SOPHOS

Sophos Firewall 功能介紹

Sophos Firewall

產品重點

- Xstream 架構透過以串流為基礎的封包處理，提供超高等級的可見度、防護能力和效能
- Xstream TLS 檢查提供高效能，支援 TLS 1.3 且效能不會降級，此外不限連接埠，使用含預設例外項目的企業級原則，並擁有獨特的儀表板可見度，以及具備相容性故障排除能力
- Xstream DPI 引擎透過一個高效能引擎，為 IPS、AV、Web、應用程式控制和 TLS 檢查提供串流掃描防護
- Xstream Network Flow FastPath 自動提供以原則驅動的智慧型可信任流量加速
- Xstream SD-WAN 提供以效能為基礎的連線選擇與零影響重新路由功能，具備 SD-WAN 監控、多站台 SD-WAN 協調工具，以及 IPsec VPN 通道流量的 FastPath 加速
- 具有互動式控制中心的專用使用者介面，會利用交通號誌燈號 (紅、黃、綠) 立即標示出需要注意的內容
- 控制中心提供多種即時深入資訊，包括端點健康狀況、未識別的 Mac 和 Windows 應用程式、雲端應用程式和影子 IT、可疑裝載、有風險的使用者、進階型威脅、網路攻擊、令人反感的網站等
- 透過智慧搜尋來最佳化兩次點擊的操作
- 原則控制中心桌面工具會監控業務、使用者和網路原則的原則活動，並追蹤未使用、停用、已變更和新的原則
- 統一原則模型可將所有的防火牆、NAT 和 TLS 檢查規則等，整合到一個包含群組、篩選和搜尋選項的單一畫面中
- 使用自訂的自動和手動群組功能，以及一目瞭然的滑鼠操作和執行指標，進行流暢的防火牆規則管理
- 所有防火牆規則都提供對防毒、沙箱、IPS、Web、應用程式、流量塑型 (QoS) 和安全心跳 (Heartbeat) 等所應用的安全性和控制的一目了然的概觀
- 預定義的 IPS、Web、應用程式、TLS 和流量控管 (QoS) 政策，可針對一般部署情境 (例如 CIPA、典型的工作場所政策等) 進行快速設定和輕鬆的客製化
- Sophos Security HeartbeatTM 連接 Sophos 端點與防火牆，共享健康狀態和遙測功能，以便即時識別出不健康或被入侵的端點
- Active Threat Response 會根據 SophosLabs、MDR 分析師或第三方提供的威脅情報源，來識別、封鎖並自動回應主動攻擊敵手
- Synchronized Application Control 同步應用程式控制可以自動識別、分類和控制網路上所有未知的 Mac/Windows 應用程式
- 雲端應用程式可見性可立即啟用影子 IT 探索功能，並提供一鍵流量控管功能
- 原則測試模擬器工具可根據使用者、IP 和一天中的時間，啟用防火牆規則和 Web 政策模擬與測試
- 使用者威脅商數可根據最近的瀏覽行為和 ATP 觸發器來識別出有風險的使用者
- 適用於 RMM/PSA 所有整合功能的設定 API
- 雲端型 NDR 整合可強化對主動攻擊敵手的偵測能力
- 每部防火牆皆內建 ZTNA 閘道，讓您隨時隨地安全存取應用程式
- 適用於多個防火牆的 Sophos Central 雲端管理和報告功能可進行群組原則管理，以及透過單一主控台管理您的所有 Sophos IT 安全產品
- 輕鬆且經過簡化的設定精靈，可在幾分鐘內快速實現立即可用的部署
- 在 Sophos Central 中零接觸部署和設定新的防火牆
- 與 Sophos MDR 和 XDR 無縫整合

基本防火牆 (Base Firewall)

