白皮书

思科安全管理器：升级至 4.X 版本以获得新的报告、监控、分析及其他功能

您将了解到的信息

思科安全管理器是一款功能强大而又方便易用的解决方案，用于为思科防火墙、虚拟专用网 (VPN) 和入侵防御系统 (IPS) 集中调配各种设备配置及安全策略。此解决方案可有效管理 10 台设备以下的小型网络，也可扩展为有效管理包含数千设备的大型网络。对于使用思科安全管理器早期版本的用户，最新的 4.X 版本提供了许多令人信服的升级理由，本白皮书概述了各种有益的功能。

概述

多年来，思科安全管理器从一款策略管理应用发展为成熟的安全管理套件。现在，此产品的 4.x 版本不仅有助于配置设备，而且支持安全专家监控设备的健康和效力、提供设备级安全报告，并使保持最新的软件和安全更新变得更加容易。如果您当前使用思科安全管理器的 3.x 系列，您将发现最新版本拥有全面而有用的功能（图 1），可帮助您管理安全操作。

思科安全管理器是一个全面的安全解决方案，旨在轻松地同时管理多项安全服务。通过各种管理功能和用户友好的界面，思科安全管理器使安全操作管理更高效，并且有助于做出更明智策略决定。

图 1. 4.x 版本推出的思科安全管理器功能

以下部分总结了最新的 4.x 版本中添加的功能

改进的配置管理器

思科安全管理器的配置管理器自 3.x 以来已得到显著改进。添加了多项功能，以简化策略管理和提高运营效率。其中一项功能是自动冲突检测，使用此功能可以维护一个清晰、有效的策略表。自动冲突检测流程可以检测思科安全管理器中一段时间内配置的大量策略，以及识别可以删除的冗余规则。另一项功能是策略捆绑，它使在数百台设备之间共享策略变成一项非常容易的任务。用户可以将多个策略分组成一个捆绑包，然后可以一次将该捆绑包分配给数百台设备。同样，自 3.x 以来，添加了多项其他功能来帮助有效管理最新的思科安全设备。

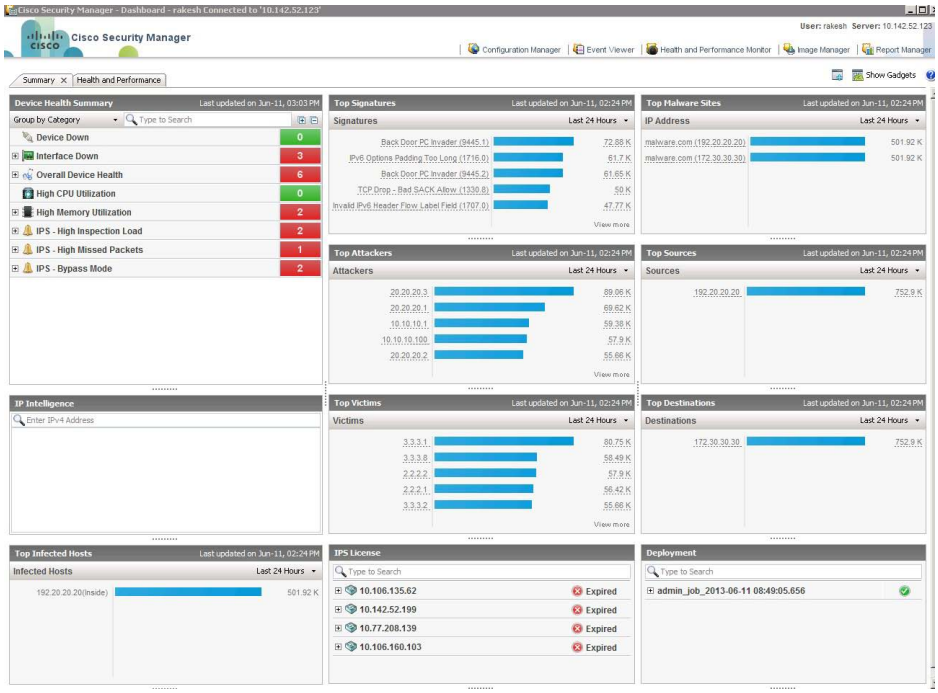
图 2. 思科安全管理器：自动冲突检测

控制面板

思科安全管理器控制面板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）和其他类似构件很好地总结了管理员需要担心和不需要担心的问题。这些构件作为任何分析的出发点。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，用户可以在“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，控制面板屏幕实际上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，以适应每位用户的需求。

