

思科安全管理器 4.4

企业在安全运营方面正面临着诸多新挑战。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，它能对多个安全设备进行高级管理和快速故障排除。思科安全管理器提供可扩展的集中化管理，管理员可高效管理多种思科安全设备、全面了解网络部署并与其他基本网络服务（如合规性系统和高级安全分析系统）安全地共享信息。为了能最大限度地提高运营效率，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 和 ASA 5500-X 系列自适应安全设备；Cisco IPS 4200、4300 和 4500 系列传感器；思科安全路由器；以及 Cisco AnyConnect® 安全移动客户端。

功能和优势

表 1 总结了思科安全管理器 4.4 的其他功能和优势。

表 1. 思科安全管理器 4.4 的功能和优势

功能	优势
防火墙配置	
管理思科安全部署	可对思科安全环境进行集中化管理，包括： <ul style="list-style-type: none"> • Cisco ASA 5500 和 5500-X 系列自适应安全设备 • Cisco IPS 4200、4300 和 4500 系列传感器设备 • Cisco AnyConnect 安全移动客户端 • 思科安全路由器 • Cisco Catalyst® 6500 系列防火墙服务模块 (FWSM) 和 ASA 服务模块 (ASASM) • 运行 Cisco IOS® 软件安全映像的思科集成服务路由器 (ISR) 平台
基于区域的策略	可在支持的设备平台上部署基于区域的防火墙 (ZBF) 策略设置
僵尸网络流量过滤器	支持 Cisco ASA 平台上的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 TrustSec 安全组标记的集成，使思科安全管理器用户能够跨各种部署配置精细且高度相关的策略
集群	提供高级故障切换功能，以支持多台 ASA 设备和负载分担机制，从而减少停机时间并提高可用性
内容过滤	支持在基于 Cisco IOS 软件的设备平台上进行内容过滤，以便根据深度内容检测过滤流量 可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来源、目的地和服务流（包括通配符）匹配，可提高管理员定义策略的效率
简化的设置	通过从设备库或配置文件中导入设备信息、在软件中添加设备信息或在设备中找到设备信息，简化配置和初始安全管理设置
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： <ul style="list-style-type: none"> • 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 (RBAC) 和工作流程
接口角色	可将规则策略应用到多组接口并对规则策略进行集中管理，以最大程度地提高灵活性和可扩展性

