SOPHOS

Security made simple.

讓網路保持在掌控之中

為什麼網路系統管理員需要完全的應用程式可見度

防火牆的進化

多年來，防火牆的作用從保護網路免受外部駭客入侵和攻擊，逐漸演變為更加關注內部威脅，亦即識別和消除潛在風險並實現合規性。此一轉變的部分原因，是為了因應威脅情勢轉向惡意軟體和攻擊應用程式弱點(而非網路周邊本身)的入侵行為。此外，提供合理的合規程度、避免資料洩漏和遺失，以及最佳化網路效能等日益增加的需求，也促成了這個向內發展的轉變。

新一代防火牆本質上是專為使用者及其應用程式提供所需的可見度和控制需求所設計。顧名思義，新一代防火牆將過去狀態式防火牆的連接埠和通訊協定提升到 OSI 模型的更高層級，以提供應用程式和使用者感知的能力。

新一代防火牆使用深度封包檢測來識別應用程式，並將其關聯到網路上的使用者或主機，以便系統管理員可以提供適當的控制。例如，其能夠幫助找出執行點對點檔案共用應用程式的使用者並加以阻擋、控制用量過大的串流媒體觀看，同時排定重要業務應用程式的優先性，如 ERP 系統、VoIP 流量和 CRM 軟體等，非常有用。

新一代防火牆應用程式控制的運作原理

防火牆識別應用程式的作法是將流量中的模式與已知的特徵碼進行比對，就好比臉孔識別一般。當您看到一張不認得的臉孔時，可以把它和照片進行比較。如果發現有吻合的結果，您就知道對方是誰；如果沒有比對成功，您就無法知道對方的身分。

「平均來說，網路中約有 60% 的流量是無法識別的。」

應用程式控制(Application Control)的運作方式完全相同。雖然有些應用程式使用名稱標籤使其易於識別，但大多數應用程式不會，部分應用程式甚至會因無法識別而躲過偵測。當然，當比對成功並且確認應用程式時，防火牆就可以控制應用程式。其可以使用流量塑形來優先處理或限制應用程式使用的頻寬，或者直接阻擋該應用程式。但若沒有比對成功，防火牆就不知道該如何處理，也無法控制它。

新一代防火牆應用程式控制的問題

正如您可以想到的，許多應用程式並沒有足夠的資訊可讓我們容易地進行比對。在大多數組織中，通常會阻擋高風險的應用程式(如 BitTorrent 用戶端)，這些應用程式會使用巧妙的手法來不斷更改流量模式和連接到組織外部的方式，以躲避偵測。這與一個人改變頭髮顏色和黏上鬍子以躲避臉孔識別無異。

其他應用程式則使用加密來躲避偵測，就如同戴著滑雪面罩的人一樣；還有許多其他應用程式會偽裝成一個瀏覽器，以便未經檢查即可通過防火牆，這就好比一個壞人偽裝成一個知名的名人；然後，還有某些應用程式因最近變更、一次性、自訂或隱藏能力高而無法成功比對出模式，就像是沒有更新近期照片的人一樣。

實際上，隨著防火牆越來越善於識別和控制不需要的應用程式，上述應用程式在躲避偵測方面的能力越來越好。

最後的結果是，今日大部分流經現代防火牆的流量都是未知、無法識別或者是過於普通而無法分類或控制的。

您的應用程式控制報告看起來就像這樣嗎？

主要應用程式

應用程式名稱	應用程式百分比
一般 UDP	25.45%
一般 HTTPS 管理	24.26%
一般 DNS	17.8%
一般 TCP	14.39%
服務 RPC 服務 (IANA)	8.86%
Bit Torrent 通訊協定 - UDP 活動 1 (Reqs SIB 5)-63	1.60%

