SOPHOS
Cybersecurity delivered.

Sophos Firewall

評估指南

目錄

歡迎使用 Sophos Firewall

感謝您選擇檢閱或評估 Sophos Firewall。本指南提供 Sophos Firewall 與市場上其他防火牆產品不同的許多功能概觀，並提供在您自己網路中探索及評估 Sophos Firewall 的實用協助。

Sophos Firewall 從一開始就專為解決現有防火牆現今的主要問題而開發。關於現今大多數防火牆，客戶最大的抱怨包含以下幾個問題：

- 對網路上的風險與活動缺乏可見度。大多數防火牆都讓人難以取得重要資訊，在篩選出優先要務方面也做得很差。
- 設定時缺少保護、功能，或是超級複雜。大多數防火牆不提供阻擋最新先進威脅的所有必要技術，或者設定太過繁瑣而大大降低正確設定的機會。
- 網路上發生事件時缺乏對事件的反應。大多數防火牆並不會對網路上出現的威脅提供任何深入資訊而且就算提供資訊也不進行任何自動回應。
- 此外缺乏工具來輕鬆架設和管理複雜的 SD-WAN VPN 覆蓋網路，並在發生中斷時難以在多個 SD-WAN 連結之間轉換。

與其他網路防火牆相比，Sophos Firewall 具有四大優勢：

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。
4. **最佳化 SD-WAN 網路**——只要簡單點擊，Sophos Firewall 中的 Xstream SD-WAN 功能即可設定複雜的 SD-WAN 覆蓋網路。 您還可以利用以效能為基礎的自動 WAN 連結選擇，以及連結之間的即時零影響轉換來最佳化應用程式效能、網路可靠性和業務連續性，同時降低連線成本。

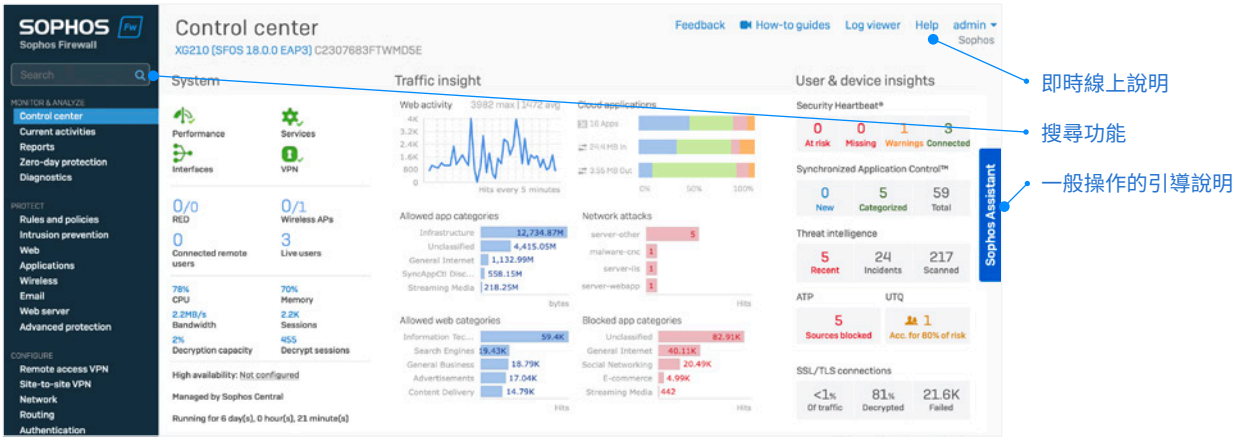
本指南將協助您直接探索及評估 Sophos Firewall 的優勢。不過在開始之前，此處有些重要資源來源可協助您設定，讓您充分利用 Sophos Firewall 的功能。

文件和自助影片

利用這些豐富的資源來幫助您快速啟動和運作：

- Sophos Firewall 文件
- Sophos Firewall 操作影片
- Sophos Firewall 培訓

您還可以按一下 Sophos Firewall 主控台右上角的「說明」選項或利用 Sophos Assistant 取得常見操作的協助，獲得各種相關內容的線上說明。



Sophos Firewall 包含幾個有用的工具，讓安裝變得簡單

啟用同步安全

若要探索及檢視同步安全，以下是一些額外注意事項：

- 如果您還沒有 Sophos Central 帳戶，可以在以下網址註冊試用版：https://central.sophos.com。
- 有了 Sophos Central 帳戶之後，務必使用 Sophos Intercept X 保護您網路上的一或多部電腦，藉此讓 Sophos Firewall 啟用 Security Heartbeat。在 Sophos Central 中，前往 [Protect Devices]，並依據您的平台下載 Endpoint Protection 安裝程式。
- 登入您的 Sophos Firewall 並按一下 [Central Synchronization] 功能表選項，以使用 Sophos Central 連接您的防火牆。您只需要輸入 Sophos Central 認證即可在 Sophos Central 中註冊 Sophos Firewall，進而啟用 Security Heartbeat、同步應用程式控制，甚至可以從 Sophos Central 管理 Sophos Firewall。

揭露隱藏的風險

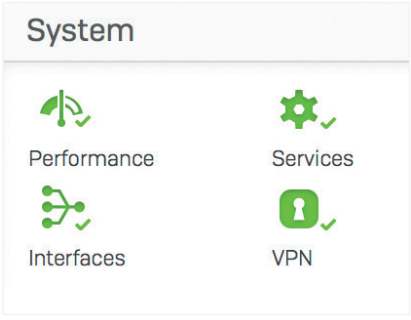
對於新型防火牆來說，能夠透過所收集的大量資訊進行剖析、將資料關聯化 (如果可能)，並只摘要出需要回應的最重要資訊是非常重要的，最好能防範於未然。

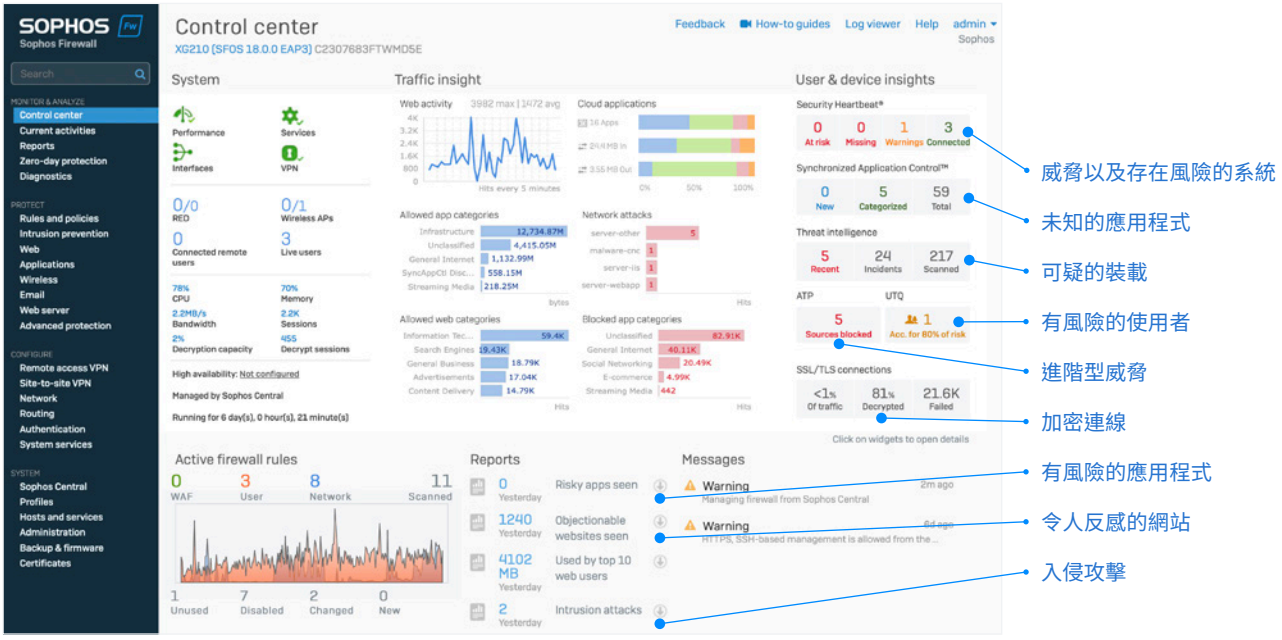
控制中心

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。

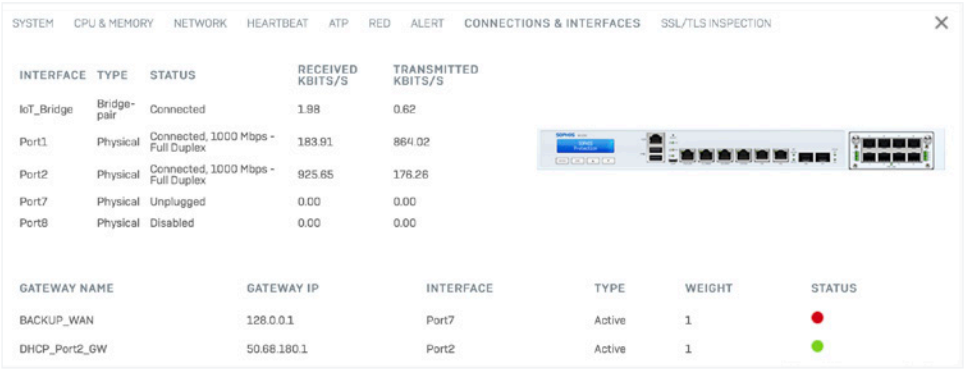
它使用「交通號誌」風格的指標，讓您的注意力放在對您最重要的事項上。

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，則表示不需要採取任何進一步的動作。

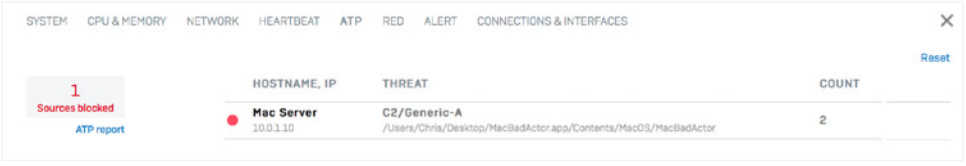




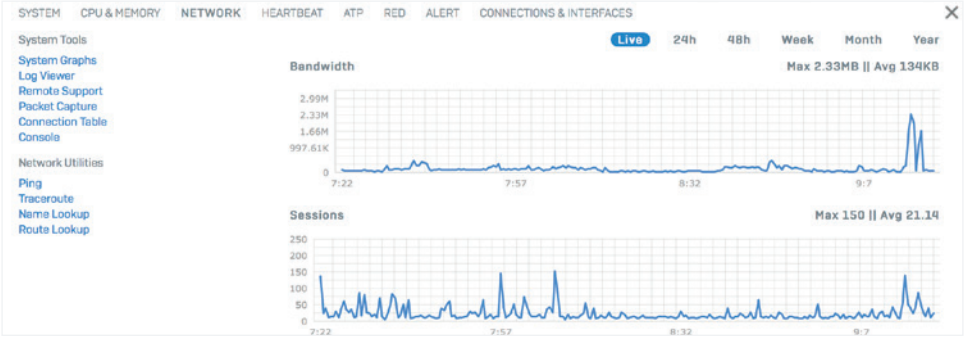
控制中心上的每個桌面工具都提供了額外資訊，只要按一下該桌面工具，即可輕鬆顯示。例如，按一下控制中心上的 Interfaces 桌面工具，就可以取得裝置上的介面狀態。



