思科安全管理器

企业在安全运营方面正临着诸多新挑战。安全技术数量的增长，复杂性提高，加之从前专门从事安全管理的 IT 员工的减少和改行等极大地增加了人为错误出现的可能性，导致安全风险和事故。要应对这些挑战，安全运营团队应采用端到端的集成管理解决方案，以确保策略实施的一致性、迅速对安全事件进行故障排除，并对整个安全解决方案部署提供总结报告。

思科® 安全管理器是一个全面的管理解决方案，它不仅可以实现以上所有目标，还能实现其他目标。它提供可扩展、集中式的管理，使管理员可以高效管理多种思科安全设备，全面了解网络部署，并高度安全地与其他基本网络服务（如合规性系统和高级安全分析系统）共享信息。为了提高运营效率，思科安全管理器还包括一套强大的自动功能，如运行状况和性能监控、软件映像管理、自动冲突检测和故障通知单系统集成。

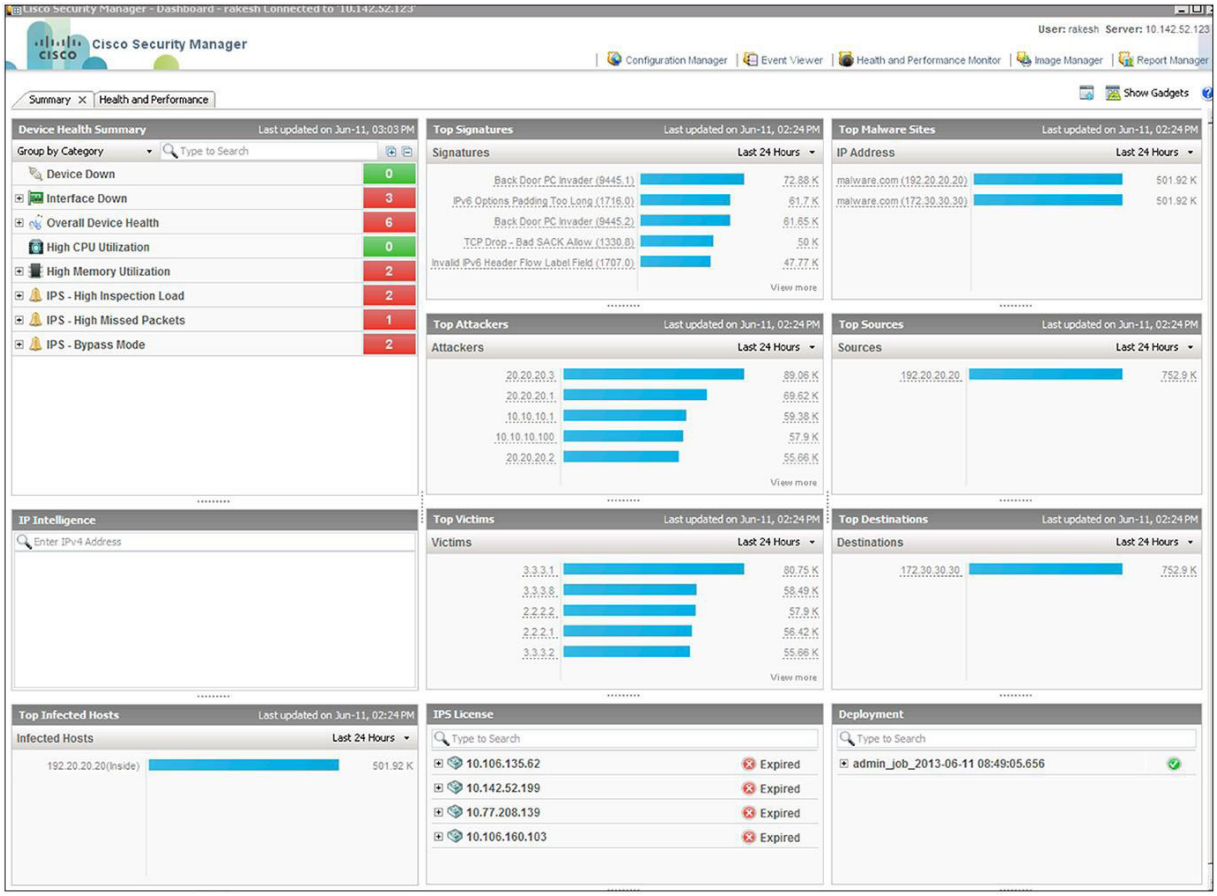
思科安全管理器支持多种思科安全设备，包括：Cisco ASA 5500 系列和 ASA 5500-X 系列自适应安全设备；Cisco IPS 4200、4300 和 4500 系列传感器；Cisco SR 500 系列安全路由器；以及 Cisco AnyConnect® 安全移动客户端。

