思科网络安全设备 (WSA) 是否提供恶意软件/间谍软件防护？

文档编号：117952

作者：Dominic Yip 和 Siddharth Rajpathak，Cisco TAC 工程师。
2014 年 7 月 16 日

目录

问题

思科网络安全设备 (WSA) 是否提供恶意软件/间谍软件防护？

思科网络安全设备 (WSA) 针对间谍软件和基于 Web 的恶意软件提供业界最全面的网关防御， 涵盖从广告软件（会导致大多数可支持性问题并消耗大量网络资源）到木马、浏览器劫持、浏览器帮助程序对象、网络钓鱼、网址嫁接、系统监控器、键盘记录器、蠕虫等更恶意的威胁。

思科网络安全解决方案的主要优势包括：

1. 集成的第 4 层 (L4) 流量监控器能够以有线连接的速度扫描所有端口，检测并拦截恶意软件和回拨活动。 通过跟踪全部 65535 个网络端口，第 4 层流量监控器可有效阻止试图绕过端口 80 的恶意软件，还可以防止恶意的 P2P 和 IRC 相关活动。
2. 代理-层处理：思科网络安全设备还包含极高性能的 Web 代理，以及集成缓存和内容加速功能。 思科网络代理设备构建于思科的专有操作系统 AsyncOS 之上，可支持最多 10 万个并行连接，比基于 UNIX 的传统代理服务器多 10 倍。 作为一款 Web 代理，它支持在应用层进行全面的内容检测 - 这一要求对于确保准确防御基于 Web 的恶意软件至关重要。
3. 业界首个网络信誉过滤器，可提供强大的外层防御。 利用 SenderBase®，思科网络信誉过滤器可对 50 多种不同的 Web 流量和网络相关参数进行分析，以准确评估 URL 的可信度。 高级安全建模技术用于单独衡量每个参数，并按 -10 到 +10 的评分范围生成一个得分。 然后，它将根据信誉得分，动态应用管理员配置的策略。
4. 采用动态导向和流引擎（DVS 引擎）的加速签名扫描。 与依靠 ICAP 和多箱部署来确保恶意软件扫描的传统架构解决方案不同，思科 WSA 引入了 DVS 引擎，可提供集成的内部扫描解决方案。 此创新平台采用高级对象解析和导向技术以及流扫描和裁决缓存机制，相较于第一代基于 ICAP 的解决方案，其扫描吞吐量提高了 10 倍。
5. 业界领先的思科防恶意软件系统利用 Webroot 的 DVS 引擎和多种签名类型，可提供最佳防护功能来抵御各种基于 Web 的威胁： 从广告软件、浏览器劫持、网络钓鱼和网址嫁接攻击，到木马、系统监控器和键盘记录器等更恶意的威胁，无所不包。 WSA 可在网关提供业界最庞大的恶意软件签名数据库。

更新日期：2014 年 7 月 16 日 文档编号：117952