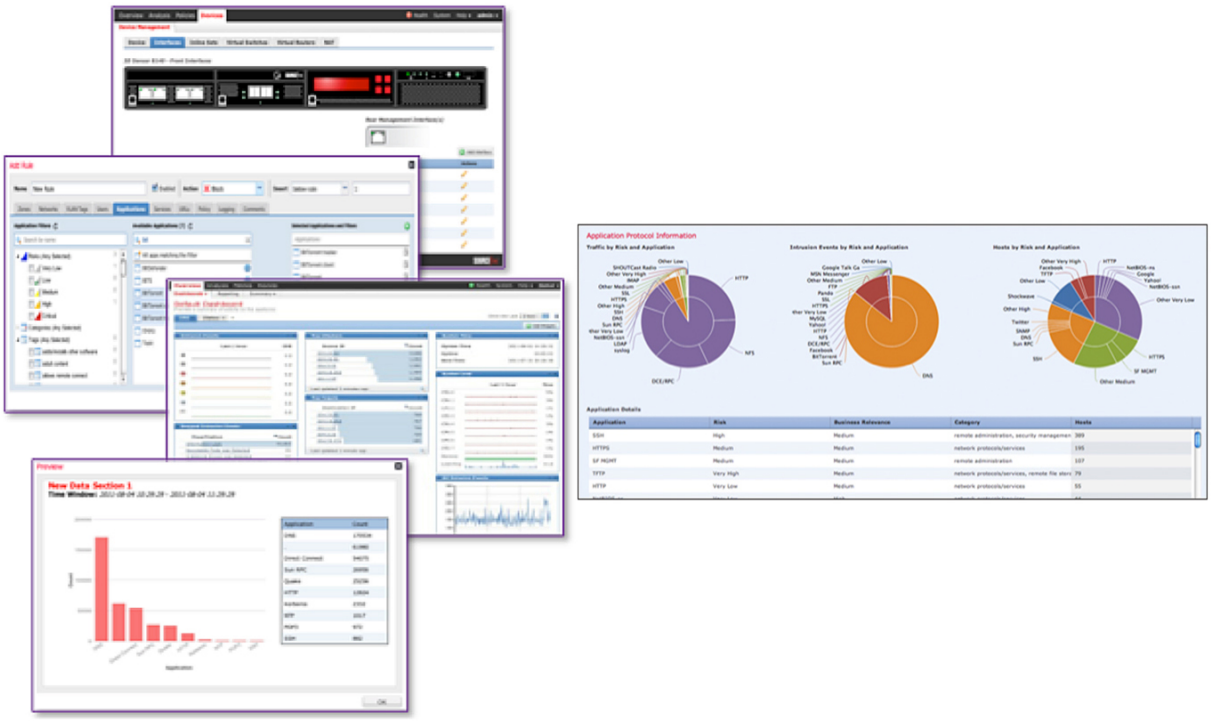
Cisco FireSIGHT 管理中心

产品概述

Cisco® FireSIGHT 管理中心可提供对所有网络元素和网络事件的整体可视性，包括物理和虚拟主机、操作系统、应用、服务、协议、用户、地理位置信息、内容和网络行为以及网络攻击和恶意软件。此安全管理控制台和数据存储库产品可为您实现安全运营提供集中的事件和策略管理点（图 1）。它能够使您自动汇聚并关联由您的网络中所部署的具备 FirePOWER 服务的 Cisco ASA 及 Cisco FirePOWER 物理或虚拟设备所生成的信息。Cisco FireSIGHT 管理中心可集中管理网络安全和操作功能，包括事件监控、分析、事件优先排序及报告等，以便您更好地保护您的企业。此外，它还可以简化运营，并自动执行多种常见的安全分析和管理任务，从而帮助您降低成本。

企业级管理

图 1. Cisco FireSIGHT 管理中心：集中的策略、事件和设备管理



Cisco FireSIGHT 管理中心可提供关于网络资源变更和操作变更的被动发现实时信息，从而可为做出明智决策提供完全的情景依据。在选择 Cisco FireSIGHT 管理中心设备时，应考虑环境中受监控的传感器设备和主机的数量，以及所要分析或存储的预期安全事件（见表 2）。所有配置均可提供以下管理功能：