思科安全管理器中的一些关键功能有助于进行简化、高效的安全管理。以下部分描述了这些功能：

控制面板

思科安全管理器控制面板（图 1）是一个基于构件的主屏幕，用户可在这个屏幕中纵览网络安全设置的运行状态、功能及其他关键性能指标。多个构件（例如设备运行状况摘要、头号入侵者、头号受害者、头号特征等）很好地总结了管理员需要关注和不需要关注的问题。这些构件作为任何安全就绪性分析的出发点。例如，在“特征”构件中，用户可以单击特定特征的已匹配次数，然后思科管理器将把用户带到事件查看器，用户可以在其中分析与该特征对应的事件。同样，管理员可以在“头号入侵者”构件中单击某个 IP 地址，然后查看与该 IP 地址有关的增值信息。因此总的来说，控制面板屏幕是思科安全管理器的安全管理员的出发点。此外，可对控制面板进行个性化定制，以适应每位管理员的需求。

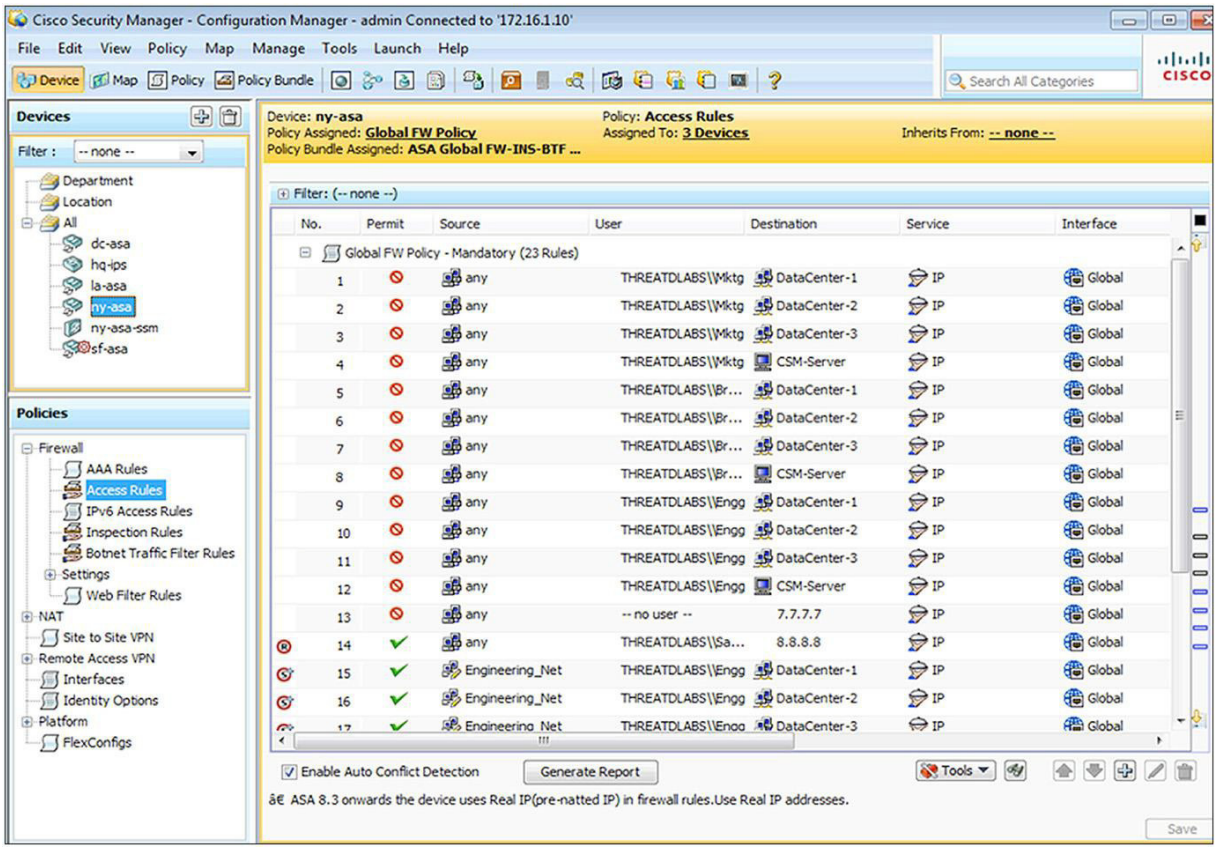
图 1. 思科安全管理器控制面板



集成策略和对象管理

思科安全管理器有助于实现安全规则和对象的重复使用，提高对整个部署中的安全威胁进行监控的能力，从而最大限度地降低出错的可能性并提高效率。管理员可以根据需要或按计划实施安全部署，并且可在必要时回滚至先前的配置。基于角色的访问控制和部署工作流程有助于确保遵守合规性流程（见图 2）。