綜合管理

- 針對大型規則集的專屬精簡化使用者介面和防火牆規則管理功能，並使用一目瞭然的規則功能和執行指示器進行分組
- 雙因素驗證 (一次性密碼) 支援系統管理員存取、使用者入口網站、IPsec 和 SSL VPN
- 圖形化使用者介面 (GUI) 中的進階登入與疑難排解工具 (如封包擷取)
- 高可用性 (HA) 支援兩部裝置以主動 - 主動或主動 - 備援模式的叢集，透過即插即用的快速 HA 設定，支援多條備援同步連線。
- 可從圖形化介面 (GUI) 使用完整的命令列介面 (CLI)
- 具備與 Azure AD 整合的基於角色的管理，實現單一登入 (SSO)
- 自動韌體更新通知，提供簡易的自動化更新流程與復原功能 (僅限擁有有效支援服務的客戶使用)
- 可重複使用並可搜尋的系統物件定義，涵蓋網路、服務、主機、時間區段、使用者與群組、用戶端與伺服器
- 自助使用者入口網站
- 設定變更追蹤
- 可根據區域對服務進行彈性的裝置存取控制
- 電子郵件或 SNMP Trap 通知選項
- SNMP 和 Netflow 支援
- 透過 Sophos Central 的集中管理支援 (僅限擁有有效支援服務的客戶使用)
- 備份與還原設定：可儲存於本機，透過 FTP 或電子郵件進行；並支援隨需、每日、每週或每月備份；升級硬體設備時還可選擇重新對應連接埠
- 支援 Let’s Encrypt 認證，可用於 WAF、SMTP、TLS 設定、熱點登入、網頁管理主控台、使用者入口網站、強制入口網站、VPN 入口網站與 SPX 入口網站
- 第三方整合功能的 API
- 介面重新命名
- Sophos Support 的遠端存取選項
- 透過 MySophos 進行雲端授權管理

防火牆、網路和路由

- 狀態式深度封包偵測防火牆
- Xstream 封包處理架構透過以串流為基礎的封包處理，提供超高等級的可見度、防護能力和效能
- Xstream TLS 檢查提供高效能，支援 TLS 1.3 且效能不會降級，此外不限連接埠，使用企業級原則，並擁有獨特的儀表板可見度，以及具備相容性故障排除能力
- Xstream DPI 引擎透過一個高效能引擎，為 IPS、AV、Web、應用程式控制和 TLS 檢查提供串流掃描防護
- Xstream Network Flow FastPath 自動提供對受信任的應用程式流量、IPSec VPN 流量以及經 TLS 加密的流量的政策驅動及智能的加速。
- 以使用者、群組、時間或網路為基礎的原則
- 根據使用者 / 群組的存取時間原則
- 跨區域、網路或根據服務類型實施原則
- 區域隔離和區域型政策支援
- 預設區域包含 LAN、WAN、DMZ、LOCAL、VPN 及 WiFi
- LAN 或 DMZ 上的自訂區域
- 可自訂的 NAT 原則支援 IP 偽裝與完整物件功能，可透過單一規則轉送或重新導向多項服務，並提供便利的 NAT 規則精靈，只需幾個步驟即可快速輕鬆建立複雜的 NAT 規則
- 具有全域智慧型全文搜尋，且可用於所有規則的可重複使用網路物件定義
- 泛流防護：DoS、DDoS 和連接埠掃描阻擋
- 根據 IP 地理位置阻擋特定國家
- 路由功能：靜態、多點傳送 (PIM-SM) 及動態路由：RIP、BGP、OSPFv3 (IPv6) 及 BGPv6
- 可複製靜態路由並啟用或停用它們，將動態 BGP 路由重新分配到 OSPFv3，使用 Blackhole 路由選項，並採用等成本多路徑 (ECMP) 實現負載平衡
- 上游代理支援
- 採用 IGMP 窺探技術的與通訊協定無關的多點傳送路由
- 橋接 STP 支援和 ARP 廣播轉發
- VLAN DHCP 支援和標記
- VLAN 橋接支援

- 巨大框架 (Jumbo Frame) 支援
- 啟用 / 停用實體介面
- 無線廣域網路支援 (不含虛擬部署)
- 802.3ad 介面連結彙總
- DNS、DHCP 和 NTP 的完整設定
- 動態 DNS (DDNS)
- IPv6 就緒標誌核可憑證
- IPv6 DHCP 前綴委派
- IPv6 通道技術支援，包括 6in4、6to4、4in6 和透過 IPsec 的 IPv6 快速部署