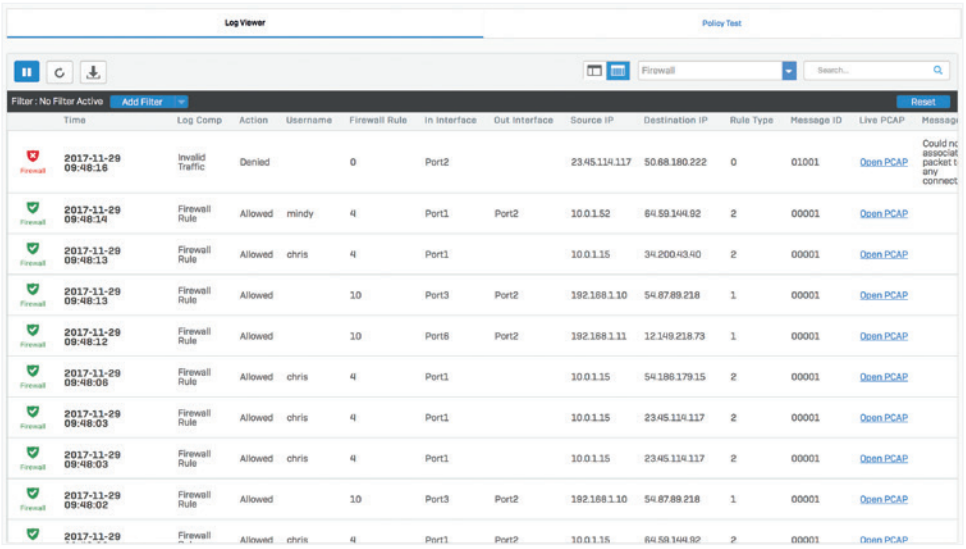
只要按一下儀表板中的 ATP (進階威脅防護) 桌面工具，也可以輕鬆確定進階威脅的主機、使用者和來源。



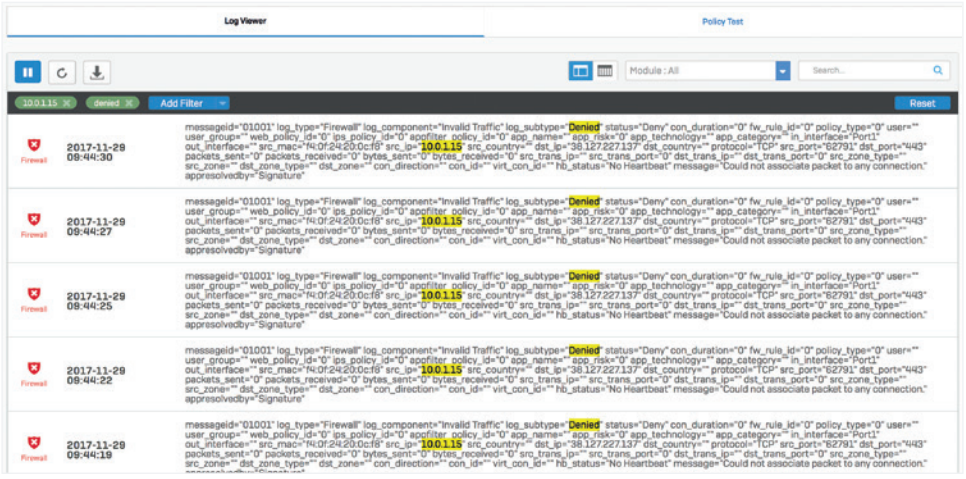
系統圖表也可以利用可選擇的時段，顯示一段時間的效能，無論是最後兩小時到上個月，還是最後兩小時到去年都可以。此外，這些圖表還可以讓您快速存取常用的疑難排解工具以解決潛在問題。



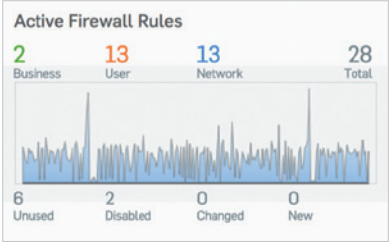
只要按一下滑鼠，就可以從每個畫面取得即時日誌檢視器。您可以在新視窗中開啟該檢視器，就可以在主控台上作業的同時，留意相關的日誌。即時日誌檢視器提供兩種檢視模式：一種是較簡單的欄位型格式 (依防火牆模組)，另一種是更詳細的統一檢視模式，包含功能強大的篩選和排序選項，可將整個系統的日誌彙總成單一即時檢視。



如果您和大多數網路管理員一樣，會懷疑防火牆規則是否太多、哪些是真正必要的防火牆規則，以及哪些是實際上不會用到的防火牆規則。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，顯示其即時圖表：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，為您提供做一些內部管理的機會。如同控制中心的其他區域般，按一下其中任何一個區域將會深入探索，在此案例中，深入探索依規則類型或狀態排序的防火牆規則表。

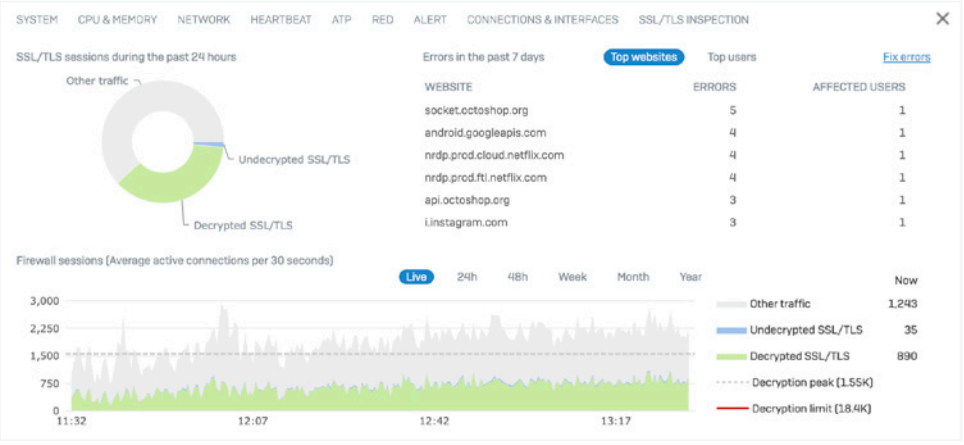


Xstream TLS 檢查

加密流量的風暴正在醞釀之中。您只需要輸入 Sophos Central 認證即可在 Sophos Central 中註冊 Sophos Firewall，進而啟用 Security Heartbeat、同步應用程式控制，甚至可以從 Sophos Central 管理 Sophos Firewall。這種成長表示網路犯罪份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。

儀表板上提供的其他工具可讓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。



Sophos Firewall 可直接從控制中心深入了解加密流量以及 TLS 檢查引起的任何問題

管理員也可以看到一個彈出的視窗，確實了解有問題的網站、原因以及遇到問題的使用者。他們可以從該處直接採取將應用程式或網站從解密中排除的動作，以防止進一步的問題。其他任何 SSL 檢查解決方案都無法那麼容易存取此資訊。

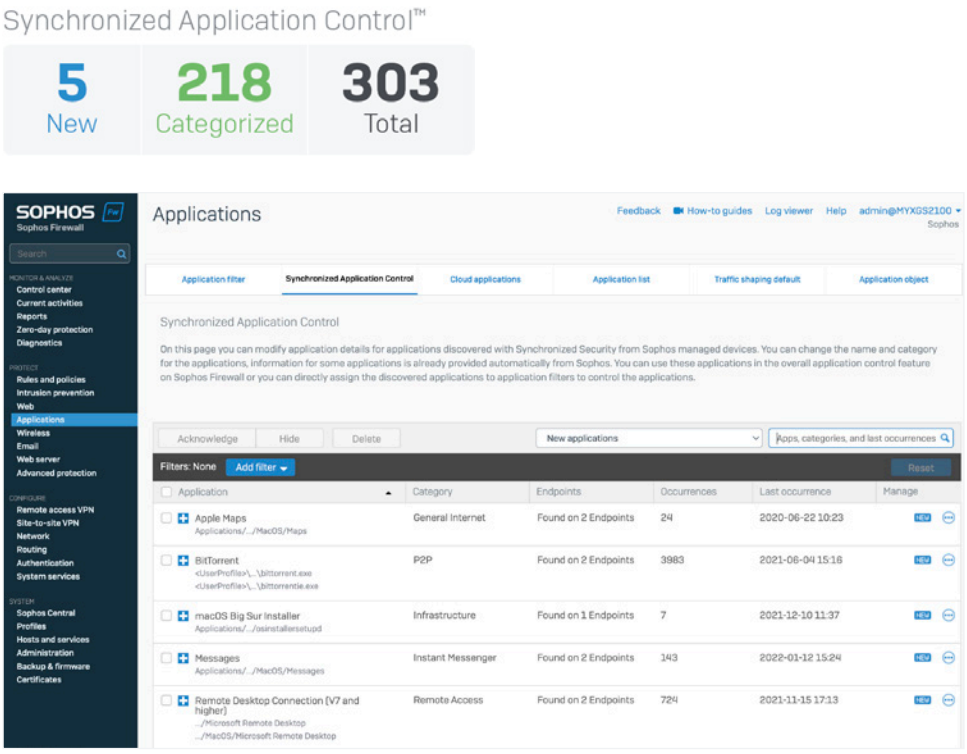
同步應用程式控制

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：未分類或標示為未知、通用 HTTP 或通用 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，自訂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接，通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。

結果是完全看不到網路上的應用程式，而看不到就無法控制。這個問題的解決方法非常簡潔且有效：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 Sophos 受管理端點。

以下是其運作方式。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。



可以自動或手動對同步應用程式控制發現的未知應用程式進行分類。

接著，端點可以分享可執行檔、路徑，通常還有其類別，並將該資訊傳回防火牆。之後在大部分的情況下，防火牆就可以利用此資訊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。

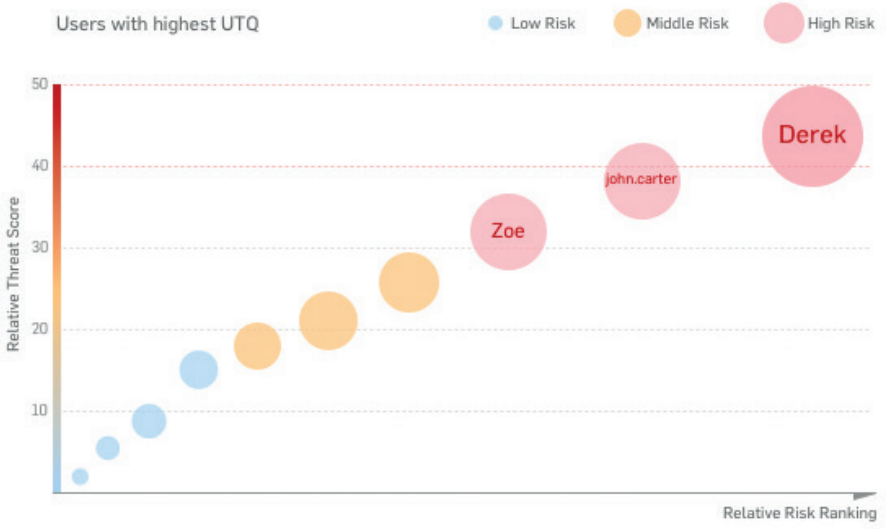
一旦將應用程式分類 (自動或透過網路管理員) 之後，該應用程式就會受到與該類別中其他應用程式相同的政策控制，因此您可以非常輕鬆地阻擋不需要且無法識別的應用程式，並優先使用想要的應用程式。

