了解Secure Web Appliance恶意软件和间谍软件防护

目录

简介

本文档介绍思科安全网络设备(SWA)的全面恶意软件和间谍软件防护功能。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Cisco SWA旨在针对各种间谍软件和基于Web的恶意软件提供强大而全面的网关防御机制。它可以有效应对各种威胁，从因造成网络资源大量消耗和支持性挑战而臭名昭著的广告软件，到更严重的威胁，包括木马、浏览器劫持程序、浏览器助手对象、网络钓鱼、域欺骗、系统监控、按键记录器

和蠕虫。

SWA的主要竞争优势

集成第4层流量监控器(L4TM)

L4流量监控器能够以线速扫描所有网络端口（共65,535个），确保全面检测和阻止恶意软件和未经授权的通信尝试。此功能可以有效地阻止尝试绕过常用端口（如端口80和443）的恶意软件，还可抑制恶意点对点(P2P)和互联网中继聊天(IRC)活动。

代理层处理

SWA集成了高性能Web代理，具有集成的缓存和内容加速功能。此Web代理由Cisco专有的AsyncOS支持，可管理比传统的基于UNIX的代理服务器多达十倍的连接。作为Web代理，它有助于在应用层进行详尽的内容检测，这对于精确防御基于Web的恶意软件至关重要。

Web信誉过滤器

作为行业先驱的Web声誉过滤器，这些过滤器提供了额外的防御层。这些过滤器利用SenderBase®评估超过50个Web流量和网络相关参数，以确定URL的可信度。高级安全建模技术可用于为每个参数分配单独的权重，最终结果是信誉得分从–10到+10不等。管理员配置的策略可根据这些得分动态调整。

动态定向和流(DVS)引擎

DVS引擎在SWA中引入加速签名扫描，与依赖互联网内容适配协议(ICAP)和多机箱部署进行恶意软件扫描的传统架构不同。此尖端平台利用复杂的对象解析、矢量化技术、流扫描和裁决缓存，与第一代基于ICAP的解决方案相比，扫描吞吐量提高了十倍。

思科防恶意软件系统

此系统利用DVS引擎以及来自Webroot的多种签名类型，提供无与伦比的保护，抵御各种基于Web的威胁。威胁范围包括广告软件、浏览器劫持程序、网络钓鱼、域欺骗攻击以及更多恶意实体，如特洛伊木马、系统监控器和按键记录器。SWA在网关拥有业界最大的恶意软件签名数据库，可确保提供全面的保护。

因此，思科网络安全设备在针对各种基于Web的威胁保护网络网关方面处于领先地位，可确保强大的保护和高性能的网络吞吐量。

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。