解決方案簡介

Sophos Firewall

SOPHOS
Cybersecurity evolved.

目錄

Sophos Firewall

Sophos Firewall 是專為解決當今防火牆所面臨的主要問題而設計，同時還提供了一個真正的新一代平台來應對今日的網際網路中加密的流量檢測和不斷發展的威脅態勢。SophosFirewall 使用一種全新的方法來識別隱藏的風險、防範威脅以及回應事件，而且不會影響效能。我們適用於 Sophos Firewall 的 Xstream 架構利用封包處理架構，可提供極高等級的可見度、保護和效能。

Sophos Firewall 可以對高風險使用者、不必要的應用程式、可疑的Payload和持續性威脅提供無可比擬的可見度。它緊密地整合了一整套容易設定與維護的現代威脅防護技術。與上一代防火牆不同，Sophos Firewall 可與網路上的其他安全系統進行通訊，使其成為受信任的實施點，以遏制威脅，自動且即時地阻擋惡意軟體在網路散播或外洩資料。

與它牌網路防火牆相比，Sophos Firewall 具有三大優勢：

1. **揭露隱藏的風險** 透過視覺化的儀表板、立即可用的雲端報告，以及獨特的風險見解，Sophos Firewall 在揭露隱藏的風險方面比其他解決方案做得更好。
2. **阻擋未知威脅** Sophos Firewall 使用了一系列非常容易設定與管理的進階防護功能，在阻擋未知威脅方面比其他防火牆更快、更容易而且更有效率。
3. **自動回應事件** 歸功於可在端點和防火牆之間共用即時情報的 Sophos Security Heartbeat™，具備同步安全功能的 Sophos Firewall 會自動回應網路上的事件。

揭露隱藏的風險

對於現代防火牆來說，能夠透過所收集的大量資訊進行剖析、關聯資料 (如果可行)，並只找出需要回應的關鍵資訊，是非常重要的，可以防範未然。

Xstream SSL 檢查

加密流量的完美風暴正在成形之中。根據 Google 的報告，網路上的加密流量已經成長到 90% 以上。這種成長表示網路犯罪分子有機會發動隱匿且難以偵測到的攻擊。畢竟，您無法阻止看不到的攻擊。遺憾的是，大多數組織對此都無能為力，因為他們目前的防火牆都無法在不大幅影響效能的前提下使用 TLS/SSL 檢查。

Sophos Firewall 及全新的 Xstream SSL 檢查引擎具備更高的負載能力以進行同時連線，並提供彈性的政策工具，可根據應掃描和可掃描的內容做出明智的決策，在適當情況下卸載流量。組織可以使用 SSL 政策工具，針對無法解密的流量、憑證、通訊協定、加密執行選項等建立企業級的 TLS/SSL 政策。Sophos Firewall 系統中的每個連接埠和應用程式均支援 TLS 1.3 和所有現代加密套件。

儀表板上的其他工具可讓系統管理員確實了解多少網路流量經過加密，以及如何處理這些流量。相較於其他解決方案，Sophos Firewall 在呈現這些資訊方面做得更好，特別是能醒目提示憑證驗證錯誤或網站不支援最新加密標準的情形。

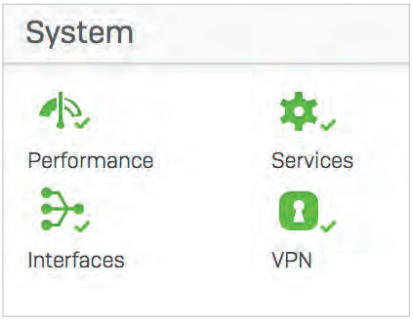
系統管理員也可以從彈出視窗了解有問題的網站、原因以及遇到問題的使用者。他們可以直接採取動作，不對這些應用程式或網站解密，以防止進一步的問題出現。其他任何 SSL 檢查解決方案都無法如此容易地取得這個資訊。

控制中心

Sophos Firewall 的控制中心為網路上的活動、風險和威脅提供前所未有的可見度。

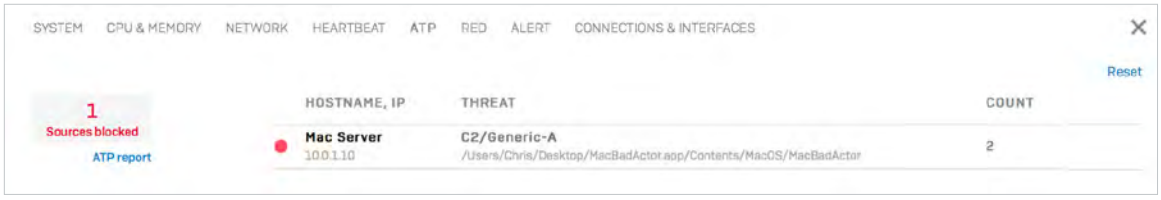
它使用「交通號誌」風格的指標，讓您的注意力放在對您最重要的事項上。

如果亮紅燈，表示需要立即注意。黃燈表示潛在問題。如果亮綠燈，表示無須採取任何動作。

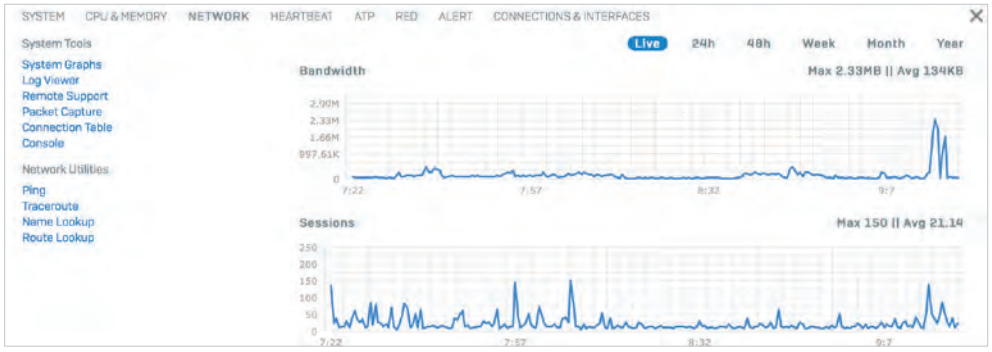


控制中心上的每個桌面工具都提供了額外資訊，只要按一下該桌面工具，即可輕鬆顯示。例如，按一下控制中心上的「介面」桌面工具，就可以取得裝置上的介面狀態。

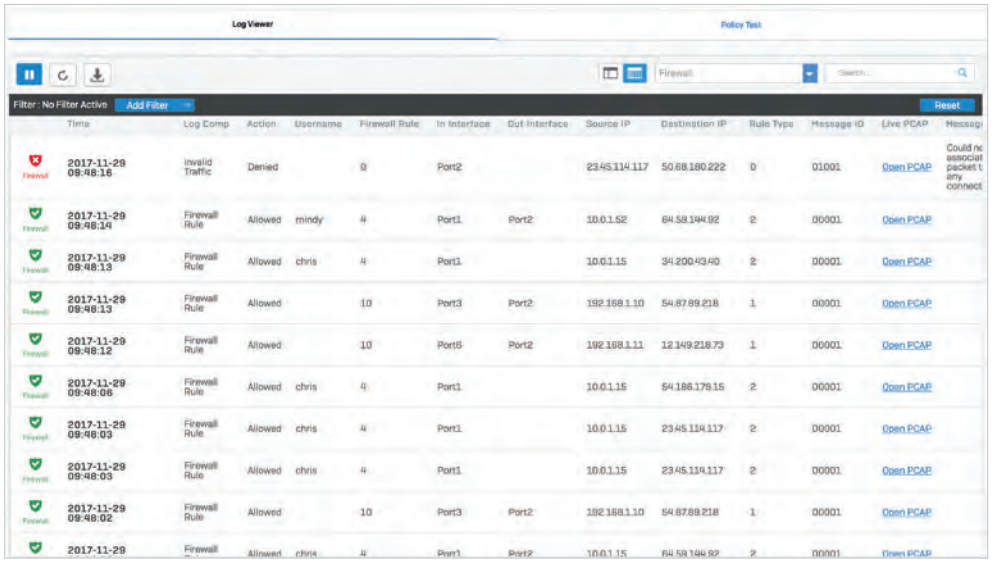
只要按一下儀表板中的「ATP」(進階威脅防護) 桌面工具，也可以輕鬆辨識和進階型威脅相關的主機、使用者和來源。