Xstream SD-WAN

- Xstream SD-WAN 支援多個 WAN 連結選項，包括 VDSL、DSL、纜線、LTE/ 行動數據，以及 MPLS
- 基於效能的 SLA 會根據抖動、延遲或封包遺失情況自動選擇最佳 WAN 連結
- 透過多條 SD-WAN 連線進行 SD-WAN 負載平衡，支援輪詢權重或工作階段持續性策略
- 零影響重新路由技術，可在連線效能低於閥值並切換至效能較佳的 WAN 連線時，維持應用程式工作階段不中斷
- SD-WAN 監控圖會即時提供所有 WAN 連結的延遲、抖動和封包遺失的深入資訊
- SD-WAN IPsec 通道流量的 Xstream FastPath 加速功能
- 同步 SD-WAN 是同步安全的功能之一，可在 Sophos 管理的端點和 Sophos Firewall 之間共用同步應用程式控制資訊時，增加應用程式識別的明確性和可靠性。
- 透過防火牆規則或原則式路由，將應用程式流量導向優先連線
- 健全的 VPN 支援，包括 IPsec 和 SSL VPN
- 具備路由功能的獨特 RED 第 2 層通道

基本流量控管和配額

- 彈性的網路或使用者流量控管 (QoS)，並包含 Web Protection 訂閱隨附增強的 Web 和應用程式流量控管選項
- 設定以使用者為基礎的上傳 / 下載或總流量配額，並可選擇週期性或非週期性限制
- 即時 VoIP 最佳化
- DSCP 標記

安全無線

- Sophos 無線存取點 (僅限 APX 系列) 可簡易即插即用部署，並會自動顯示於防火牆控制中心
- 利用內建的無線控制器集中監控和管理所有存取點 (AP) 和無線用戶端
- 橋接存取點到區域網路、VLAN 或一個具備用戶端隔離選項的單獨區域
- 每個射頻都支援多個 SSID，包括隱藏的 SSID
- 支援多種安全和加密標準，包括 WPA2 個人和 WPA2 企業
- 通道寬度選擇選項
- 透過主要和輔助伺服器支援 IEEE 802.1X (RADIUS 驗證)
- 支援 802.11r (快速轉換)
- 支援無線熱點的 (自訂) 憑單認證、當天密碼認證，或是接受條款和條件的認證
- 具備圍牆花園 (walled garden) 選項的無線訪客網際網路存取
- 以時間為基礎的無線網路存取
- 透過 Sophos 支援的 AP 進行無線中繼和橋接網狀網路模式
- 自動頻道選擇背景最佳化
- 支援 HTTPS 登入

驗證

- 同步使用者識別 (Synchronized User ID) 利用同步安全技術，無需在 Active Directory 伺服器或用戶端安裝代理程式，即可在 Sophos 端點與防火牆之間共享目前登入的 Active Directory 使用者識別
- 透過以下方式進行驗證：Active Directory、eDirectory、RADIUS、LDAP 和 TACACS+
- Active Directory 單一登入 (SSO)、STAS、SATC 的伺服器驗證代理程式
- 單一登入：Active directory、eDirectory、RADIUS 帳戶處理
- Azure AD 單一登入 (SSO) 供系統管理員存取 Webadmin 主控台
- Azure AD 單一登入 (SSO) 供使用者透過強制入口網站進行網頁存取驗證
- 透明 AD 單一登入 (SSO) 並強制執行 HSTS，支援透過 HTTP 或 HTTPS 的 Kerberos 及 NTLM 連線協議
- 支援 Azure AD 群組匯入與角色基礎存取控制 (RBAC)
- Windows、Mac OS X、Linux 32/64 的用戶端驗證代理程式

- 瀏覽器 SSO 驗證：透通的代理驗證 (NTLM) 和 Kerberos
- 瀏覽器驗證入口網站
- iOS 和 Android 的驗證憑證
- IPsec、SSL、L2TP、PPTP 的驗證服務
- 對使用 Active Directory 和 Google G Suite 的環境提供 Google Chromebook 驗證支援
- 透過 LDAP 用戶端整合 Google Workspace，支援 Google Chromebook 單一登入 (SSO)
- 以 API 為基礎的驗證

使用者自助服務與 VPN 入口網站

- 支援 VPN 入口網站的 Entra ID (Azure AD) 單一登入 (SSO)
- 下載 Sophos Authentication Agent (SAA)
- 下載 SSL 遠端存取用戶端 (Windows) 和設定檔 (其他作業系統)
- 熱點存取資訊
- 變更使用者名稱和密碼
- 檢視個人網際網路使用量
- 存取被隔離的郵件和管理使用者的阻止 / 允許寄件者清單 (需要 Email Protection)