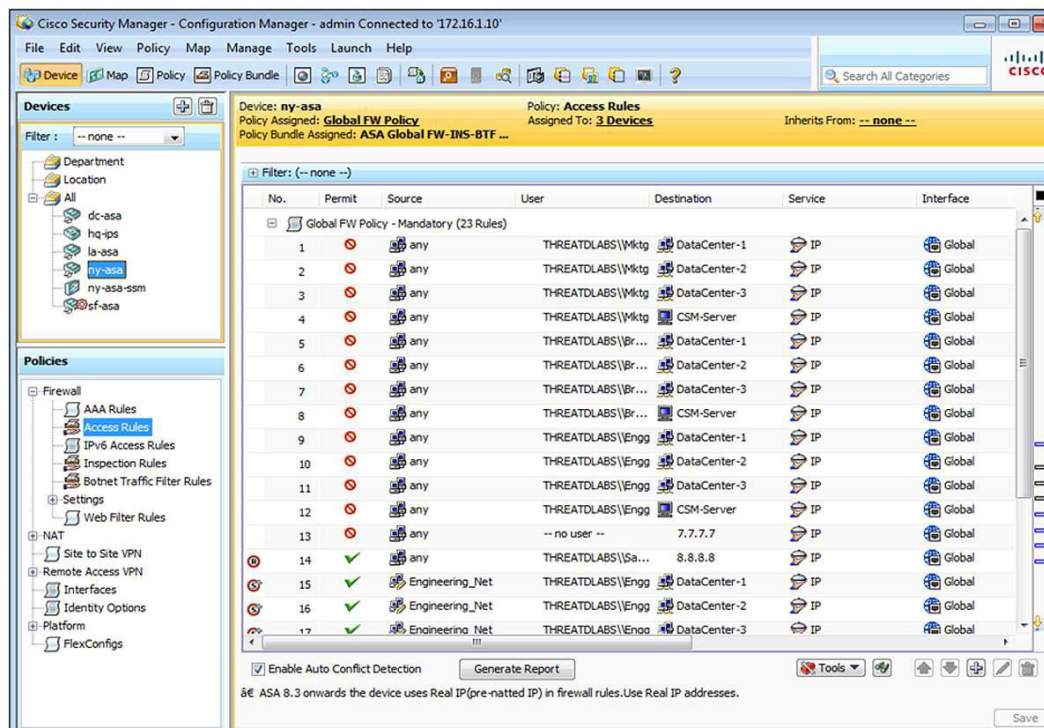
功能	优势
IPS 配置	
配置和更新策略	使管理员能够针对以下设备轻松高效地管理基于入侵保护系统 (IPS) 的配置和更新策略： <ul style="list-style-type: none"> • Cisco IPS 4200 和 4300 系列传感器 • Cisco ASA 高级检测和防御安全服务模块 (AIP-SSM) • Cisco ASA 高级检测和防御安全服务卡 (AIP-SSC) • Cisco Catalyst® 6500 系列入侵检测系统服务模块 2 (IDSM-2) • Cisco IDS 网络模块 • Cisco IPS 高级集成模块 (AIM) • Cisco IOS IPS
特征更新	可以在将特征部署到企业之前进行新特征和更新特征的增量供应
威胁研究	允许管理员在分发特征更新之前，根据从安全智能运营中心 (SIO)、Cisco Security IntelliShield 安全告警管理器服务和 Cisco IPS 安全研究团队建议获得的分析见解来调整环境
更新向导	能够根据状态和详细信息通知进行高效自动化的 IPS 更新、调度和策略分发
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；且所有其他 IPS 策略都可以分配给其他 IPS 设备并实现共享
策略回滚	包括 IPS 策略回滚、配置归档以及特征的复制或创建
CSV 导出	用于特征、事件动作过滤器和特征增量设置等精选 IPS 功能的逗号分隔值 (CSV) 导出可以促进此数据在不同思科安全管理器服务器实例之间的存储和交换
VPN 配置	
VPN 向导	提供站点到站点、中心辐射型、全网状和外联网 VPN 的简单配置
支持各种常见 VPN 部署方案	适用于常见 VPN 部署方案，支持组加密传输 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	允许对 VPN 进行集中管理
效率和可用性功能	
通知单集成	可使用单个票证标识符标记多个票证系统中进行的更改，使其易于查询和审核
全局搜索	允许查找配置数据库中使用特定 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该对象的策略的详细信息外，还可以指向使用特定策略对象的确切规则，这样，管理员便能够快速查找对象的使用信息
自动冲突检测	提供有关规则冲突的清晰图像，以简化规则优化和故障排除
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	使管理员能够监控状态并对安全问题进行故障排除，包括： <ul style="list-style-type: none"> • 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，可用于监控选定设备或选定时间范围 • 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： <ul style="list-style-type: none"> • 以图表和网格形式查看 • 以 PDF/Excel 格式导出 • 按计划通过邮件发送
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： <ul style="list-style-type: none"> • 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 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

功能	优势
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	可对网址、服务、设备设置、时间范围或 VPN 参数等对象进行单次定义，然后进行重复使用，以避免手动输入值
其他功能	
第三方设备支持	支持“非经管”端点和第三方设备
安全服务管理	允许管理集成安全服务，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经验等级
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	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 资源管理器要素 (RME)，以帮助执行软件分发或设备清单报告等运营功能
运行状况和性能监控	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

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。管理员可按需或按计划实施安全部署，并根据需要回滚至先前的配置。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 1）。