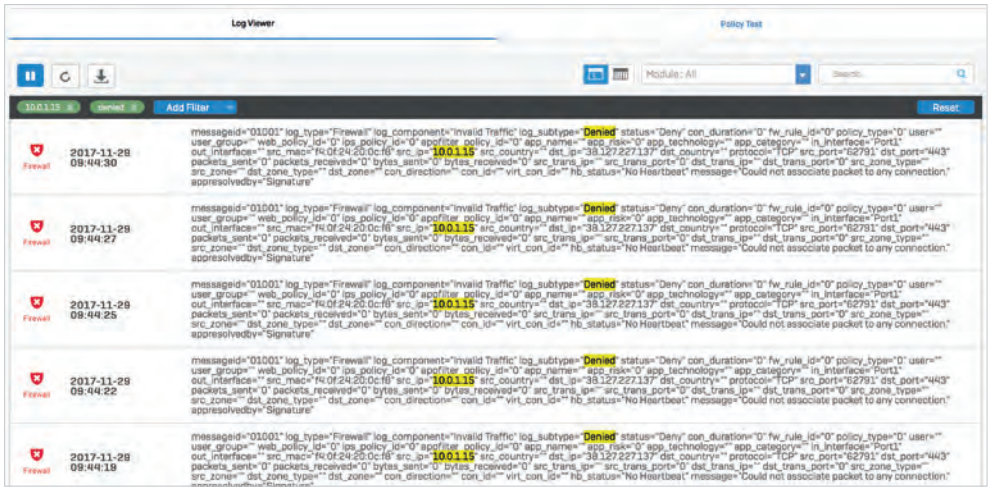
系統圖表也可以用來顯示一段時間的效能，無論是前兩個小時到上個月，甚至是去年都可以。此外，它們還能讓您快速使用常用的疑難排解工具以解決潛在問題。



只要按一下滑鼠，就可以從每個畫面取得即時日誌檢視器。您可以在新視窗中開啟該檢視器，就可以在主控台上作業的同時觀看相關的日誌。即時日誌檢視器提供兩種檢視模式：一種是較簡單的欄位型格式 (依防火牆模組)，另一種是更詳細的統一檢視模式，包含功能強大的篩選和排序選項，可將整個系統的日誌彙總成單一即時檢視。



如果您和大多數網路管理員一樣，或許會想知道防火牆規則是否過多，以及哪些是真正必要的，哪些是實際上不會用到的。有了 Sophos Firewall，您再也不用猜測了。



「使用中的防火牆規則」桌面工具可針對防火牆處理的流量，依下列規則類型顯示即時圖表：商業應用程式、使用者和網路規則。它也可以依狀態顯示使用中的規則計數，包括未使用的規則，讓您有機會進行整理。如同控制中心的其他區域般，按一下任何一者都可以深入探索。在此案例中，我們深入探索防火牆規則表 (依規則類型或狀態排序)。

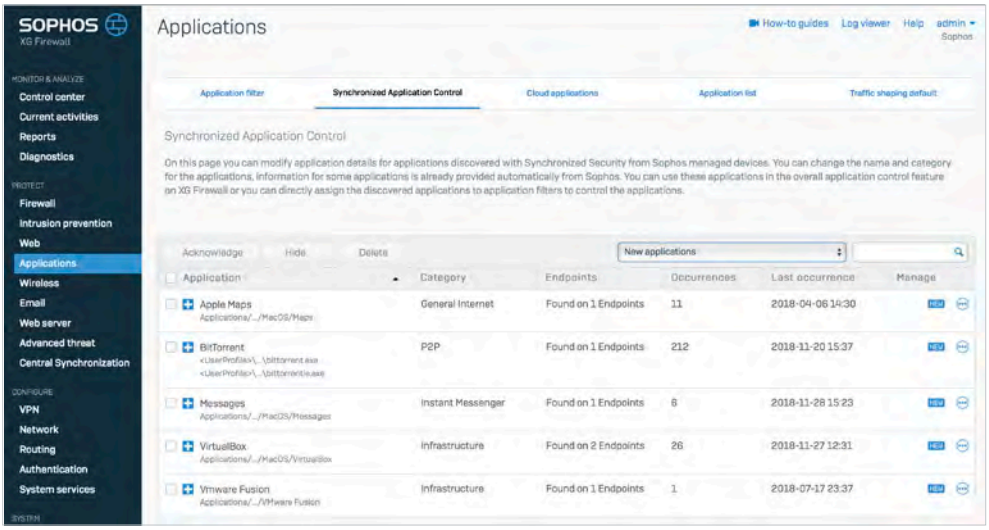
同步應用程式控制

現今新一代防火牆的應用程式控制問題是，無法識別大部分的應用程式流量：這些流量未經分類或標示為未知，使用一般 HTTP 或一般 HTTPS。

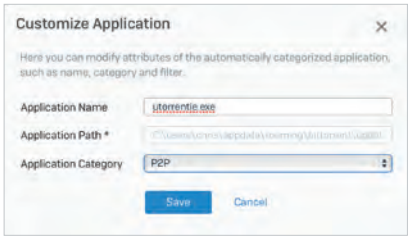
原因很簡單，因為所有防火牆應用程式控制引擎都依賴特徵碼和模式來識別應用程式。此外，如同您所預料，客製化的垂直市場應用程式 (例如醫療和財務應用程式) 絕對都不會有特徵碼。其他隱匿型應用程式 (如 BitTorrent 用戶端和 VoIP 以及即時通訊應用程式) 會一直改變其行為與特徵碼，以逃避偵測和控制。許多應用程式現在使用加密躲避偵測，而某些應用程式只是使用類似於通用網頁瀏覽器的連線，然後透過防火牆向外進行通訊，因為連接埠 80 和 443 在大多數的防火牆上通常暢通無阻。

結果，我們完全看不到網路上的應用程式，而看不到就無法控制。這個問題的解法非常簡潔且有效：Sophos 同步應用程式控制，其使用我們獨特的同步安全連線搭配受 Sophos 管理的端點。