一般防火牆儀表板顯示無法識別的類別

問題有多嚴重？

為了更為了解這個問題所影響的廣泛程度，Sophos 最近對中型企業進行了一項調查，以確認其應用程式流量無法識別和控制的程度：

- 近 70%的企業採用了具應用程式感知能力的新一代防火牆或 UTM
- 平均來說，有 60%的流量是未知的...許多企業宣稱他們的應用流量中高達 90%是不明的如果您擔心這種情況對企業安全性、責任或效能的影響，那麼您並不孤單。
- 82%的受訪者非常擔心缺乏應用程式可見度所帶來的安全風險
- 65%擔心這可能會對網路效能造成影響
- 40%擔心潛在的法律責任和合規性風險

目前缺乏應用程式可見度的主要問題：

您對無法識別的網路流量有什麼顧慮？(複選)

安全顧慮

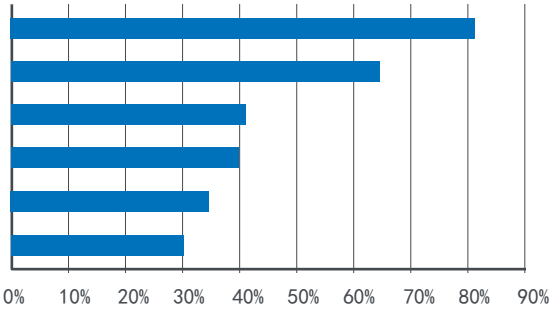
效能顧慮

生產力顧慮

責任和合規性顧慮

優先性問題

可見度顧慮



主要的隱匿性和無法識別的應用程式

這些隱匿性應用程式因存在弱點而帶來高度安全風險，以及包含可能不適當 或非法內容而導致合規性風險，並帶來對生產力和頻寬消耗的風險。

- 即時通訊 (IM) 和會議應用程式 (例如 Skype、TeamViewer)
- BitTorrent 和其他 P2P 用戶端 (例如 uTorrent、Vuze、Freenet)
- 代理和通路用戶端 (例如 Ultrasurf、Hotspot Shield、Psiphon)
- 遊戲 (例如 Valve 和 Steam)

不幸的是，您幾乎不可能知道網路上是否執行了這些應用程式，因為在大多數情況下，防火牆特徵碼根本在大多數情況都無法比對成功。

除了這些應用程式之外，還有不計其數的應用程式可能是良性且可能不需要的，它們使用通用的 HTTP 和 HTTPS 連線來穿越防火牆進行通訊，因為幾乎所有企業都開啟防火牆的埠 80 和 443 以供網際網路存取。在您的報告中，這些應用程式只會出現在 HTTP、HTTPS、SSL、網頁瀏覽和其他一般無用的類別中。

也許最重要的是，如垂直應用程式、ERP 解決方案、CRM 軟體和其他重要的特殊業務應用程式因未被偵測到，導致受到大量網路瀏覽行為和其他不需要應用程式的流量壓力所壓迫，只因為它們不夠流行或數量不夠多到足以製作特徵碼。

幸運的是，這個問題有一個相當簡潔的解決方案。

解決方案

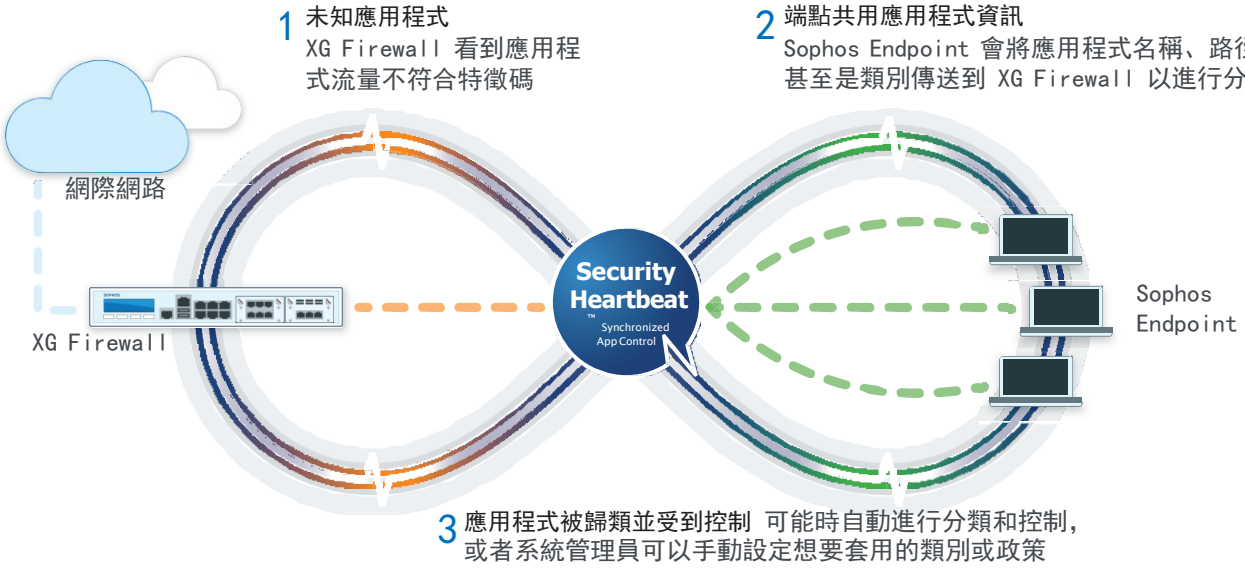
雖然新一代防火牆需要依靠深度封包檢測、模式比對和特徵碼來嘗試識別出在網路中傳播的應用程式，但是端點的獨特位置使其可以絕對清楚地知道哪些可執行檔正在產生所有的網路流量。因此，解決方案應運而生，作法是將端點與防火牆連接起來，以共享這些有價值的資訊。幸運的是，Sophos 已經擁有可以簡單且有效實現這一目標的技術：同步安全 (Synchronized Security)。

Sophos Synchronized Security 是一種革命性的全新 IT 安全方法，可使安全產品能夠共享資訊並共同協作，提供即時深入資訊、無與倫比的保護和自動事件回應能力。

同步安全創新技術中的 Security Heartbeat™(安全心跳)可將由 Sophos Central 管理的端點與 Sophos XG Firewall 相連，共享端點健康狀態，以便即時識別出面臨風險的系統。當端點或防火牆偵測到威脅時，就會即時發出流量燈號指示和警示，立即識別出相關的電腦、使用者和處理序。SecurityHeartbeat 最重要的優點之一，可能是防火牆可以在防火牆規則中包含端點健康狀態，以便實現自動回應，限制存取或者完全隔離被破壞的系統，直到清理完畢為止。藉此可將回應時間從幾小時縮短到幾秒鐘，並有助於降低感染擴散到網路其他部分的風險。

另一個同步安全創新是 Synchronized App Control(同步應用程式控制)。正如名稱所示，Synchronized App Control 可利用 Sophos 獨特的同步安全生態系統有效且簡潔地解決問題，在網路上識別未知、隱匿型或自訂應用程式的流量。Synchronized App Control 利用其與端點的資訊共享能力來確定網路上無法識別的應用程式流量的來源，可以去除掉今日覆蓋在網路上的層層面紗。

Synchronized App Control 的運作原理



這是自從構思新一代防火牆以來，在網路應用程式可見度和控制方面的第一個重大突破。

當受 Sophos Central 管理的端點連接到有 XG Firewall 的網路時，它將會建立 Security Heartbeat™連線以共享健康和安全狀態以及遙測功能。此外，端點還將使用此一連線與防火牆共享所有網路應用程式的身分。

當應用程式是隱匿性、自訂、新建立或使用通用連線時，防火牆將無法使用傳統的特徵碼技術來確認應用程式的身分，此時端點提供的應用程式資訊將可用於識別、分類和控制這些應用程式。如果可行，由端點分享資訊得知的應用程式將被自動分類到適當的類別。接著可以自動對新識別和分類的應用程式套用已經在防火牆上實施的任何應用程式控制政策。

例如，一個具隱匿能力的 BitTorrent 用戶端將被自動分類到對等(Peer-to-Peer)的應用程式類別。如果防火牆實施了一個阻擋點對點應用程式的有效應用程式控制政策，則會自動阻擋新的 BitTorrent 流量，而且無須任何網路管理員的介入。

效益：

識別未知的應用程式

Synchronized App Control 可發現網路上所有目前無法看到的應用程式， 包括所有新的應用程式以及通常使用加密技術隱匿防火牆控制的通道、代理和VPN 應用程式。這產生了一個巨大的盲點，以及各種合規性、效能和安全的風險。如果目前擁有可以阻擋或流量塑形這類應用程式的政策，被新識別出來並分類到某類別的應用程式將被自動套用相同的政策。此外，可以容易地識別出相關的使用者和主機，以便在可行時進行管理和調校。

排定自訂應用程式的優先性

Synchronized App Control 將可立即識別出目前防火牆無法看到的自訂業務應用程式，例如財務、CRM 客戶關係管理、ERP 企業資源規劃、製造過程和其他對貴組織非常重要的網路應用程式。Synchronized App Control 首次提供應用程式流量塑形和 QoS 政策的機會，以確保這些關鍵性應用程式可以獲得適當的優先性和最佳效能。

控制隱匿型應用程式

Synchronized App Control 會自動發現所有為躲避偵測和控制而不斷 改變連線和通訊方式的隱匿型應用程式。實際上，Synchronized App Control 一勞永逸地終結了這些手法。無論這些應用程式試圖如何隱匿，它們都無法逃避 Synchronized App Control 的掌握。

「這是自從構思新一代防火牆以來，在網路應用程式可見度和控制方面的第一個重大突破。」

需要的 Sophos 產品：

Sophos 提供了一個完整的 IT 安全產品生態系統，簡單整合就可以提供同步安全。您可以非常輕鬆地實現 Security Heartbeat™和 Synchronized App Control，並且獲得它們所帶來的安全性、可見度和控制能力。您至少需要 Sophos XG Firewall 和 Intercept X，但是這兩種產品都可以補強的方式部署在現有的 IT 安全基礎架構中，以提供同步安全，而無須中斷或更換現有安全產品。

Sophos XG Firewall 可以與現有防火牆串接，也能作為主要的防火牆閘道。當 XG Firewall 以探索模式(也稱為 TAP 模式)連線到交換器的鏡像埠時，它也可以用報告和監看模式運作。

在端點部份，Intercept X可以與現有的桌上型防毒解決方案一起部署，或者您可以選擇使用 Sophos Central Endpoint Advanced，獲得來自 Sophos 的完整端點保護。這兩款產品在 Windows 和 Mac 平台上都支援 XG Firewall 的同步安全。

總結

新一代防火牆無法提供其承諾的應用程式感知能力。以特徵碼為基礎的應用程式偵測技術，在有效性方面存在著先天的限制，這意味著當今網路上的大部分應用程式流量無法被識別和檢查。這是一個明顯且嚴重的問題，會造成龐大的安全性、生產力、效能和合規性風險。

幸運的是，我們有一個簡潔而有效的解決方案：Synchronized App Control 利用 Sophos 獨特的 Security Heartbeat™技術，在受 Sophos Central 管理的端點和 XG Firewall間連線，以絕對明確的方式共享網路應用程式資訊。

具備 Synchronized App Control 功能的 XG Firewall 可以自動識別、分類和控制網路上所有未知的應用程式流量。這是網路可見度和控制方面的一個重大突破，遠勝過所有其他的新一代防火牆。

關於湛揚科技

湛揚科技為 SOPHOS 台灣專業代理商，同時也為安克諾斯 Acronis 台灣總代理，協同通路合作夥伴為各產業使用者提供高效能的防毒、防火牆、備份解決方案，為企業與政府機關提供性價比最佳的資安服務及產品，建置最適合的防護及專業技術服務。如您對 SOPHOS 想瞭解更多，或進一步需求，歡迎洽詢湛揚科技，我們有專業資安團隊提供您詳細產品簡報，產品免費測試，讓您快速體驗 SOPHOS 強大有效的防護能力！

SOPHOS 專業代理商 湛揚科技 www.t-tech.com.tw
台北：(02)2735-3512 技服電話：(02)7718-5588
高雄：(07)972-7388 技服信箱：support@t-tech.com.tw