



FORCEPOINT次世代防火牆 (NGFW)

串聯整個企業網路並保護員工及其資料



Protecting the human point.

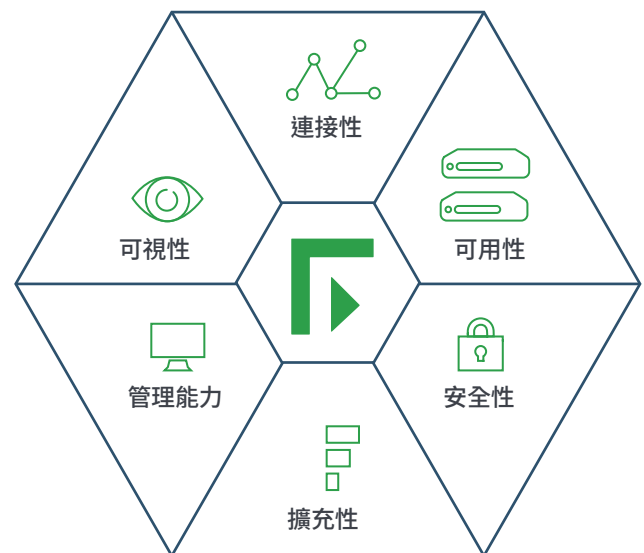


Forcepoint NGFW

是最安全有效可中央管理的企業防火牆，保持運作，永不中斷

Forcepoint次世代防火牆以極致的效能、可用性與安全性保護整個企業網路的員工與資料。受到世界上數以千計客戶信賴，Forcepoint網路安全解決方案讓企業、政府機構與其他組織以有效且經濟的方式解決關鍵的問題。

Forcepoint的網路安全解決方案可無縫地進行集中管理，不論是實體機、虛擬機或在雲端。管理者透過中央管理介面在分秒內即可部署、監控與更新數以千計的防火牆、VPN、IPS，網路維運費用大幅減少50%。進階的防火牆與網路叢集功能可降低停機時間，同時管理者可依據業務需求，快速透過精準的控制措施，在不犧牲效能下阻擋進階攻擊、防止資料竊取並適當管理加密流量。



防火牆與IPS結合

- ▶ 不只是Forcepoint的NGFW在NSS Labs的2017次世代防火牆評比中獲得最高等級的評價，內建的入侵防禦系統(IPS)也同樣獲得最頂級評價。且無須額外的授權或使用另外工具來導入強效的入侵防禦政策。

阻擋資料外洩與竊取

- ▶ Forcepoint在Gartner2017企業防火牆魔術象限中，是在有遠見者(Visionary)象限中具有最高執行能力的，它能提供廣泛的進階存取控制與深入檢查功能以防範導致關鍵資料或智慧財產外洩與竊取的進階威脅。
- ▶ 進階規避技術(Advanced Evasion Techniques, AET)是現今攻擊的常見手法，作為偵測AET的先驅，Forcepoint NGFW能阻斷攻擊者嘗試隱匿惡意程式碼，發現異常並防禦網路中的漏洞攻擊。



獲NSS Labs
2016次世代IPS
「推薦」評等



獲NSS Labs
2017次世代
防火牆「推薦」
評等最高分

「我們看見了把路由器與進階防火牆功能結合在一起的機會，可以加強每個據點的安全還能增加網路頻寬。我們需要一個有中央控管的解決方案，在我們每次新增一個行動業務據點的時候可以直接複製，這樣可以減少我們IT同仁的管理負擔。」

— Carglass資訊技術部總監Christophe Hazeman



絕佳的維運效率能減輕您總持有成本負擔

Forcepoint NGFW是專門設計來降低網路管理複雜度以及所需時間，並且讓網路維持運作平順且安全。分析師指出80%的IT總持有成本(TCO)是在購買之後發生¹，網路維運團隊需要花費大量時間去部署新的防火牆、監控網路活動、更新政策、軟體升級以及事件回應。

Forcepoint NGFW是以統一的軟體核心所建造，能提供一致性的功能、加速且對所有的部署模式都能集中管理。Forcepoint NGFW安全管理中心(Security Management Center, SMC)能同時配置、監控並且管理多達2,000台NGFW設備---不論實體機、虛擬機或在雲端，都能透過單一中央管理介面完成。