以下是它的運作方式。當 Sophos Firewall 看到無法利用特徵碼識別的應用程式流量時，會詢問端點是哪個應用程式產生該流量。



端點會分享該可執行檔的名稱、路徑，通常還有類別，並將該資訊傳回防火牆。以後防火牆就可以利用此資訊，在大部分情況中自動分類並控制該應用程式。



如果 Sophos Firewall 無法自動判斷正確的應用程式類別，系統管理員可以設定所需的類別，或將應用程式指派給現有的政策。

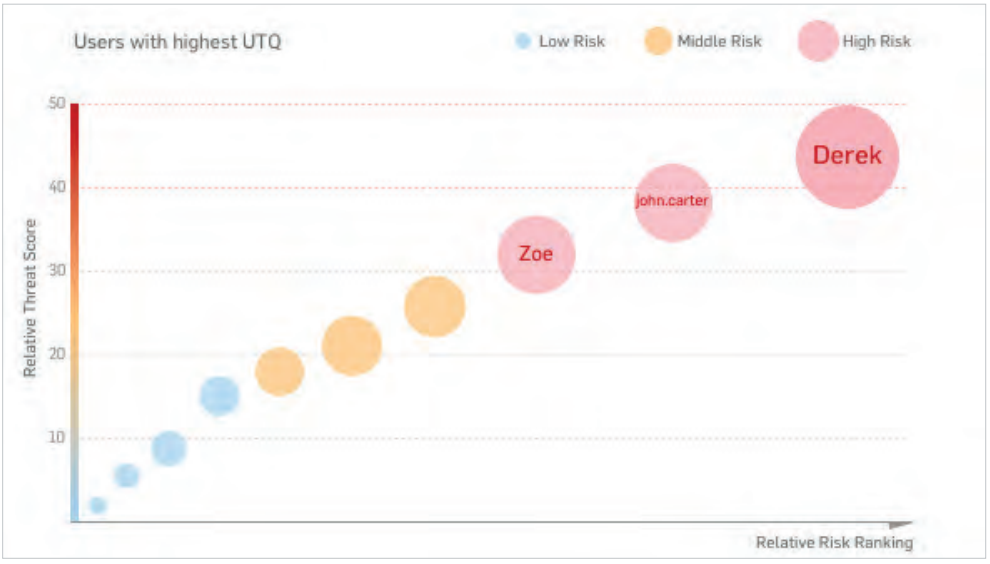
一旦將應用程式分類 (自動或透過網路管理員) 之後，該應用程式就會受到與該類別中其他應用程式相同的政策控制，因此您可以非常輕鬆地阻擋不需要且無法識別的應用程式，並優先使用想要的應用程式。

同步應用程式控制是應用程式可見度和控制方面的一項突破，可絕對明確地管理網路上使用中的每個應用程式，包括之前無法識別或未受管理的應用程式。

風險最高的使用者

研究證明，使用者是安全鏈中最薄弱的環節。好消息是，人類行為模式可以經過分析，並用來預測和預防攻擊。此外，使用模式有助於看出公司資源的利用效率，以及使用者政策是否需要進行微調。

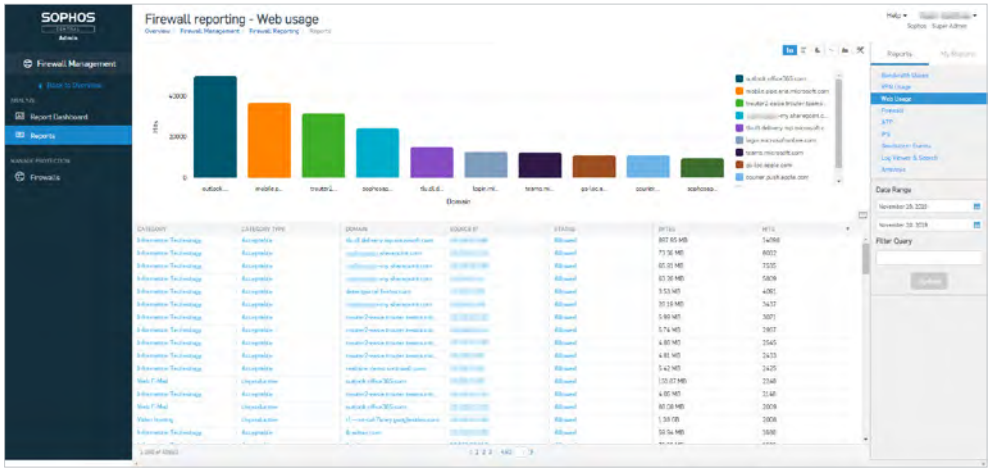
Sophos 使用者威脅商數 (UTQ) 可協助安全管理員根據可疑的網路行為、威脅和感染歷史記錄，找出暴露在風險下的使用者。使用者的 UTQ 風險分數高，可能表示由於缺乏安全意識、惡意軟體感染，或蓄意的惡意行為而導致的意外行為。



掌握造成風險的使用者和活動，有助於網路安全管理員採取所需的動作，以教育風險最高的使用者，或實施更嚴格或更適當的政策，讓使用者行為受到控制。

彈性的報告選項

Sophos Firewall 在 NGFW 和 UTM 產品中是獨一無二的，可透過高度的自訂功能，免費提供彈性的雲端式和立即可用的報告選項。Sophos 集中式防火牆報告 (CFR) 可讓組織經由分析結果，更深入地了解網路活動。CFR 具備一組完整的內建報告和可產生數百種變化的工具，可提供有關使用者行為、應用程式使用狀況、安全事件等的可執行情報。互動式報告和一目瞭然的報告儀表板可讓系統管理員深入分析儲存在 Sophos Central 帳戶中的 syslog 資料，取得以視覺呈現且易於了解的精細檢視。然後可以對這些資料進行趨勢分析，識別出安全狀況中的缺口，並找出可能需要變更的政策。



Sophos Firewall 也提供立即可用的報告功能。您可以獲得一組全方位的報告，這些報告可按類型方便地管理，並具備多個內建儀表板。防火牆的所有領域 (包括流量活動、安全、使用者、應用程式、Web、網路、威脅、VPN、電子郵件以及合規性) 都有數百個可自訂參數的報告。您可以輕鬆地安排以電子郵件將定期報告傳送給您或指定的收件者，並將報告儲存為 HTML、PDF 或 CSV。

阻擋未知威脅

若要防禦最新的網路威脅，需要所有相關的技術共同運作，並由網路管理員統籌指揮。遺憾的是，大部分防火牆的運作方式更像是一邊雜耍一邊演奏的一人樂隊，也就是在這裡設定防火牆規則、那裡設定網頁政策、再到其他地方設定 TLS/SSL 檢查，並在完全不同之處設定應用程式控制。

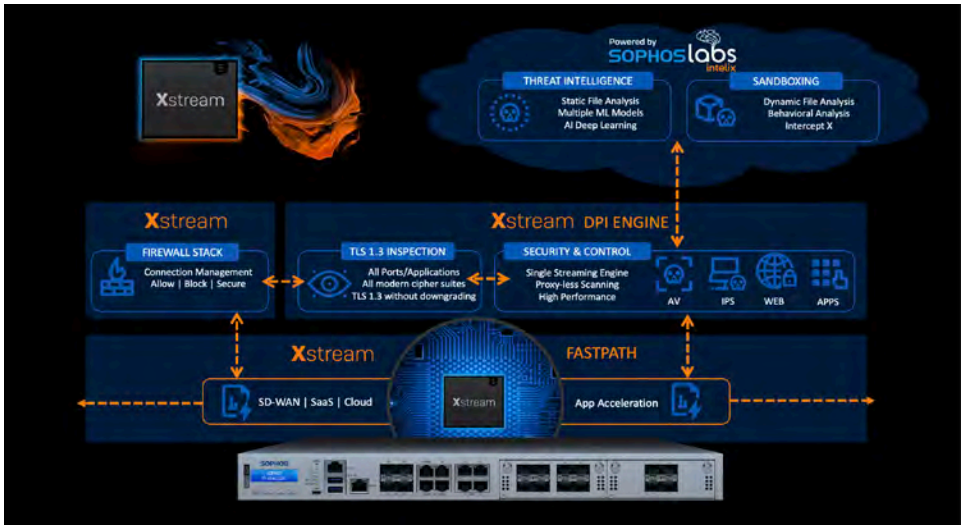
在 Sophos，我們相信您不僅需要最先進的保護技術，我們也了解這些技術必須易於設定、部署與管理日常工作，因為設定錯誤的保護往往比完全沒有保護更糟糕。