基本 VPN 選項

- 站台對站台 VPN：SSL、IPsec、256 位元 AES/3DES、PFS、RSA、X.509 憑證、預共用金鑰
- Sophos RED 站台對站台 VPN 通道 (穩固且輕量)
- Xstream FastPath 加速 IPsec 通道流量 (支援站台對站台與遠端存取)
- AWS VPC 匯入、監控和管理工具
- L2TP、PPTP
- 具備流量選擇器的路由型 VPN
- 遠端存取：SSL、IPsec、iPhone/iPad/Cisco/Android VPN 用戶端支援
- IKEv2 支援
- IPsec 連線具狀態的高可用性 (HA) 故障轉移，適用於 RBVPN、PBVPN 與遠端存取 VPN，可在 HA 故障轉移期間不中斷現有工作階段事件
- 透過 SNMP 監控 IPsec VPN 通道狀態
- 進階 IPsec 支援獨立預共享金鑰 (PSK) 與 DH 群組 27–30/ RFC6954
- 透過使用者入口網站下載 Windows SSL 用戶端和設定

Sophos Connect 用戶端

- 驗證：預共用金鑰 (PSK)、PKI (X.509)、權杖和 XAUTH
- 支援 Entra ID (Azure AD) 單一登入
- 為遠端連線使用者啟用 Synchronized Security 同步安全和 Security Heartbeat 技術
- 智慧型分割通道技術，以最佳化流量路由
- NAT 穿越支援技術
- 用戶端端監視器，以取得連線狀態的圖形化概觀
- 支援 Mac (IPsec) 和 Windows (SSL/IPsec) 用戶端

網路防護

入侵防禦 (IPS)

- 高效能的新一代 IPS 深度封包偵測引擎，具備可應用在防火牆規則的選擇性 IPS 模式，可實現最佳效能和防護
- 數千種特徵碼
- 精細的類別選擇
- 支援自訂 IPS 特徵碼
- IPS 原則智慧篩選器可啟用動態原則，隨著新模式新增而自動更新

Active Threat Response 與 Security Heartbeat™

- Active Threat Response 可自動監控與封鎖透過 Sophos X-Ops 威脅情資來源所識別的 APT 和其他威脅，提供多層次 DNS、AFC 與防火牆偵測機制，有效防禦試圖聯絡惡意目的地的殭屍網路與主動攻擊敵手
- 當搭配 Xstream Protection 的 Sophos Firewall 與 Sophos MDR/XDR 結合時，Active Threat Response 可自動監控與封鎖由 Sophos 或客戶 / 合作夥伴安全營運中心 (SOC) 分析師所發布的 MDR/XDR 威脅情資所識別的威脅
- Active Threat Response 可搭配 Xstream Protection，自動監控並封鎖來自產業、垂直領域或區域性威脅情報來源的第三方威脅情資
- Sophos Synchronized Security Heartbeat 可即時標示遭入侵的裝置，當其試圖連線至 Active Threat Response 或其相關威脅情資所識別的任何威脅指標時，會顯示為紅色心跳狀態。 心跳狀態亦會由 Sophos 管理的端點裝置監控，並與防火牆共享資訊，包括主機、使用者、程序、事件次數與入侵時間等詳細資料

- Sophos Security Heartbeat 狀態條件可套用至任何防火牆規則，當裝置遭入侵時，將自動限制其對網路資源與區段的存取，直到裝置清除無虞為止。
- 若受管理的端點遭到入侵，Sophos Firewall 也會自動啟動橫向移動防護，通知所有健康的 Sophos 管理端點拒絕來自該遭入侵裝置的流量，即使在同一 LAN 區段內也能有效隔離該裝置。

SD-RED 裝置管理

- 集中管理所有 SD-RED 裝置
- 無需設定：自動透過雲端佈建服務進行連線
- 使用數位 X.509 憑證和 AES 256 位元加密的安全加密通道
- 能在不同位置間可靠傳輸所有流量的虛擬乙太網路
- 透過集中定義的 DHCP 和 DNS 伺服器設定進行 IP 位址管理
- 當一段時間沒有活動後，由遠端取消授權 SD-RED 裝置
- 通道流量壓縮
- VLAN 連接埠設定選項