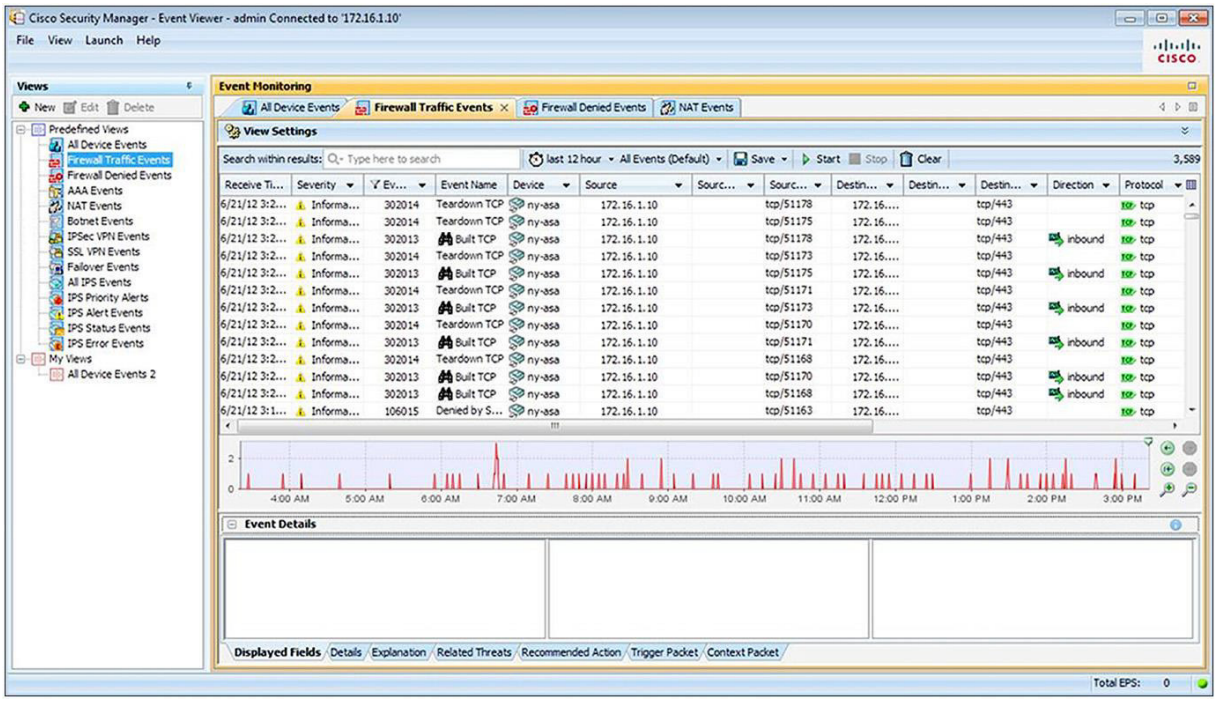
图 2. 思科安全管理器的安全策略管理



事件管理和故障排除

集成的事件管理有助于查看实时和历史事件，以便快速进行事件分析和故障排除，并且提供从事件到源策略的快速导航。此外，通过使用高级过滤和搜索功能，管理员能够快速识别并隔离引发关注的事件。事件管理器和配置管理器之间的交叉链接缩短了防火墙规则和入侵防御系统 (IPS) 特征的故障排除时间（见图 3）。

图 3. 思科安全管理器的事件管理和故障排除



思科安全管理器的事件管理器可以提供以下功能：

- 支持由 Cisco ASA 设备、思科防火墙服务模块 (FWSM) 和 Cisco Catalyst® 6500 系列 ASA 服务模块创建的系统记录消息，以及来自 Cisco IPS 传感器的安全设备事件交换 (SDEE) 消息
- 支持查看实时事件和历史事件
- 交叉链接至防火墙访问规则和 IPS 特征，可快速导航至源策略
- 预先捆绑的一组视图，支持防火墙、IPS 和 VPN 监控
- 可自定义的视图，支持监控选定的设备或选定的时间范围
- 直观的 GUI 控制，支持搜索、分类和过滤事件
- 可开启或关闭针对选定安全设备进行事件收集的管理选项
- ping、路由跟踪和数据包跟踪器等工具，用于进行进一步故障排除

有关多供应商环境的事件管理、事件关联和历史事件分析的详细信息，请访问：http://www.cisco.com/go/securitypartners。

报告

思科安全管理器可根据在整个安全部署过程中收集的事件和其他基本信息生成详细的系统报告（图 4）。表 1 列出了可用的系统报告。此外，管理员还可以定义并保存预定义的报告，以满足特定的报告需要。无论是系统生成的报告还是预定义的报告，都可以用 PDF 或 CSV 文件格式导出或按计划通过邮件发送。用户还可从特定的图表查找更多细节以查看其他信息，作进一步的分析。