追求簡單性的承諾一直是 Sophos DNA 的關鍵。但或許更重要的是，Sophos 非常樂意接受變化，並採取必要的步驟以不同的角度思考，以提供更好的保護，最終帶來更佳的使用者體驗。

Sophos Firewall 的做法與眾不同，讓結果有很大的差異。

Xstream 的保護和效能

當您需要保護網路安全免受威脅時，防火牆效能不應降低。Sophos Firewall 的 Xstream 封包處理架構的核心元件之一是高速深度封包檢查 (DPI) 引擎。這個 DPI 引擎可為 IPS、Web、防毒和應用程式控制，以及我們的 Xstream SSL 檢查，提供無 Proxy 的單遍安全掃描。



建立新連線後，防火牆堆疊將對其進行處理，決定要允許、阻擋還是掃描流量中的威脅。如果流量需要安全掃描，它會將封包轉送到無 Proxy 的高效能串流 DPI 引擎，無論封包是否經過加密，該引擎都將進行掃描。這僅用於最初的幾個封包。之後，防火牆堆疊便會退場，並將處理完全卸載到 DPI 引擎。這種做法可大幅改善延遲和效能。

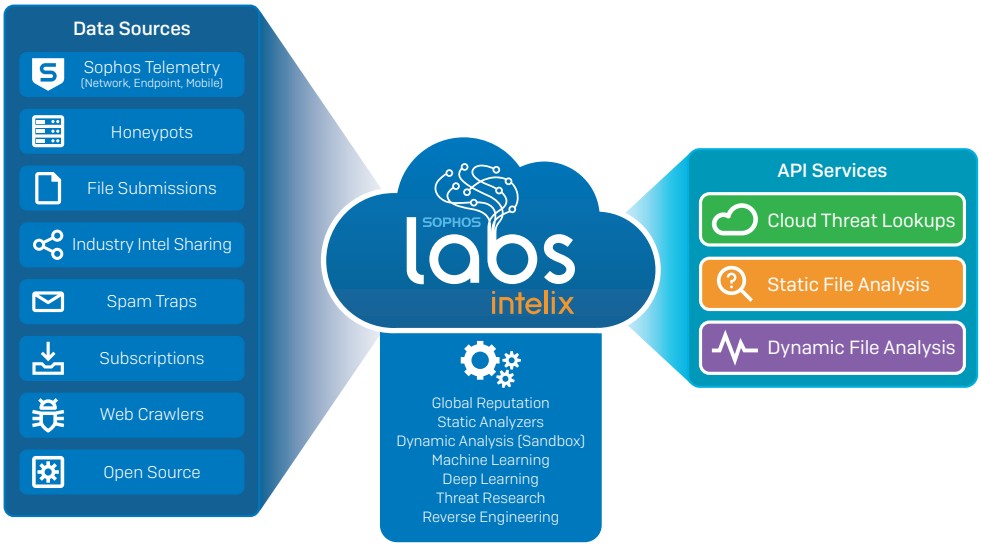
之後，如果該串流被視為是安全的且無須進一步檢查，DPI 引擎會將其完全卸載到 Sophos Network Flow FastPath，這是一個為受信任流量提供加速的路徑。如此一來，其他資源就無需檢查不需要檢查的流量，可大幅提升效能。

零時差威脅防護

隨著勒索軟體等進階威脅變得更有針對性和隱匿性，因此我們迫切需要預測性零時差威脅識別和防護。終極的解決方法包含兩個方面：

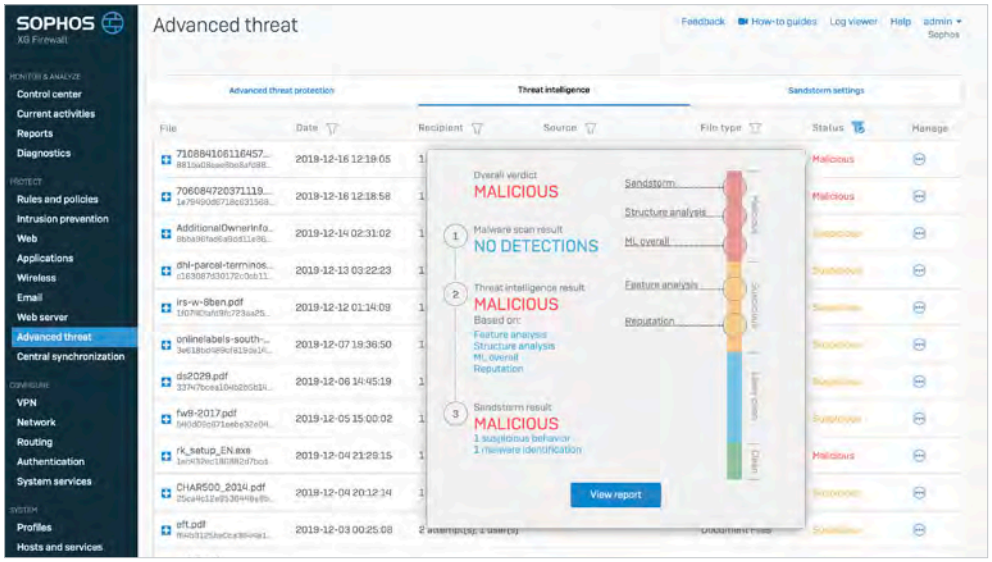
1. **靜態機器學習分析** - 利用多個人工神經網路機器學習模型，結合全球信譽和深度檔案掃描，無須即時執行檔案就可以進行預測性分析和偵測。
2. **動態的執行階段沙箱分析** - 在雲端沙箱環境中即時引爆惡意軟體，以無與倫比的洞察力來了解檔案活動，以找出未知威脅的真實性質和能力。

Sophos Firewall 具備了這兩項 SophosLabs Intelix 支援的重要保護技術。SophosLabs 是我們廣受好評的 Tier 1 網路安全威脅研究實驗室，已經開發出最終的威脅分析和情報平台 SophosLabs Intelix。它使用最新的機器學習技術、數十年的威脅研究成果以及 PB 級的情報，可提供無與倫比的保護，以抵禦前從未見的最新威脅。



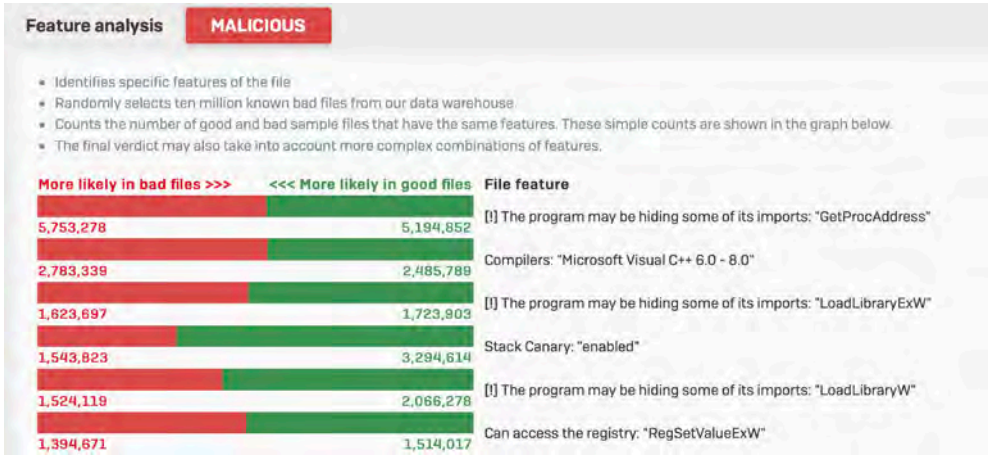
當 Sophos Firewall Xstream DPI 引擎對進入網路的檔案進行防毒分析，並確定存在攻擊程式碼時，它會暫時保留該檔案，並將其傳送到雲端的 SophosLabs Intelix 服務去進行靜態和動態檔案分析。然後，它會經由威脅情報桌面工具和這個可點擊的報告，將摘要結果提供到 Sophos Firewall 的控制中心，並只在檔案乾淨時才將其傳送到下載者或電子郵件收件人。

