新世代防火牆：投資檢查清單

您將會學到

購買新世代防火牆 (NGFW) 時，您會想判斷這個解決方案能否為整個企業提供全方位的保護。您需審視八個必備功能。NGFW 應能：

1. 緊密整合安全功能，提供有效的威脅與進階惡意軟體防護
2. 提供完整且整合的管理
3. 提供可行的入侵指標，用以識別網路和端點上出現的惡意軟體活動
4. 提供全方位網路可視性
5. 即便使用者的 VPN 關閉，也可隨時隨地予以保護
6. 協助降低複雜度和成本
7. 整合及配合第三方安全解決方案
8. 提供投資保護

本白皮書將深入說明這份檢查清單，同時提供確實有效的 NGFW 解決方案可帶來的效益範例。

背景

單獨依賴時間點防禦與技術的網路安全系統，無法跟上今日多重向量攻擊方法複雜且不斷進化的腳步。實際上，根據思科 2016 年度資安報告，機智的攻擊者正利用合法的線上資源發起活動和提高收益。其手法包括過濾掉伺服器容量以竊取資料並索取贖金，以及使用惡意瀏覽器延伸模組來洩漏資料。[1] 組織必須持續努力採取可能的最佳威脅防護措施，不過同時也須將注意力集中在偵測用時 (TTD)，因為對手的規避活動增加，這是重要度日漸提高的指標。目前業界的 TTD 措施為期 100 至 200 天，所需時間太長了。[2]

新世代防火牆 (NGFW) 的推出是一大邁進，不過典型 NGFW 將焦點放在應用程式存取控制，對於威脅防禦功能少有著墨。典型 NGFW 也失去了可視性，且無法在使用者位於傳統網路周邊之外或是繞過 VPN 存取網際網路時保護使用者。部分 NGFW 已加入第一代入侵防禦及各種未整合的產品，但是若要防禦老練攻擊者和進階惡意軟體所帶來的風險，這些解決方案的幫助並不大，而且也無法以簡單且符合成本效益的方式保護漫遊使用者。此外，這些 NGFW 在感染發生後提供的援助少之又少，無法協助調查、遏止或快速修復感染。

現今的多重向量和持續性威脅、流動的 IT 環境及不斷提高的網路需求，促使更多組織尋求更優異的 NGFW 解決方案。他們需要一個可提供分層式威脅防護和整合防禦功能的解決方案，也想採用可透明協作、追蹤使用者，以及在攻擊滲透網路時可減輕風險的頂尖安全技術。

這份檢查清單和本文件所列出的購買考量事項，可輔助您確認所投資的 NGFW 解決方案確實有效。防火牆應能提供網路的整體全貌，以及利用級別有效分析即時威脅與網路流量，且應能協助組織防禦針對性和持續性的惡意軟體攻擊（包括浮現的威脅在內），同時也應可降低複雜度。

基礎

評估解決方案的第一步為考量 NGFW 的基礎，這將會是您做出購買決策的起點。若要提供整合式防禦及多層式威脅防護，NGFW 必須建置在可設定狀態的全方位防火牆基礎上，並同時尋找具有經實證效能系譜的解決方案。

NGFW 基礎應採用可設定狀態的全面性檢查引擎，且能提供全方位的基本威脅可視性，讓您保護重要資產。NGFW 也具備充分的健全度，即使在啟用多個服務的狀態下，也可提供高度有效的大規模威脅防護。此外，不僅需有能力識別威脅，也需能識別連線至網路的使用者和裝置，並監視其活動以判斷異常情況。NGFW 還必須延伸防護範圍，在漫遊使用者未連線至公司網路時也予以保護。最後，應在單一主控台中提供全方位的可視性及相互關聯的資訊以利深入管理。

1. 思科 2016 年度資安報告：http://www.cisco.com/c/en/us/products/security/annual_security_report.html
2. 同上。

NGFW 檢查清單

參閱本檢查清單，確認您考慮採用的 NGFW 解決方案可同時且即時地提供防護、強制執行政策、達成一致性以及擷取和共用內容。

1. 該解決方案緊密整合了安全功能，可提供有效的威脅和進階惡意軟體防護。

NGFW 應具備緊密整合且互相通訊的安全層。雲端運算和行動能力等新型態工作方式正在擴展攻擊面的面積。所有安全層的威脅情報關聯性可識別溜進典型防護和逃避偵測間隙的攻擊。此程度的防護需要網路和端點上的防禦功能持續協調，讓安全團隊可迅速追蹤威脅和展開修復活動。