70%

防火牆部署時間
加快²

53%

IT人員花費時間
減少²

73%

事件回應時間
加快²

零接觸部署

為遠端辦公室或分支機構據點部署Forcepoint NGFW，不需工程師到現場安裝，可節省時間與成本。設備能從Forcepoint的安裝雲(Installation Cloud)自動下載初次配置設定值，減少手動安裝的需要。

智慧政策，一鍵升級

Forcepoint智慧政策(Smart Policies)以熟悉的用語來顯示企業營運流程，如使用者、應用程式、位置等名稱。更可透過變數功能取代固定的IP或連接埠等設定值，使政策在網路中被快速動態套用。管理者只要點擊一下，就能快速地更新並發布政策到全球所有受影響的防火牆上。

更快速地回應事件

Forcepoint SMC能輕鬆地提供視覺化並分析網路中正在發生的事，網路管理者可以根據回應的資料繼續往下探究，以快速調查網路行為模式與異常，並將調查結果轉為可立即採取的行動。

Forcepoint NGFW是專為降低總持有成本(TCO)而設計

- 
- ▶ 硬體
 - ▶ 訂閱與授權
 - ▶ 支援

FORCEPOINT如何 降低看不見的成本：

- ▶ 統一的解決方案：實體機、虛擬機、雲端
- ▶ 內建IPS、VPN、NGFW、代理伺服器
- ▶ 零接觸部署
- ▶ 每層級皆有高可用性
- ▶ 用平價寬頻實現SD-WAN控制
- ▶ 中央管理，一鍵部署
- ▶ 可升級的軟體
- ▶ 重複使用的硬體
- ▶ 依應用程式與版本控制存取



穩定的高可用性可大幅降低網路停機時間

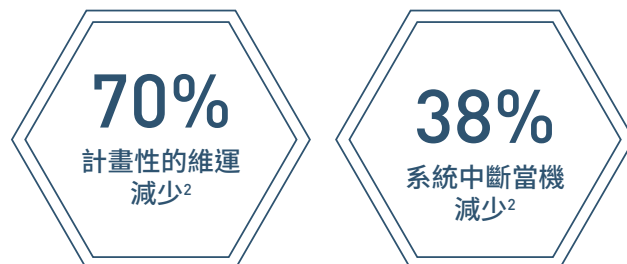
Forcepoint NGFW以永不停機為設計理念，即使遇到任何不可預期的問題也能維持運作。因此高可用性的功能（指處理機器離線或線路斷線的能力）被內建在每種層級：包含防火牆設備、網路連線與管理平台。Forcepoint NGFW能夠降低停機時間以提升您營運持續性並維持營運順暢。

能讓運作不中斷的進階防火牆叢集技術

以群組（包含非成對，例如3台防火牆）方式一起部署Forcepoint NGFW作為叢集式防火牆，即使單一設備發生服務中斷依然能讓網路維持運作，甚至能混合不同型號以延長現有設備的使用壽命。

零停機時間的更新與軟體升級

透過Forcepoint NGFW，毋須離線更新防火牆安全政策，不需中斷連線就能快速回應安全事件，並且無縫更新設備軟體——不需另外計畫服務中斷時間或丟棄任何封包。



支援多ISP與安全加密SD-WAN叢集

Forcepoint是能將不同網路鏈結叢集一起的先驅廠商之一，Multi-Link VPN技術能輕鬆地同時混合商用的寬頻連線與專線來減少單點失效的問題、降低網路成本、增進效能並改善服務品質。

彈性管理能力

Forcepoint NGFW安全管理中心(Security Management Center, SMC)能讓您使用多台伺服器來持續管理你的網路並進行事件調查，即使主要伺服器已離線。

「我們維運的是一個有極高吞吐量的大型網路環境，所以效能是我們對新防火牆解決方案最主要的考量。Forcepoint NGFW是理想的選擇，因為它整合最先進的安全功能以及強大穩固的性能。」