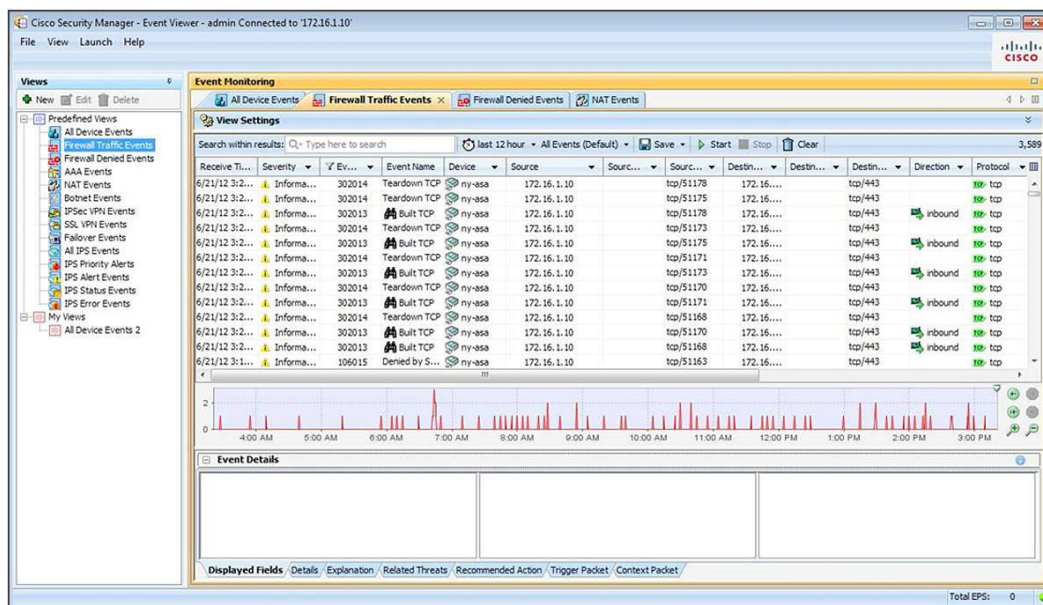
图 1. 思科安全管理器 4.4 的安全策略管理



事件管理和故障排除

集成事件管理有助于查看实时和历史事件，以进行快速事件分析和故障排除，并提供从事件到源策略的快速导航。此外，通过高级过滤和搜索功能，管理员能够快速识别和查出关联的事件。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 IPS 特征的故障排除时间（见图 2）。

图 2. 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（图 3）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。表 2 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。无论系统生成的报告还是预定义的报告，所有报告都可以 PDF 或 CSV 文件格式导出或通过电子邮件按计划发送。