尋找可提供全方位防護且聚焦於威脅的 NGFW。NGFW 解決方案中的威脅偵測功能不僅可協助安全團隊發現和阻止惡意軟體，也有助於瞭解惡意軟體。

2. NGFW 包括整合管理。

僅僅是緊密整合安全功能並不足夠，NGFW 還必須在提供單一管理介面且簡化作業程序的平台上進行整合。透過中央主控台管理所有安全功能，可簡化整合安全架構的管理作業，且可加快偵測和回應的速度。對於人力不足或缺少專業技術的資安部門而言，具備處理現今不斷變動且複雜的威脅並同時降低複雜度的能力至關重要。

3. NGFW 提供可行的入侵指標以識別惡意軟體活動。

入侵指標 (IoC) 會在主機上使用「標記」表示可能已發生感染。IoC 與網路和端點安全情報相關聯，可識別與主機和端點有關的惡意軟體活動，並提供高度準確的可疑與惡意行為可視性。

擁有上述功能的 NGFW 解決方案可實現更快速的識別、遏制和修復。

4. NGFW 提供全方位網路可視性。

NGFW 應以清晰且全面的觀點審視網路上隨時發生的情形，藉此提供內容相關的完整覺察。可視性應包括使用者與裝置、虛擬機器間的通訊、威脅與弱點、應用程式與網站存取、檔案傳輸以及更多內容。

全方位的網路可視性需要持續且被動監視網路中的所有資產，您可透過自動化使用此資訊，進而最佳化安全有效性。動態控制項應即時回應 IT 環境或威脅概況中的變動。解決方案應提供即時的深入分析，協助資安團隊識別和解決資安缺口、微調資安政策，最終減少重大事件的數量。

NGFW 也應能自動化發生攻擊後的防禦回應，包括調查和遏止感染，自動化將可進一步減輕資安團隊的負擔。

5. 即便使用者的 VPN 關閉，NGFW 也可隨時隨地予以保護。

NGFW 必須在公司網路周邊之外提供可視性和防護，就算使用者直接連線至網際網路也一樣。解決方案必須能將防護範圍延伸至行動使用者，這些使用者時常仰賴雲端應用程式完成工作，他們可能會在無意間繞過 VPN，或是不再需要存取公司網路便可完成工作。若採用整合做法，便不再需要部署用來保護漫遊使用者的額外代理程式。

6. NGFW 有助於降低複雜度和成本。

能有效防禦進階威脅的 NGFW 也應提供：

- 防禦層的整合安全
- 高擴充性
- 日常安全工作自動化

整合的多層式做法可提供更優異的威脅可視性，並因而達到更有效的防護。將多個產品合併到單一平台上，也可消除購買和管理多個解決方案的複雜度和成本。因此，合併可解決最常見的障礙以獲得更優異的安全性：資源限制。[3]

3. 思科 2016 年度資安報告

擁有多層式威脅防護功能的 NGFW 能協助資安管理員提供一致且健全的大規模安全性，且可支援小型分公司、網際網路邊緣站點，甚至是實體和虛擬環境中的大型數據中心。

NGFW 解決方案應自動化以下活動：

- **影響評估**：NGFW 應自動建立威脅與主機弱點情報、網路拓撲和攻擊內容間的關聯。這項評估能協助資安分析人員將注意力完全集中在需監視和迅速回應的入侵活動。
- **政策調整**：NGFW 應自動化在整個企業中一致地佈建、調整和強制執行資安政策的程序。如此一來資安團隊便可最佳化安全有效性，且可即時回應有所變動的情況和新攻擊。資安政策管理自動化對於資源短缺的 IT 部門而言尤其重要。
- **使用者識別**：NGFW 應能輕易將使用者身分歸類至資安事件。此功能可為資安分析人員節省時間，有助於更迅速地遏止和修復威脅。

7. NGFW 可順暢且透明地整合及配合第三方資安解決方案。

與第三方解決方案整合可加深 NGFW 解決方案提供的多層式防護，將基本安全層結合到一個平台上，並透過整合介面集中管理。這套做法可簡化資安部署和進行中的作業活動，且支援現有資安技術，並共享情報以協調和簡化回應程序。