無用戶端 VPN

- Sophos 獨特的加密式 HTML5 自助服務入口網站，且支援 RDP、SSH、Telnet 和 VNC

Web 防護

Web 防護和控制

- 串流 DPI Web 防護或明確代理 (Explicit Proxy) 模式檢查
- 同一來源 IP 上的多個使用者每次連線，明確代理都會對其進行驗證
- 增強的進階型威脅防護
- URL 篩選器資料庫中有由 SophosLabs 所支援的數百萬個網站，高達 92 種不同的網站類別分類
- 根據使用者 / 群組的瀏覽配額時間
- 根據使用者 / 群組的存取時間原則
- 惡意軟體掃描：在 HTTP/S、FTP 和以 Web 為基礎的電子郵件上阻擋所有形式的病毒、Web 惡意軟體、木馬程式和間諜軟體
- 透過 JavaScript 模擬進行進階的 Web 惡意軟體防護
- 可即時從雲端查閱最新的威脅情報以提供即時防護
- 透過第二個獨立的惡意軟體偵測引擎 (Avira) 進行雙重掃描
- 即時或批次模式掃描
- 網址嫁接防護
- 對 O365 實施租用戶限制
- SSL 通訊協定通道偵測和強制執行
- 憑證驗證
- 高效能網頁內容快取
- 強制快取 Sophos 端點更新
- 透過 MIME 類型、副檔名和主動內容類型 (如 Activex、applet 和 cookies 等) 進行檔案類型篩選
- 根據原則實施 YouTube for Schools (使用者 / 群組)
- 為主要搜索引擎提供 SafeSearch 功能 (以 DNS 為基礎) (使用者 / 群組)
- Web 關鍵字的監控和強制功能，可以登錄、報告或阻止符合關鍵字列表的網頁內容，並可選擇上傳自訂清單
- 阻擋可能不需要的應用程式 (PUA)
- 適用於教師或工作人員的 Web 原則複寫選項，允許他們臨時使用特定使用者可完全自訂和管理的被阻止網站或類別
- 在 Google Chromebook 上執行使用者 / 群組原則

雲端應用程式可見度

- 控制中心螢幕工具能顯示上傳和下載到雲端應用程式，並被分類為新的、被核准、未核准或許可的資料量
- 快速找出影子 IT
- 深入取得使用者、流量和資料的詳細資訊
- 一鍵使用流量控管原則
- 按類別或數量篩選雲端應用程式使用情況
- 詳細且可自訂的雲端應用程式使用情況報告，以用於完整的歷史報告

應用程式防護與控制

- 同步應用程式控制功能可以自動識別、分類和控制網路上所有未知的 Windows 和 Mac 應用程式流量，在 Sophos 管理的端點和防火牆中共用資訊
- 利用數千種應用程式的模式，進行以特徵碼為基礎的應用程式控制

- 應用程式可見度和控制以找出影子 IT
- 應用程式控制智慧型篩選器可啟用動態原則，可在新模式出現時自動更新
- 微型應用程式搜尋和控制
- 採用以類別、特徵 (如頻寬和消耗產能)、技術 (如 P2P) 和風險層級為基礎的應用程式控制
- 可根據各使用者或網路規則實施應用程式控制原則

Web 和應用程式流量控管

- 增強的流量控管 (QoS) 選項，可根據網頁類別或應用程式限制或確保上傳 / 下載的優先性，以及個別或共用的位元速率

DNS 防護 (DNS Protection)

基於雲端的 DNS 服務

- 網域名稱解析服務
- 高效能基於雲端的 DNS 服務
- 由 SophosLabs 與 AI 驅動
- 在 DNS 查詢階段即封鎖惡意網址
- 提供精細的合規性控管，可依網站類別封鎖不當網站
- 由 Sophos Central 管理

NDR Essentials

網路偵測與回應

- 基於雲端的 NDR
- 由 AI 驅動
- 可在不進行 TLS 解密的情況下偵測加密的威脅通訊
- 偵測網域產生演算法
- 對潛在威脅進行評分，並針對超出自訂閥值的威脅發出警示
- 完整的報告與日誌支援