最後一步很重要，因為許多防火牆的進階型惡意軟體解決方案通常在分析完成前就將檔案傳送給使用者，如果最終檔案被判定是威脅，那麼可能會造成災害且清理代價昂貴。



靜態機器學習分析

靜態檔案分析利用多種機器學習模型來分析檔案的各種特性、特徵、遺傳性質和信譽，並將其與 SophosLabs 資料庫中數百萬個已知的良性或惡意檔案進行比對，以在幾秒鐘內判定任何新的和過去前所未見的檔案。它可以快速且有效地識別新威脅和現有威脅的變種，特別是不容易被沙箱技術偵測到的威脅，例如包含惡意軟體的受密碼保護檔案。

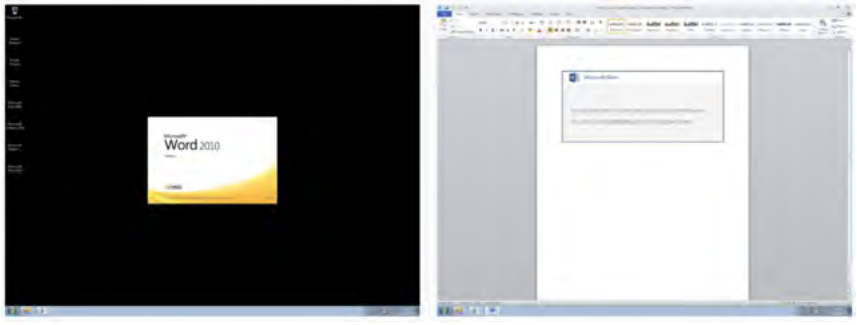


動態的執行階段沙箱分析

沙箱技術首次出現時，只有大型企業才能負擔得起。但是現在，歸功於 Sophos Sandstorm 之類的雲端型沙箱解決方案，即使是最小型的企業也負擔得起。這是首次，中小型組織可以透過深度學習技術使用沙箱技術，此技術遠遠超越了幾年前企業花費數百萬美元部署的專用內部部署沙箱解決方案。

由於它採用雲端架構，因此不需要額外的軟體或硬體，也不會對防火牆效能造成影響。經 Xstream DPI 引擎判定包含攻擊程式碼的任何檔案 (例如電子郵件附件或 Web下載)，會被自動上傳到 SophosLabs Intelix 雲端沙箱並引爆，同時進行靜態分析 (如上)，以在允許檔案進入網路前判斷它的執行階段行為。

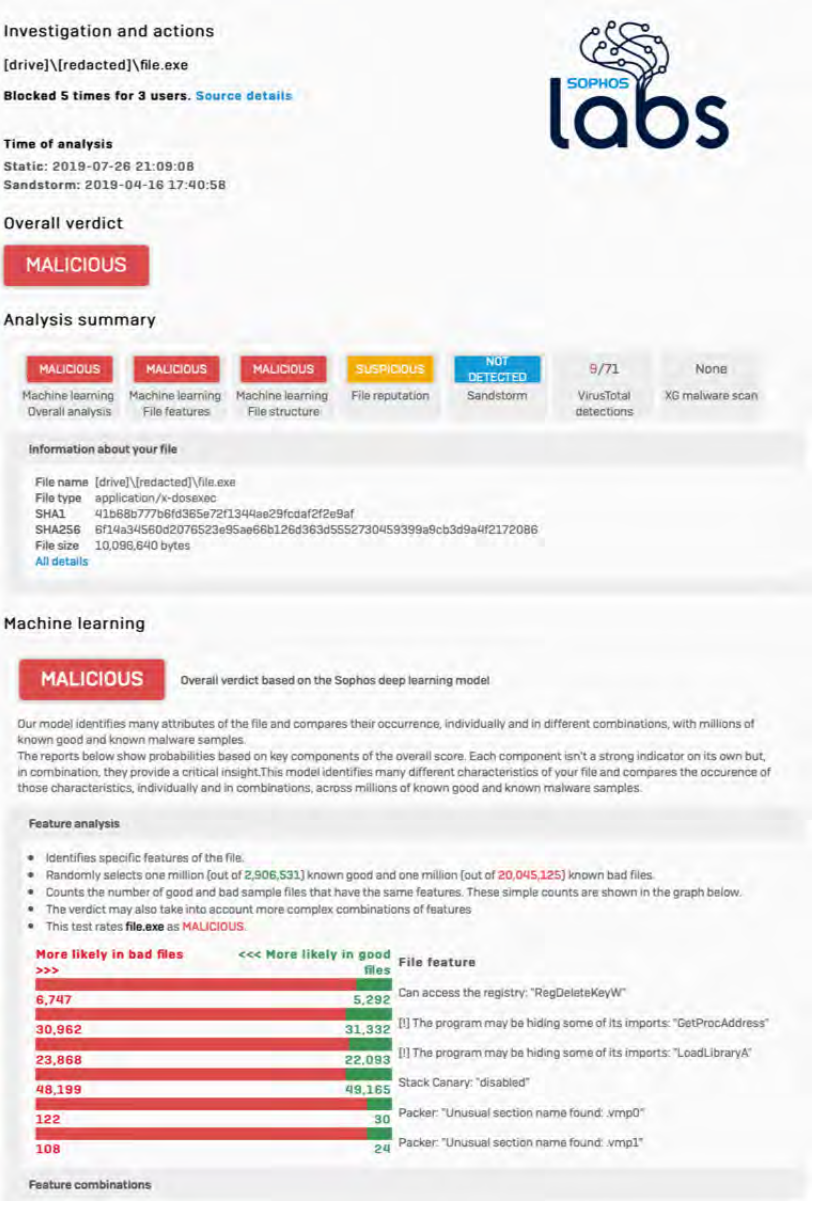
為了識別威脅，SophosLabs 已將領先業界的 Intercept X 新一代端點產品中的最新保護技術整合到 Sophos Sandstorm 中，包括深度學習、漏洞利用偵測和CryptoGuard (可即時偵測作用中的勒索軟體加密檔案)。它還會監控所有檔案、記憶體、登錄檔和網路活動，找出惡意行為的特徵以做出判定。其他防火牆均無法如全球最佳的威脅防護 Intercept X 般提供這種即時分析，也無法提供如同 Sophos Firewall 的深入資訊和報告能力，包括檔案執行時會發生什麼情形的完整畫面截圖。