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，可為網路上正在使用的每個應用程式提供絕對的明確性，包括之前無法識別或不受控制的應用程式。

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，使用模式有助於說明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。

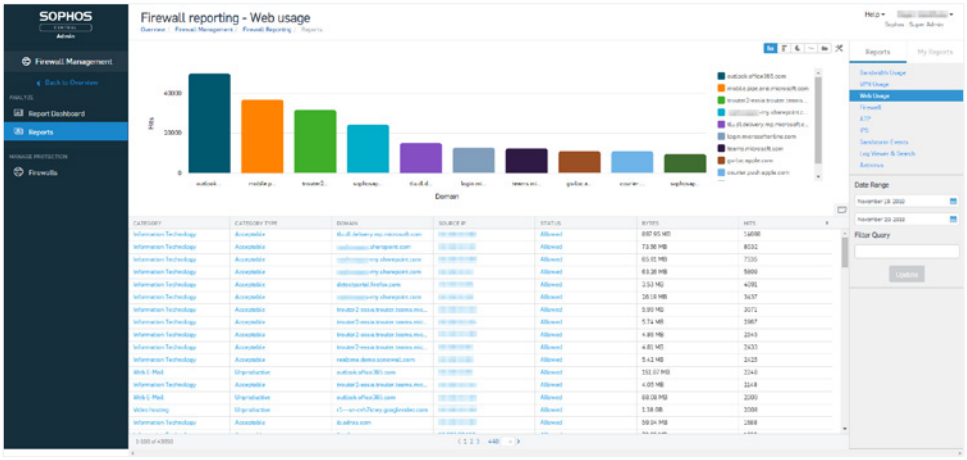


Sophos Firewall 能一目了然地顯示高風險的使用者。

知道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) 可讓組織透過分析，更深入了解網路活動。CFR 透過一組完整的內建報告和建立數百個變體的工具，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管理員深入分析儲存在 Sophos Central 帳戶中的 syslog 資料，以獲得以視覺格式呈現且易於了解的精細檢視。然後可以對資料進行趨勢分析，以識別安全狀況中的差距，並突顯潛在政策變更的必要性。



Sophos Firewall 提供了多種內建和中央型雲端報告選項。

Sophos Firewall 也提供立即可用的報告功能。從一組完整的報告中選擇，方便按類型整理，而且提供數個內建的儀表板。在防火牆的所有區域 (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。您可以輕鬆地排定將定期報告以電子郵件傳送給您或您指定的收件者，並將報告儲存為 HTML、PDF 或 CSV。

阻擋未知威脅

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，也就是在一個區域設定防火牆規則、在另一個區域設定網頁政策、在其他區域設定 TLS/SSL 檢測，並在產品完全不同的部分設定應用程式控制。

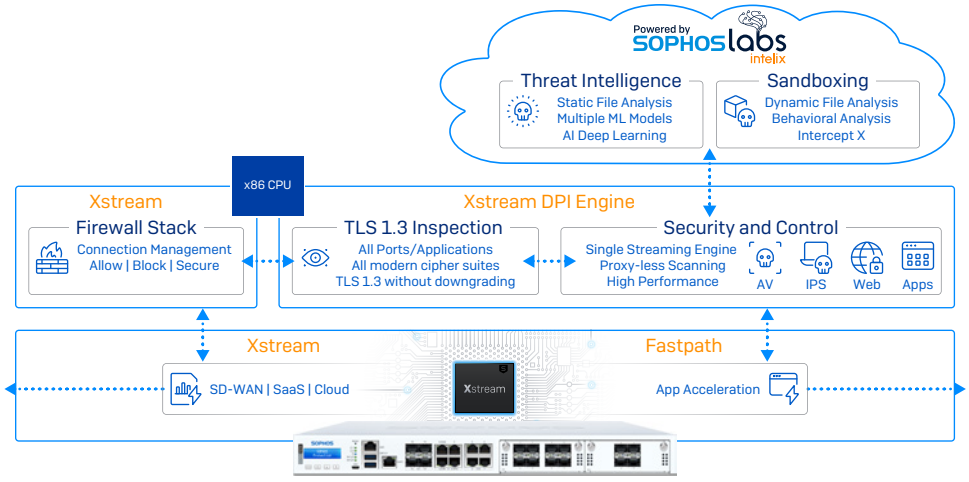
在 Sophos，我們不僅相信您需要最先進的保護技術，而且我們也了解，該技術必須易於設定、部署與管理日常工作，因為設定錯誤的保護往往比完全沒有保護更糟糕。

對簡單的承諾一直是 Sophos DNA 的關鍵部分。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方式運作，以提供更好的保護，最終獲得更佳的使用者體驗。

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。



Sophos Firewall 的 Xstream 架構與可程式化 Xstream 串流處理器能提供強大的保護和效能。

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，防火牆堆疊便會退開，並將處理完全卸載到 DPI 引擎。如此可大幅改善延遲和效能。

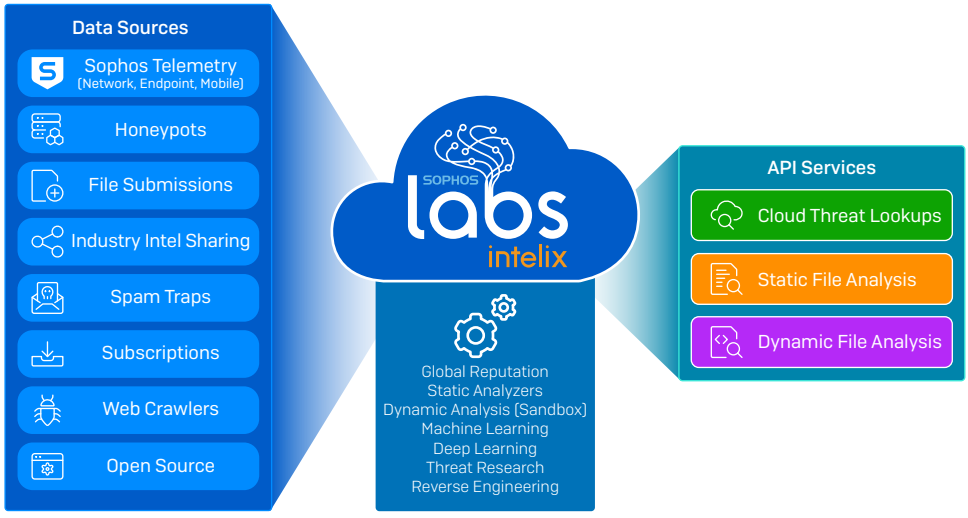
之後，如果該資料流被視為是安全的且不再需要進一步檢查，則 DPI 引擎可以將流程完全卸載到 Sophos Network Flow FastPath，這可為受信任的流量提供加速的路徑。如此可透過使其他資源不檢查不需要它的流量，進而大幅提升效能。

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。終極的解決方法有兩個方面：

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。

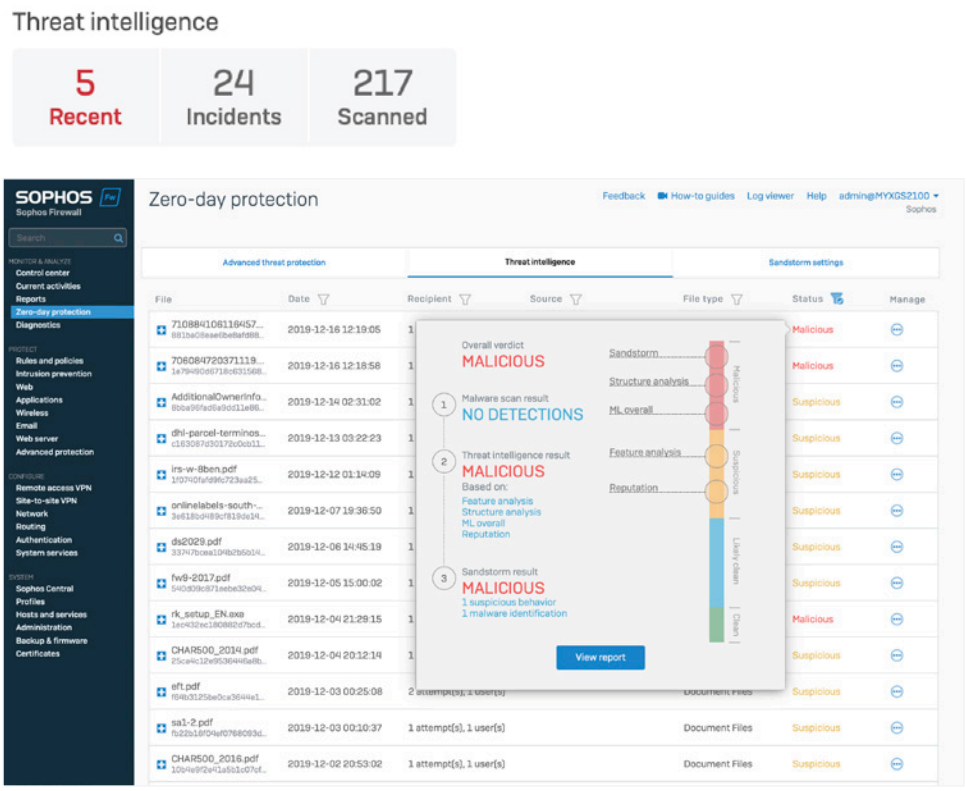
Sophos Firewall 具備了這兩項 SophosLabs Intelix 支援的重要保護技術。SophosLabs 是我們廣受好評的 Tier 1 網路安全威脅研究實驗室，已經開發出最終的威脅分析和情報平台 SophosLabs Intelix。它使用最新的機器學習技術、數十年的威脅研究成果以及 PB 級的情報，可提供無與倫比的保護，以抵禦前從未見的最新威脅。