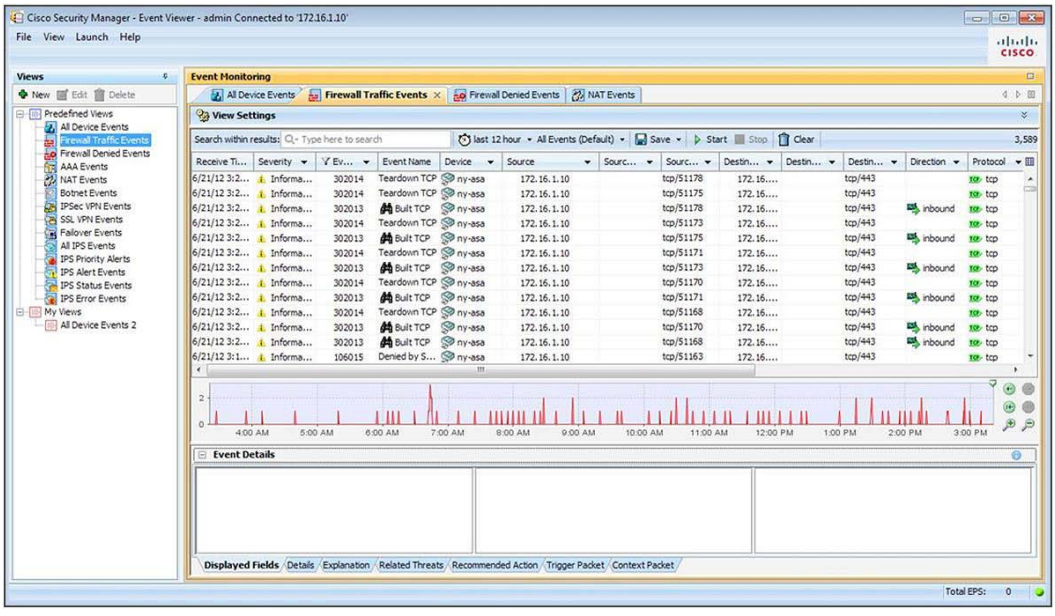
图 3. 思科安全管理器控制面板



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 4）。

图 4. 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

报告

思科安全管理器（图 5）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 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向下挖掘以查看其他信息，作进一步的分析。

