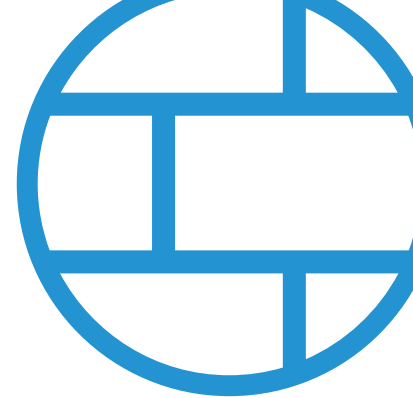


SOPHOS

Security made simple.



XG Firewall 功能

Sophos XG Firewall

主要功能

- 具備互動式控制中心的專屬使用者介面
- 經過最佳化，任何動作都可在 3 個步驟內完成
- 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，以及總覽型的政策實施指標
- 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，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
- 探索模式 (TAP 模式) 在試用和 PoC 時提供無縫整合
- 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
- 新的虛擬和軟體授權模式是根據 CPU 和記憶體資源為基礎

基本防火牆

一般管理

- 專用且簡化的使用者介面
- 經過最佳化，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)
- 高可用性 (HA) 支援以主動-主動或主動-被動模式叢集兩台裝置。
- 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
- 自助服務使用者入口網站
- 設定變更追蹤
- 根據區域對服務進行彈性的裝置存取控制
- 電子郵件或 SNMP 設陷通知選項
- SNMP 和 Netflow 支援
- 來自 Sophos Firewall Manager 或 Sophos Cloud Firewall Manager 的集中管理支援
- 備份和還原設定：本機、透過 FTP 或電子郵件；隨需、每日、每週或每月
- 提供 API 供第三方整合
- 提供由遠端存取 Sophos Support 的選項
- 透過 MySophos 採用雲端型授權管理

防火牆、網路和路由

- 狀態式深度封包檢測防火牆
- FastPath 封包最佳化技術
- 以使用者、群組、時間或網路為基礎的政策
- 根據使用者/群組的存取時間政策
- 跨區域、網路或服務類型實施政策
- 支援區域隔離和以區域為基礎的政策
- 提供 LAN、WAN、DMZ、LOCAL、VPN 和 WiFi 的預設區域
- 針對 LAN 或 DMZ 自訂區域
- 可自訂具備 IP 偽裝功能的 NAT 政策
- 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
- 路由：靜態、多重傳送 (PIM-SM) 和動態 (BGP、OSPF)
- 採用 IGMP 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

XG Firewall 功能

- ▶ 支援 VLAN DHCP 和標記
- ▶ 支援多重橋接
- ▶ 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
- ▶ 無線 WAN 支援 (虛擬部署中不可用)
- ▶ 802.3ad 介面連結聚合
- ▶ 完全設定 DNS、DHCP 和 NTP
- ▶ 動態 DNS
- ▶ IPv6 支援和通道支援，包括 6in4、6to4、4in6，以及透過 IPSec 快速部署 IPv6 (6rd)

基本流量塑型和配額

- ▶ 彈性的網路或以使用者為基礎的流量塑型 (QoS) (Web Protection 訂閱中包含增強的網頁和應用程式流量塑型選項)
- ▶ 設定使用者上傳/下載、總流量和週期性或非週期性的流量配額
- ▶ 即時 VoIP 最佳化

保護無線

- ▶ 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
- ▶ 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
- ▶ 透過用戶端隔離選項，橋接 AP 到 LAN、WAN 或不同的區域
- ▶ 每個無線電支援多個 SSID，包括隱藏的 SSID
- ▶ 支援最新的安全和加密，包括 WPA2 Personal 和 Enterprise
- ▶ 支援 IEEE 802.1X (RADIUS 驗證)
- ▶ 支援 802.11r (快速轉換)
- ▶ 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 (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
- ▶ 對支援的 AP 提供無線中繼和橋接網狀網路模式
- ▶ 在背景最佳化自動通道選擇
- ▶ 支援 HTTPS 登入
- ▶ 偵測流氓 AP (Rogue AP)

驗證

- ▶ 透通的代理驗證 (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 驗證服務
- ▶ 驗證入口網站

使用者自助服務入口網站

- ▶ 下載 Sophos Authentication Client
- ▶ 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情形
- ▶ 存取隔離的郵件 (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 認證、預共用金鑰
- ▶ L2TP 和 PPTP
- ▶ 遠端存取：SSL、IPSec、iPhone/iPad/Cisco/Android VPN 用戶端支援
- ▶ 適用於 Windows 的 SSL 用戶端，以及透過使用者入口網站下載設定檔