Sophos Firewall 的零時差保護由 SophosLabs Intelix 機器學習分析提供支援。

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。

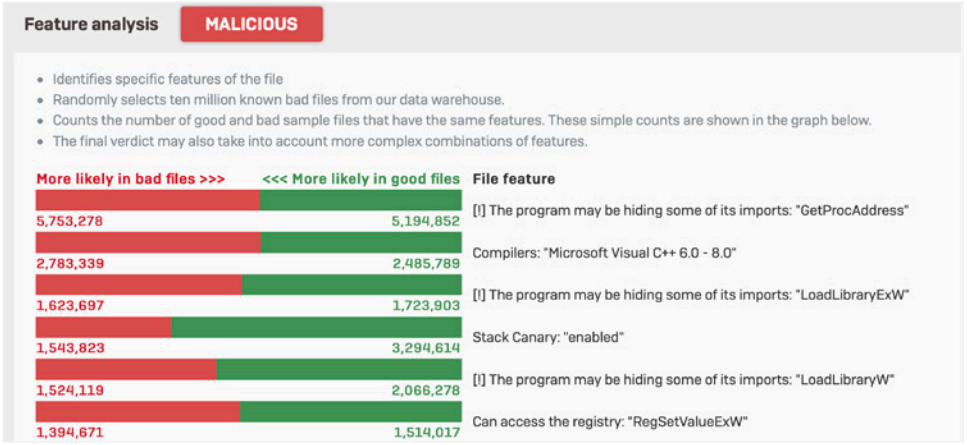
最後一步很重要，因為許多防火牆的進階型惡意軟體解決方案通常在分析完成前就將檔案傳送給使用者，如果最終檔案被判定是威脅，那麼可能會造成災害且清理代價昂貴。



Sophos Firewall 的零時差保護可在新威脅進入網路之前識別出它們。

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。



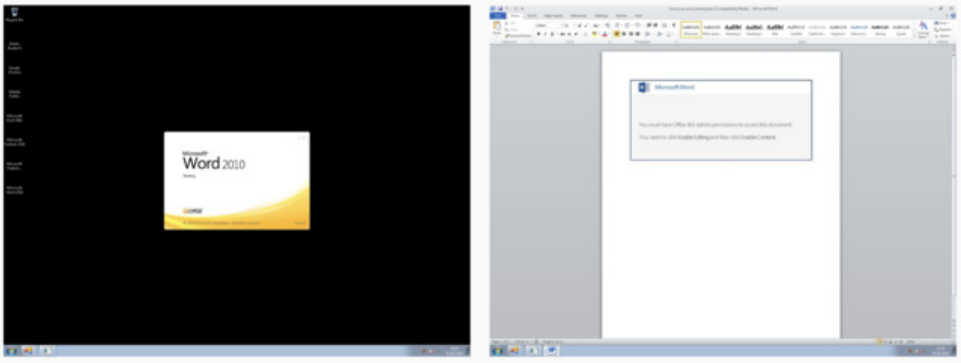
使用多種機器學習模型，以分析可疑檔案中的零時差威脅。

動態執行階段沙箱分析

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。中小型組織第一次透過深度學習技術存取沙箱，此技術遠遠超過了幾年前企業部署數百萬美元的專用內部部署沙箱解決方案功能。

由於它是雲端架構的，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。

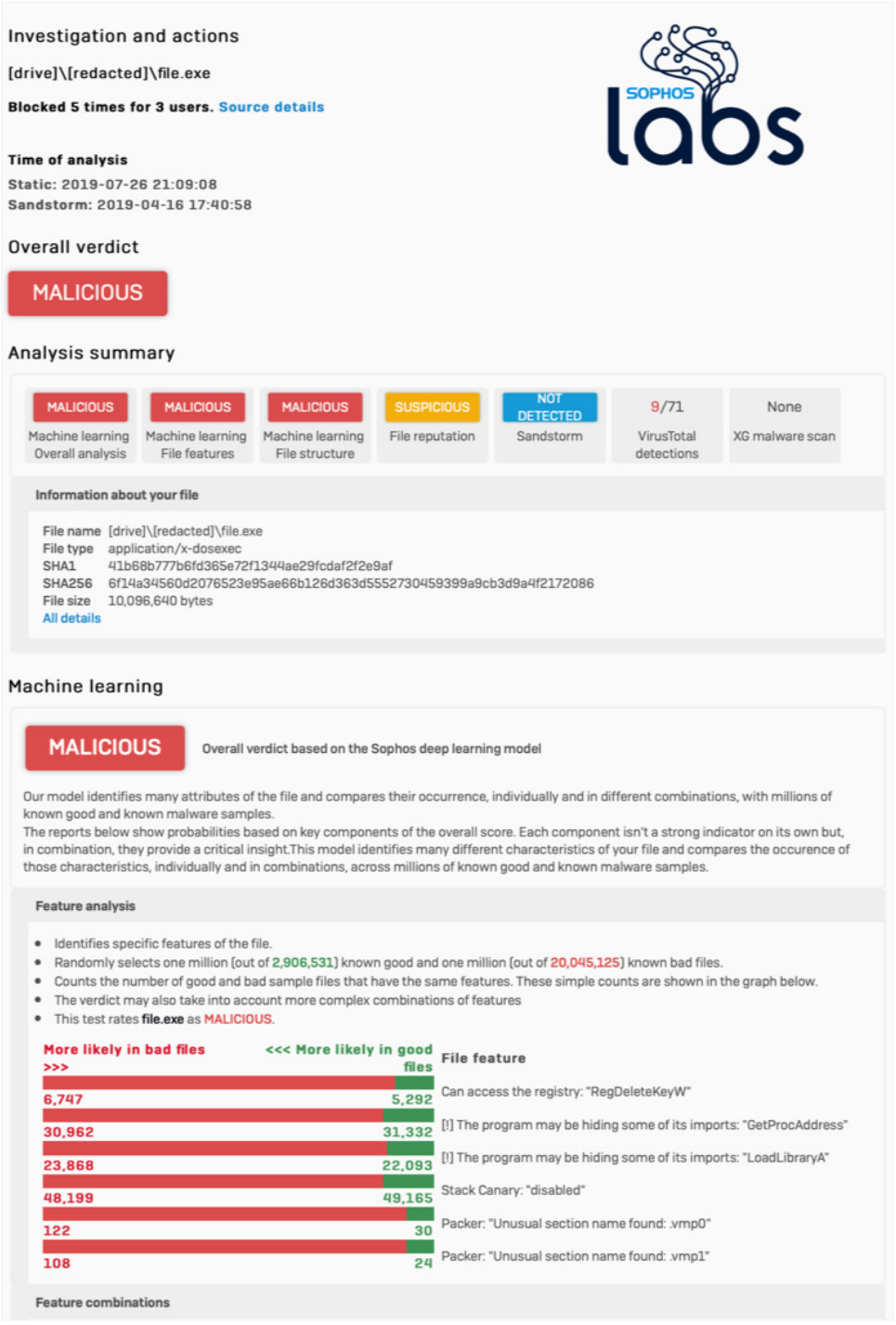


沙箱執行階段分析可在安全環境中引爆檔案，以確定其行為並提供畫面截圖供您查看。

沙箱在偵測出躲藏在沒有明顯惡意特徵的正常檔案中的隱藏威脅特別有效。包含巨集的 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

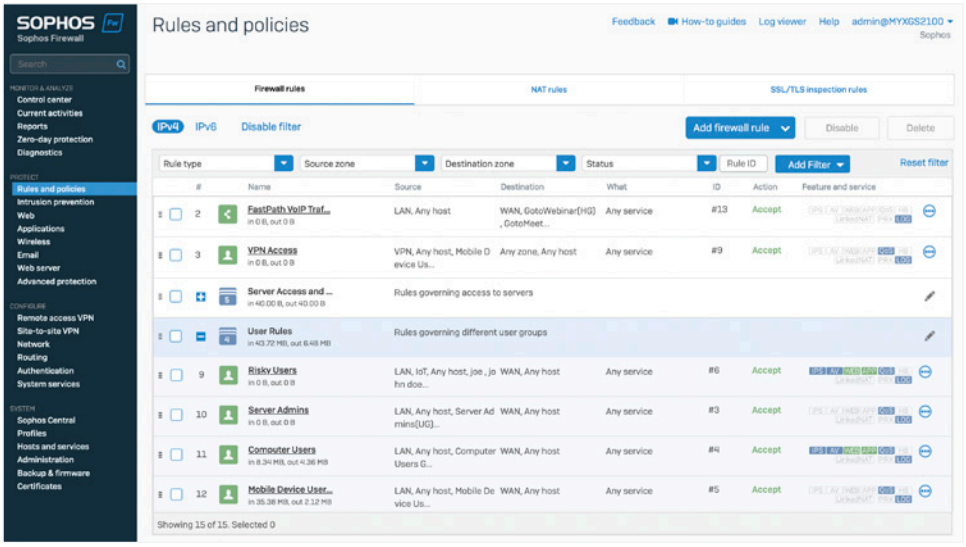
Sophos Firewall 分析的每個檔案都會隨附一個報告，提供各種分析結果和判定的完整詳細資訊。該報告包含 6 種不同的要件，包括各種機器學習分析、檔案信譽、沙箱，甚至是第三方 VirusTotal 的資料。



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域中，而且通常需要有數個不同的規則才能提供必要的保護，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管理集合到一個統一的畫面中，而不必在管理控制台上尋找適當的政策。您現在可以檢視、篩選、搜尋、編輯、新增、修改所有防火牆規則，並將其組織到單一位置。



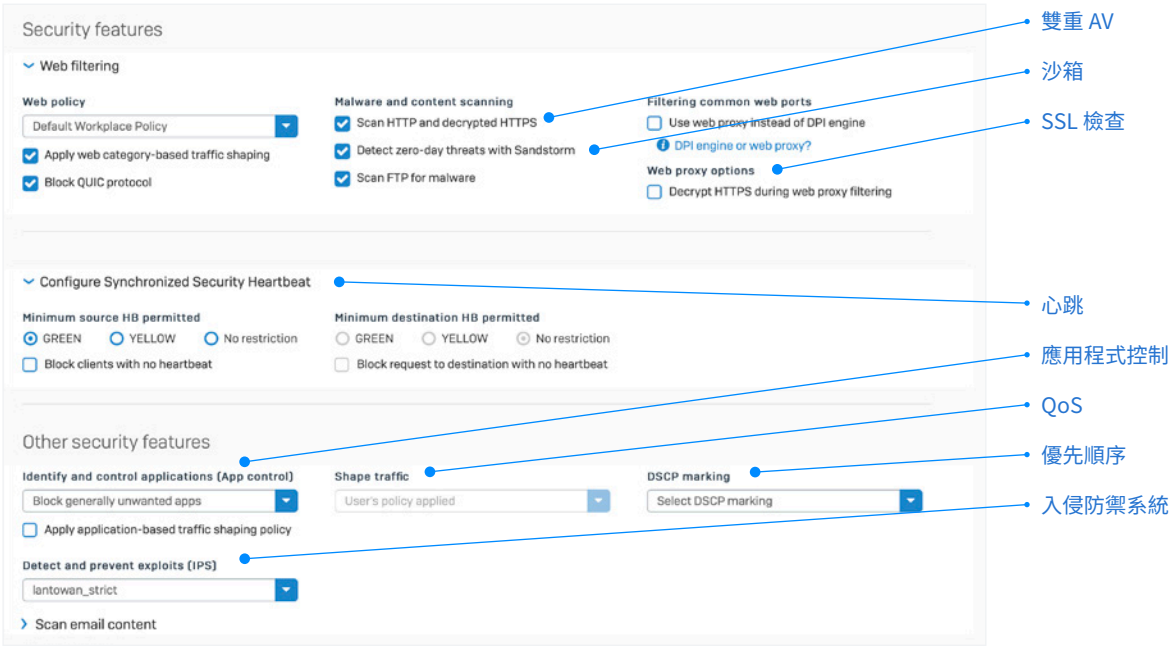
Sophos Firewall 將存取政策、NAT 和 TLS 檢查的所有規則集中在一處，以便於管理。

