-240 VAC（额定） 90-264 VAC（最小/最大） 100 VAC 时最大 9.5 A 208 VAC 时最大 4.5 A	90 至 264 VAC 自适应范围 100-120 VAC（额定） 200-240 VAC（额定） 100VAC 时峰值 7.6 A 208VAC 时峰值 3.65 A	100-240 VAC（额定） 90-264 VAC（最小/最大） 100 VAC 时最大 9.5 A 208 VAC 时峰值 4.5 A	-
气流	自前而后	自前而后	自前而后	自前而后	自前而后	自前而后	-
工作温度	10 °C 到 35 °C	5 °C 到 35 °C	5 °C~40 °C	5 °C 到 35 °C	5 °C~40 °C	5 °C 到 35 °C	-

虚拟思科 Firepower 管理中心的性能高度依赖于所选的虚拟环境：CPU、内存、存储等。

共享功能

- 集成的无人值守管理 (LOM)
- 集中管理思科下一代安全解决方案：NGIPS、NGIPS 及应用控制、NGFW

注：在处理具备 FirePOWER 服务的思科 ASA 产品时，思科 Firepower 管理中心仅管理部署的 FirePOWER 部分。

表 4 列出了管理中心能够管理的受支持的思科 Firepower 产品版本，以及相关硬件平台。

表 4. 支持的 Firepower 版本及其关联的平台

管理平台	软件版本级别	硬件平台
思科 Firepower 管理中心	**思科 Firepower 威胁防御 6.x (NGFW)**	**ASA 5500-X（ASA 5585-X 除外）** 思科 FirePOWER 4100 系列 思科 FirePOWER 9300
	FirePOWER 服务 6.x	**ASA 5500-X**
	思科 Firepower NGIPS 6.x	**思科 Firepower 7000** 思科 Firepower 8000
	面向 ISR 6.x 的 FirePOWER 威胁防御（思科 Firepower 服务）	**4000 系列 ISR** ISR G2
	FirePOWER 服务 5.4.x	**ASA 5500-X**
	思科 Firepower NGIPS 5.4.x	**思科 Firepower 7000** **思科 Firepower 8000**

虚拟机监控程序兼容性

思科 Firepower 管理中心虚拟设备支持表 5 中列出的虚拟机监控程序版本。

表 5. 虚拟设备虚拟机监控程序支持

虚拟机监控程序	版本和详细信息	虚拟思科 Firepower 管理中心版本
VMware vSphere	5.1、5.5、6.0 • ESXi 服务器 • vCenter 服务器（可选） • 适用于 Windows 或 Linux 的 vSphere Web 客户端、vSphere 客户端或 OVF 工具	5.4、6.0
KVM	Ubuntu 14.04 LTS Red Hat Enterprise Linux (RHEL) 7.1 版	6.1
Amazon Web Services	AWS 实例类型：c3.xlarge 和 c3.2xlarge	6.0.1、6.1

订购信息

许可

从 6.0 版开始，不再要求必须具备许可证密钥才能使用思科 Firepower 管理中心。5.4 版及更早版本将要求具备产品密钥 (PAK) 或智能密钥。升级到第 6.0 版将免除该要求。

思科智能网络支持服务

屡获殊荣的思科智能网络支持服务™ 让您的 IT 员工可以随时直接联系思科技术支持中心 (TAC) 工程师并访问 Cisco.com 资源。您可以收到快速、专业的答复以及解决严重网络问题所需的特别说明。

智能网络支持服务提供以下设备级支持：

- 思科 TAC 的专业工程师一年 365 天、每天 24 小时面向全球提供服务
- 随时访问 Cisco.com 中丰富的在线知识库、资源和工具
- 硬件更换选项包括 2 小时、4 小时和下一工作日 (NDB) 先行更换，以及返修 (RFR)
- 操作系统软件持续更新，包括已获许可的功能集中的次要版本和主要版本
- 通过思科 Smart Call Home 对选定设备实施主动诊断，发出实时风险通告

此外，通过可选的思科智能网络支持服务现场服务，我们可以派遣现场工程师到场安装更换部件，并帮助确保网络运行良好。有关智能网络支持服务的详细信息，请访问：
http://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html。

订购方法

表 6 提供了思科 Firepower 管理中心物理设备和虚拟设备以及备用硬件的订购信息。请查阅思科网络安全订购指南，了解其他配置选项和附件。

表 6. 订购信息

思科 Firepower 管理中心（硬件）设备	
部件号	**产品说明**
FS750-K9	思科 Firepower 管理中心 750 机箱，1 机架单元 (RU)
FMC1000-K9	思科 Firepower 管理中心 1000 机箱，1RU
FS2000-K9	思科 Firepower 管理中心 2000 机箱，1RU
FMC2500-K9	思科 Firepower 管理中心 2500 机箱，1RU
FS4000-K9	思科 Firepower 管理中心 4000 机箱，1RU
FMC4500-K9	思科 Firepower 管理中心 4500 机箱，1RU
思科 Firepower 管理中心（硬件）备件	
FS-PWR-AC-650W=	适用于 FS2000、FS4000 的思科 Firepower 650W 交流电源
FS-PWR-AC-779W=	适用于 FMC1000、FMC2500、FMC4500 的 770W 思科交流电源
思科 Firepower 管理中心（软件）虚拟设备	
FS-VMW-SW-K9	思科 Firepower 管理中心、虚拟 (VMWare) Firepower 许可证
FS-VMW-10-SW-K9	思科 Firepower 管理中心，虚拟 (Vmware) Firepower 许可证（适用于 10 台设备）
FS-VMW-2-SW-K9	思科 Firepower 管理中心，虚拟 (Vmware) Firepower 许可证（适用于 2 台设备）

要下订单，请访问思科订购主页。

保修信息

如需查看保修信息，请访问 Cisco.com 的产品保修页面。

思科服务

思科广泛提供各种服务计划，帮助客户快速制胜。这些创新型服务计划通过将人员、流程、工具及合作伙伴巧妙结合来实现，从而大幅提升了客户满意度。思科服务有助于保护您在网络上的投资，优化网络运营，并可为新的应用合理地配置网络，以提高网络智能化，增强业务能力。有关思科安全服务的详细信息，请访问 http://www.cisco.com/go/services/security。

思科 Capital

提供融资服务，助您实现目标

思科 Capital 可帮助您获得所需的技术来实现目标并保持竞争力。我们可以帮助您减少资本支出、加速业务发展、并优化投资和投资回报率。借助思科 Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。思科 Capital 可以为您提供一种可预测的支付方式。思科 Capital 目前已在 100 多个国家/地区推出融资服务。了解更多。

相关详细信息

有关详情，请参考以下链接：

- 思科 Firepower 管理中心
- 思科 Firepower 下一代防火墙
- 思科 Firepower 下一代 IPS (NGIPS)
- 思科高级恶意软件防护 (AMP)
- 面向 ISR 的思科 Firepower 威胁防御
- 思科安全服务

有关运营商环境中的思科 Firepower 的信息，请访问：http://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷

C78-736775-01 02/17