在偵測躲藏在正常檔案中且沒有明顯惡意特徵的隱藏威脅時，沙箱特別有效。包括有巨集的 Office 檔案，或是已經被破壞的良性可執行檔或應用程式更新。

威脅防護報告

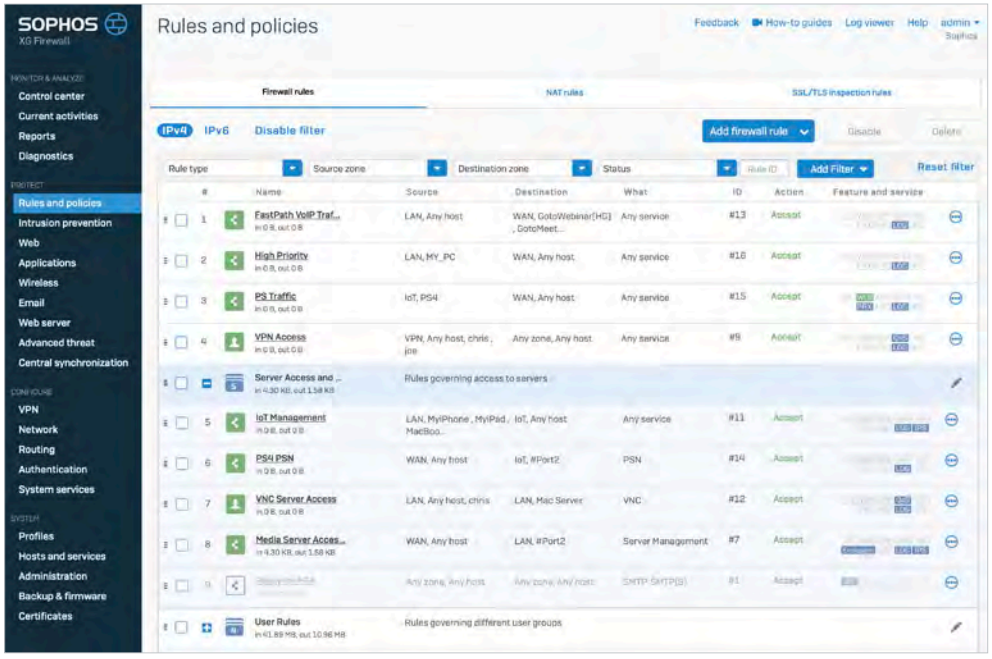
Sophos Firewall 分析的每個檔案都會隨附一個報告，提供各種分析結果和判定的完整詳細資訊。該報告包含 6 種不同的要件，包括各種機器學習分析、檔案信譽、沙箱，甚至是第三方 VirusTotal 的資料。



統一式規則管理

管理防火牆可能是非常具有挑戰性。多個規則、政策和安全設定分佈在各個功能區塊中，而且通常需要數個不同的規則才能提供必要保護，因此要做的事情很多。

藉由 Sophos Firewall，我們徹底重新架構了防火牆規則的組織方式，以及安全狀態的管理方式。我們將所有防火牆規則和實施項目集合到單一畫面中，再也無需在管理主控台上尋找適當的政策。現在，您可以從單一位置檢視、篩選、搜尋、編輯、新增、修改所有防火牆規則。

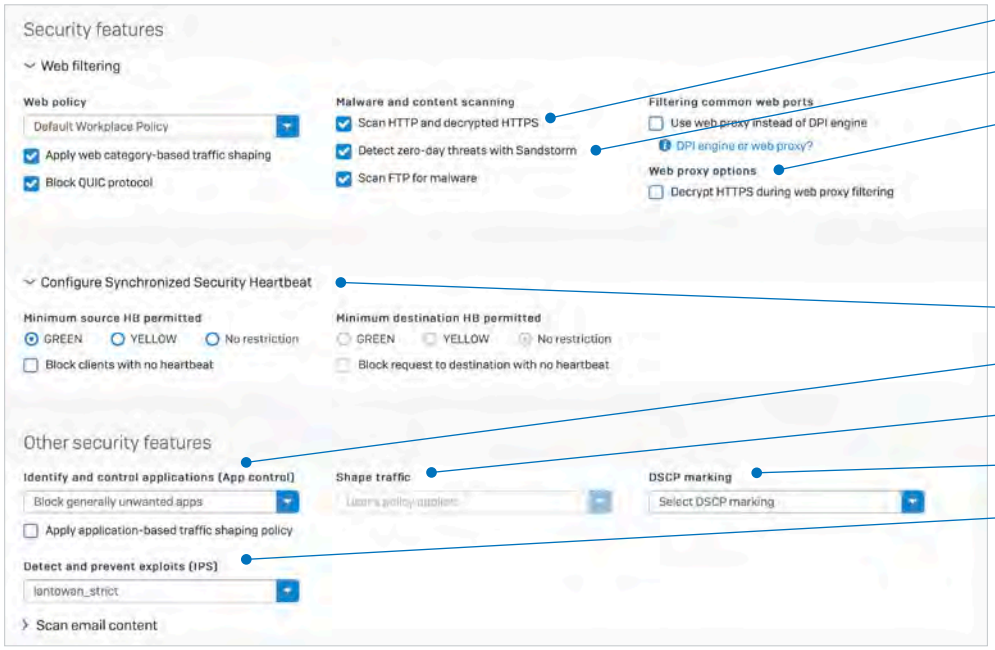


此外，將規則針對使用者、商業應用程式、NAT、TLS/SSL 檢查和網路分門別類，讓您更容易僅檢視所需的政策，同時提供一個便於管理的畫面。

指標圖示可提供和政策相關的重要資訊，例如類型、狀態和實施狀態等。

管理安全態勢快速概覽

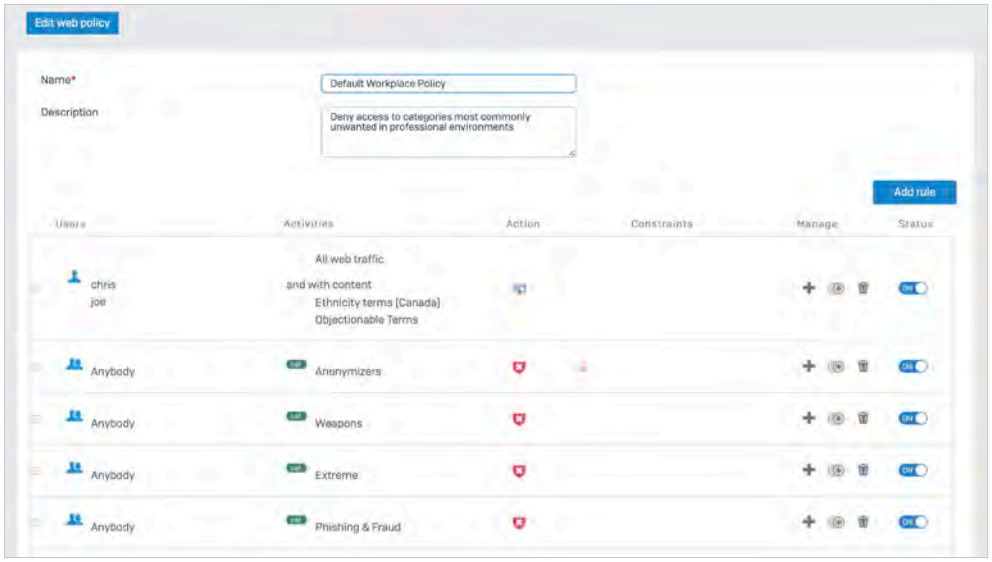
無論是透過雲端的 Sophos Central 帳戶還是 Sophos Firewall 使用者介面，Sophos 都可以輕鬆設定和管理新型保護所需的一切，而且全都可從單一畫面完成。



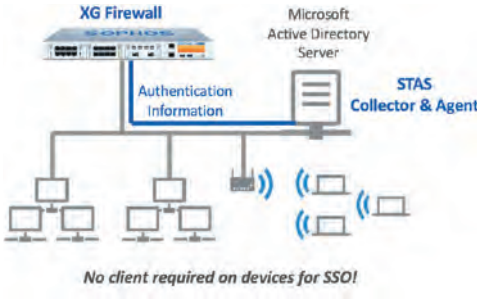
您可以針對防毒、TLS/SSL 檢查、沙箱、IPS、流量塑形、網頁和應用程式控制、Security Heartbeat、NAT、