零時差威脅防護

動態的沙箱分析

- 完全整合到您的 Sophos 安全解決方案儀表板
- 檢查包含可執行內容的可執行檔和文件 (包括 .exe、.com、.dll、.doc、.docx、.docm 和 .rtf 與 PDF)，以及包含上列任何檔案類型的壓縮檔 (包括 ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet)
- 積極的行為、網路和記憶體分析
- 偵測規避沙箱的行為
- 使用深度學習的機器學習技術可掃描所有下載的執行檔
- 包括 Sophos Intercept X 的漏洞利用防禦和 CryptoGuard 防護技術
- 提供包含螢幕擷取畫面的詳盡惡意檔案報告，並可直接從儀表板釋放分析後的檔案給使用者
- 對檔案類型、例外狀況和分析後動作可提供彈性的使用者和群組原則
- 支援單次下載連結

靜態威脅情報分析

- 所有內含作用程式碼的檔案，並透過 Web 下載或以電子郵件附件進入防火牆，比如執行檔和有可執行內容的文件 (包括 .exe、.com、.dll、.doc、.docx、.docm 和 .rtf 與 PDF)，以及包含上列任何檔案類型的壓縮檔 (包括 ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet)，都會自動傳送以進行威脅情報分析
- 檔案會對照 SophosLabs 的大量威脅情報資料庫進行檢查，並接受多種機器學習模型的分析，以識別新的和未知的惡意軟體
- 豐富的報告功能，包括用於分析檔案的儀表板桌面工具、分析檔案的詳細列表和分析結果，以及概述每個機器學習模型結果的詳細報告

Central 協調

SD-WAN 協調

- 透過簡單且自動化的精靈，在網路位置間使用最佳化架構 (星狀、網狀拓撲或部分組合) 建立站台間的 VPN 通道，以進行 SD-WAN 和 VPN 協調。
- 支援 IPsec、SSL 或 RED VPN 通道。與 SD-WAN 功能無縫整合，以便安排應用程式優先性、路由最佳化，並利用多個 WAN 連結來提高彈性和效能

Central Firewall Reporting Advanced

- 可用於歷史防火牆報告的 30 天雲端資料儲存，並具備進階功能可保存、排程和匯出自訂報告

XDR 與 MDR 整合

- 可與 Sophos XDR 和 MDR 整合，將遙測與威脅情報導入用於威脅狩獵與分析
- Sophos Active Threat Response 可運用來自 MDR 與 XDR 分析師的威脅情資，以自動識別、封鎖並隔離網路上的主動威脅
- Synchronized Security 同步安全的 IoC 遙測會收集與威脅、使用者、程序與已遭入侵裝置相關的重要資料

電子郵件防護

電子郵件防護和控制

- 使用 SMTP、POP3 和 IMAP 支援進行電子郵件掃描
- 基於專利的迴圈模式偵測技術的信譽評等服務，搭配垃圾郵件爆發監控
- 在 SMTP 交易期間阻擋垃圾郵件和惡意軟體
- DKIM 和 BATV 反垃圾郵件防護
- 垃圾郵件灰名單和寄件者原則架構 (SPF) 防護
- 進行收件者驗證以防電子郵件地址錯誤
- 透過第二個獨立的惡意軟體偵測引擎 (Avira) 進行雙重掃描
- 可即時從雲端查閱最新的威脅情報以提供即時防護
- 自動特徵碼和特徵更新
- 智慧型的主機出站中繼支援
- 檔案類型偵測 / 阻擋 / 掃描附件
- 接受、拒絕或丟棄過大的郵件
- 偵測電子郵件中的網路釣魚 URL
- 使用預定義的內容掃描規則，或使用精細的原則選項和例外設定的一組條件建立自訂規則
- 對 SMTP、POP 以及 IMAP 的 TLS 加密支援
- 自動對所有外寄郵件附加簽名檔
- 電子郵件封存
- 透過使用者入口網站，進行以個別使用者為基礎的阻擋，以及維護允許的寄件者清單

電子郵件隔離管理

- 垃圾郵件隔離摘要和通知選項
- 可根據日期、寄件者、收件者、主旨當成搜尋與篩選選項，以隔離惡意軟體和垃圾郵件，並可依需要釋放和刪除郵件
- 自助服務使用者入口網站可檢視和釋放被隔離的郵件