图 4. 思科安全管理器中的报告管理器

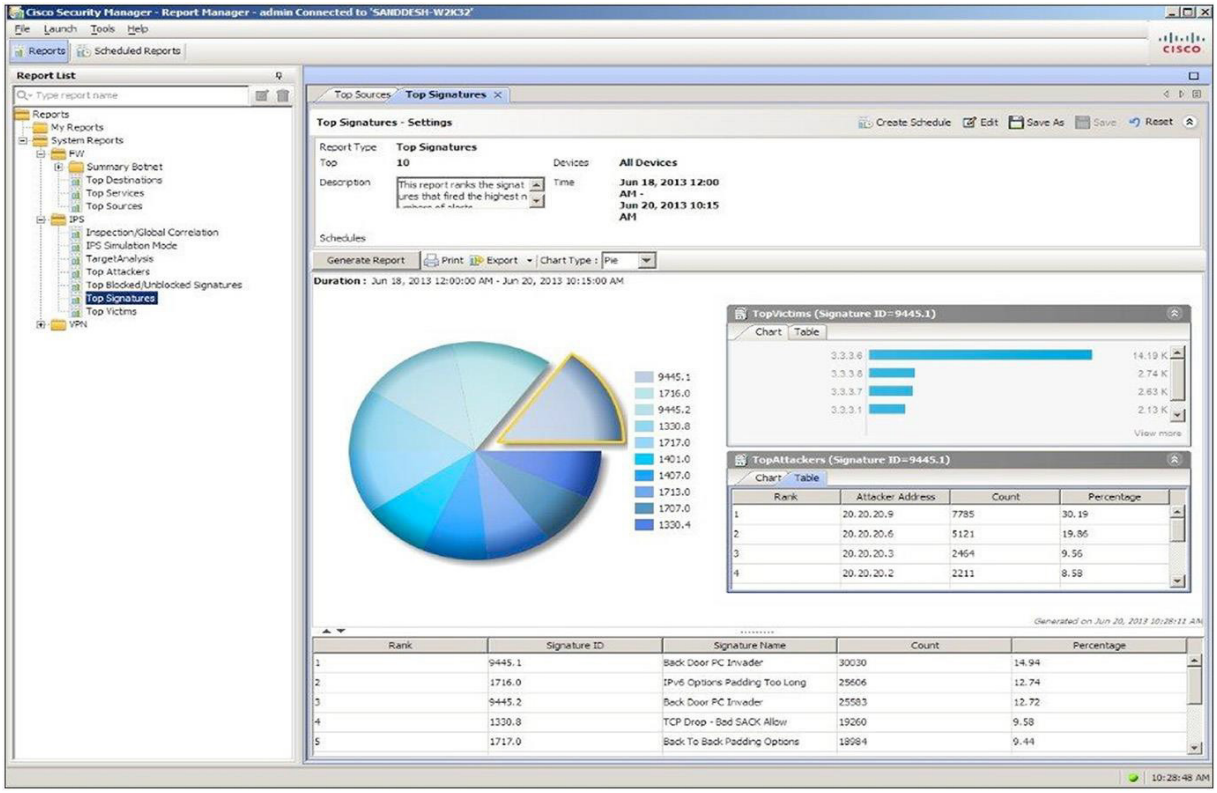


表 1. 思科安全管理器系统报告

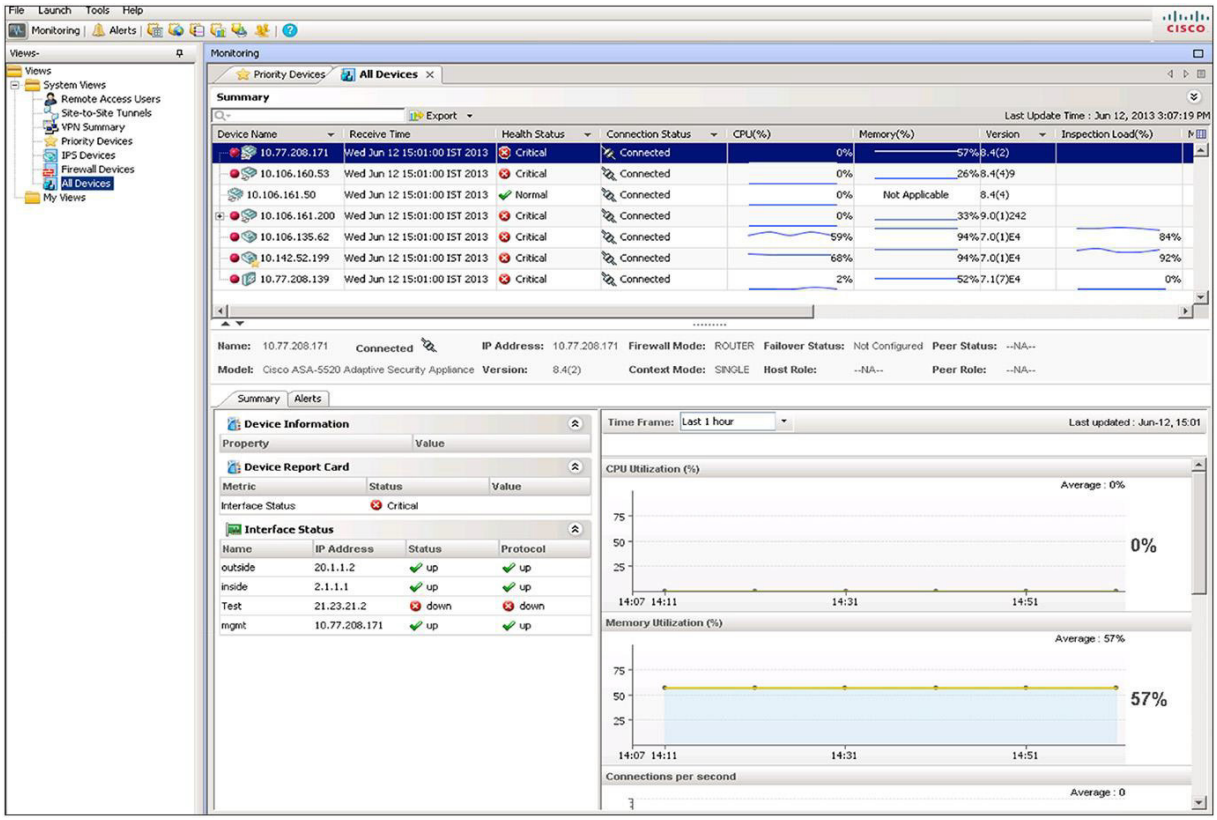
防火墙	IPS	VPN
• 受感染最多的主机 • 恶意软件最多的端口 • 恶意软件最多的网站 • 最常访问的网站 • 使用最多的服务 • 最主要来源	• 检测/全球互联 • IPS 模拟模式 • 目标分析 • 头号入侵者 • 被拦截/未被拦截的最多特征 • 头号特征 • 头号受害者	• 带宽占用最高的用户 (SSL/IPsec) • 持续时间最长的用户 (SSL/IPsec) • 吞吐量最高的用户 (SSL/IPsec) • 用户报告 • VPN 设备使用情况报告

运行状况与性能监控

通过持续分析安全环境并在达到预设的阈值时发送警报，集成的运行状况和性能监控可帮助管理员提高工作效率。可以为关键防火墙故障切换、IPS 传感器应用故障或过量 CPU 或内存利用率等事件设置自定义警报通知。

