思科 S 系列网络安全设备的高级网络报告

简介

高级网络报告是一款附加报告解决方案，可为思科® S 系列网络安全设备生成的日志快速创建索引并进行分析。这款基于 Splunk 的工具可为具有较高流量和存储需求的客户提供可扩展的报告，让报告管理员能够收集网络使用情况和恶意软件威胁的详细信息。

基于目录组的报告

借助高级网络报告，管理员可以根据 Active Directory 等中央身份验证服务器中定义的组或用户 ID 生成报告。可以根据身份验证组定义的职能或地区限制，轻松创建报告。可以创建仅允许经理查看一组定义的目录组（例如他们的下属）的角色，从而保护不属于这些组的个人的隐私。

详细的第 4 层流量监控器 (L4TM) 可视性

高级网络报告支持管理员运行有关非网络端口活动的报告。这些 L4TM 报告可连接与特定端口和用户相关联的主机，并且可用于确定与非标准端口相关的恶意行为，无需使用许多传统网络安全解决方案。

SOCKS 报告

对于使用 SOCKS 代理设置的客户，高级网络报告可让管理员获取有关 SOCKS 流量的信息。

历史数据导入

在进行取证调查时，可以将历史日志导入到高级网络报告中。任何时间段的日志均可导入报告工具中以供分析使用，从而使人力资源和法律部门能够执行跨越多年的取证调查。如果需要，管理员可以调整特定用户的网络活动。

应该如何使用高级网络报告？

思科 M 系列和 S 系列设备上的本地报告可满足大多数客户的报告需求。高级网络报告是备选的报告解决方案，适用于需要为高事务量提供扩展存储或基于目录组的报告的客户。高级网络报告的格式与 S 系列和 M 系列设备本地的报告格式相同。

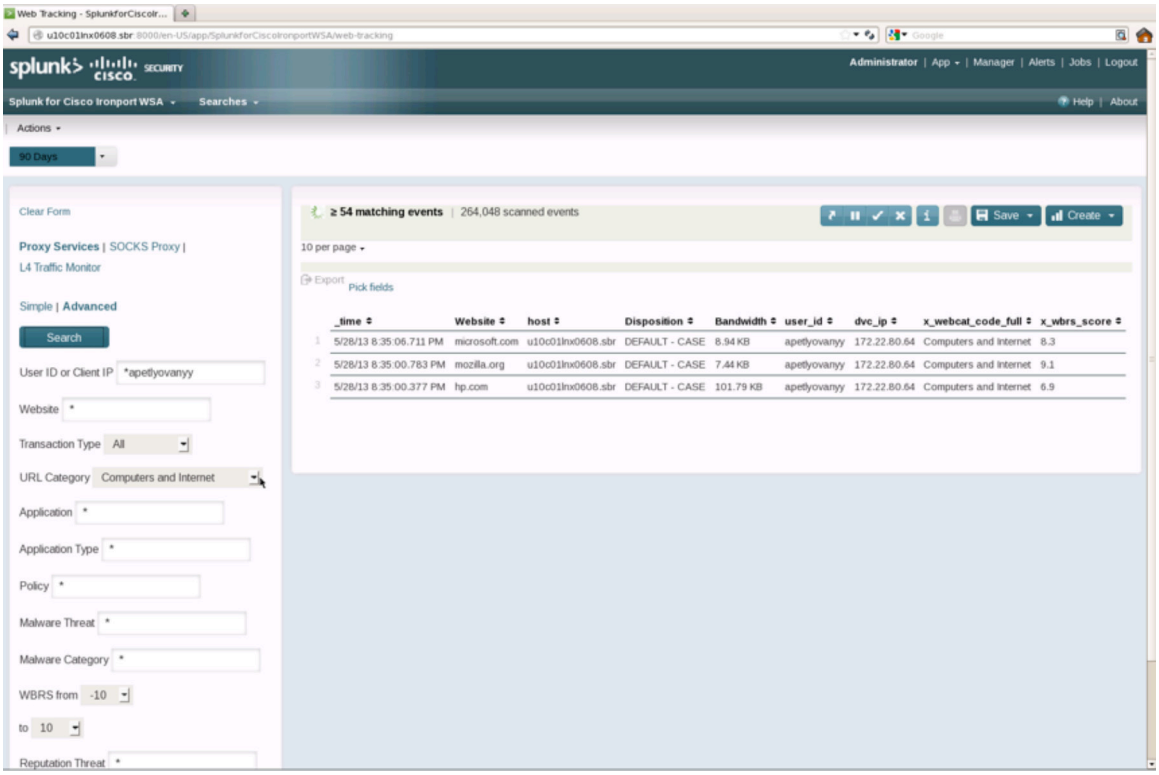
思科高级网络报告的最新版本中包括哪些功能？

新增报告功能。现在，高级网络报告可提供与运行 AsyncOS® 7.7 的思科网络安全设备相同的报告。这样，报告功能不仅可提供 SOCKS 报告，而且还能对 SOCKS 与 L4TM 事务进行网络跟踪和基于表单的搜索。

Splunk 5.0 支持。高级网络报告受 Splunk 5.0 平台支持。

高强度性能测试。思科使用海量数据测试了 WSA 高级网络报告功能，并发布了报告加载时间。在用户指南开头的“调整和扩展建议”部分可以找到这些测试结果。

图 1. 被阻止的 URL 类别和事务的 Splunk 报告



系统要求

在 Windows 和 Red Hat Linux 上运行的高级网络报告。不支持高级网络报告的生产实例虚拟化。推荐硬件可以是商用级别，最低规格如下所示。

- Intel x86 64 位芯片架构（带 2 个 CPU，每个 CPU 4 个核心，每核心 2.5-3 GHz）
- 16 GB RAM
- 4 个 300 GB SAS 10,000 RPM 硬盘，RAID 10（800 IOPS 或更高）
- 千兆以太网网络接口卡 (NIC)；建议为管理网络提供第二个 NIC

注：推荐拥有超过 25,000 名用户的组织使用这些硬件规格。

请与您的客户团队联系并参考文档，以便了解贵组织运行高级网络报告所需的硬件规格。

更多详情

如需请求获取高级网络报告的评估版本，请与您的思科客户团队联系。

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 C78-729104-00 07/13