電子郵件加密與 DLP

- 提供獨家 SPX 加密技術，可用以防護外寄的郵件訊息
- 收件者自我註冊的 SPX 密碼管理
- 將附件新增到 SPX 安全回覆中
- 完全透明運作，不需要額外的軟體或用戶端
- DLP 引擎可自動掃描電子郵件和包含敏感資料的附件
- 適用於 PII、PCI、HIPAA 等的預封裝敏感資料類型內容控制清單 (CCL)，該清單由 SophosLabs 所維護

Web 伺服器防護

Web 應用程式防火牆防護

- 反向代理
- URL 強化引擎，具備深度連結和目錄跨越防禦功能
- 表單強化引擎
- SQL 插入防護
- 跨站台指令碼防護
- 雙防毒引擎 (Sophos 與 Avira)
- HTTPS (TLS/SSL) 加密卸載
- 使用數位簽章的 Cookies 簽章
- 以路徑為基礎的路由
- 地理 IP 政策強制執行
- 自訂加密套件配置與 TLS 版本強制執行
- HSTS 與 X-Content-Type-Options 強制執行
- Outlook Anywhere 通訊協定支援
- 反向驗證 (卸載)，在存取伺服器時可用於以表單為基礎和基本的驗證
- 虛擬伺服器和實體伺服器抽象
- 整合式負載平衡器可將訪客分配到多台伺服器
- 可根據需要以精細的方式略過個人檢查
- 符合來源網路或指定目標網址的請求
- 支援 AND/OR 邏輯運算式
- 輔助各種設定和非標準部署的兼容性
- 變更 Web 應用程式防火牆效能參數的選項
- 掃描大小限制選項
- 允許 / 阻止 IP 範圍
- 伺服器路徑和網域支援萬用字元
- 自動附加用於驗證的前置詞 / 後置詞

報告和記錄

Central Firewall Reporting

- 具備彈性自訂選項的預定義報告
- Sophos Firewall 報告功能 (硬體、軟體、虛擬和雲端)
- 直覺的使用者介面提供資料的圖形化表示
- 報告儀表板提供過去 24 小時的事件總覽
- 輕鬆掌握網路活動、趨勢和可疑的攻擊
- 輕鬆備份日誌並提供快速檢索，以供稽核之用
- 簡化的部署，無需技術專業

Central Firewall Reporting Advanced

- 多防火牆彙整報告
- 保存自訂報告範本
- 排程報告功能
- 以 PDF、CFV 或 HTML 格式匯出報告
- 最多一年的資料儲存 (每防火牆)
- 用於威脅狩獵的 MDR/XDR 資料湖連接器

內建的報告功能

注意：Sophos Firewall 報告功能是免費的，但可用的日誌、報告和小工具取決於各自的防護模組授權許可證。

- 數百個立即可用的報告和自訂報告選項：儀表板 (流量、安全和使用者威脅商數)、應用程式 (應用程式風險、已封鎖應用程式、已同步應用程式、搜尋引擎、Web 伺服器、Web 關鍵字比對、FTP)、網路和威脅 (Active Threat Response 與威脅情報源、Security Heartbeat、IPS、無線、零時差威脅防護)、VPN、電子郵件、合規性 (HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3 和 CIPA)
- 目前活動監控：系統健康狀態、當前使用者、IPsec 連線、遠端使用者、有效連線、無線用戶端、隔離和 DoS 攻擊
- SD-WAN 連線效能監控，涵蓋抖動 (jitter)、延遲與封包遺失
- 匿名報告
- 透過具彈性頻率選項的報告群組，排程發送報告給多個收件者
- 匯出報告成 HTML、PDF、Excel (XLS)
- 報告書籤
- 根據類別自訂日誌的保留功能
- 具有行檢視和詳細檢視的全功能日誌檢視器，提供強大的篩選器和搜尋選項、包含超連結的規則 ID，以及資料檢視自訂功能