通过简单的彩色编码界面，管理员能够立即识别处于紧急状态下的所有设备，并查看经常监控的属性（例如 CPU 或内存利用率），以便快速确定整个安全部署中的所有设备的总体运行状况和性能。可根据需要使用详细图表来获取有关每个设备的运行状况、流量和性能指标的其他信息。图 5 显示了主监控界面。

图 5. 思科安全管理器中的运行状况与性能监控

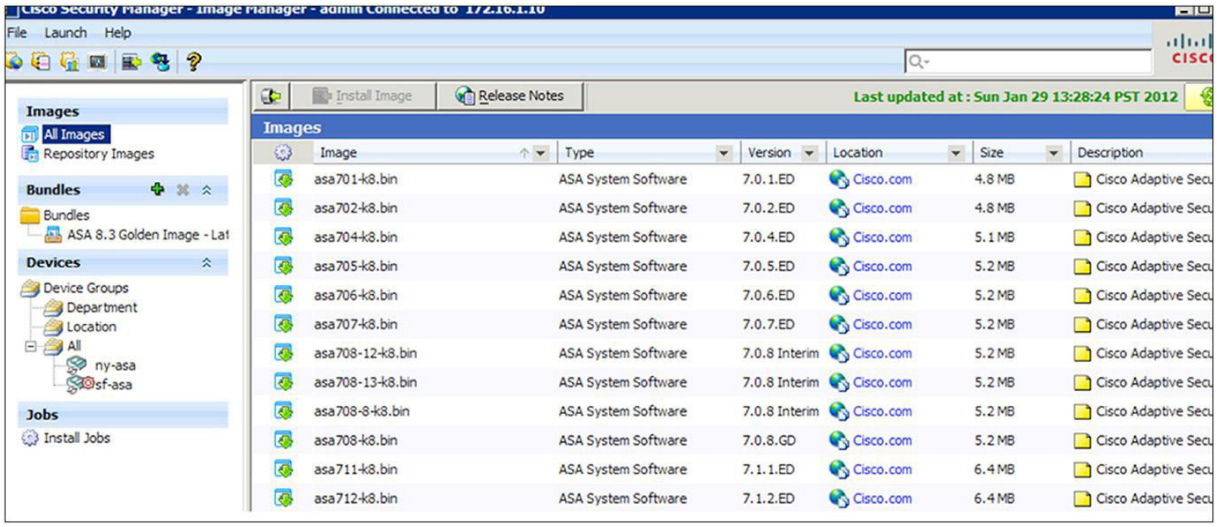


这些运行状况和监控功能也可供新的 Cisco ASA 集群功能可用。

软件映像升级

可使用直观向导升级防火墙软件映像。此向导引导管理员完成在下载映像、创建映像捆绑包及验证映像是否适合每个设备时所需的步骤。然后，此工具执行备份、关闭设备并执行更新。可以对每个防火墙单独执行更新，也可以成组运行更新以最大程度提高速度和效率。此过程是自动进行的，因此可以在夜间运行或在非关键时间运行，以减少运营环境中断。图 6 显示了思科安全管理器的映像管理主界面。