NGFW 應透過第三方技術的開放 API 支援豐富多元的解決方案「生態系統」，這些技術包括：

- 弱點管理系統
- 網路虛擬化和資安資訊與活動管理 (SIEM) 系統
- 網路存取控制 (NAC)
- 網路鑑識
- 事件回應工作流程

8. 解決方案提供投資保護。

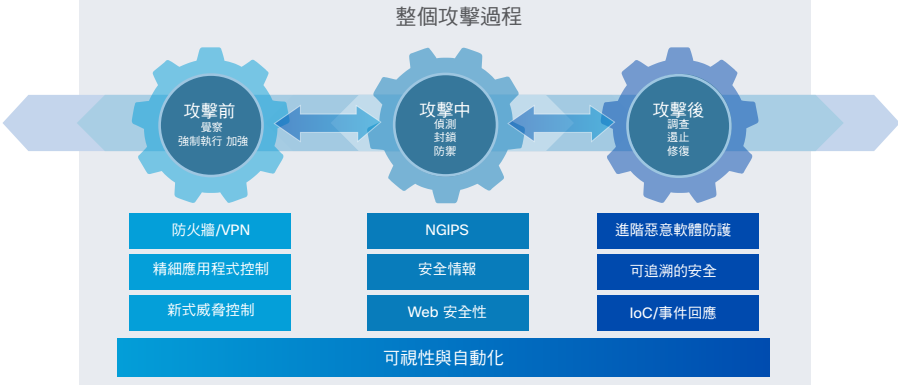
投資新世代資安解決方案時，您所尋求的是能為整個企業提供全方位保護的產品。除了直接購買，您可能還想考慮替代產品。NGFW 廠商應提供不同的購買選項，讓貴組織有機會能：

- 透過更短的 IT 生命週期與主動式管理降低成本和提高生產力
- 藉由「智慧授權」和「企業授權」選項節省開支，這兩個選項可最佳化軟體使用且提供彈性，讓您可在就緒時快速部署
- 配合目前的企業策略和未來願景更新技術資產，並維持可預測的預算
- 採用端對端且價格實惠的財務解決方案，其中包括硬體、軟體和第三方輔助設備。

符合本檢查清單的 NGFW：思科 Firepower NGFW

思科 Firepower™ NGFW 符合上述檢查清單所列出的條件。實際上，這是唯一完全整合、聚焦於威脅，且可在整個攻擊過程（攻擊之前、期間和之後）中讓組織處於更安全的環境、更快速減輕進階威脅以及更有效簡化作業的 NGFW（請見圖 1）。

圖 1. 貫穿整個攻擊過程的整合威脅防禦



思科 Firepower NGFW 是專門針對威脅和進階惡意軟體防護的新紀元所設計，能為所有規模的組織提供前所未有的可視性和即時威脅防護。思科 Firepower NGFW 囊括了在同類型產品中表現獨占鰲頭的各種設備，具備以下特色：

- **完全整合**：從網路到端點，任何端點可能存在的地方皆提供防火牆整合可視性與政策管理、應用程式控制、威脅預防和進階惡意軟體防護功能。
- **聚焦於威脅**：提供全方位網路可視性、優異的威脅情報及威脅預防功能，可解決已知與未知威脅。其可追溯的安全技術可協助您快速回應成功的攻擊。[4]

思科 Firepower NGFW：單一平台中的多層式威脅防禦

如圖 2 所示，思科 Firepower NGFW 可在一個平台上提供以下功能：

- **絕佳多層式威脅防護**可抵禦已知與未知威脅，包括針對性和持續性惡意軟體攻擊在內。思科 Firepower NGFW 中包含全世界部署最廣泛的可設定狀態防火牆技術。此外，也提供新世代 Intrusion Prevention System (IPS)、進階惡意軟體防護、應用程式可視性與控制，以及基於信譽的 URL 篩選功能搭配應用程式層 VPN，全部皆涵蓋在單一設備上的單一解決方案中。另外也和內嵌在網路中的其他思科解決方案整合，可自動化網路分段以快速遏止威脅。
- **思科®進階惡意軟體防護** (AMP) 提供領先業界的入侵偵測有效性、低總持有成本和絕佳的保護價值，並使用巨量資料來偵測、瞭解和封鎖進階惡意軟體疫情。AMP 提供阻止安全層所忽略的威脅所需的可視性及控制。
- **整合管理**可透過思科 Firepower 管理中心進行，這是思科 Firepower NGFW 的神經中樞，管理員可在此管理數以百計的設備。管理中心透過功能多元的主控台，提供基於角色的防火牆政策和組態管理、超過 4000 部設備的存取控制、入侵保護政策以及進階惡意軟體分析。
- **可行的 IoC** 與詳細網路和端點事件資訊相關聯，能為資安團隊提供更深入的惡意軟體感染可視性。NGFW 解決方案也可為所有入侵事件建立關聯，並自動針對目標執行攻擊影響評估。
- **全方位網路可視性與控制**可透過管理中心實現，管理中心會提供前所未有的網路可視性和自動化，讓您可回應有所變動的情況和新攻擊。資安團隊可隨時查看網路上發生的事：使用者、裝置、虛擬機器間的通訊、弱點、威脅、用戶端應用程式、檔案和網站。內容覺察功能可協助資安團隊偵測多重向量威脅，與惡意軟體檔案軌跡結合後，有助於調查感染和判斷根本原因，進而加快修復速度。
- **漫遊使用者未使用公司網路時也可予以保護**。思科 Umbrella Roaming 是藉由雲端提供的資安服務，且可透過思科 AnyConnect® 用戶端納入思科 Firepower NGFW 中。Umbrella Roaming 會於 DNS 層提供保護，讓您可在威脅抵達您的筆記型電腦前先行封鎖。此外，不需要額外代理程式便可隨時隨地強制執行安全性。Umbrella Roaming 能以最簡單方式隨時隨地保護使用者，即使使用者的關閉 VPN 時也一樣。

思科 Firepower NGFW 的整合威脅防禦架構所提供的安全性，比起其各部分加總的安全效果還顯著，這套架構也具備以下功能：

- **可降低成本與複雜度的自動化**：思科 Firepower 管理中心可協助管理員簡化建立威脅關聯、評估威脅影響、自動調整資安政策，以及輕鬆將使用者身分歸類為資安事件的作業程序。管理中心會持續監視網路如何與時更迭，並自動評估威脅以判斷須立即留意的威脅。有了這項深入分析，資安團隊可將回應重心放在修復和調適其網路防禦上。
- **第三方整合**：為改善總持有成本，思科 Firepower NGFW 可流暢且透明地配合第三方資安解決方案，包括弱點管理掃描器、軟體管理及故障申告系統。您可針對所有解決方案一致地共用情報、內容和政策控制項。與思科 OpenSource 功能和 OpenAppID 配合的開放系統、聚焦於應用程式的開放偵測語言，以及可讓 IT 團隊建立、共用和實作應用程式偵測的 Snort® 的處理模組，也可為您帶來效益。

4. NSS Labs 的 NGFW 資安價值圖 (Security Value Map for NGFWs) 與缺口偵測系統 (Breach Detection Systems)；思科在兩份報告中的表現皆獨領風騷。
http://www.cisco.com/web/offers/NSSLabsReportNGFW.html https://info.sourcefre.com/2015NSSBreachDetectionReport-CDC.html?AMPPage

圖 2. 思科 Firepower NGFW

思科 Firepower NGFW：其他購買考量事項

選擇思科 Firepower NGFW 做為您的 NGFW 解決方案時，您即享有許多優勢。

保護投資

我們會依據能滿足特定業務和預算要求的條款提供思科® 財務管理租賃計劃。透過公平市場價值租賃，組織可付費使用非其所屬的設備。您享有視需求升級或更新設備的彈性，不會再發生技術過時情形。

服務與技術支援

思科連續第五年（共計八年）榮獲 J.D. Power 認證技術服務與支援計劃的認可。[5] 適用於思科 Firepower NGFW 的思科服務與支援產品項目如下：

- **思科防火牆移轉服務**，由思科資安工程師與思科資安專業合作夥伴提供，可協助組織順暢移轉至思科 Firepower NGFW。思科會提供專業的指引和支援，協助在移轉過程中維持安全性，並改善程序完整性的準確度。
- **思科遠端管理服務**可藉由持續管理安全網路，協助進一步降低總持有成本。貴組織的 IT 團隊可專注處理其他增值業務優先要務。
- **思科網路最佳化服務**採用智慧分析工具並搭配直覺式圖形介面，提供絕佳的網路效能深入分析。組織可降低網路複雜度、提高營運表現、監視政策合規性、降低風險以及主動偵測和預先阻止潛在的網路中斷情形。
- **思科智慧網路全面關護™服務**可輔助組織減少網路停機和其他重大網路問題。您可享有全年無休的專業技術支援，以及彈性的硬體服務涵蓋範圍與主動式裝置診斷。

如需下載軟體

請前往思科軟體中心下載思科 Firepower 服務軟體。

更多資訊

如需瞭解詳細資訊，請造訪：

- www.cisco.com/go/ngfw 深入瞭解思科 Firepower NGFW 設備
- www.cisco.com/go/asafps 深入瞭解具備 FirePOWER 服務的思科 ASA
- www.cisco.com/go/services/security 深入瞭解思科防火牆移轉服務
- www.cisco.com/go/smartnet 深入瞭解思科智能網路支援服務
- www.ciscocapital.com 取得其他資訊及當地思科租賃部門代表的連結

5. 〈思科連續第五年及總計八年榮獲認證技術服務與支援計劃的卓越表現備受肯定〉J.D. Power 新聞稿，2014 年 7 月 21 日：http://www.jdpower.com/press-releases/certifed-technology-service-and-support-program。

C11-737476-00 06/16