Symantec
A Division of Broadcom

解決方案簡介

網頁應用防火牆--WAF

為企業應用程式提供最全面的安全性保護

快速一覽

賽門鐵克網頁應用程式防火牆 (WAF：Web Application Firewall)，可全面保護行動以及網頁應用程式並加快運行速度

提供最新一代網頁應用程式安全性
- 保護網站免受 OWASP Top 10 等及其他的影響。

加快應用程式效能
- 確保依您的部署規模滿足需求。

可部署在 AWS 雲端服務上
- 為 AWS 託管的應用程式和伺服主機提供全面的網頁應用程式安全性。

提供靈活精細的政策控制
- 保護網頁應用程式與網頁內容，並執行法規與公司政策。

介紹

網頁伺服主機是惡意程式最佳的宿主也是最快的感染媒介，攻擊者經常將網頁伺服主機作為其攻擊目標，以幫助他們託管和散播惡意軟體。Verizon 的《2020 年數據洩露調查報告》發現，Web 網頁應用程式攻擊是企業面臨最常見的威脅之一。

為了減輕商譽的危害和持續運營的風險，許多企業正在佈建網頁應用程式防火牆 (WAF)，以保護網頁內容並強制執行網頁應用程式的安全性和隱私權。為了確保他們實施的安全性不會對網頁性能產生不利影響，許多企業選擇了賽門鐵克網頁應用程式防火牆 (WAF)，該防火牆能夠保護和加速網頁應用程式以實現最佳生產力。

賽門鐵克網頁應用程式防火牆是賽門鐵克網頁應用程式安全解決方案的一部份，可以更輕鬆、更有效地運用和保護網頁應用程式來滿足您的業務需求。借助 Symantec WAF，您可以在應用程式周圍安全地設置政策和保護，以使您的員工、供應商和客戶能夠完成工作。賽門鐵克網頁應用程式防火牆 (WAF) 基於業界領先的 ProxySG 平台，可解決當今的安全問題，包括：開放網路軟體安全計畫十大弱點 (OWASP Top10)，以進階政策、控制、責任和效能功能提供完善的防護。

賽門鐵克與眾不同--WAF 的快速交付

賽門鐵克從 2001 年開始，就一直為網頁提供安全性保護，並獲得世界上大多數備受推崇和要求最嚴苛的組織所信任。WAF 是對 Symantec Proxy 代理部署的自然延伸，使企業能夠受益於我們領先業界的 ProxySG 中已經提供的所有安全性、網頁加速和控制功能。Symantec WAF 可透過 ProxySG 或 ASG 來啟用反向代理功能，並且可以經由購買網頁應用程式保護或 WAF 授權來啟用。同時，可以使用反向代理或 SG 虛擬硬體裝置，將 WAF 部署在 Amazon Web Services（AWS）* 中。

* 使用 SRP-VA-C2S 或虛擬硬體裝置型號：ARP-VA-C2S，Amazon Web Services（AWS）支援當前可用於 T2.Large、M4.Large、C4.Large

最新一代應用程式安全性

賽門鐵克網頁應用程式防火牆 (WAF) 提供了進階的最新一代保護，可解決當今的關鍵安全問題，包括 OWASP 針對 Web 應用程式的十大漏洞。WAF 對入站和出站內容進行進階威脅分析，以檢測並保護您的基礎架構免受攻擊。WAF 通過兩種引擎提供保護，一是基於特徵的引擎，能夠阻止已知威脅模式；二是進階無特徵引擎，旨在發現網頁流量中未知攻擊和零時差攻擊。

賽門鐵克網頁應用程式防火牆 (WAF) 最新一代的內容性質檢測引擎可以準確理解內容上下文，體現攻擊檢測技術的根本轉變，從整體上提高了攻擊識別能力的準確性和可靠性。內容性質檢測引擎可用於抵禦當今許多網頁應用程式攻擊，包括代碼注入、HTML 注入、目錄遍歷、命令注入、JSON 驗證、SQL 注入和跨站腳本攻擊。管理員可以設置靈活的政策，以利用 WAF 的所有進階保護功能。

WAF 也可以隔離原始伺服器與網際網路的直接存取來保護網頁基礎架構。此外，WAF 監視您的網頁伺服器和其他與代理相關的設備，讓伺服器和客戶端進行嚴格的 HTTP /HTML 協議驗證，以確保活動合法。您還可以透過使用 WAF 作為 SSL/TLS 終點來保護用戶對網頁應用程式的存取。WAF 提供伺服器和客戶端憑證支援，以及網頁服務加密 / 解密的數位簽章驗證，以確保通訊的完整性。作為 SSL/TLS 終點，WAF 減輕了 Web 伺服器對 SSL 的解密 / 加密的負擔，以提高整體性能並減輕中間人攻擊 (MITM) 的風險。