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

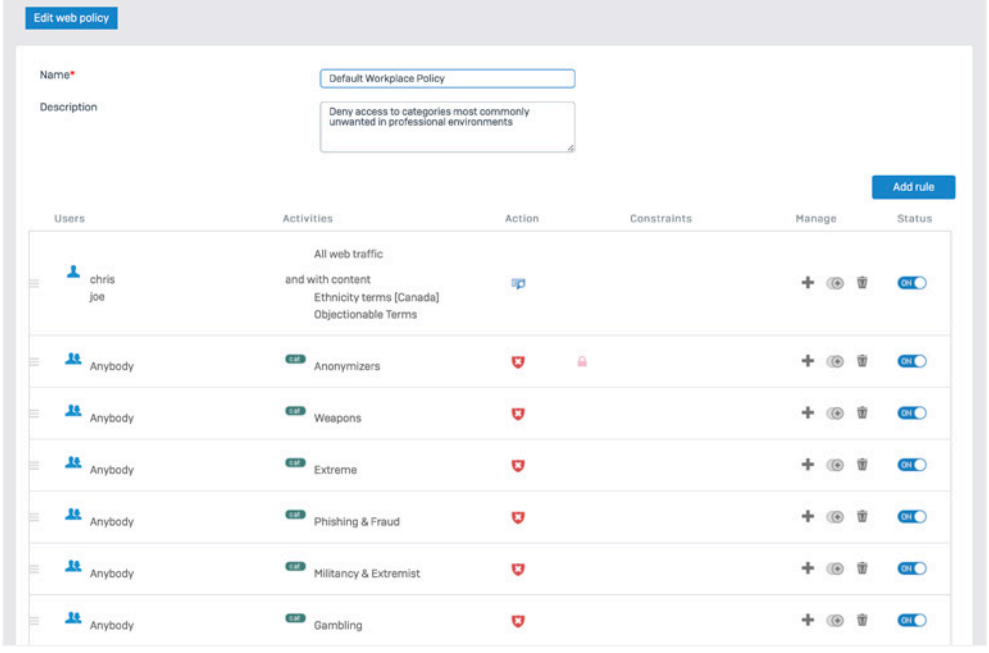
無論是透過雲端的 Sophos Central 帳戶還是 Sophos Firewall 使用者介面，Sophos 都可以輕鬆設定和管理新型保護所需的一切，而且全都可從單一畫面完成。



在一個畫面上使用預定義或自訂政策設定您的所有安全狀態。

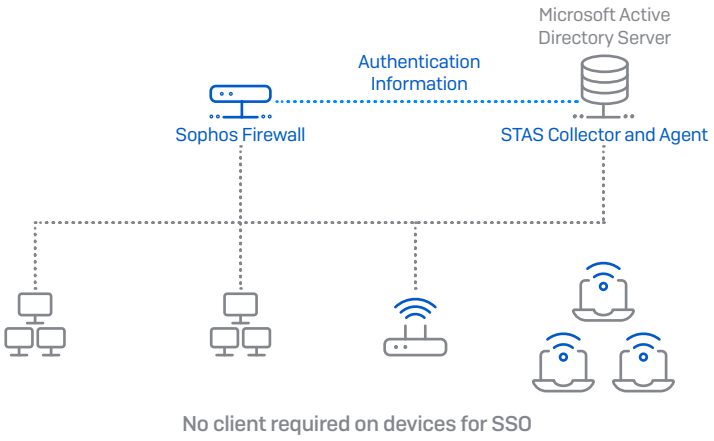
您可以針對防毒、TLS/SSL 檢查、沙箱、IPS、流量塑形、網頁和應用程式控制、Security Heartbeat、NAT、路由，以及優先順序，設定與管理安全及控制措施，全都從單一位置且按規則、使用者或群組為基礎來進行。

此外，如果您想要查看任何監管的政策正在執行哪些操作，甚至進行變更，則可以在原地進行編輯，而不必離開防火牆規則並存取產品的其他部分。



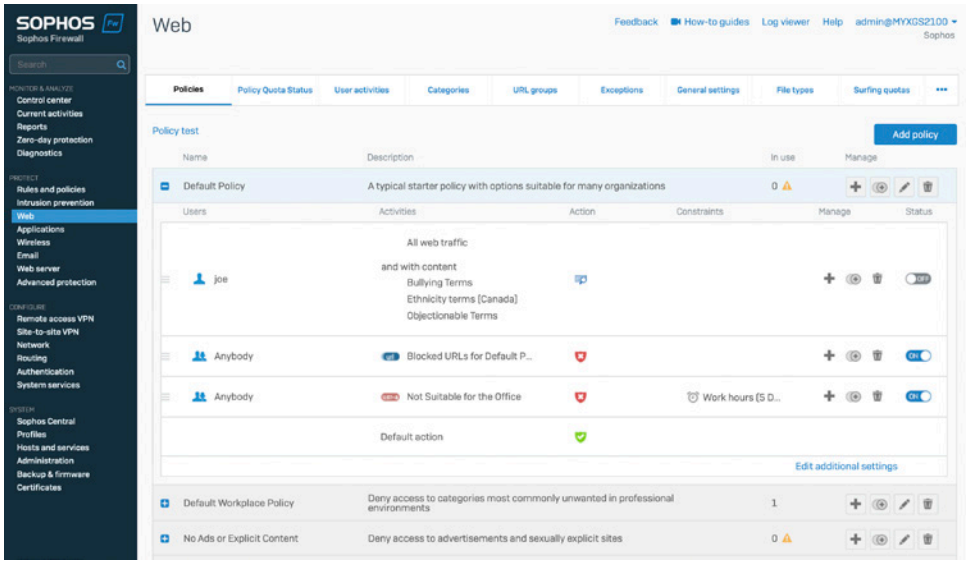
無需離開防火牆規則畫面即可一目了然地檢視政策詳細資訊並進行修改。

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 之類的目錄服務整合，以便進行簡單、可靠且透明的單一登入驗證。



企業級安全網頁閘道

網頁保護與控制是任何防火牆中不可或缺的功能，但遺憾的是，這在大多數的防火牆實作中都是事後諸葛。我們打造企業級網頁保護解決方案的經驗為我們提供了部署這種通常僅在企業安全 Web 閘道 (SWG) 解決方案中才能找到的網頁政策控制的背景和技術訣竅，且其成本只要十分之一左右。我們實作了一種自上而下的繼承政策模式，這使得建立複雜的政策變得簡單且直覺。大多數常見的部署 (例如典型的工作環境、教育的 CIPA 合規性等等) 中都包含了預先定義的現成政策範本。也就是說，您可以利用隨手可得的簡單微調與自訂選項，立即達到並符合標準。



強大的企業級 Web 政策提供精細控制的能力。

事實上，我們知道網頁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巨資，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 合規性預先封裝的網頁政策
- 對關鍵字的內容篩選和報告
- 基於使用者/群組政策的 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

根據關鍵字清單，網頁政策現在包含記錄、監視，甚至強制執行動態內容相關政策的選項。此功能在教育環境中特別重要，可確保線上兒童安全，並利用與自我傷害、霸凌、激進或其他不當內容相關的關鍵字，向學生提供深入見解。關鍵字庫可以上傳到防火牆，並套用至所有網頁過濾政策作為附加條件，其動作包括記錄、監控，或阻擋包含相關關鍵字的搜尋結果或網站。

提供全面的報告，以識別搜尋或取用相關關鍵字內容的關鍵字比對和使用者，以便在有風險的使用者成為真正的問題之前主動介入。

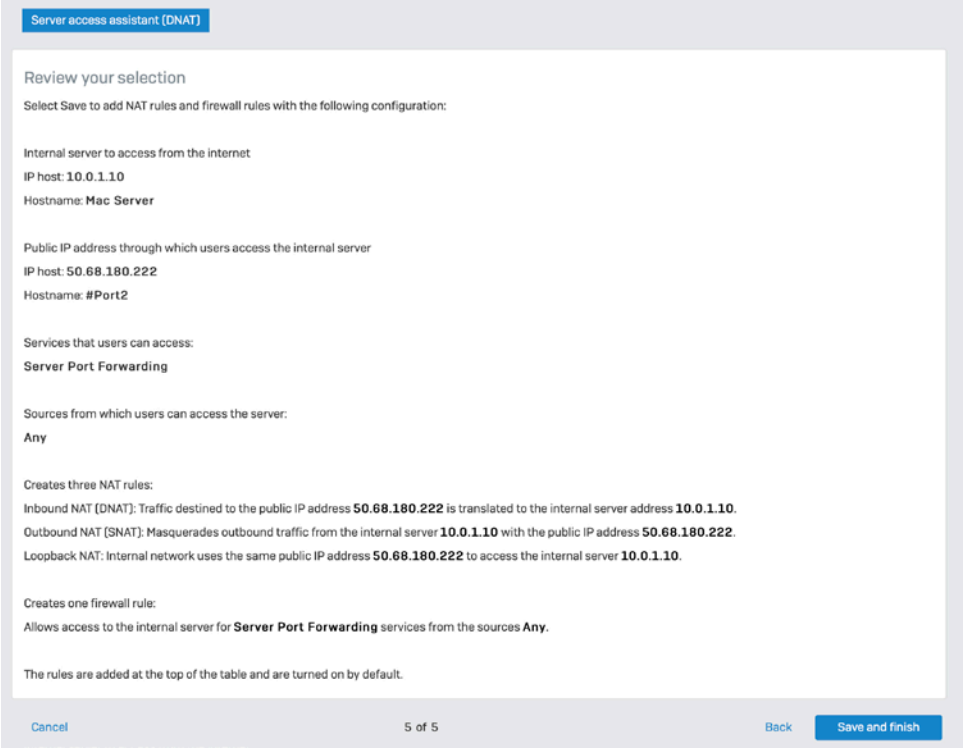
Sophos Firewall 可以立即協助您實現 CIPA 政策合規性，快速符合規範。它還會根據使用者/群組政策，對 SafeSearch 和 YouTube 限制提供彈性且強大的控制。此外，可以授予教師設定和管理自己的政策覆寫的選項，讓他們的教室能夠存取通常作為課程一部分而遭阻擋的網站。

這是簡化過的強大網頁政策。

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) 和目的地 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，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，進而減少建立與設定 NAT 規則所需的時間。

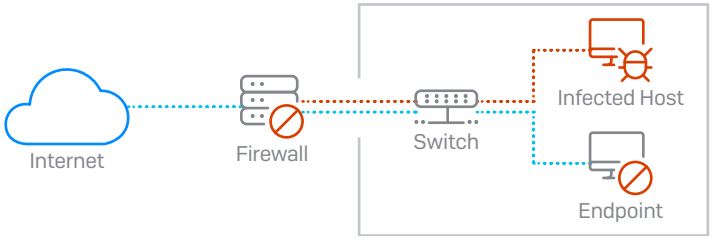


利用功能強大但直覺的 NAT 規則精靈，只需單擊幾下即可建立複雜的存取控制措施。

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 和 Security Heartbeat 可以自動隔離網路上受感染的主機。

