SOPHOS
Security made simple.

XG Firewall 功能

Sophos XG Firewall

重要功能

- 具有交互式控制中心的專用使用者界面
- 最佳化的 3 點擊到任意位置操作 (3-clicks-to-anywhere)
- 政策控制中心 (Policy Control Center) 桌面工具會監控業務、使用者和網路政策的政策活動，並追蹤未使用、停用、已變更和新的政策
- 利用新的統一式政策模式，可在具有強大的篩選和搜索選項的單一畫面上管理所有的業務、使用者和網路政策
- 提供常見業務應用程式 (如 Microsoft Exchange、SharePoint、Lync) 和更多以 XML 定義的政策範本，以實現自訂化和共享。
- 詳盡的防火牆政策描述和一目瞭然的政策實施指標
- 在單一畫面上自訂每個使用者或網路政策的 IPS、Web、應用程式和流量塑形 (QoS) 設定
- 跨防火牆多個關鍵區域的第 8 層使用者身分識別感知
- Sophos 安全活動訊號 (Security Heartbeat) 將 Sophos 端點與防火牆連接起來，共享健康狀態和遙測功能，以便即時識別出不合格或受駭的端點
- 對 Sophos Security Heartbeat 的政策支援可自動隔離或限制對受駭端點的網路存取行為
- 使用者威脅商數 (User Threat Quotient) 可根據最近的瀏覽行為和 ATP 觸發器來識別出有風險的使用者
- 應用程式風險計數器 (Application Risk Meter) 根據網路中應用程式風險層級提供整體風險因素
- 適用於 RMM/PSA 所有整合功能的設定 API
- 可無縫整合試用版和 PoC (概念驗證) 的探索模式 (TAP 模式)
- Sophos Firewall Manager 提供全功能的集中式管理，有硬體、軟體或虛擬設備等款式
- 新的虛擬和軟體授權模式，可根據 CPU 和記憶體資源授權

基本防火牆

綜合管理

- 專用的簡化使用者界面
- 3 點擊到任意位置操作
- 自我記錄的功能表系統
- 圖形化使用者介面 (GUI) 中的進階疑難排解工具 (如封包擷取)
- 高可用性 (HA) 支援以主動-主動 (active-active) 或主動-被動 (active-passive) 模式可叢集兩部裝置。
- 可從 GUI 使用完整的命令列介面 (CLI)
- 以角色為基礎的管理
- 自動韌體更新通知，並具備輕鬆的自動更新程序和回復功能
- 網路、服務、主機、時段、使用者和群組、用戶端和伺服器的可重複使用系統物件定義
- 自我服務的使用者入口網站
- 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
- 來自 Sophos Firewall Manager 或 Sophos Cloud Firewall Manager 的中央管理
- 備份與還原設定：可依需要於每日、每週或每月在本機透過 FTP 或電子郵件進行設定
- 適用於第三方整合的 API
- Sophos Support 的遠端存取選項
- 透過 MySophos 進行雲端授權管理

XG Firewall 功能

防火牆、網路和路由

- 狀態式深度封包偵測防火牆
- FastPath 封包最佳化
- 使用者、群組、時間或網路型政策
- 根據使用者/群組的存取時間政策
- 跨區域、網路或根據服務類型實施政策
- 區域隔離和區域型政策支援。
- LAN、WAN、DMZ、本機、VPN 和 WiFi 的預設區域
- LAN 或 DMZ 上的自訂區域
- 可偽裝 IP 的可自訂 NAT 政策
- 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：靜態、多點傳送 (PIM-SM) 和動態 (RIP、BGP、OSPF)
- 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
- 多重橋接支援
- WAN 連結平衡：多重網際網路連線、自動連結健康狀況檢查、自動容錯移轉、自動加權平衡以及精細的多路徑規則
- 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
- IPv6 支援，包括 6in4、6to4、4in6 和透過 IPSec 的 IPv6 快速部署

基本流量塑形和配額

- 彈性的網路或使用者型流量塑形 (QoS) (Web Protection 訂閱中包含增強的 Web 和應用程式流量塑形選項)
- 對上傳/下載或總流量，以及周期性或非週期性設定使用者的流量配額
- 即時 VoIP 最佳化

安全無線

- Sophos 無線存取點 (AP) 採用簡單的即插即用部署 — 自動回報至防火牆接受控管
- 利用內建的無線控制器由中央監控和管理所有存取點和無線用戶端
- 橋接存取點到區域網路、VLAN 或一個使用用戶端隔離選項的單獨區域
- 每個無線電都支援多個 SSID，包括隱藏的 SSID
- 支援最新的安全和加密，包括 WPA2 個人和 WPA2 企業
- 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、當天密碼認證或是一般使用說明的接受認證
- 提供訪客無線存取網際網路，並附帶圍牆花園 (walled garden) 選項
- 以時間為基礎的無線網路存取
- 透過 Sophos 所支援的 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
- 惡意 AP 掃描

驗證

- 透通的代理驗證 (NTLM/Kerberos) 或用戶端驗證
- 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
- 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
- 適用於 IPSec、L2TP、PPTP、SSL 的驗證服務

- 網頁驗證入口

使用者自助服務入口網站

- 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 (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、預先共用金鑰
- L2TP、PPTP
- 遠端存取：SSL、IPsec、iPhone/iPad/ Cisco/Android VPN 用戶端支援
- 透過使用者入口網站下載 Windows SSL 用戶端和設定

IPsec 用戶端 (另外販售)

- 驗證：預共用金鑰 (PSK)、PKI (X.509)、智慧卡、權杖和 XAUTH
- 加密：AES (128/192/256)、DES、3DES (112/168)、Blowfish、RSA (高達 2048 位元)、DH 群組 1/2/5/14、MD5 和 SHA-256/384/512
- 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
- 多種語言：德文、英文和法文