路由，以及優先順序，設定與管理安全及控制措施，全都從單一位置且按規則、使用者或群組為基礎來進行。

此外，如果您想要查看監管政策正在執行哪些操作，甚至是進行變更，都可以原地進行編輯，而不必離開防火牆規則並進行其他產品操作。

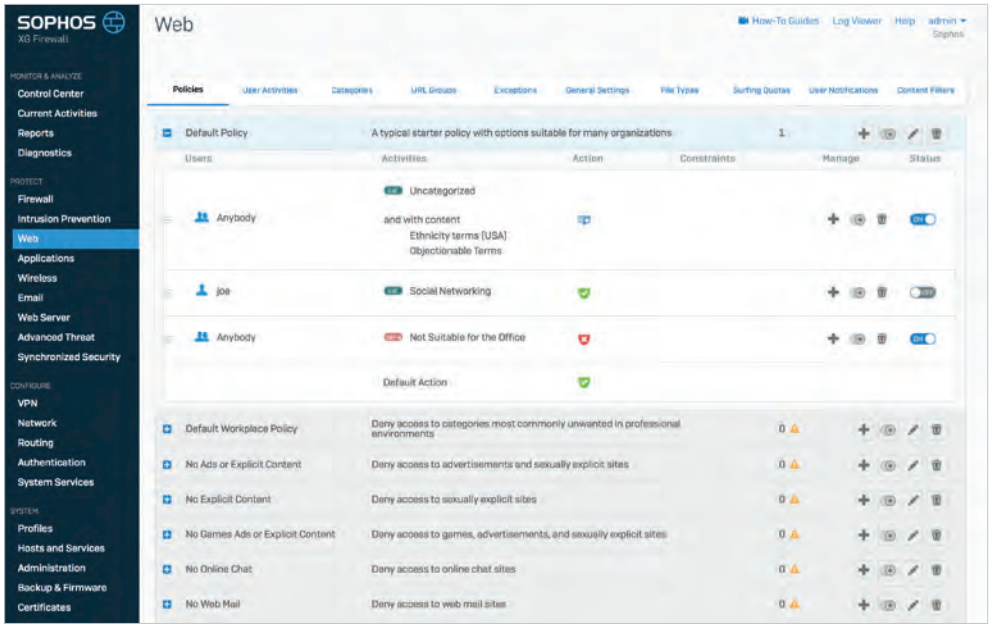


彈性的驗證選項可讓您輕鬆得知使用者的身分，並包含目錄服務，例如 Active Directory、eDirectory 和 LDAP，以及 NTLM、Kerberos、RADIUS、TACACS+、RSA、用戶端代理程式或管制入口網站。而 Sophos Transparent Authentication Suite (STAS) 則可以與 Microsoft Active Directory 等的目錄服務整合，以便進行簡單、可靠且透明的單一登入驗證。



企業級安全 Web 閘道

Web 保護與控制是任何防火牆中不可或缺的功能，但遺憾的是，大多數的防火牆實作中都是最後才想到這一點。我們在打造企業級 Web 保護解決方案方面的經驗，為我們提供了部署 Web 政策控制措施的背景和知識，這些功能通常是您在價格十倍左右的企業安全 Web 閘道 (SWG) 中才能找到的。我們實作了一種自上而下的繼承政策模型，因此可以更簡單且直覺地建立複雜的政策。大多數常見的部署 (例如典型的工作環境、教育的 CIPA 合規性等) 中都包含了預先定義好的現成政策範本。也就是說，您可以利用容易的微調與自訂選項，立即建立政策並符合規範。



事實上，我們知道 Web 政策是防火牆日常工作中經常發生變化的因素之一，這就是為什麼我們投入大量心力開發，使您可以根據使用者和業務需求輕鬆管理與調整政策的原因。您可以輕易地自訂使用者和群組、活動 (包括 URL、類別、內容篩選與檔案類型)、動作 (阻擋、允許或警告)，以及新增或調整時間和星期幾的限制。

教育功能

Sophos Firewall 提供了幾樣功能，非常適合對 Web 政策和合規性有嚴格要求的教育環境。教育專屬功能包括：

- 為 CIPA 合規性預先封裝的 Web 政策
- 對關鍵字的內容篩選和報告
- 以使用者/群組政策為基礎的 SafeSearch 和 YouTube 限制設定
- 可以由教師管理的阻止頁面複寫
- 可及早識別潛在問題的全方位內建報告

Web 政策現在可根據關鍵字清單，加入記錄、監視，甚至是根據動態內容實施政策的選項。此功能在教育環境中特別重要，透過篩選與自我傷害、霸凌、激進或其他不當內容的關鍵字，可確保線上兒童安全並向學生提供深入資訊。可以將關鍵字庫上傳到防火牆，並套用至所有 Web 篩選政策作為篩選條件，並採取包括記錄、監控，或阻擋相關關鍵字的搜尋結果或網站等動作。

提供完整的報告，以找出符合關鍵字比對結果，以及正在搜尋或使用特定關鍵字內容的使用者，以便在高風險的使用者成為實際問題之前主動干預。

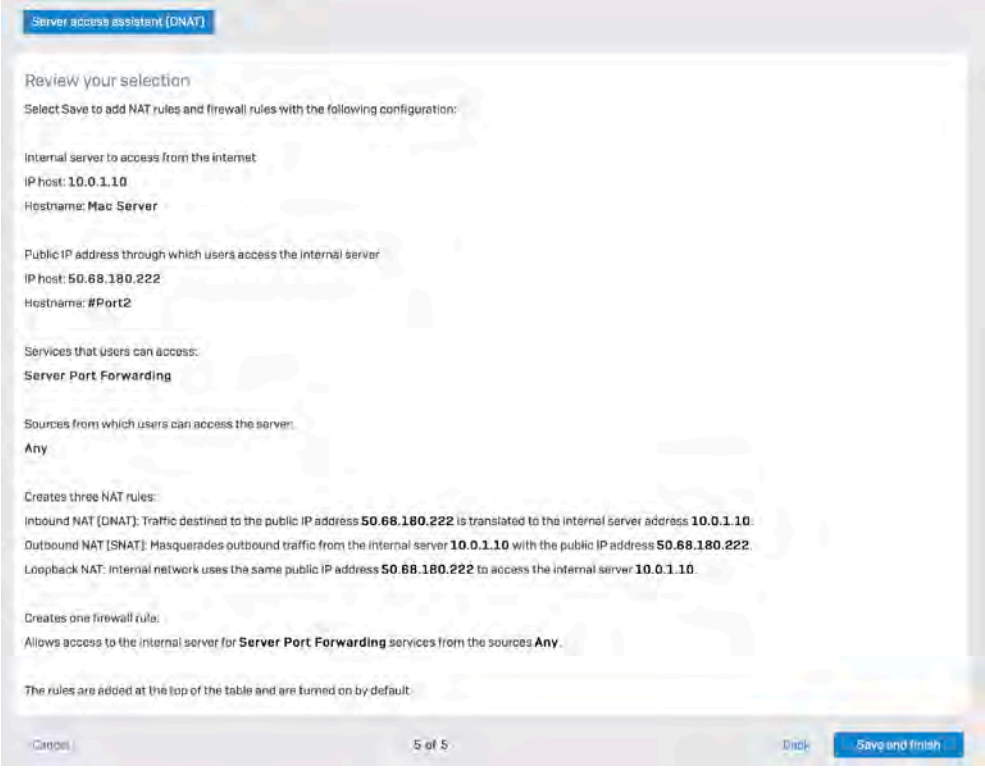
Sophos Firewall 可以立即協助您實現 CIPA 政策合規性，快速符合規範。它還會根據使用者/群組政策，對 SafeSearch 和 YouTube 限制提供彈性且強大的控制。此外，可以授予教師設定和管理自己的政策覆寫的選項，讓他們的教室能夠瀏覽課程需要但遭阻擋的網站。