精細的政策控制

網頁應用程式防火牆 (WAF) 可讓管理員依據需求來建立遵循、合規以及安全性的政策。ProxySG 中強大的政策引擎提供管理員可以根據需要建立廣泛而靈活的政策，包括 URL 重寫、SSL/TLS 驗證和強制。您也可以根據存取企業網站的最終用戶的地理位置來設置政策，以幫助減輕風險並符合法規、公司政策和遵循等要求。

使用 Geo-IP，可以讓您識別特定客戶的 IP 位址，以了解對方來自何處 (地理位置)，以便可以對他們的存取做出適當的決定。Geo-IP 情資資料庫是由賽門鐵克全球情報智慧網路 (GIN:Global Intelligence Netork) 所支援，因此任何變動都將立即反映在 IP 位址中。客戶端的真實 IP 位址是必需的，可以從來源 IP 位址或 HTTP 請求標頭（例如 x-forwarded-for）獲得。

加速應用程式效能

賽門鐵克網頁應用防火牆 (WAF)，讓您得以加快網頁應用程式和內容的交付，確保獲得一致、令人滿意的體驗，可以大大提高用戶的工作效率。賽門鐵克網頁應用防火牆 (WAF)，提供整合式的快取、串流分流和頻寬控制，以獲得最佳效能。

此外，您可以透過可能佔用大量資源的功能轉移到 WAF（例如用戶身份驗證、SSL 終止和 Web 內容最佳化）來提高網頁主機群 (Web Farm) 的延伸能力。WAF 可以執行 HTTP、HTTPS、TCP、ICAP 和 ICMP 的運行狀況檢查，以幫助您監視網頁內容、伺服器以及整體環境，並在出現問題後儘快克服和解決這個問題，並向您發出告警。

