主要新功能

Sophos Firewall OS v22

安全設計

Sophos Firewall 健康檢查

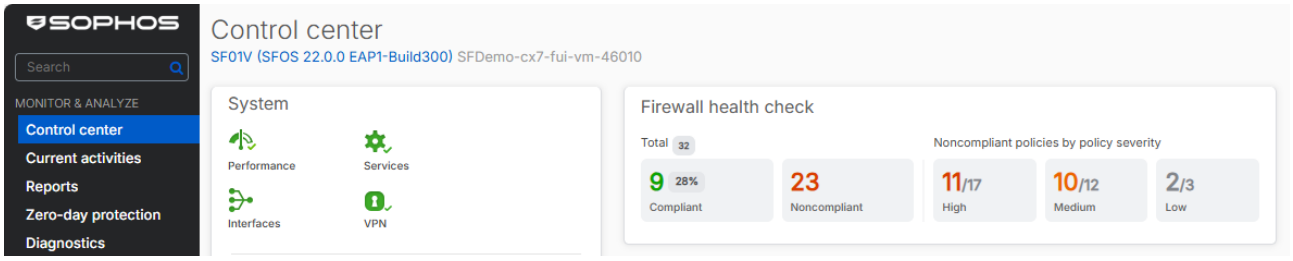
暴露於網際網路的網路基礎架構（例如防火牆）越來越常成為攻擊者鎖定的目標，被用作發動進一步攻擊的潛在入口點。這使得加強與保護此類網路基礎架構的安全性再次成為焦點。

在 Sophos ，我們對安全性極為重視。我們支持並採納由 CISA 所提出的「安全設計 (Secure by Design)」原則，將客戶安全視為核心要求。 在過去數個版本中，我們持續投入資源，將「安全設計」原則落實於所有產品之中，包括 Sophos Firewall。 近年來，Sophos Firewall 已多次更新，積極強化產品防禦力、簡化漏洞修補流程，並協助用戶偵測是否正遭受攻擊。 正如您所知，Sophos Firewall 獨家提供「空中下載修補 (OTA hotfix)」安全更新，可在不中斷服務的情況下修補新出現的漏洞。Sophos 也是唯一主動監控安裝基礎、協助提早偵測攻擊跡象的廠商。

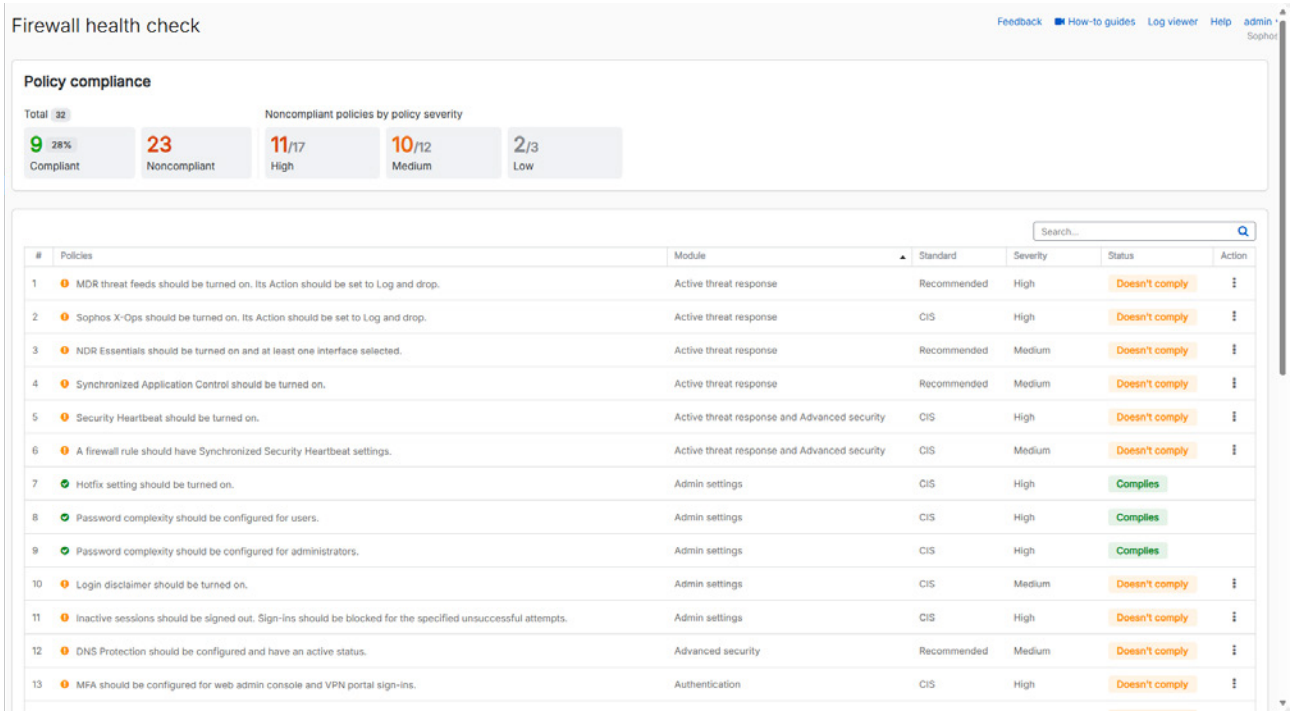
然而，作為我們的合作夥伴與客戶，您也必須盡一份心力，確保您的網路安全基礎架構保持在最佳防護狀態。這代表您需要隨時更新韌體，並確保防火牆已依照網路安全最佳實務設定至最優狀態，以最大化安全防護並消除任何可能被攻擊者利用的意外弱點。