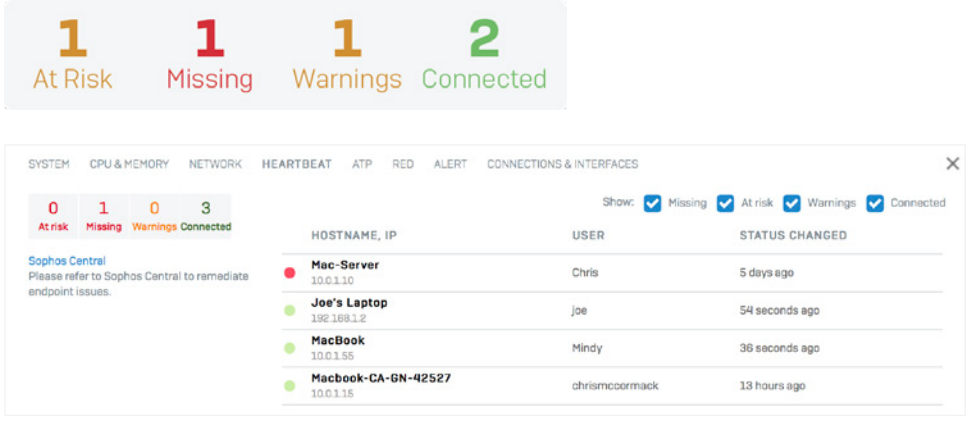
Sophos Firewall 會以獨特的方式，將連線主機的健康狀態整合到防火牆規則中，讓您自動限制對任何受感染系統之敏感網路資源的存取，直到淨化為止。

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通常無法干預的相同網路區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，只有在您的端點和防火牆在協調防禦或同步防禦上共同運作時才有可能。

Security Heartbeat

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。這個同步安全產品的簡單步驟 (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。



您可以在控制中心上看到網路的 Security Heartbeat™ 狀態。

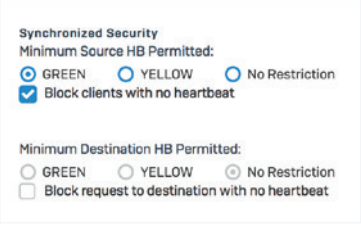
Security Heartbeat 不僅可以立即識別進階威脅是否存在，還可以用來傳達有關威脅性質、主機系統以及使用者的重要資訊。或許最重要的是，Security Heartbeat 也可以自動採取動作，以隔離或限制對受感染系統的存取，直到沒有惡意軟體為止。這項令人振奮的技術已經徹底改變 IT 安全解決方案識別和回應進階威脅的方式。

適用於防火牆後面受管理端點的 Security Heartbeat 可以處於下列其中一種狀態：

綠色心跳狀態表示端點裝置狀況良好，而且可以存取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。您可以選擇在問題解決之前，黃色心跳可以存取的網路資源。

紅色心跳狀態表示裝置可能有受到進階威脅感染的風險，而且可能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，可以在清理完成之前，輕鬆地隔離具有紅色心跳狀態的系統，以降低資料遺失的風險或阻止感染散佈。



將 Security Heartbeat 要求設定為任何防火牆規則的一部分。

只有 Sophos 可以提供諸如 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，而且正爭相實作類似的解決方案，但它們都處於明顯的劣勢：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及業界領先防火牆解決方案。

這是個零信任世界

信任在 IT 中已經成為一個危險的字眼，尤其是在隱含信任時。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都是有缺陷的設計。

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——世界上最受信任的網路安全平台，將這些不同且互補的技術整合到一個雲端管理主控台中，以幫助您協調和監控零信任網路。

同步安全——網路安全，在端點、ZTNA、防火牆和其他系統之間持續共用資訊，彼此提供深入資訊和可見性。

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

Sophos Firewall 圍繞用戶、裝置、應用程式、網路等建立分段或微邊界。

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。

最佳化 SD-WAN 網路

很少有網路術語能夠像 SD-WAN (或廣域網路中的軟體定義網路) 一樣引起轟動。所有這些話題都伴隨著等量的實用資訊和令人困惑的言論。因此，SD-WAN 已經發展成針對不同的對象代表的涵義不同，而有些人仍在努力弄清楚它到底是什麼。

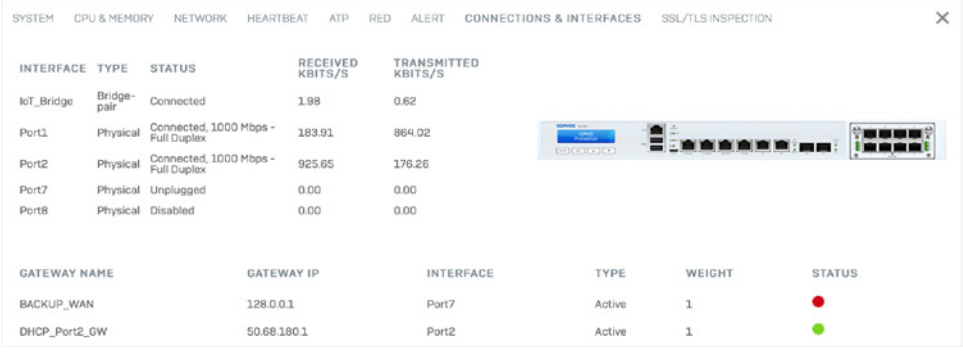
從根本上來說，SD-WAN 通常是想要實現以下四個網路目標中的一或多個目標：

- **降低連接成本**——傳統 MPLS (多重通訊協定標籤交換) 連線的價格昂貴，因此組織轉向更經濟實惠的寬頻 WAN 選擇，例如纜線、DSL 和 3G/4G/LTE
- **業務連續性**——組織需要在 WAN 故障或中斷時，可提供備援、路由、容錯移轉和工作階段保存的解決方案
- **關鍵應用程式的品質**——組織一直在尋求即時掌握應用程式流量和效能，以維持關鍵性商業應用程式的工作階段品質
- **更簡單的分公司 VPN 協調**——在不同地點之間的 VPN 協調通常很複雜而且耗時，這就是為什麼擁有簡化和自動化部署與設定的工具非常重要的原因

具備 Xstream SD-WAN 的 Sophos Firewall 使您能夠透過一整套 SD-WAN 協調、管理以及效能和可靠性最佳化選項，簡單且經濟地實現最宏大的 SD-WAN 目標。

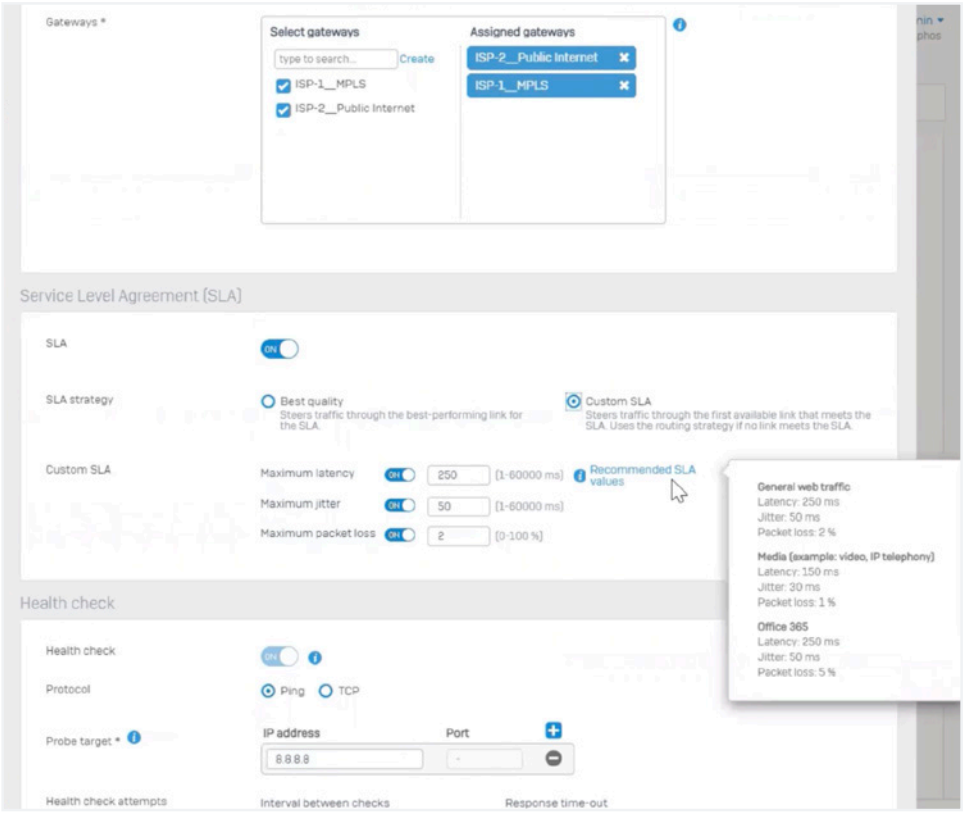
Xstream SD-WAN

管理多個 WAN 連結上的應用程式流量路由，是 SD-WAN 的一個關鍵要素，而具備 Xstream SD-WAN 的 Sophos Firewall 可提供強大而彈性的連結管理解決方案，無論您使用的是多個 MPLS、DSL、電纜還是行動數據。



WAN 連結狀態顯示在介面底部的狀態工具上，可透過儀表板開啟。

SD-WAN 設定檔定義了跨多個 WAN 連結閘道的路由這側，可根據 WAN 連結效能無縫、高效率重新路由應用程式連結。連結轉換會即時發生，完全不影響應用程式工作階段，並且不會中斷，即使在最具破壞性或不穩定的 ISP 環境中也能提供流暢的連續性、應用程式效能和最佳使用者操作。



架設以效能為基礎的 SD-WAN 設定檔既直覺又簡單。

可根據第一個可用或以效能為基礎的連結標準建立 SD-WAN 設定檔路由策略。效能監控標準包括抖動、延遲和封包遺失，並且可以在 PING 和 TCP 探測方面使用多個探測目標。

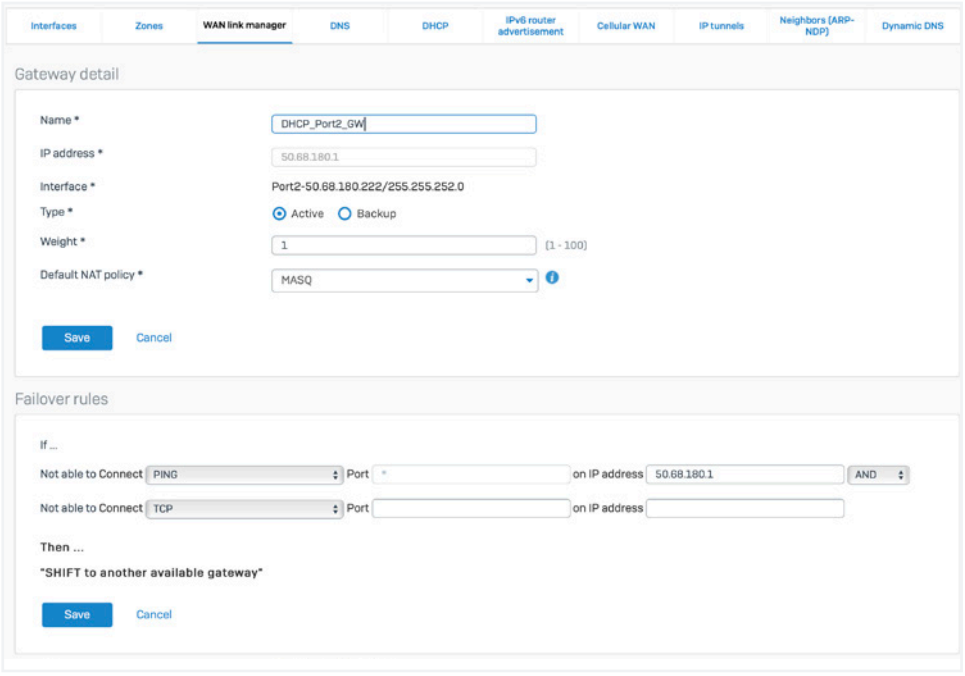
SD-WAN 設定檔可根據效能或自訂 SLA 政策自動選擇最佳連結，這些政策定義了最大可接受抖動、延遲或封包遺失的閥值，然後會重新路由到效能更好的連結上，不會影響任何作用中的連結。