图 6. 思科安全管理器中的软件映像升级向导



对思科安全管理器基于 API 的访问

通过高度安全的基于 API 的访问，思科安全管理器可以与其他基本网络服务（如合规性系统和高级安全分析系统）共享信息，以简化安全操作并确保合规。使用表述性状态传输，外部防火墙合规性系统可以直接请求访问由 Cisco 安全管理器管理的任何安全设备的数据。这些第三方客户端程序也可以通过 API 在思科安全管理器 (CSM) 中添加、删除或修改防火墙访问策略和策略对象。这些 API 与 CSM 的工作流程功能无缝集成，因此在通过 CSM API 自动进行策略配置时管理员可以实施严格的控制。

其他功能和优势：

表 2 总结了思科安全管理器的其他功能和优势。

表 2. 思科安全管理器：其他功能和优势

功能	优势
防火墙配置	
管理思科安全部署	便于集中管理思科安全环境，包括： • Cisco ASA 5500 系列和 5500-X 系列自适应安全设备 • Cisco IPS 4200、4300 和 4500 系列传感器 • Cisco AnyConnect 安全移动客户端 • Cisco SR 500 系列安全路由器 • Cisco Catalyst 6500 系列防火墙服务模块和 ASA 服务模块 • 运行 Cisco IOS® 软件安全映像的思科集成服务路由器 (ISR) 平台

功能	优势
基于区域的策略	必要时在支持的设备平台上设置基于区域的防火墙策略。
僵尸网络流量过滤器	支持 Cisco ASA 平台上的思科僵尸网络流量过滤器，可在应用层检测和拦截僵尸网络的“回拨”活动。
与 Cisco TrustSec® 安全组标记集成	提供与 Cisco TrustSec 安全组标记的集成，以便思科安全管理器用户可在部署中配置详细且高度相关的策略。
Cisco ASA 集群	提供高级故障切换功能以支持多台 Cisco ASA 设备和负载平衡机制，从而缩短停机时间并提高可用性。
内容过滤	在基于 Cisco IOS 软件的设备平台上支持内容过滤，以根据深度的内容检测过滤流量。 支持使用单个规则表管理多个设备平台。
高效的策略定义	通过清楚地显示哪些规则与特定的来源、目标和服务流程相匹配（包含通配符），提高管理员定义策略的效率。
系统日志转发	除了思科安全管理器内置的事件查看器外，思科安全管理器还支持将 ASA 防火墙生成的日志转发至两个远程收集器。
简化的设置	通过允许从设备存储库或配置文件中导入设备信息、在软件中添加设备信息或从设备本身发现设备信息，来简化配置和初始的安全管理设置。
简化的操作	利用以下工具，可以在减少错误和优化安全环境的同时大幅减少手动任务： • 规则冲突检测、命中次数分析、规则组合器，以及其他用于分析和优化规则设置的强大工具。 • 可帮助确保无差错部署和流程合规性的基于角色的访问控制和工作流程。
接口角色	可对接口组应用规则策略并集中管理它们，以便最大限度地提高灵活性和可扩展性。
IPS 配置	
配置和更新策略	轻松高效地为以下各项管理基于 IPS 的配置和更新策略： • Cisco IPS 4200 和 4300 系列传感器 • Cisco ASA 高级检测和防御安全服务模块 (AIP-SSM) • Cisco ASA 高级检测和防御安全服务卡 (AIP-SSC) • Cisco Catalyst 6500 系列入侵检测系统服务模块 2 (IDSM-2) • Cisco IDS 网络模块 • Cisco IPS 高级集成模块 (AIM) • Cisco IOS IPS
特征更新	可以增量调配新的和更新的特征，然后将它们部署到企业中。
威胁研究	允许管理员在分发特征更新之前，根据从思科安全智能运营中心 (SIO)、Cisco Security IntelliShield® 告警管理器服务和 Cisco IPS 安全研究团队建议获得的分析见解来配置环境。
更新向导	允许根据状态和详细信息通知进行高效的自动化 IPS 更新、计划和策略分发
可重复使用的策略	可使 IPS 特征策略和事件操作过滤器能够分配到任何设备并被继承：所有 IPS 策略都可以分配给其他 IPS 设备并与其共享。
策略回滚	包括 IPS 策略回滚、配置存档以及特征的克隆或创建。
操作简单	提供一种在特征与为这些特征生成的事件之间轻松导航的方式；直观的用户界面提供用于调整和管理特征的简单机制。
风险评级类别	动态计算可以划分至某个风险范围并定义为某个类别的风险评级值。可将特征分配至某个风险评级类别，并可相应地为其分配在命中特征时要执行的操作。
全局事件操作	可将多个事件操作添加至某个风险评级类别，以便对该风险评级范围内的所有特征全局应用这些操作。而且，必要时还可从特征中过滤某个事件的特定操作。
特征注释	多个用户可向一个特征添加注释，以后可用合并的方式查看该签名的注释。
CSV 导出	为选定的 IPS 功能（例如特征、事件操作过滤器和特征数据设置）提供逗号分隔值 (CSV) 格式的导出，以便您在思科安全管理器服务器实例之间存储和交换此数据。
VPN 配置	
VPN 向导	轻松配置站点到站点 VPN、中心辐射型 VPN、全网状 VPN 和外部网 VPN。
支持各种常见 VPN 部署方案	支持常见 VPN 部署方案以及组加密传输 VPN (GET VPN)、动态多点 VPN (DMVPN) 和通用路由封装 (GRE) IP 安全 (IPsec)，包括动态 IP 和分层证书。
多情景配置	通过在位于多个地点的不同分支机构之间进行安全配置，提供策略分段和灵活性。
远程配置	集中管理 VPN。

功能	优势
效率和可用性功能	
通知单集成	可使用单个通知单标识符来标记多个通知单系统中进行的更改，以便在进行审计时轻松查询更改。
全局搜索	可在配置数据库中查找使用特定 IP 地址或服务的所有设备、策略和策略对象。
查找使用情况	除了提供有关所有使用某个特定对象的所有策略的详细信息外，还通过指向使用该策略对象的确切规则来帮助管理员快速查找有关对象的使用信息。
自动冲突检测	提供有关规则冲突的清晰信息以简化规则优化和故障排除过程。
IPv4 和 IPv6 交叉兼容性	支持配置统一的 IPv4 和 IPv6 策略及规则，以帮助加快部署并增强策略配置之间的兼容性。
集成事件管理	通过提供以下功能来帮助管理员监控状态和诊断安全信息： • 接收来自 Cisco ASA 设备的系统日志消息，以及来自 Cisco IPS 传感器的安全设备事件交换 (SDEE) 消息 • 支持查看实时事件和历史事件 • 交叉链接至防火墙访问规则和 IPS 特征，可快速导航至源策略 • 预捆绑的一整套防火墙、IPS 和 VPN 监控视图 • 可自定义的视图，支持监控选定的设备或选定的时间范围 • 直观的 GUI 控制，支持搜索、分类和过滤事件 • 可开启或关闭针对选定安全设备进行事件收集的管理选项 • 在环境中检测到 ASA CX 部署时启动 Cisco Prime™ 安全管理器；这使通过思科安全管理器来管理 CX 成为可能
报告管理器	支持系统报告和创建预定义的报告，可以对所有报告执行以下操作： • 以图表和网格形式查看 • 以 PDF 或 Excel 文件格式导出 • 按计划通过邮件发送 • 扫描以获取详细信息
批量操作	减少了包含大量设备的网络中的管理消耗。功能包括： • 批量导入和导出策略对象 • 批量添加离线设备 • 批量导入设备级重写 • 批量自动更新整个网络中部署的所有 Cisco ASA 设备的软件映像，为大规模部署更新提供一种更加快速且灵活一致的方式
设备分组	允许管理员根据业务功能或位置创建和定义设备组，然后将同一组内的所有设备作为单个设备进行管理。
策略对象管理器	一次定义网络地址、服务、设备设置、时间范围或 VPN 参数之类的对象，然后重复使用以避免手动输入值。
其他功能	
第三方设备支持	支持“非受管”终端和第三方设备
安全服务管理	管理集成安全服务，包括 VPN 服务质量 (QoS)、路由和网络准入控制 (NAC)。
多个应用视图	在应用中提供多个视图，以支持不同的使用案例和体验等级。
灵活的部署选项	可按需或按计划实施安全部署。
回滚	如果需要，可将部署回滚至先前的配置。
基于角色的访问控制	可定义和执行最多五个管理员角色；还可通过可选的思科安全访问控制服务器 (ACS) 获取更多角色名额。
工作流程	在部署策略时，可为每个管理员分配特定任务，并进行正式的变更控制和跟踪。
分布式部署	包括自动更新服务器和思科网络服务配置引擎，以简化对可能包含动态地址或 NAT 地址的大量远程防火墙的更新。
与思科云网络安全集成	使用户可以通过思科安全管理器定义防火墙规则，并提供了用于将网络流量转发到思科云网络安全的选项。
运营管理	包括 CiscoWorks 资源管理器基础 (RWAN)，以便为软件分发或设备清单报告等运营功能提供帮助。
运行状况与性能监控	持续分析普通和集群的安全环境，并在达到预设阈值时发送告警。
IP 情报	已将 IP 情报嵌入多项功能中。在报告管理器（分析特定图表时）以及运行状况和性能监控中，用户可从主屏幕的“头号入侵者”和“头号受害者”等构件中查看某个 IP 地址的 FQDN 和位置信息等增值信息。IP 情报本身也以可添加至控制面板的独立构件形式存在。