Sophos Firewall v22 透過全新的「健康檢查 (Health Check)」功能 讓您更輕鬆地維持防火牆的最佳安全狀態。這項新功能會評估防火牆中數十項不同的設定，並與 CIS 基準及其他安全最佳實務進行比對，立即提供潛在風險區域的洞察。 它會識別所有高風險設定，並提供具體建議與可深入檢視的導引，讓您能輕鬆修正問題。

此新功能包含一個全新的控制中心儀表板小工具概覽，以及可透過點選進入或在主選單「防火牆健康檢查 (Firewall health check)」項目下開啟的詳細檢視頁面。



健康檢查摘要會顯示在新的控制中心小工具中，您只需按一下即可深入查看完整的健康檢查結果。



您可以透過主選單的「監控與分析 (Monitor and Analyze)」區段，或透過控制中心小工具來進入新的健康檢查功能，以檢視設定中可能存在的風險或是進一步執行最佳化。

新世代 Xstream 架構

Sophos Firewall 自 v18 起引入 Xstream 架構，作為核心技術之一，讓 XGS 系列設備能充分發揮其強大的運算效能與擴充能力。自那之後，Sophos Firewall 的 Xstream 架構持續擴展與調整，為客戶的網路帶來更高的效能。 這一切都歸功於 Sophos Firewall Xstream 架構的可程式化特性——它不依賴客製化的 ASIC 晶片，且同樣能在一般用途 CPU、虛擬化 CPU，以及配備專用流量處理器的 XGS 系列機型上穩定運作。

Sophos Firewall v22 引入了新一代 Xstream 架構，重新設計了控制平面 (control plane，可理解為控制核心)，以實現最高等級的安全性與可擴充性，為未來發展奠定基礎。 新的控制平面支援模組化、隔離化與容器化運作，例如 IPS 等服務，可以像「應用程式」一樣在防火牆平台上獨立執行。 它同時實現了完整的權限分離，以強化安全性。此外，高可用性 (HA) 部署現在具備自我修復功能，能持續監控系統狀態並自動修正設備間的差異。

而最終成果是一個超高安全、可擴充且精簡的架構，專為未來而設計。 這項新世代 Xstream 架構為高度安全、可擴充與模組化的容器化服務、n 節點叢集，以及支援高效能遠端管理與自動化的完整 RESTful API 奠定了基礎。

強化核心

Sophos Firewall OS 的新世代 Xstream 架構建立在全新的強化核心 (版本 6.6 以上) 之上，提供更高的安全性、效能與可擴充性，以充分發揮現有與未來硬體的潛能。 這個新核心具備更嚴密的程序隔離機制，並能更有效防禦側通道攻擊，同時針對多種 CPU 漏洞提供防護 (包含 Spectre、Meltdown、L1TF、MDS、Retbleed、ZenBleed、Downfall)。 此外，它還包含強化的 usercopy 機制、堆疊金絲雀 (stack canaries)，以及核心位址空間配置隨機化 (KASLR)。

遠端完整性監控

Sophos Firewall OS v22 現已整合 Sophos XDR Linux 感測器，可即時監控系統完整性，包括未經授權的設定變更、規則匯出、惡意程式執行企圖、檔案竄改等行為。這項功能協助 Sophos 安全團隊主動監控安裝基礎，能更快速地識別、調查並回應任何潛在攻擊。 這是一項其他防火牆廠商所沒有提供的額外安全防護能力。

全新防惡意程式引擎

Sophos Firewall OS v22 整合了最新版 Sophos 防惡意程式引擎，具備強化的零時差即時偵測能力，可偵測新興威脅。此引擎結合 SophosLabs 全球信譽查詢系統，利用每五分鐘或更短時間即更新一次的雲端惡意檔案資料庫。它同時導入 AI 與機器學習模型偵測，並將強化的遙測資料回傳至 SophosLabs，加速新興威脅的分析與偵測。

其他安全性與可擴充性強化項目

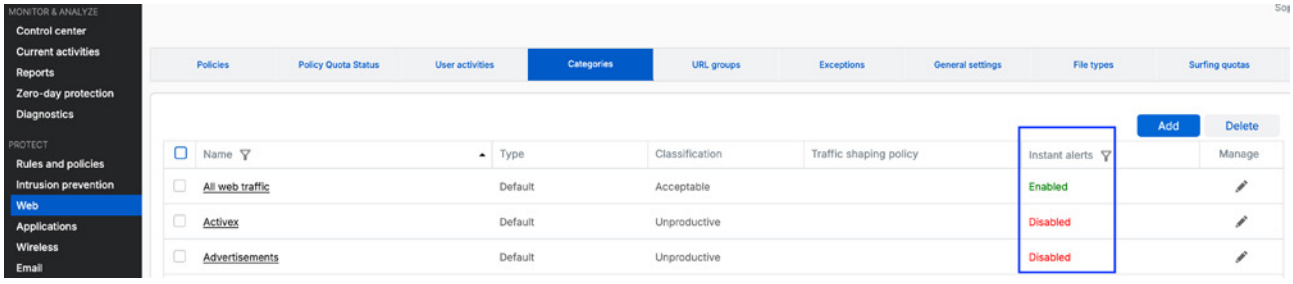
透過 SSL 與憑證鎖定進行韌體更新 —— 確保更新伺服器的真實性，防止攻擊者藉由此途徑進行滲透。

主動式威脅回應記錄改進 —— 新增更細緻的記錄控制，針對內送與外送流量提供更準確的日誌過濾，以減少暴力破解等重複事件造成的雜訊。 新增支援辨識並比對內送轉送流量（如 WAF、DNAT 等）與第三方、NDR Essentials 及 MDR 威脅情報饋送，以強化對外部發起威脅的偵測能力。同時新增支援針對外送流量比對 NDR Essentials 與第三方威脅情報來源的 IP 位址，以識別並封鎖受感染且未受管控的裝置。

NDR Essentials 威脅分數記錄 —— 現在在主動威脅回應記錄中會包含威脅分數，提供更高的可見性、報告與分析能力。

NDR Essentials 資料中心設定 —— 現在可選擇 NDR Essentials 流量分析的資料中心區域，以符合地區或資料儲存規範需求。系統預設會自動選擇延遲最低的區域。

即時網頁類別警示 —— 現在可針對受限制的網頁類別設定即時警示，這對於必須遵循特定網路存取規範的英國與愛爾蘭 (UKI) 教育機構特別有用。系統可每 5 分鐘寄送一次電子郵件通知，內含日期、時間、使用者、類別、網域等完整報告。 此新功能可在「網頁 > 類別」中找到。



輕鬆為任意網頁類別新增即時警示。

XML API 存取控制強化 —— API 設定現已移至主選單的「管理 (Administration)」項目下。現在可依 IP 位址、IP 範圍與網路物件定義 API 存取權限，最多支援 64 個物件 (先前僅支援 10 個 IP)。

裝置存取的 HTTP/2 與 TLS 1.3 支援 —— 網頁管理主控台、VPN 入口與使用者入口網站現已支援 TLS 1.3，提供更強的加密保護。

精簡管理與提升使用體驗

與每個 Sophos Firewall 發布一樣，這次的版本也包含了幾項使用體驗提升功能，使日常管理更加輕鬆。

導覽效能提升 —— 現在可在不等待目前頁面載入完成的情況下，直接切換至任何功能表項目或索引標籤，使使用介面的導覽速度更快。

透過 SNMP 進行硬體監控 —— 新增眾多合作夥伴與客戶長期要求的功能，並可從 SFOS 介面下載 MIB 檔案。支援的監控項目包括 CPU 溫度、NPU 溫度、風扇轉速、電源供應狀態 (適用於 XGS 2100 以上型號)，以及所有支援 PoE 的 XGS 機型 (除 XGS 116(w) 外) 的 PoE 電力測量。

sFlow 監控 —— 可依設定的取樣率 (預設為 400，最低可設為 10) 提供即時流量資料。支援任意實體介面 (含子介面，如別名、VLAN 等)，最多可設定 5 個收集器。請注意：啟用監控的介面會停用 FastPath 功能。

NTP 伺服器設定 —— NTP 伺服器現在預設為「使用預設 NTP 伺服器 (Use pre-defined NTP server)」。

XFRM 介面使用者介面強化 —— 新增分頁支援，以及搜尋與篩選選項，方便管理大量 XFRM 介面。

SG UTM 功能

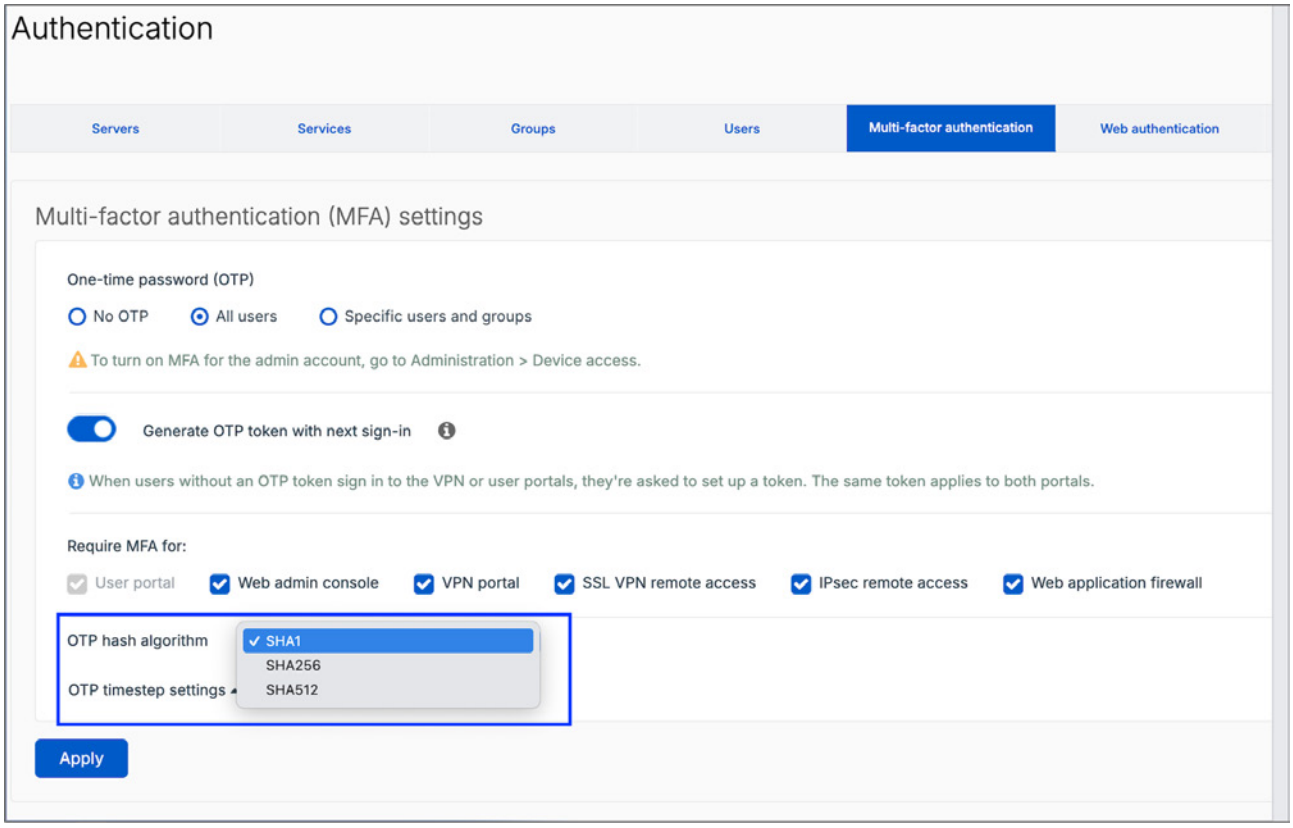
由於 SG UTM 產品線即將於 2026 年 7 月 30 日終止支援，部分正在轉換至 Sophos Firewall 的用戶會特別歡迎以下新功能：

OTP 權杖支援 SHA-256 與 SHA-512 —— SG UTM 用戶高度要求的功能現已可在 Sophos Firewall 中使用，適用於 Google、Sophos 應用程式與管理員使用者。

WAF 的多重要素驗證 (MFA) 支援 —— 為 Sophos Firewall 內建的 Web 應用程式防火牆 (採表單式驗證) 新增多重驗證功能，進一步提升安全性並實現功能一致性。

稽核追蹤記 —— 新增完整稽核記錄功能，支援變更前後追蹤，以符合最新 NIST 標準。 在第一階段中，詳細稽核記錄涵蓋防火牆規則、物件與介面。使用者可從「診斷 > 記錄」中下載詳細稽核檔案。 稽核資料以 XML 格式呈現變更前後的差異。未來版本將在記錄檢視器中直接顯示差異內容。

更強大的 WAF 安全性 – 現在會話由 SFOS 管理，而非由客戶端 cookie 管理，使其更難被劫持，並提升整體防護。當不需要驗證轉發時，驗證可以完全卸載至 SFOS 處理，從而降低內部 WAF 伺服器的曝險。



多重要素驗證 (MFA) 現已延伸支援至 WAF，並支援 SHA-256 ／ SHA-512。

台灣業務窗口
電子郵件: Sales.Taiwan@Sophos.com

2025-10-16 ZHTW (DD)