图 3. 思科安全管理器中的报告管理器

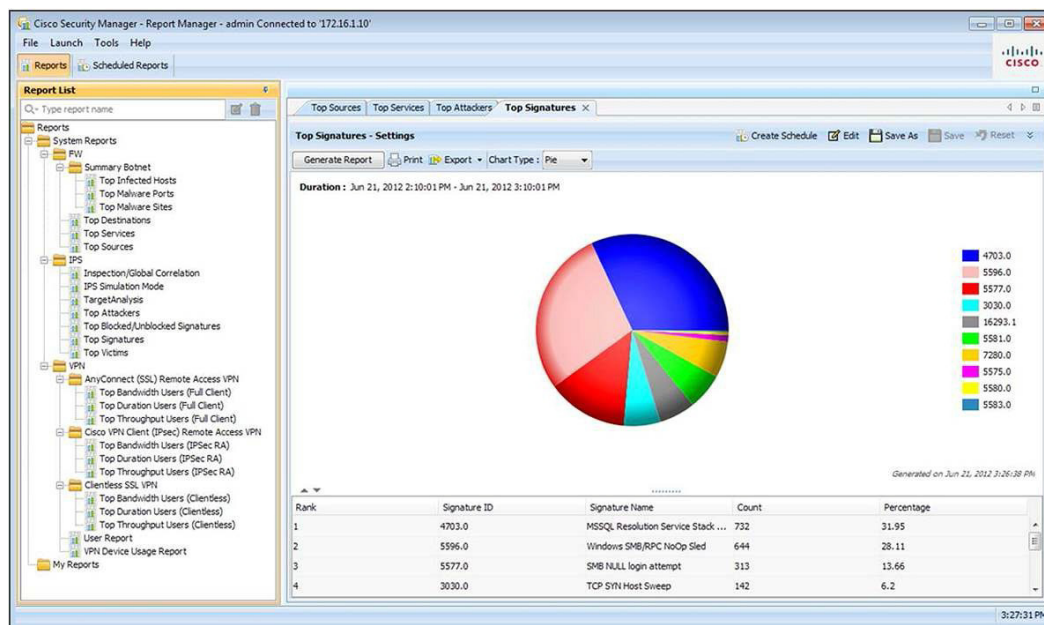


表 2. 思科安全管理器系统报告

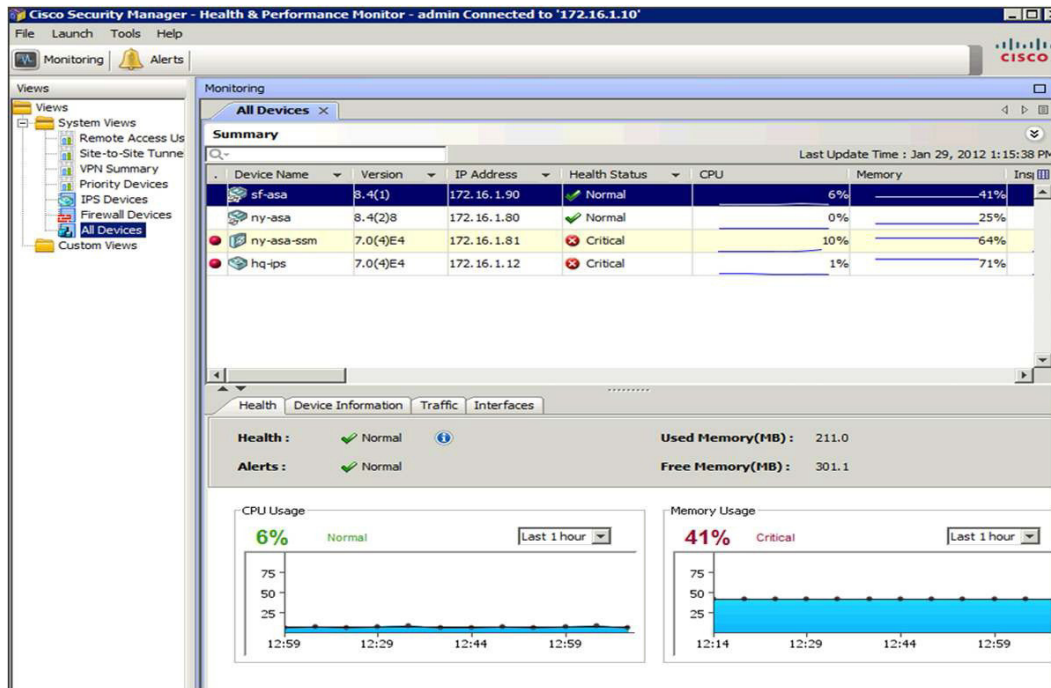
防火墙	IPS	VPN
<ul style="list-style-type: none"> ● 受感染最多的主机 ● 恶意软件最多的端口 ● 恶意软件最多的网站 ● 最常访问的网站 ● 使用最多的服务 ● 最主要来源 	<ul style="list-style-type: none"> ● 检测/全球互联 ● IPS 模拟模式 ● 目标分析 ● 头号入侵者 ● 被拦截/未被拦截的最多特征 ● 头号特征 ● 头号受害者 	<ul style="list-style-type: none"> ● 带宽占用最高的用户 (SSL/IPsec) ● 持续时间最长的用户 (SSL/IPsec) ● 吞吐量最高的用户 (SSL/IPsec) ● 用户报告 ● VPN 设备使用情况报告