技术规格

如需获得思科安全管理器的详细硬件规格和估算指南，请访问：http://www.cisco.com/go/csmanager。

设备支持

表 3 总结了思科安全管理器支持的设备产品系列。有关包含有支持的设备软件版本的详细列表，请参见“Supported Devices and OS Versions for Cisco Security Manager”（思科安全管理器 4.4 支持的设备和操作系统版本），网址为：http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html。

表 3. 思科安全管理器支持的思科设备概述

支持的设备
Cisco PIX 网络安全设备
Cisco ASA 5500 系列和 ASA 5500-X 系列自适应安全设备
思科集成服务路由器（包括 800、1800、2800 和 3800 系列）
思科集成服务路由器 G2（包括 1900、2900 和 3900 系列）
Cisco ASR 1000 系列汇聚服务路由器
Cisco 7600 系列路由器
Cisco 7500 系列路由器
Cisco 7300 系列路由器
Cisco 7200 系列路由器
Cisco 7100 系列路由器
Cisco 3200 系列路由器
Cisco 2600 系列路由器
Cisco Catalyst 6500 系列防火墙服务模块 (FWSM)
Cisco Catalyst 6500 系列 VPN 服务模块 (VPNSM)
Cisco 7600 系列/Catalyst 6500 系列 IPSec VPN 共享端口适配器 (VPN SPA)
Cisco Catalyst 6500 系列入侵检测系统服务模块 2 (IDSM-2)
Cisco IPS 4200 系列传感器
Cisco ASA 5500 系列的 Cisco AIP-SSM
Cisco ASA 5500 系列的 Cisco AIP-SSC
集成服务路由器的 Cisco IPS AIM
接入路由器网络模块 - 思科入侵检测系统 (NM-CIDS) 的 Cisco IPS 模块
Cisco Catalyst 3550、3560、3560E、3750、3750 城域系列和 4500 系列交换机；以及 Cisco Catalyst 4948 和 4948 10 千兆以太网交换机

订购信息

思科安全管理器产品公告介绍了许可选项和订购详情。公告发布位置：http://www.cisco.com/go/csmanager。

可订购的思科安全管理器最新版本为 4.7 版

思科服务

思科采用生命周期方法提供服务，并与合作伙伴共同提供种类繁多的安全服务组合，因此，企业可以设计、实施、运营和优化能够避免关键业务流程受到攻击和破坏、保护隐私并支持策略和合规性控制的网络平台。

思科服务有助于保护您在网络上的投资，优化网络运营，并合理地配置您的网络，使新的应用能够增强网络智能并拓展您企业的能力。有关思科服务的详细信息，请访问：http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html。

- **思科安全智能运营中心 (SIO)** 为预警威胁和漏洞情报与分析、Cisco IPS 特征和迁移技术提供了中心位置。请通过 http://www.cisco.com/security 访问 Cisco SIO 并将其加入书签。
- **Cisco Security IntelliShield 告警管理器服务**提供可自定义、基于 web 的威胁和漏洞告警服务，使企业可以轻松、及时地访问关于所在环境潜在漏洞的准确、可靠信息。
- **思科软件应用支持 (SAS) 服务**通过全天候提供技术支持和软件更新，使思科安全管理器保持正常运行。
- **思科安全优化服务**有助于组织将网络保持在最佳的运行状态。网络基础设施是敏捷和灵活业务的基础。思科安全优化服务支持不断发展的安全系统，在规划和评估组合、设计、性能调整及对系统变更提供持续支持过程中，能够应对不断变化的安全威胁。

思科安全管理器软件属于思科软件应用支持 (SAS) 服务协议的技术支持服务范围，包括以下方面：

- 无限制访问思科技术服务中心 (TAC)，获得一流的支持。技术支持由经过思科安全软件应用培训的思科软件应用专家提供。全年 365 天，每周 7 天，每天 24 小时，思科在全球范围内提供全天候支持。
- 注册后访问 Cisco.com，这里收集的应用工具和技术文档可帮助您诊断网络安全问题、了解新技术和最新的创新性软件增强功能。实用工具、白皮书、应用设计数据表、配置文档和案件管理工具有助于扩展您的内部技术能力。
- 访问应用软件错误修复和维护以及次要软件版本。

更多详情

有关思科安全管理器的详细信息，请访问 http://www.cisco.com/en/US/products/ps6498/index.html，或者与您的客户经理或思科授权技术提供商联系。您还可以发送邮件至 ask-csmanager@cisco.com。

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 C78-730892-01 08/14