這是經過簡化的強大 Web 政策。

簡化的 NAT 設定

任何想要設定 NAT (網路位址轉譯) 規則的人都知道這有多麼不容易。但其實不一定非得如此。Sophos Firewall 包含完整的企業 NAT 功能，可在單一規則中使用精細選擇條件進行強大且彈性的 NAT 設定，包括來源 NAT (SNAT) 和 目標 NAT (DNAT)。若要簡化複雜的 DNAT，易於使用的精靈可引導您完成建立完整 NAT 設定的程序，只需要按幾下滑鼠即可。

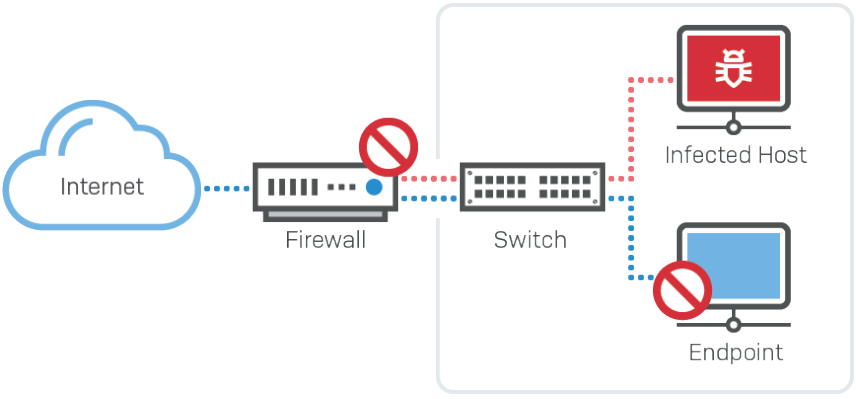
建立防火牆規則時，系統管理員也可以使用便利的 Linked NAT 選項。Linked NAT 將會自動建立對應的 NAT 設定規則，進而減少建立設定 NAT 規則所需的時間。



自動回應事件

網路管理員最常要求的防火牆功能之一，就是能夠自動回應網路上的安全事件。

Sophos Firewall 是唯一一款能夠完整識別網路上的感染來源，並自動限制受感染的裝置存取其他網路資源做為回應的網路安全解決方案。這是透過我們獨一無二的 Sophos Security Heartbeat 所達成，它會共享 Sophos 受控端點與防火牆之間的遙測功能和健康狀態。



Sophos Firewall 會以獨特的方式，將連線主機的健康狀態整合到防火牆規則中，讓您自動限制對任何受感染系統之敏感網路資源的存取，直到淨化為止。

Sophos Firewall 不僅可以隔離端點，使其無法存取防火牆中的網路其他部分，還可以藉助網路上所有狀況良好的端點，進一步在端點層級隔離受感染的主機。

我們將其稱之為「橫向移動防禦」，可以隔離並防止威脅或攻擊者透過網路橫向移動到其他系統，即使它們位於防火牆無法干預的相同網段或廣播網域中也是如此。這是一種非常簡單有效的解決方案，可以因應網路上的主動攻擊者所面臨的挑戰。此外，只有在端點和防火牆能共同協調防禦或同步防禦時才有可能實現。

安全心跳

Sophos Security Heartbeat 會使用 Sophos 管理端點與 Sophos Firewall 之間的安全連結，即時共用情報。這個在安全產品之間同步的簡單步驟 (以往是獨立運作的)，可建立更有效的保護，抵禦進階惡意軟體和目標式攻擊。

Security Heartbeat 不僅可以立即識別進階威脅是否存在，還可以用來傳達有關威脅性質、主機系統以及使用者的重要資訊。或許最重要的是，Security Heartbeat 也可以自動採取動作，以隔離或限制對受感染系統的存取，直到沒有惡意軟體為止。這項令人振奮的技術已經徹底改變 IT 安全解決方案識別和回應進階型威脅的方式。

適用於防火牆後受管理端點的 Security Heartbeat 可以是以下一種狀態：

綠色心跳狀態表示端點裝置狀況良好，而且可以取得所有適當的網路資源。

黃色心跳狀態表示裝置中可能含有不需要的應用程式 (PUA)、不符合規範，或遇到其他問題的警告。黃色心跳時，您可以在問題解決之前選擇可以使用的網路資源。

紅色心跳狀態表示裝置可能有受到進階型威脅感染，而且會嘗試回傳到僵屍網路或命令與控制伺服器。在防火牆中使用 Security Heartbeat 政策設定時，您可以在裝置清理完成之前輕鬆地隔離紅色心跳狀態的系統，以降低資料遺失的風險或阻止感染擴散。

只有 Sophos 提供了如 Security Heartbeat 的解決方案，因為 Sophos 是端點和網路安全解決方案的領導者。雖然其他廠商都開始意識到這是 IT 安全的未來，而且爭相實作類似的解決方案，但它們都沒有優勢：因為它們沒有同時擁有可以整合在一起的業界領先端點解決方案以防火牆解決方案。

這是個零信任的世界

信任在 IT 領域是一個危險的字眼，尤其是當這種信任是絕對 (亦即無條件或不容置疑的) 時。事實證明，建立一個封閉的大型公司邊界，並信任內部的所有內容是一種有缺陷的設計。

零信任是一種全面的安全解決方案，可以因應這些變化以及組織運作與回應威脅的方式。這是一種思考和實現安全性的模型和理念。

無論是公司網路內部還是外部，都不應該自動信任任何人和任何事物。但是，最終有些事物需要受到信任。在「零信任」中，這種信任是臨時的，而且參考多個資料來源所建立，此外會不斷進行重新評估。

零信任可讓我們控制整個資產，從辦公室內部向外到我們使用的雲端平台。公司邊界之外不再缺乏控制權，也不再需要與遠端使用者抗爭。

我們如何邁向零信任並充分利用其提供的所有優勢？儘管沒有人可以透過單一解決方案提供零信任，但 Sophos 擁有多種安全技術和控制措施，可加速並簡化您邁向零信任的旅程。

Sophos Central 我們的雲端型網路安全平台將這些完全不同的互補技術整合到單一中樞，以協助您協調和監控零信任網路。

同步安全 可在系統之間持續共用資訊，進而彼此提供深入資訊和可見度的網路安全。

Sophos Firewall 在使用者、裝置、應用程式、網路等周圍建立區段或微邊界。

Server Protection 和 Intercept X 為每個裝置指派一個裝置健康狀態，以便在其中一個裝置受到感染時自動隔離這些裝置，並阻止其與其他裝置連線。

託管式威脅回應 (MTR) 服務 監控整個網路上的所有使用者活動，並識別可能遭駭的使用者認證。

Sophos ZTNA 提供真正的零信任網路存取解決方案，以安全地將使用者連線到應用程式和資料。

輕鬆地將 Sophos Firewall 加入至任何網路

Sophos Firewall 系列硬體設備提供彈性的部署選項，所有 1U 款式都具有標準的開放旁路連接埠，也以 FleXi Port 模組方式提供，以便在 2U 設備上也能啟用此功能。旁路連接埠可讓 Sophos Firewall 以橋接模式安裝到現有的防火牆環境中。如果 Sophos Firewall 需要關機或重新開機以更新韌體，旁路連接埠可讓流量繼續流動，以確保網路不中斷，進而提供業務連續性。此功能無需替換任何現有的網路基礎架構，提供了完全沒有風險的新部署選項。更重要的是，我們的新一代端點保護 Intercept X 可與任何現有的桌面防毒產品搭配使用，無需替換任何產品即可在任何網路中部署完整的 Sophos 同步安全解決方案。

Sophos Firewall：網路安全變得更簡單。

索取價格資訊

根據您的需求，在 www.sophos.com/firewall-quote 上索取免費報價

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com

21-03-24 WP-EN (PS)

SOPHOS