运行状况和性能监控

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。

通过简单的颜色编码界面，管理员能够立即识别临界状态下的所有设备，并查看常用的监控属性（例如 CPU 或内存利用率），以快速确定安全部署过程中所有设备的一般运行状况和性能。可根据需要使用详细图表来获取有关各设备运行状况、流量和性能指标的其他信息。图 4 显示了主监控界面。

图 4. 思科安全管理器中的运行状况与性能监控

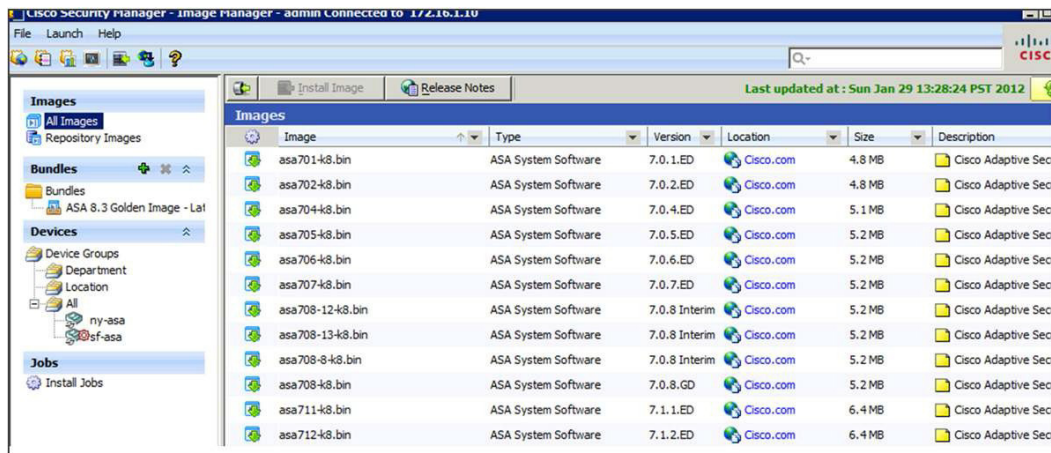


这些运行状况和监控功能也可供新的 ASA 集群功能可用。

软件映像升级

可使用直观向导升级防火墙软件映像。该向导将引导管理员完成下载映像、创建映像捆绑以及确保映像适合各设备所需的步骤。然后，该工具将执行备份、停止设备并执行更新。可对每个防火墙分别执行更新，也可以成组运行更新，以最大程度地提高速度和效率。该过程自动完成，因此可以通宵运行或在非关键时间运行，以尽量减少运营环境的中断。图 5 显示了思科安全管理器的主映像管理界面。

图 5. 思科安全管理器软件映像升级



对思科安全管理器基于 API 的访问

基于 API 的访问使思科安全管理器可以安全地与其他基本网络服务（如合规性和高级安全分析系统）共享信息，从而简化其安全运行和合规性。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。

技术规格

如需获得思科安全管理器 4.4 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 4.4 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 4.4”（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 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 (VPN SM)
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，4500、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>。

思科安全管理器标准版

思科安全管理器专业版

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，优化网络运行，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)** 为威胁和漏洞情报及分析、Cisco IPS 特征和迁移技术的早期预警提供中心位置。请通过 <http://www.cisco.com/security> 访问 Cisco SIO 并将其加入书签。
- **Cisco Security IntelliShield 安全告警管理器服务** 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** 可帮助组织始终保持最佳网络运行状态。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 4.4 的更多信息，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。

 思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1110R)

美国印刷

C78-727090-00 03/13