图 5. 思科安全管理器中的报告管理器

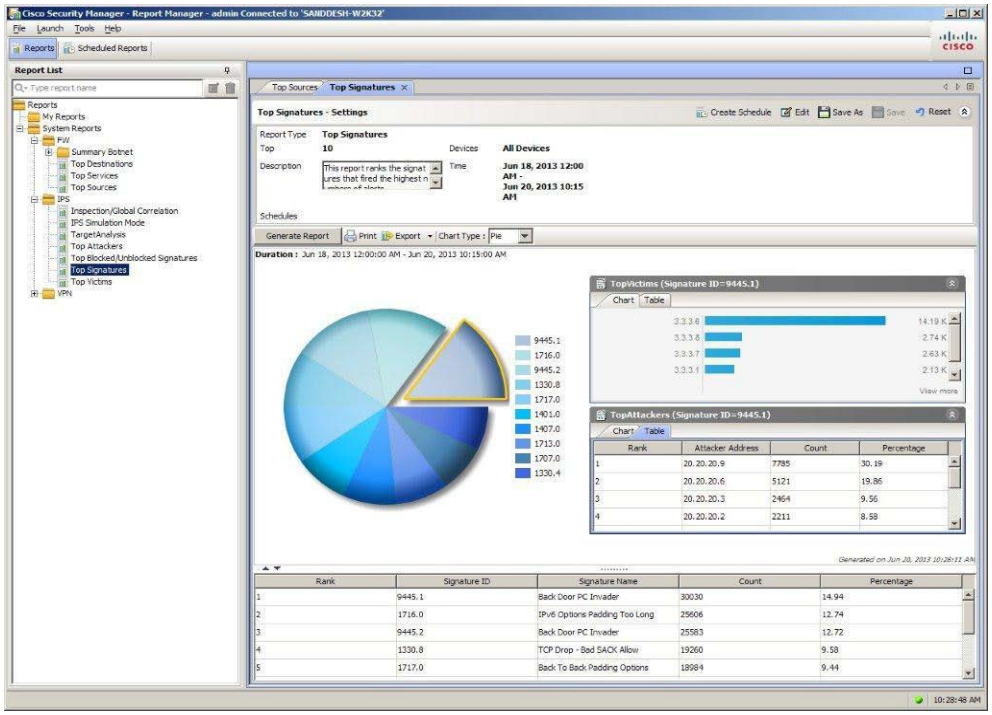


表 1. 思科安全管理器系统报告

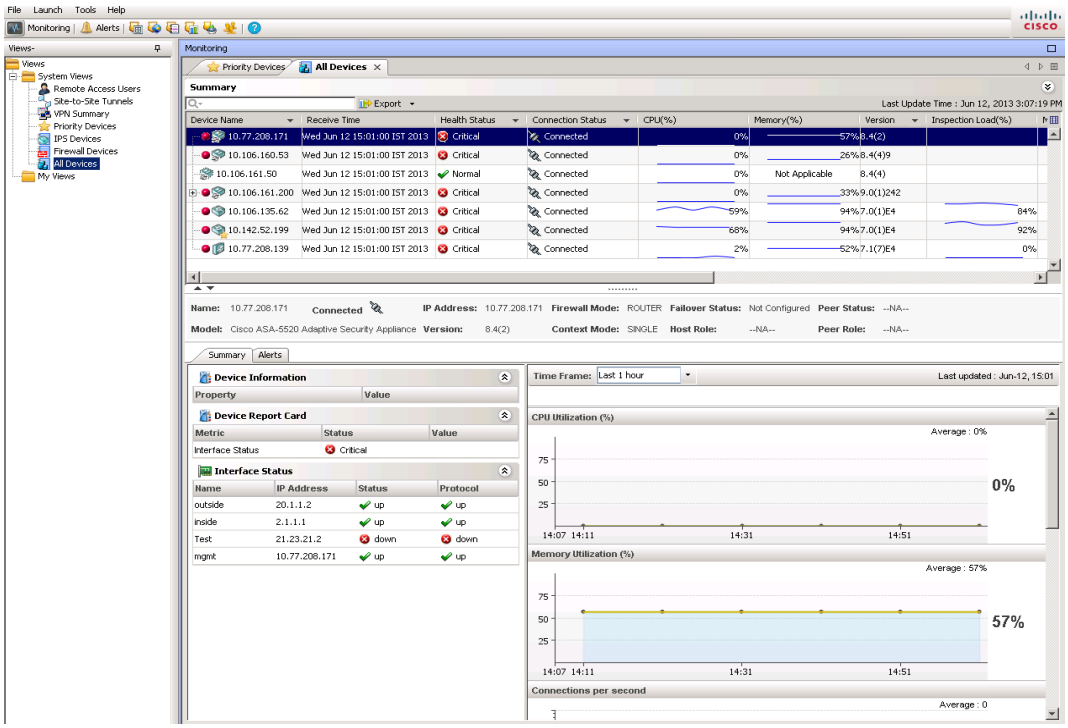
防火墙	IPS	VPN
• 受感染最多的主机 • 恶意软件最多的端口 • 恶意软件最多的网站 • 最常访问的网站 • 使用最多的服务 • 最主要来源	• 检测/全球互联 • IPS 模拟模式 • 目标分析 • 头号入侵者 • 被拦截/未被拦截的最多特征 • 头号特征 • 头号受害者	• 带宽占用最高的用户 (SSL/IPsec) • 持续时间最长的用户 (SSL/IPsec) • 吞吐量最高的用户 (SSL/IPsec) • 用户报告 • VPN 设备使用情况报告

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 6 显示了主监控界面。

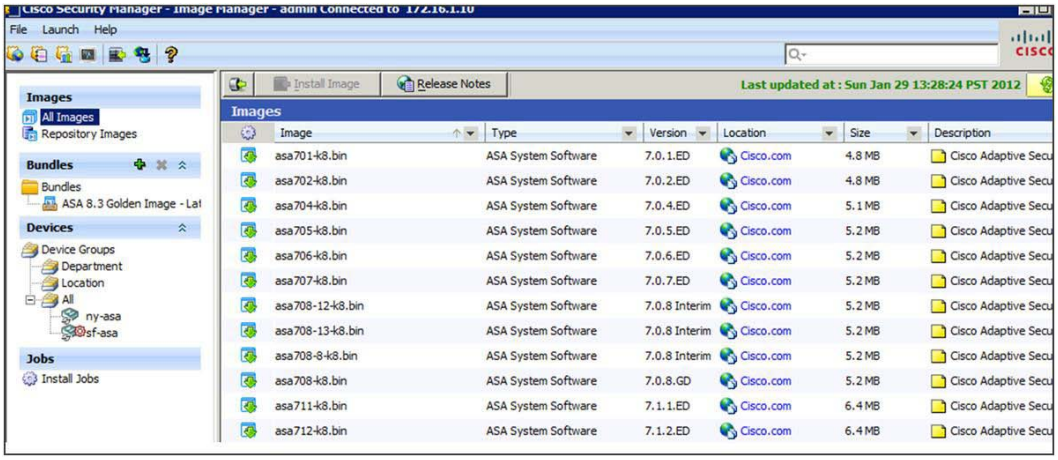
图 6. 思科安全管理器中的运行状况与性能监控



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 7 显示了思科安全管理器的映像管理主界面。

图 7. 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

如需获得支持的设备和设备软件版本的详细列表，请参阅“Supported Devices and OS Versions for Cisco Security Manager”（思科安全管理器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。

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。

提供两个产品包：

- 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 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**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 C11-731704-00 05/14