要求

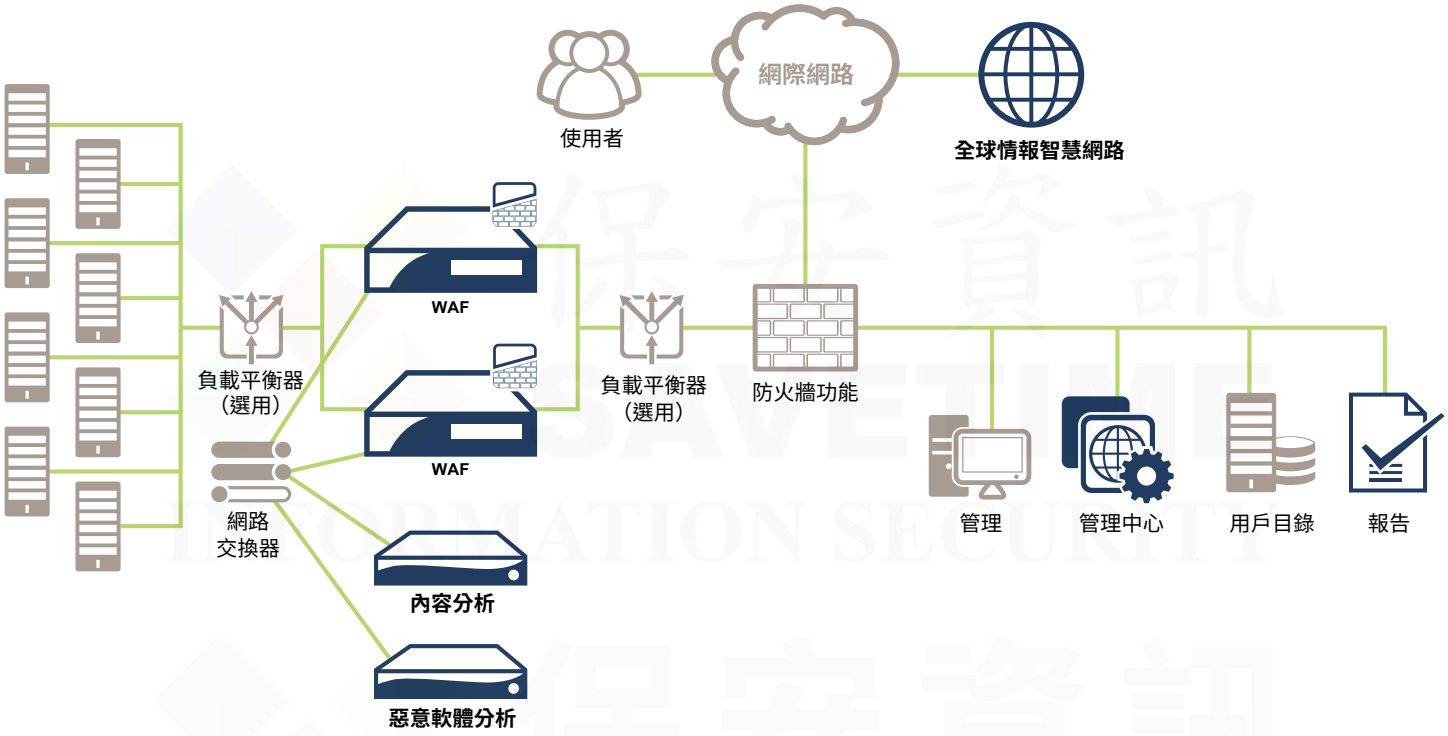
要利用 Symantec WAF 的所有安全性和效能 (加速)，您需要：

- Symantec Reverse Proxy（硬體或虛擬）、ProxySG、以及 Proxy Edition 或 SG 虛擬硬體裝置（不支援 MACH5 版本）*
- Web 應用程式保護或 WAF 授權 - 依設備 SKU 按年度訂閱
- 至少要 SGOS 6.5.3 才可以使用應用程式保護的基本功能；完整的應用程式保護需要 SGOS 6.6.2 或更高版本
- 至少要 SGOS 6.5.1 才能使用 Geo-IP 功能

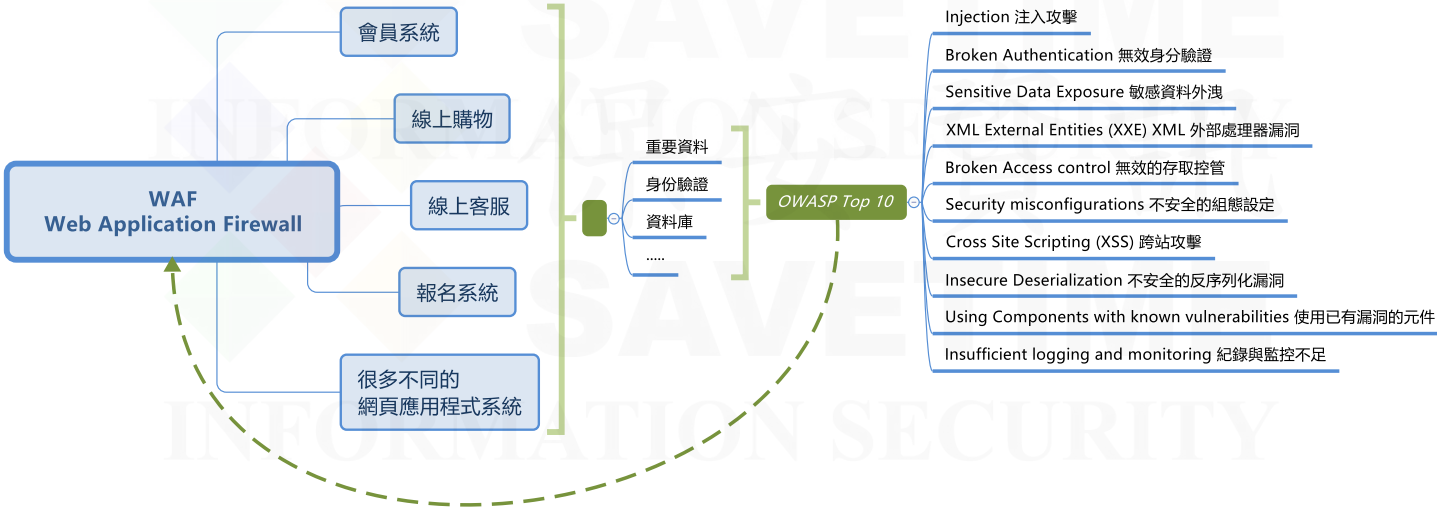
強烈建議您使用 Symantec Management Center 和 Reporter 解決方案來優化 WAF 的管理並獲取特定於 WAF 的報告。

* 使用 SRP-VA-C2S 或虛擬硬體裝置型號：ARP-VA-C2S，Amazon Web Services（AWS）支援當前可用於 T2.Large、M4.Large、C4.Large

典型的 WAF 本地部署示意圖



常見的 WAF 防護應用示意圖



關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號

電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw