



XG Firewall 功能

Sophos XG Firewall

重要功能

- ▶ 具備互動式控制中心的專屬使用者介面
- ▶ 經過最佳化的操作方式，3 個步驟內完成任何動作
- ▶ 政策控制中心桌面工具可監控企業、使用者和網路政策的活動，並且追蹤未使用、停用、變更和產生新政策的行為
- ▶ 新的統一政策模型可由單一畫面管理所有的企業、使用者和網路政策，並且提供強大的篩選和搜尋選項
- ▶ 提供一般業務應用程式範本，如 Microsoft Exchange、SharePoint、Lync 和更多 XML 的定義，以便提供自訂和共用的能力
- ▶ 使用自然語言描述的政策，並可總覽政策實施指標
- ▶ 可在單一畫面中，針對各使用者或網路政策自訂 IPS、網頁、應用程式和流量塑型 (QoS) 設定
- ▶ 跨越防火牆主要領域的第 8 層使用者身分感知
- ▶ Sophos Security Heartbeat 會連接起 Sophos 端點和防火牆，並且共用健康狀態和遙測數據，以便立即識別出不健康或被駭的端點
- ▶ 支援 Sophos Security Heartbeat 的政策可自動隔離遭駭端點或限制存取它們的行為
- ▶ 使用者威脅商數 (User Threat Quotient) 可根據最近的瀏覽行為和 ATP 觸發器資訊識別出高風險的使用者
- ▶ 應用程式風險表 (Application Risk Meter) 可根據網路上應用程式的風險等級提供整體風險係數
- ▶ 提供所有功能的設定 API，以供 RMM/PSA 整合之用
- ▶ 可在試用和 PoC (一開始只有命令列) 時無縫整合探索模式 (TAP 模式)
- ▶ 結合 Sophos Firewall Manager 提供全功能的集中式管理，並有硬體、軟體或虛擬設備等多種款式可供選擇

一般管理

- ▶ 專用且經簡化的使用者介面
- ▶ 任何動作都可在 3 個步驟內完成
- ▶ 自我記錄的功能表系統
- ▶ 在圖形化使用者介面 (GUI) 中提供進階疑難排解工具 (如封包擷取)
- ▶ 可由圖形化使用者介面中取得完全命令列介面 (CLI)
- ▶ 角色型管理
- ▶ 自動化的韌體更新通知，以及容易的自動化更新程序和回復功能
- ▶ 可重複使用的系統物件定義，包含網路、服務、主機、時段、使用者和群組、用戶端和伺服器
- ▶ 自我服務使用者入口網站，以進行一鍵式 VPN 安裝
- ▶ 設定變更追蹤
- ▶ 電子郵件或 SNMP 設陷通知選項
- ▶ 支援 SNMP

防火牆路由和服務

- ▶ 支援區域隔離和以區域為基礎的政策
- ▶ 提供 LAN、WAN、DMZ、本地、VPN 和 WiFi 的預設區域
- ▶ 針對 LAN 或 DMZ 自訂區域
- ▶ 路由：靜態、多重傳送 (PIM-SM) 和動態 (BGP、OSPF)
- ▶ 採用 IGMP 窺探 Snooping 進行無關通訊協定的多重路由
- ▶ 以 STP 支援和 APR 廣播轉向進行橋接
- ▶ WAN 連結平衡：多個網際網路連線、自動連結狀態檢查、自動故障轉移、自動和加權平衡，以及精細的多路徑規則
- ▶ 802.3ad 介面連結聚合
- ▶ 完全設定 DNS、DHCP 和 NTP
- ▶ IPv6 支援和通道支援，包括 6in4、6to4、4in6，以及透過 IPSec 快速部署 IPv6 (6rd)
- ▶ 支援 Sophos Remote Ethernet Device (RED)
- ▶ 支援 VLAN DHCP 和標記
- ▶ 支援多重橋接

進階型威脅保護和可同步安全性

- 偵測並阻擋試圖使用多層式的 DNS、AFC、HTTP Proxy 和防火牆連線指揮與控制 (C&C) 伺服器的網路流量
- Sophos Security Heartbeat 會立刻偵測出受駭的端點，包括主機、使用者、程序、事件數，以及遭駭的時間
- Sophos Security Heartbeat 的政策可限制存取網路資源的行為，或完全隔離受駭系統，直到它們被清理完畢

網路保護和控制

- 狀態式深度封包檢測防火牆
- FastPath 封包最佳化技術
- 入侵防禦：高效能、次世代的 IPS 深度封包檢測引擎
- 可選擇 IPS 模式以最大化效能和保護能力
- 洪流防禦：DoS、DDoS 和連接埠掃描阻擋能力
- 根據地理位置 IP 阻擋國家
- 站台對站台 VPN：SSL、IPSec、256 位元 AES/3DES、PFS、RSA、X.509 認證、預共用金鑰
- 遠端存取：SSL、IPSec、iPhone/iPad/Cisco VPN 用戶端支援
- 網路、使用者，或以網頁為基礎的流量塑形 (QoS)
- 網路流量配額可以無限制地自訂整體或個別網路流量的配額
- 即時 VoIP 最佳化

驗證

- 透過的代理驗證 (NTLM/Kerberos) 或用戶端驗證
- 使用以下進行驗證：Active Directory、eDirectory、RADIUS、LDAP 和 TACACS+
- Active Directory SSO、STAS、SATC 的伺服器驗證代理程式
- Windows、Mac OS X、Linux 32/64 的用戶端驗證代理程式
- iOS 和 Android 的驗證憑證
- 單一登入：Active Directory、eDirectory
- IPSec、L2TP、PPTP 和 SSL 的驗證服務
- 驗證入口網站

VPN 選項

- IPSec、SSL、PPTP、L2TP、Cisco VPN (iOS)、OpenVPN (iOS 和 Android)
- 無須用戶端的入口網站，使用 Sophos 獨家的加密 HTML5 自助服務入口網站，其支援 RDP、HTTP、HTTPS、SSH、Telnet 和 VPN
- 支援 Sophos Remote Ethernet Device (RED)

VPN IPsec 用戶端

- 驗證：預共用金鑰 (PSK)、PKI (X.509)、智慧卡、記號

和 XAUTH

- 加密：AES (128/192/256)、DES、3DES (112/168)、Blowfish、RSA (至多 2048 位元)、DH groups 1/2/5/14、MD5 和 SHA-256/384/512
- 智慧型區分通道功能以最佳化流量路由
- 支援 NAT 穿越 (NAT-traversal)
- 用戶端監聽器，提供連線狀態的圖性化概觀
- 多國語系：德文、英文、法文

VPN SSL 用戶端

- 經過驗證的 SSL (TLS) 型安全性
- 最低系統需求
- 支援不同存取等級的設定檔
- 支援 MD5、SHA、DES、3DES 和 AES
- 能穿越所有防火牆，無論其是否具備代理和 NAT
- 支援 iOS 和 Android

Remote Ethernet Device (RED) 支援

- 集中管理所有 RED 設備
- 無須設定：透過雲端佈建服務自動連線
- 使用數位 X.509 憑證和 AES256 加密保護加密通道
- 藉由防火牆訂閱的網路、網頁和電子郵件安全，可以完全保護 RED 站台
- 虛擬乙太網路可以在不同位置間可靠地傳輸流量
- 使用集中定義的 DHCP 和 DNS 伺服器設定管理 IP 位址
- 在停止作用一段時間後，可由遠端停用 RED 裝置的授權
- 壓縮通道流量 (RED 50、RED 10 第 2、3 版)
- VLAN 連接埠設定選項 (RED 50)

安全的無線

- 透過隨插即用輕鬆部署 Sophos 無線存取點—它們會自動出現在防火牆控制中心中
- 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
- 整合的安全性：防火牆會自動路由所有 Wi-Fi 流量
- 每個無線電都支援多個 SSID
- 強型加密支援最新的無線驗證功能，包含 WPA2-Enterprise 和 IEEE 802.1X (RADIUS 驗證)
- 提供 (自訂) 證書、每日密碼或接受條件與條款的熱點支援
- 提供圍牆花園 (Walled Garden，特定營運商服務項目) 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
- 在背景最佳化自動通道選擇
- 支援 HTTPS 登入

網頁保護和控制

- ▶ 完全透通的使用者型網頁篩選，無須使用任何代理設定
- ▶ 由 SophosLabs 支援的 URL 篩選資料庫中包含數百萬個網站，涵括 92 個類別
- ▶ 以使用者、群組、時間或網路為基礎的政策
- ▶ 瀏覽配額時間
- ▶ 惡意軟體掃描：阻擋在 HTTP/S、FTP 和網頁型電子郵件中所有形式的病毒、網頁惡意軟體、木馬程式和間諜軟體
- ▶ 使用 JavaScript 模擬的進階網頁惡意軟體保護
- ▶ Live Protection 即時雲端查詢可取得最新的威脅情報
- ▶ 提供第二種獨立的惡意軟體偵測引擎 (Avira) 以供雙重掃描之用
- ▶ 即時或批次模式的掃描
- ▶ 網址嫁接防禦
- ▶ 使用可自訂規則和例外，針對使用者或網路政策進行 HTTP 和 HTTPS 掃描
- ▶ SSL 通訊協定通道偵測和實施
- ▶ 憑證驗證
- ▶ 高效能的網頁內容快取
- ▶ 強制快取 Sophos 端點的更新
- ▶ 根據 mime 類型、副檔名和可作用內容類型 (如 ActiveX、applet、cookie 等) 進行檔案類型篩選
- ▶ 可實施 YouTube for Schools
- ▶ 實施 SafeSearch

應用程式保護和控制

- ▶ 使用數千個應用程式的特徵檔和第 7 層模式來增強應用程式控制
- ▶ 根據類別、特性 (如使用頻寬和產能)、技術 (如 P2P) 和風險等級進行應用程式控制
- ▶ 針對個別使用者或網路規則實施應用程式控制政策
- ▶ 自訂應用程式流量塑形選項，以限制或確保上傳/下載的優先性，以及個別或共用的位元速率