Central 管理

Sophos Central

- 適用於多個防火牆的 Sophos Central 雲端管理和報告功能可進行群組原則管理，以及透過單一主控台管理您的所有 Sophos IT 安全產品
- 群組原則管理可一次性修改物件、設定和原則，並自動同步到群組中的所有防火牆
- 工作管理器提供完整的歷史稽核紀錄，以群組原則變更的狀態監視
- Sophos Central 中的備份韌體管理可儲存每個防火牆的最後五個設定備份檔，並可釘選其中一個以便永久保存和易於使用
- 可由 Sophos Central 排程進行韌體更新，自動且輕鬆地隨時進行更新
- 零接觸部署可以在 Sophos Central 中執行初始設定，將設定匯出，以便在啟動外部裝置時用快閃磁碟機將設定載入裝置，然後自動將裝置連線回 Sophos Central

零信任網路存取

- 整合的 Sophos ZTNA 閘道器，實現對託管於防火牆後方的應用程式的安全存取
- 由 Sophos Central 管理

Sophos Firewall 功能摘要 (依訂閱)

	Xstream Protection 套裝組合							單獨購買		
	Standard Protection 套裝組合					*單獨購買*				
	Base Firewall	Network Protection	Web Protection	DNS Protection	僅限搭售組合的功能	Zero-Day Protection	Central Orchestration	Central Firewall Reporting Advanced	Email Protection	Web Server Protection
綜合管理 (包括 HA)	●									
Xstream 架構	●									
防火牆、網路和路由	●									
Xstream SD-WAN	●									
基本流量控管和配額	●									
安全無線	●									
驗證	●									
自我服務的使用者入口網站	●									
VPN (IPsec、SSL 等)	●									
RED 站台對站台 VPN	●									
Sophos Connect VPN 用戶端	●									
入侵防禦 (IPS)		●								
Active Threat Response										
Sophos X-Ops 威脅情報源		●								
MDR/XDR 威脅情報源					●					
第三方威脅情報源					●					
Synchronized Security Heartbeat		●								
SD-RED 裝置管理		●								
無用戶端 VPN		●								
同步應用程式控制			●							
Web 防護與控制			●							
應用程式防護與控制			●							
雲端應用程式可見度			●							
Web 和應用程式流量控管			●							
DNS 安全與合規性				●						
NDR Essentials					●					
動態沙箱分析						●				
威脅情報分析						●				
SD-WAN 協調							●			
Central Firewall Reporting 資料 *		7 天	7 天	7 天	7 天	7 天	30 天	最多一年	7 天	7 天
CFR Advanced 功能							●	●		
電子郵件防護和控制									●	
電子郵件隔離管理									●	
電子郵件加密與 DLP									●	
Web 應用程式防火牆防護										●
內建日誌 / 報告功能	●	●	●	●	●	●	●	●	●	●
Sophos Central Management**		●	●	●	●	●	●	●	●	●
ZTNA 閘道**		●	●	●	●	●	●	●	●	●

請注意：XGS 87 和 XGS 88 型號不支援某些功能，包括內建報告、雙防毒掃描、WAF 防毒掃描和電子郵件傳輸代理 (MTA) 功能

MSP 授權許可選項與上述內容略有不同

* 資料儲存保留時間依據平均網路使用量估算，實際依日誌資料量而異。儲存估算工具。

** 包含於任一搭售組合、支援或防護訂閱中。僅擁有基本授權許可證 (Base License) 的客戶必須加購支援服務，方可使用上述功能。

支援計畫

	增強支援 (ENHANCED SUPPORT) (包含在 Standard 與 Xstream Protection 搭售組合中)	增強 PLUS 支援 (ENHANCED PLUS SUPPORT) (可作為 Enhanced Support 的升級)
全天候 24/7 多管道支援 (電話、入口網站、即時聊天)，包含遠端協助與自助知識庫，以及使用支援論壇	●	●
韌體下載、更新與維護版本 **	●	●
Sophos Central 管理、報告與 ZTNA 閘道器功能	●	●
作用中裝置的提前硬體更換服務	●	●
被動 HA 裝置的提前硬體更換服務 *		●
SD-RED 與 APX 裝置的提前硬體更換服務		●
VIP 優先服務 (直接與資深工程師通話)		●
遠端顧問服務 (每年 2 至 8 小時)		●

* 若要啟用被動 HA 裝置的提前 RMA 更換服務，作用中裝置必須具備 Enhanced Plus 支援授權許可證
請參閱《Sophos 支援服務指南》以了解完整資訊。
** 注意：單獨購買模組必須加購支援服務才能收到韌體更新

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com

25-04-16 FL-ZHTW (MP)