透過延遲、抖動和封包遺失的即時和歷史圖表，可以輕鬆監控 SD-WAN 網路的效能。提供即時、過去 24 或 48 小時，或者是過去一週或一個月等時間線選擇。 還包括 SD-WAN 效能和路由的進階日誌功能。

即時監控各種 WAN 連結的效能。

對 SD-WAN VPN 流量的 Xstream FastPath 加速

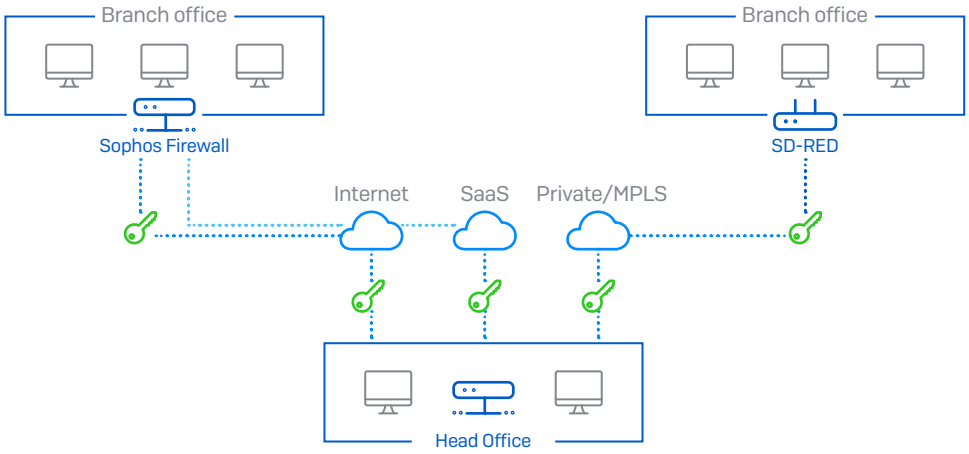
Sophos Firewall 使用整合在 XGS 系列設備中的 Xstream 串流處理器來對 IPsec VPN 通道流量進行硬體加速。藉此可以大幅提高效能，將 IPsec 通道所需的部分 CPU 密集型處理轉移到 Xstream 串流處理器，例如 ESP 封裝/加密和解封裝/解密。這個新功能充分利用了 Xstream 串流處理器中的硬體加密功能，並可釋放 CPU 資源以用於其他工作，例如對特定流量進行深度封包檢查。 用於 IPsec 流量的 Xstream FastPath 加速適用於站台到站台和遠程存取 VPN 流量。



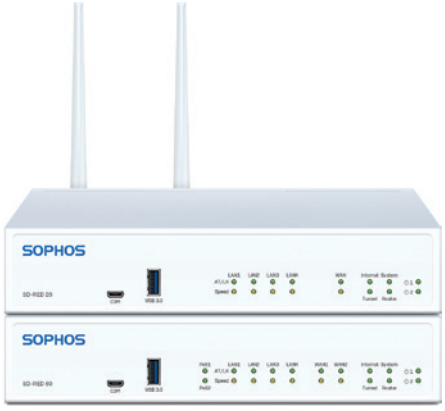
Sophos Firewall WAN 連結管理，包括平衡和容錯移轉規則。

分公司連線能力

長期以來，在無須使用者介入的分公司部署，以及使用我們獨特的 SD-RED 裝置連線等，Sophos 一直都是業界先驅。這些實惠的裝置對於非技術人員而言非常容易部署，而且在裝置與中央防火牆之間提供了強大且安全的第 2 層 (Layer 2) 通道。

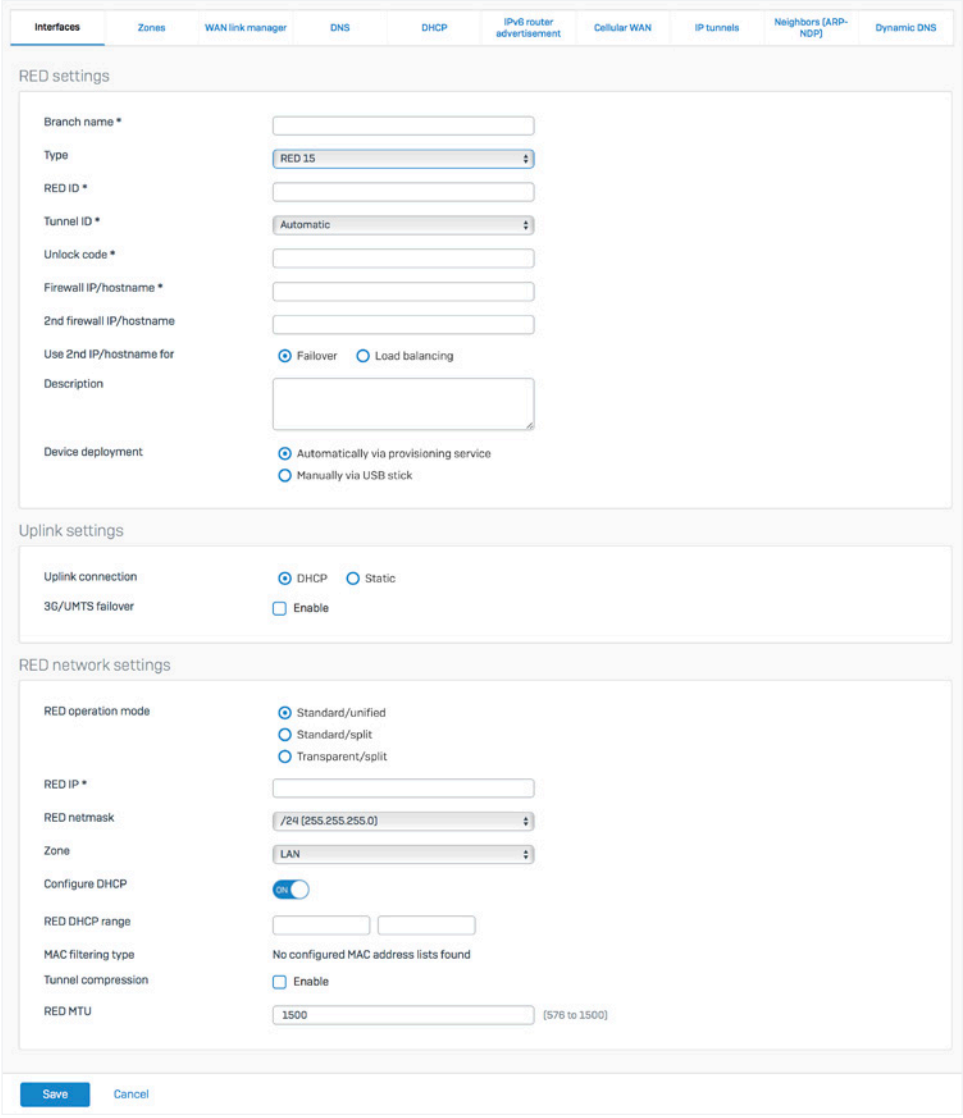


Sophos Firewall 和 SD-RED 裝置提供通道選項，可透過 SD-WAN，以簡單且經濟實惠的方式連線分公司。



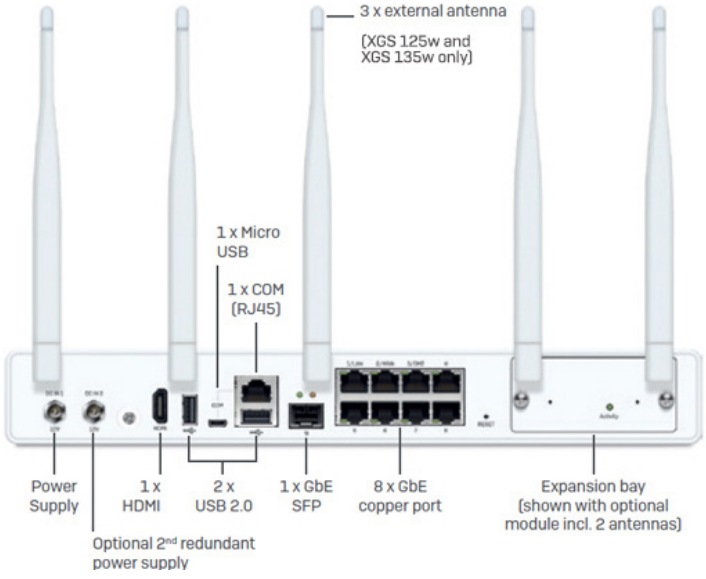
Sophos SD-RED 裝置為 SD-WAN 分支連線提供經濟實惠，而且無須使用者介入的解決方案。

部署 SD-RED 裝置再容易不過了：您只需要在防火牆中記下裝置的序號，然後將裝置運送到遠端位置即可。遠端站台上的任何非技術人員只需要將裝置連線，裝置就會自動與我們的雲端部署服務聯繫，以便與您的 Sophos Firewall 建立安全的通道連線。



Sophos SD-RED 可提供靈活、安全且經濟實惠的 SD-WAN 分公司連線解決方案。

我們的桌上型 XGS 系列設備也是提供彈性連線選項的絕佳分公司 SD-WAN 連線的解決方案，包括 VDSL 和行動數據，以及銅軸和光纖介面，並支援我們強大的 SD-RED 通道功能。

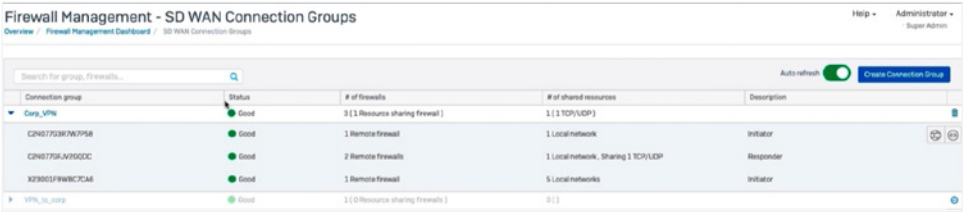


此處所示的桌上型機型 (如 XGS 135w) 隨附適用於 LTE/行動數據、VDSL、銅軸或光纖 WAN 連線的選項。

VPN 支援與協調

如果您曾經在不同的防火牆之間架設過多個 VPN 通道，就會知道這個過程又費時又煩人。Sophos Firewalls 可在 Sophos Central 中進行多種 SD-WAN 協調，使得在多個防火牆之間互連多個通道成為一項快速而簡單的工作。

您只需選擇要加入 SD-WAN 連結群組的受管理防火牆，然後選擇希望每個站台都可以存取的網路資源即可。只需簡單點擊，您就可以看到 SD-WAN VPN 覆蓋網路開始成形，因為所有必要的防火牆存取規則和通道 (包括備援) 都是自動建立的。



只需單擊幾下即可快速架設複雜的 SD-WAN 覆蓋網路，並透過 Sophos Central 進行監控。

無論您需要全網狀網路、中心輻射型拓撲，還是介於兩者之間的某種拓撲，Sophos Central 都會自動處理後端所有必要的通道和防火牆架設，以啟用您的 SD-WAN 覆蓋網路。

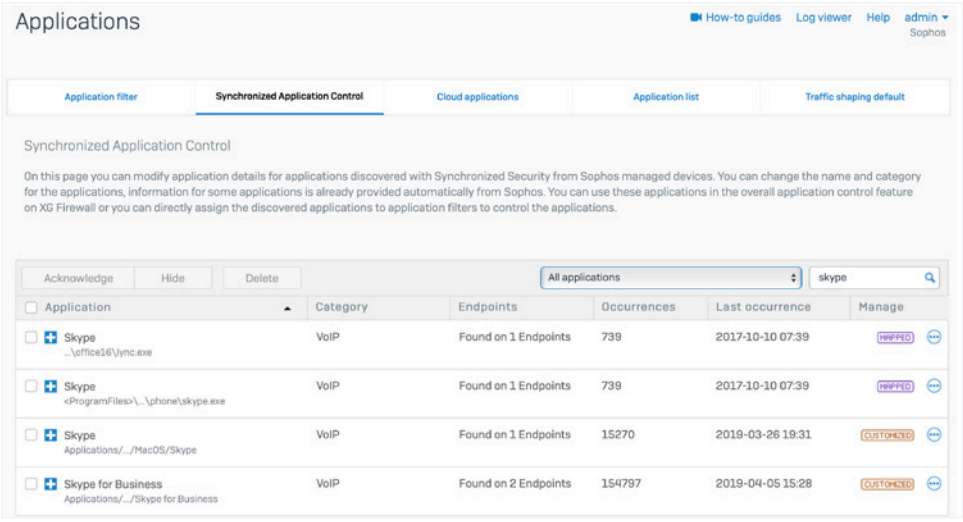
當然，Sophos Firewall 支援您想要的所有標準站台到站台 VPN 選項，包括 IPsec 和 SSL。我們甚至提供自己獨特的 SD-RED 第 2 層通道，此通道具有非常強大的路由功能，而且經過驗證，在諸如衛星連結等高延遲情況下都非常可靠。

應用程式可見度和路由

實現 SD-WAN 目標的另一個重要功能是應用程式路徑選擇和路由，用於確保品質並將 VoIP 等關鍵性應用程式的延遲降至最低。

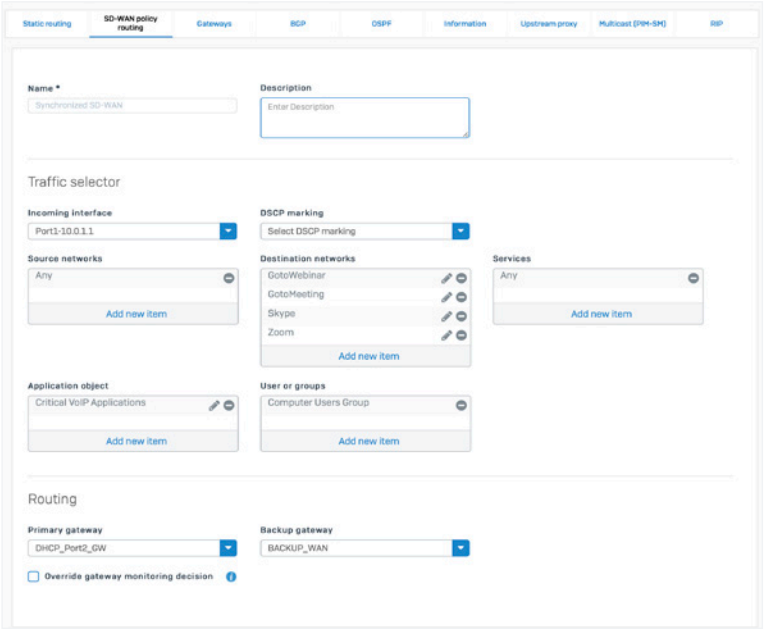
當然，您無法路由無法識別的內容，因此，準確、可靠的應用程式識別和可見度非常重要。這是 Sophos Firewall 和 Sophos Synchronized Security 提供絕佳優勢的一個領域。同步應用程式控制對所有網路連線應用程式提供 100% 的清晰度和可見度，在識別關鍵性應用程式 (尤其是模糊或自訂的應用程式) 方面具有顯著優勢。

同步 SD-WAN 是 Synchronized Security 的一個功能，提供 SD-WAN 應用程式路由的其他功能。同步 SD-WAN 可利用在 Sophos 受控端點和 Sophos Firewall 之間共用同步應用程式控制資訊時，隨之帶來的額外應用程式識別清晰度和可靠性。現在，過去無法識別的應用程式也可以加入到 SD-WAN 路由政策中，進而提供其他防火牆無法匹敵的應用程式路由控制和可靠性。



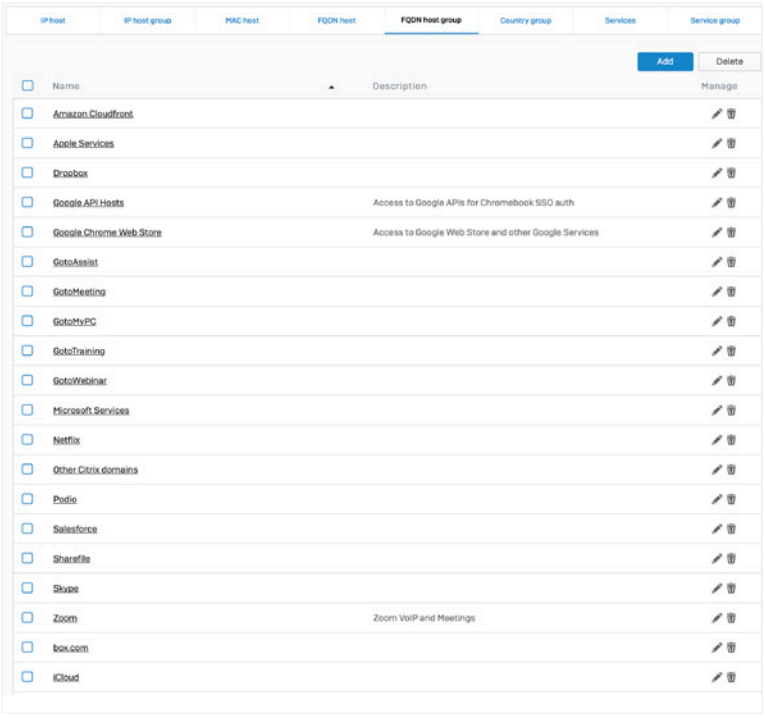
同步應用程式控制可百分之百識別所有網路連線應用程式，使其易於排定關鍵性應用程式的優先順序並加以路由。

Sophos Firewall 也可以在每個防火牆規則 (包括依使用者和群組) 中啟用應用程式型路由和路徑選擇。精細的政策型路由 (PBR) 控制能夠利用主要或備用閘道 WAN 連線定義路由，並針對重播方向進行設定。將這些功能結合起來後，可以輕鬆地將重要的應用程式流量引導到最佳 WAN 介面。



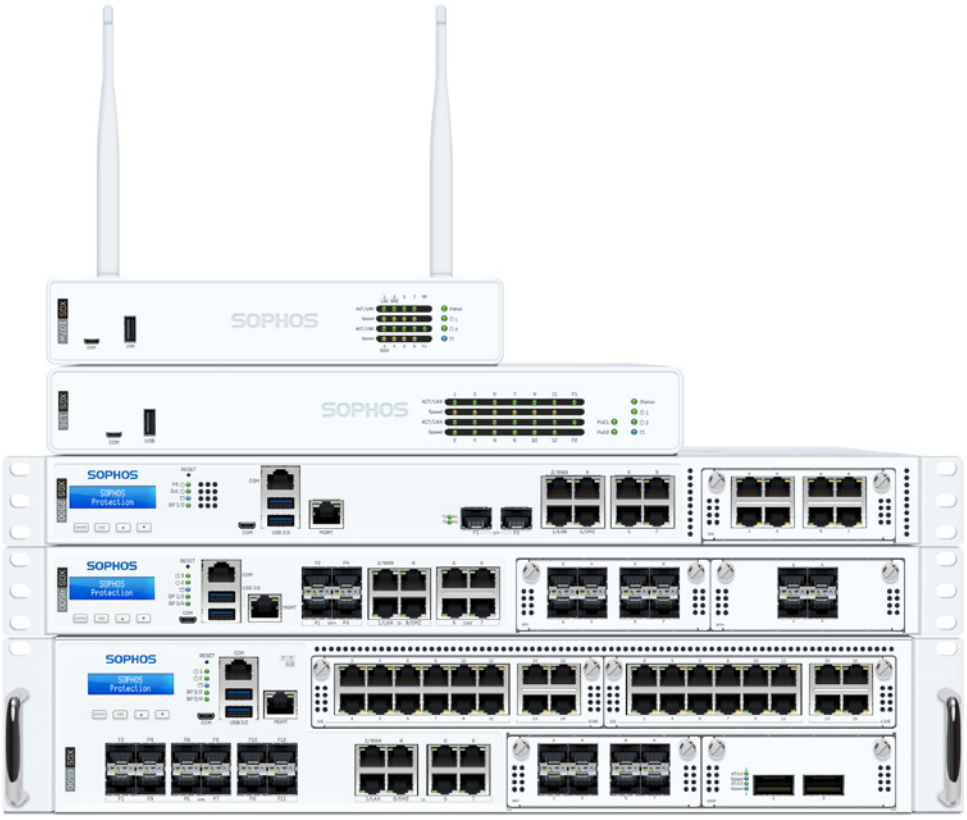
SD-WAN 政策型路由提供彈性的工具，可路由重要的應用程式流量。

Sophos Firewall 也包含預先定義的完整網域名稱 (FQDN) 物件以供常見的 SaaS 雲端服務使用，其中隨附立即可用的數千個 FQDN 主機定義以及輕鬆加入更多定義的選項。



預先定義的 FQDN 主機物件可簡化路徑選擇和應用程式型路由。

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。此功能允許使用完全沒有風險的新部署選項，而不需要替換任何現有的網路基礎架構。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，進而在任何網路中部署完整的 Sophos 同步安全解決方案，無需替換任何產品。

Sophos Firewall：網路安全變得更簡單。

索取價格

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

22-03-30 ZHTW (DD)