Sandstorm Protection 訂閱

Sandstorm Cloud Sandbox Protection

- 完全整合到您的 Sophos 安全解決方案
- 檢查包含可執行內容的可執行檔和文件
- Windows 執行檔 (包括 .exe、.com 和 .dll)
- Word 文件 (包括 .doc、.docx、docm 和 .rtf)
- PDF 文件
- 可於壓縮檔內偵測到上述任何檔案類型
- (ZIP、BZIP、GZIP、RAR、TAR、LHA/ LZH、7Z、Microsoft Cabinet)
- 支援超過 20 種檔案類型
- 可在真實環境中執行檔案分析動態惡意軟體行為
- 提供詳盡的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
- 分析時間平均不到 120 秒
- 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政策
- 支援單次下載連結

Network Protection 訂閱

入侵防禦 (IPS)

- 高效能的新一代 IPS 深度封包偵測引擎，具備選擇性 IPS 模式，可實現最佳效能和保護
- 數千種特徵碼
- 支援自訂 IPS 特徵碼
- 彈性的 IPS 政策部署，可完全自訂並作為任何網路或使用者政策的一部分

ATP 和 Security Heartbeat™

- 進階型威脅防護 (偵測並阻止嘗試使用多層式 DNS、AFC 和防火牆來聯繫命令控制伺服器的網路流量)
- Sophos Security HeartBeat™ 會立即識別出受駭的端點，包括主機、使用者、處理序、事件數和受駭時間
- Sophos Security Heartbeat™ 的政策可以限制對網路資源的存取或完全隔離遭駭的系統，直到威脅被清除為止

Remote Ethernet Device (RED) VPN

- 所有 RED 裝置的中央管理
- 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 AES256 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 RED 裝置
- 通道流量壓縮
- VLAN 連接埠設定選項 (RED 50)

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、HTTP、HTTPS、SSH、Telnet 和 VNC

Web Protection 訂閱

Web 保護和控制

- 適用於防惡意軟體和 Web 篩選的完全透通代理
- 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/群組的存取時間政策
- 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
- 可即時從雲端雲中查閱最新的威脅情報達到即時保護功能
- 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
- 可在任何網路或使用者政策中設定 HTTP 和 HTTPS 掃描與強制，並完全可自訂和支援例外情況
- SSL 通訊協定通道偵測和強制
- 憑證驗證
- 高效能網頁內容快取
- 強制快取 Sophos Endpoint 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
- YouTube for Schools 強制
- SafeSearch 強制

應用程式保護與控制

- 採用特徵碼和數千種應用程式的第 7 層模式來增強應用程式控制
- 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政策

Web 和應用程式流量塑形

- 增強的流量塑形 (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

Email Protection 訂閱

電子郵件保護和控制

- 使用 SMTP、POP3 和 IMAP 支援進行電子郵件掃描
- 具垃圾郵件疫情監控能力的信譽服務採用專利的循環模式偵測 (Recurrent-Pattern-Detection) 技術
- 在 SMTP 交易期間阻擋垃圾郵件和惡意軟體
- 透過第二個獨立的惡意軟體偵測引擎 (Avira) 進行雙重掃描
- 可即時從雲端雲中查閱最新的威脅情報達到即時保護功能
- 自動特徵碼和模式更新
- 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
- 使用者預定義的內容掃描規則，或可建立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

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

電子郵件加密和 DLP

- 提供獨家的 SPX 加密技術，用以保護外寄的郵件訊息
- 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
- 完全透通，不需要額外安裝用戶端軟體
- 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 Server Protection 訂閱

Web 應用程式防火牆保護

- 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
- 跨站台指令碼保護
- 雙防毒引擎 (Sophos 與 Avira)
- HTTPS (SSL) 加密卸載
- 使用數位簽章的 Cookies 簽章
- 以路徑為基礎的路由
- 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
- 掃描尺寸限制選項
- 允許/阻止 IP 範圍
- 伺服器路徑支援萬用字元
- 自動附加用於驗證的前置詞/後置詞

記錄和報告

注意：個別日誌、報告和桌面工具的可用性依啟用軟體訂閱而有不同。

- 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、搜尋引擎、網頁伺服器、FTP)、網路和威脅 (IPS、ATP、無線、Security Heartbeat)、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
- 報告匿名
- 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
- 可根據類別自訂保留功能的完整日誌檢視器

XG Firewall 功能摘要 (依訂閱)

功能: (如表所列)		FullGuard Plus				
			FullGuard			
			EnterpriseGuard			
	基本防火牆	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
綜合管理 (包括 HA)	●					
防火牆、網路和路由	●					
基本流量塑形和配額	●					
安全無線	●					
驗證	●					
自我服務的使用者入口網站	●					
基本 VPN 選項	●					
IPsec 用戶端	個別販售					
Sandstorm Protection		●				
入侵防禦 (IPS)			●			
ATP 和 Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
無用戶端 VPN			●			
Web 保護和控制				●		
應用程式保護與控制				●		
Web 和應用程式流量塑形				●		
電子郵件保護和控制					●	
電子郵件隔離管理					●	
電子郵件加密和 DLP					●	
Web 應用程式防火牆保護						●
日誌和報告	●		●	●	●	●

台灣業務窗口
電話: +886 2 7709 1980
電子郵件: Allan.Lan@Sophos.com

香港業務窗口
電話: +852 2520 2608
電子郵件: saleshk@sophos.com

中國業務窗口 (北京)
電話: 400 650 6598
電子郵件: salescn@sophos.com

中國業務窗口 (上海)
電話: +86 21 3251 7160
電子郵件: salescn@sophos.com

16-12 FLNA (SM)