網站伺服器防火牆 *AxtWAF 1000*

【產品簡介】

Axtronics AxtWAF 1000 是超越傳統防火牆的新一代網路資安設備，可以針對合法在網頁程式上輸出入的資料，進行正確性及威脅性過濾，防止駭客利用系統漏洞送出可竊取資料或植入木馬程式的網頁訊息，保證企業資訊和客戶資訊不受侵擾。

AxtWAF 1000 動態掃描所保護的網頁架構，透過最新正向行為檢視技術，讓合法的擷取網頁行為通過。此外，AxtWAF 1000 亦可利用客製化字串、攻擊特徵正規化分析多層解碼、已知類型或變種攻擊名單即時阻擋等技術，過濾各種 Web 應用程式資安威脅。

【優異性能】

- 正向行為模型動態掃描網頁架構，只允許合法擷取網頁行為通過。
- 負向行為剖析針對攻擊特徵多層次解碼，及時阻擋 Web 應用攻擊。
- 有效防止 SQL Injection 等竊取資料及木馬植入行為，維護公司機密、客戶資料，確保商譽和網路商業營運正常。
- 直覺式剖繪檔(Profile)政策設定，直接於線上安裝及更新，節省營運成本、提升營運效率。
- 統計報表豐富，可依攻擊及指定統計時間間隔等方式產生報表，確實掌握網路應用系統資安狀況。
- 具備多重自行防護功能，可隱藏機敏資訊，系統運作不中斷。

【規格】

■ 硬體規格(採用硬體式架構)

1. 網路介面(10/100/1000Mbps RJ45)：6 ports(最多 4 個光纖介面) 。
2. AC 電源：100-240V,50-60 Hz。
3. 電源供應器：350W。
4. 尺寸外型：440 (W)x270(D)x44(H) 1U / 19 吋機架式規格。
5. 系統效能：整體處理效能 Throughput 達 1000Mbps(1GBps)。

■ 防禦偵測能力

1. Web application attacks(支援 HTTP、HTTPS 及 XML 應用攻擊) 。
2. SQL Injection(SQL 注入或 SQL 資料隱碼攻擊) 。
3. Session Hijacking(連線截奪) 。
4. Cross Site Scripting (XSS) (跨站指令碼攻擊或跨網站腳本攻擊) 。
5. Buffer Overflow(緩衝區溢位攻擊) 。
6. Cookie Poisoning(資訊塊中毒) 。
7. 提供網站(Web Site)攻擊與網頁(Web Page)參數竄改攻擊之防禦與偵測。
8. 提供即時阻斷攻擊能力。
9. 防禦 Cookie 竄改與 Cookie 植入攻擊。

■ 網路設定

1. 支援 Inline 運作模式。
2. 支援 Monitor 運作模式。
3. 支援 Reverse Proxy 運作模式。

■ 系統管理

1. 提供 CLI(Command Line Interface)、SSH 命令列管理介面與 Web-based 管理介面 。
2. 透過管理介面更新韌體。
3. 遠端接收紀錄。
4. 支援紀錄搜尋。
5. 於偵測到入侵攻擊時具被即時事件警報(Alert)可依設定以 E-mail 或 SNMP Trap 或 SysLog 通知系統管理者。
6. 提供紀錄管理(Syslog / Event logs)功能。
7. 提供警訊(alarm)及 E-mail notify 功能。
8. 提供韌體更新系統及組態異動功能。
9. 支援網路設備 HA(High Availability)備援功能。

■ 統計資訊與報表

1. 可依攻擊自動分類並與統計來源 IP 位址等資訊。
2. 可指定統計時間間隔、監看特定 IP、或針對特定網頁之攻擊。
3. 可產生 HTML 格式報表資料。
4. 可設定攻擊來源排名條件，並顯示工及種類、攻擊目標及描述。
5. 可顯示受保護網站之正向存取規則(由系統自動學習產生)，供管理者參考及調校。
6. 可顯示黑白名單過濾結果，以及對映之規則。
7. 可產生客製化報表。
8. 可產生圖型化攻擊分析資訊。
9. 可輸出報表進行分析作業。

■ 保固範圍

1. 設備硬體三年內保固服務。
2. 管理系統三年內升級服務。
3. 提供特徵資料庫 (Signature Database)網路線上三年免費更新服務。
4. 保固卡填回註冊後提供上述保固服務。

文佳科技股份有限公司
http://www.axtronics.com.tw
308新竹科學園區研發一路9號2樓
電話(03)6662050 傳真(03)6662051
E-MAIL: sales@axtronics.com.tw