電子郵件保護和控制

- ▶ 信譽服務可根據專利的循環模式偵測技術，對垃圾郵件爆發的情形進行監控
- ▶ 在 SMTP 交易期間攔截垃圾郵件和惡意軟體
- ▶ 偵測電子郵件中的網路釣魚 URL
- ▶ 整體和個別使用者網域和位址的黑名單/白名單
- ▶ 使用 Active Directory 帳戶驗證收件者
- ▶ 電子郵件掃描 (支援 SMTP 和 POP3)
- ▶ 雙重防毒引擎 (Sophos & Avira)
- ▶ 真正檔案類型 (True-File-Type) 偵測/封存檔掃描
- ▶ 掃描嵌入式的郵件格式：使用 MIME 類型檢查阻擋惡意和無用的檔案
- ▶ 隔離無法掃描或檔案過大的郵件

- ▶ 篩選無限制數目的網域和郵箱中的郵件
- ▶ 自動更新特徵檔和模式
- ▶ Sophos 線上防毒即時雲端查詢

電子郵件加密和 DLP

- ▶ 專利申請中的 SPX 加密，可進行單向加密
- ▶ 收件者自我註冊 SPX 密碼管理
- ▶ 新增附件到 SPX 安全回信中
- ▶ 對 SMTP 電子郵件進行透通的加/解密和數位簽章
- ▶ 完全透通，不需要額外的軟體或用戶端
- ▶ 能對經過加密的電子郵件進行內容/病毒掃描
- ▶ 對所有金鑰和憑證進行集中式管理—不需要發放金鑰或憑證
- ▶ 可自動掃描電子郵件和附件中機密資料的 DLP 引擎
- ▶ 針對 PII、PCI、HIPAA 和其他規範提供預封裝的機密資料內容控制清單 (CCLs)，此清單是由 SophosLabs 所支援

使用者自助服務入口網站

- ▶ SMTP 隔離：檢視並放行被隔離的郵件
- ▶ 寄件者黑名單/白名單
- ▶ 熱點存取資訊
- ▶ 下載 Sophos Authentication Agent (SAA)
- ▶ 下載遠端存取用戶端軟體和設定檔
- ▶ HTML5 VPN 入口網站可對使用預訂服務的預訂主機開放無用戶端的 VPN 連線
- ▶ 下載 HTTPS 代理的 CA 憑證

網頁應用程式防火牆保護

- ▶ 反向代理
- ▶ 具備深度連結和目錄穿越防禦的 URL 強化引擎
- ▶ 表單強化引擎
- ▶ SQL 隱碼攻擊防護
- ▶ 跨站台執行指令碼防護
- ▶ 雙重防毒引擎 (Sophos & Avira)
- ▶ HTTPS (SSL) 加密卸載
- ▶ 對 cookie 進行數位簽章
- ▶ 以路徑為基礎的路由
- ▶ 支援 Outlook Anywhere 通訊協定
- ▶ 存取伺服器時進行表單型和基本型驗證的反向驗證 (卸載)
- ▶ 虛擬伺服器和實體伺服器抽象
- ▶ 整合式的負載平衡器可將訪客分散到多個伺服器
- ▶ 依需要以精確的方式跳過個別的檢查
- ▶ 比較來自來源網路或特定目標 URL 的請求

XG Firewall 功能

- 支援邏輯 AND/OR 運算子
- 協助不同設定和非標準部署達成相容性
- 提供變更 WAF 效能參數的選項
- 掃描大小限制選項
- 允許/阻擋 IP 範圍
- 伺服器路徑支援萬用字元
- 自動套用前置/後置字元以供驗證

記錄與報告

- 數百個立即可用的報告和數十個自訂報告選項
- 資料匿名
- 可根據報告群組，經由數種具彈性的頻率選項排程提供報告給多個收件者
- 根據類別自訂日誌保留
- 完全日誌檢視器
- 提供流量、安全和使用威脅商數等儀表板
- 提供使用者應用程式風險、阻擋使用者應用程式、網頁風險、已阻擋網頁意圖、搜尋引擎、網頁伺服器使用情形、網頁伺服器保護，以及使用者資料傳輸和 FTP 流量的應用程式報告
- 入侵攻擊、進階威脅防禦、無線和 Security Heartbeat 等網路與威脅報告
- VPN 報告
- 電子郵件使用情形和保護報告
- HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3 和 CIPA 等合規性報告

英國和全球銷售

電話：+44 (0)8447 671131
Email：sales@sophos.com

北美銷售

免付費電話：1-866-866-2802
Email：nasales@sophos.com

澳大利亞和紐西蘭

電話：+61 2 9409 9100
Email：sales@sophos.com.au

亞洲銷售

電話：+65 62244168
Email：salesasia@sophos.com

牛津·英國 | 波士頓·美國

© 2015 版權所有，Sophos Ltd. 保留一切權利。

英格蘭和威爾斯註冊編號 No. 2096520，The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos Ltd. 的註冊商標。所有提及其他產品和公司名稱均屬各自擁有者的商標或註冊商標。