瞭解Secure Web Appliance惡意軟體和間諜軟體防護

目錄

簡介

本檔案介紹Cisco Secure Web Appliance(SWA)全面的惡意軟體和間諜軟體防護功能。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Cisco SWA旨在針對各種間諜軟體和基於Web的惡意軟體提供強大而全面的網關防禦機制。它可以有效地應對各種威脅，從因導致網路資源大量消耗和支援性挑戰而臭名昭著的廣告軟體，到更嚴重的威脅，包括特洛伊木馬程式、瀏覽器劫持程式、瀏覽器幫助程式對象、網路釣魚、域欺騙程式、

系統監控程式、鍵盤記錄程式和蠕蟲。

SWA的關鍵優勢

整合式第4層流量監控器(L4TM)

L4流量監控器能夠以線速掃描所有網路埠（共65,535個），確保全面檢測和阻止惡意軟體和未經授權的通訊嘗試。此功能可有效地阻止惡意軟體嘗試繞過公共埠（如埠80和443），還可抑制惡意點對點(P2P)和網際網路中繼聊天(IRC)活動。

代理層處理

SWA採用高效能Web代理，具有整合的快取和內容加速功能。該Web代理由Cisco專有的AsyncOS提供支援，可管理比傳統的基於UNIX的代理伺服器多達十倍的連線。作為Web代理，它有助於在應用層進行詳盡的內容檢測，這對於精確防禦基於Web的惡意軟體至關重要。

Web聲譽過濾器

作為行業先驅的Web聲譽過濾器，這些產品提供了額外的防禦層。這些過濾器利用SenderBase®評估超過50個Web流量和網路相關引數，以確定URL的可信度。採用高級安全建模技術為每個引數分配單獨的權重，最終得到範圍從–10到+10的信譽評分。管理員配置的策略根據這些評分動態調整。

動態向量化和串流(DVS)引擎

DVS引擎在SWA中引入加速簽名掃描，與依賴網際網路內容適配協定(ICAP)和多盒部署進行惡意軟體掃描的傳統架構不同。此尖端平台利用複雜的對象解析、向量化技術、流掃描和判定快取，與第一代基於ICAP的解決方案相比，掃描吞吐量提高了十倍。

思科防惡意軟體系統

此系統利用DVS引擎以及源自Webroot的多種簽名型別，提供無與倫比的保護，抵禦各種基於Web的威脅。威脅範圍包括廣告軟體、瀏覽器劫持程式、網路釣魚、域欺騙攻擊以及更多惡意實體（如特洛伊木馬程式、系統監控器和鍵盤記錄程式）。SWA在網關擁有業界最大的惡意軟體簽名資料庫，確保全面保護。

因此，思科網路安全裝置在針對各種基於Web的威脅保護網路網關方面處於領先地位，可確保強大的保護和高效能網路吞吐量。

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。