- 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
- 稳健的高可用性选项，有助于避免出现单点故障
- 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、安全信息和事件管理 [SIEM]、故障通知单和补丁管理）集成的开放式 API

除了提供广泛的情报外，Cisco FireSIGHT 管理中心还可提供深入的详情，包括：

- **趋势和高级统计：**帮助经理和高层主管及时了解某个时间点的安全状况及其变化情况（改善或恶化）
- **事件详情、合规性和调查分析：**帮助了解整个安全事件过程中发生的所有情况，以便增强防御措施、加强漏洞控制，并为执法和诉讼提供协助
- **工作流：**轻松导出数据，以提升事件响应水平，从而改善响应管理

无与伦比的可视性和见解

表 1 展示了 Cisco FireSIGHT 管理中心如何针对多数传统安全技术无法检测到的威胁途径，提供全面的情景感知。

表 1. Cisco FireSIGHT 管理中心：完全堆叠可视性

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

安全管理自动化，实现动态防御

Cisco FireSIGHT 管理中心可持续监控网络的实时变化。它能够自动评估新威胁，以确定哪些威胁会对您的企业造成影响。然后，它能够重点围绕补救做出响应，并根据变化的状况，改变网络防御措施。它还能自动执行策略调整等关键安全活动，为您节省时间和精力，并确保防御和应对措施始终处于最佳状态。

部署模式的选择

Cisco FireSIGHT 管理中心可按物理或虚拟设备方式进行部署。物理部署的 Cisco FireSIGHT 设备能够支持最大限度的可集中管理的传感器和事件存储。虚拟部署的 Cisco FireSIGHT 设备能够确保对现有基础设施调配的便利性。它们可通过 VMware vSphere 调配进行轻松部署，并可在 VMware 基础设施内部进行部署，以保护物理网络中的资产。Cisco FireSIGHT 5.x 版虚拟设备可在 VMware ESX 和 ESXi 上托管。Cisco FireSIGHT 管理中心最多可管理 25 个物理或虚拟设备。

产品规格

表 2 对比了可用的 Cisco FireSIGHT 管理中心物理设备和虚拟设备的功能和吞吐量。

表 2. Cisco SireSIGHT 管理中心设备型号




功能	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS3500	FireSIGHT FS-VMW-SW
受管理设备的最大数量	10	35	150	25
IPS 事件的最大数量	2000 万台	3000 万台	1.5 亿台	-
事件存储	100 GB	125 GB	400 GB	-
最大网络映射（主机/用户）	2,000/2,000	50,000/50,000	300,000/300,000	-
最大流量（每秒流量）	2,000 fps	6,000 fps	10,000 fps	-
高可用性	无人值守管理 (LOM)	RAID 1、LOM、高可用性配对	RAID 5、LOM、高可用性配对	-

注意： 要使用传感器功能，必须配备 Cisco FireSIGHT 管理中心设备。所有传感器许可和管理均由 Cisco FireSIGHT 管理中心处理。

订购信息

表 3 展示了 Cisco FireSIGHT 管理中心物理设备和虚拟设备以及附加备用硬件的订购信息。

表 3. Cisco FireSIGHT 管理中心订购信息

Cisco FireSIGHT 管理中心（硬件）设备	
部件号	**产品说明**
FS750-K9	Cisco FireSIGHT 管理中心 750 机箱，1U
FS1500-K9	Cisco FireSIGHT 管理中心 1500 机箱，1U
FS3500-K9	Cisco FireSIGHT 管理中心 3500 机箱，1U
Cisco FireSIGHT 管理中心（硬件）备件	
FS-PWR-AC-650W=	Cisco FireSIGHT 650W 交流电源
Cisco FireSIGHT 管理中心（软件）虚拟设备	
FS-VMW-SW-K9	Cisco FireSIGHT 管理中心、虚拟 (VMWare) FireSIGHT 许可证

要下订单，请访问思科订购主页。

有关详情，请参考以下链接：

- 具备 FirePOWER 服务的 Cisco ASA 防火墙
- Cisco FirePOWER 设备
- Cisco FireSIGHT 管理中心
- 思科安全服务：http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html。

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 C78-732251-00 08/14