IPSec 用戶端 (另外選購)

- ▶ 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

Network Protection 訂閱授權

入侵防禦 (IPS)

- ▶ 高效能、新世代的 IPS 深入封包檢測引擎具備選擇性 IPS 模式，可發揮最大效能和保護能力
- ▶ 數千個特徵檔
- ▶ 支援自訂 IPS 特徵檔
- ▶ 彈性的 IPS 政策部署，可成為任何網路或使用者政策的一部分，並可完全自訂

ATP 和 Security Heartbeat™

- ▶ 進階型威脅偵測 (偵測並阻擋試圖使用多層式的 DNS、AFC 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

Remote Ethernet Device (RED) 支援

- ▶ 集中管理所有 RED 裝置
- ▶ 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
- ▶ 虛擬乙太網路可以在不同位置間可靠地傳輸流量

XG Firewall 功能

- 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
- VLAN 連接埠設定選項 (RED 50)

無用戶端 VPN

- 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

Web Protection 訂閱授權 網頁保護和控制

- 完全透通的代理，以供防惡意軟體和網頁篩選之用
- 增強的進階型威脅防護
- 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
- 根據使用者/群組的瀏覽配額時間政策
- 根據使用者/群組的存取時間政策
- 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
- 利用完全可自訂的規則和例外，掃描 HTTP 和 HTTPS，以及實施任何網路和使用者政策
- 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
- 微型應用程式 (micro app) 的探索與控制
- 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
- 網頁與應用程式流量塑型
- 增強的流量塑型 (QoS) 選項可根據網頁類別或應用程式，限制或保證上傳/下載或總流量的優先性，以及個別與共用的位元率

Email Protection 訂閱授權 電子郵件保護和控制

- 電子郵件掃描 (支援 SMTP 和 POP3)
- 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
- 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
- Live Protection 即時雲端查詢可取得最新的威脅情報
- 自動更新特徵檔和模式
- 檔案類型偵測/阻擋/掃描附件
- 接受、退回或丟棄過大的郵件
- 偵測電子郵件中的網路釣魚 URL
- 使用預定義內容掃描規則或根據一組條件建立自己的自訂規則
- 對 SMTP、POP 和 IMAP 提供 TLS 加密支援
- 自動對出埠郵件附加簽名
- 電子郵件歸檔

電子郵件隔離管理

- 垃圾郵件隔離摘要和通知選項
- 根據日期、寄件者、收件者、主旨等篩選器選項隔離惡意軟體和垃圾郵件，並提供放行和刪除郵件的理由
- 自助服務的使用者入口網站可觀看和放行被隔離的郵件

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
- 完全透通，不需要額外的軟體或用戶端
- 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 (CCL)，此清單是由 SophosLabs 所支援

Web Server 訂閱授權 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

XG Firewall 功能

- 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
- 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

注意：日誌、報告和桌面工具會根據啟用的軟體訂閱個別提供

- 數百個立即可用的報告和自訂報告選項：
- 儀表板 (流量、安全性和使用者威脅商數)、應用程式 (應用程式風險、阻擋的應用程式、搜尋引擎、網頁伺服器、FTP)、網路與威脅 (IPS、ATP、無線、Security Heartbeat)、VPN、電子郵件、合規性 (HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3、CIPA)
- 目前活動監控：系統健康狀態、線上使用者、IPSec 連線、遠端使用者、線上連線、無線用戶端、隔離和 DoS 攻擊
- 報告匿名化
- 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
- 報告可匯出為 HTML、PDF、Excel (XLS)
- 報告書籤
- 完全日誌檢視器，具備根據類別自訂保留的功能

XG Firewall 功能摘要 (根據訂閱選項)

功能 (如上所列)	FullGuard License				
	EnterpriseGuard License				Web Server Prot.
	Base Firewall	Network Protection	Web Protection	Email Protection	
一般管理 (包括 HA)	●				
防火牆、網路與路由	●				
基本流量塑型與配額	●				
保護無線	●				
驗證	●				
自助服務使用者入口網站	●				
基本 VPN 選項	●				
IPSec 用戶端	個別販售				
入侵偵測 (IPS)		●			
ATP & Security Heartbeat™		●			
Remote Ethernet Device (RED) VPN		●			
無用戶端 VPN		●			
網頁保護和控制			●		
應用程式保護和控制			●		
網頁和應用程式流量塑型			●		
電子郵件保護與控制				●	
電子郵件隔離管理				●	
電子郵件加密與 DLP				●	
網頁應用程式防火牆保護					●
日誌和報告	●	●	●	●	●

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。

SOPHOS