— Cegedim公司網路架構師

Forcepoint NGFW在NSS Labs 2017次世代防火牆安全性評比 中排名第一

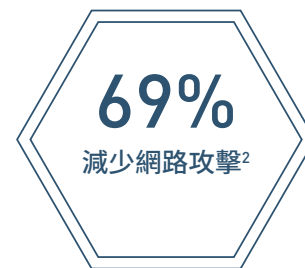
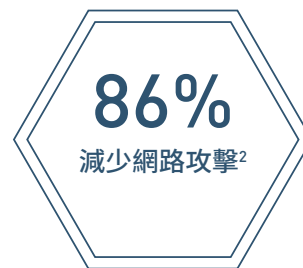
無與倫比的安全性，減少 的是盜竊而非效能

Forcepoint NGFW在NSS Labs 2017次世代防火牆安全性評比中排名第一。它內建廣泛的安全功能（包括VPN、IPS、NGFW與安全代理伺服器），讓你免於在不同產品之間周旋、苦惱軟體授權或在忙於管理各類設備，甚至可以為安全設備重新規劃不同的角色，以延長你基礎設備的使用壽命。

透過Forcepoint安全管理中心(SMC)，你可以針對每個連線運用不同種類的安全技術，例如依應用程式類別、依組織、依位置或依其他不同條件，完全不需要犧牲網路效能。

兼顧隱私下對加密流量的控制

透過Forcepoint NGFW，可無痛處理對內或對外日益增多的加密傳輸流量。使用加速解密功能，可檢查HTTPS與其他SSL/TLS通訊協定來拒絕或允許特定HTTP指令或在HTTPS中的URL區段——即使是部署在虛擬化或雲端的环境。Forcepoint NGFW的SSH安全代理伺服器功能提供對於



關鍵應用程式進階控制能力，此外透過智慧政策功能可輕鬆遵循隱私法規與內部實務，避免當使用者與銀行、壽險公司或其他機敏單位溝通時洩露個人資料。

沙箱與進階惡意程式偵測

對網路流量中的檔案，Forcepoint NGFW採用多種掃描技術包括信譽審查、內建的反惡意程式掃描並使用Forcepoint進階惡意程式偵測(Advanced Malware Detection)服務。此一強大的雲端系統使用業界領先的沙箱與其他進階技術來分析檔案行為、發掘並攔阻惡意程式碼，企業組織可彈性選擇雲端或本地版本以滿足維運需求。



強固的防護以避免入侵

Forcepoint是抵禦進階規避技術(Advanced Evasion Techniques, AET)的先驅,我們完整通訊協定正規化(full protocol normalization)技術能阻擋攻擊者嘗試隱匿惡意程式碼、發現異常並防止對網路發動漏洞攻擊。

保護關鍵應用程式

Forcepoint NGFW能對使用加密HTTPS連線的關鍵應用程式提供流量完整檢查的代理伺服器保護技術,這項技術來自於我們Sidewinder防火牆,Sidewinder防火牆受到全球許多最機敏的網路用戶的依賴,它進一步擴展了我們獨特的代理伺服器功能,讓管理者有能力控制HTTPS流量,可允許或阻擋特定URL或HTTPS請求的種類。

整合URL過濾—更為鞏固的安全

Forcepoint NGFW提供一種快速、彈性的方式來執行網頁存取政策,以符合規範並阻擋存取釣魚網站以及惡意或不受歡迎的內容。Forcepoint全球智能網路威脅情資服務(Threat Seeker Intelligence Cloud)提供了廣泛的、不斷更新的且能在網頁存取政策中直接使用的URL分類,對於使用者的網站存取行為提供動態的控制。

業務轉型—將企業應用程式移轉上雲端

Forcepoint NGFW為在AWS或Azure雲端上執行的工作提供防護。透過現有SMC系統進行管理時,可從雲端市集上直接部署Forcepoint NGFW。這將有助於企業組織使用與內部資料中心、辦公室、分店、分支機構和其他雲端環境相同的業界領先的安全與連線功能,來保護他們在雲端的應用程式與其他工作。

端點白名單與黑名單應用程式控制

Endpoint Context Agent提供執行在本機與使用者裝置上應用程式的白名單與黑名單機制,例如它能让管理者指定哪些瀏覽器或版本可以連結網際網路。可依據企業組織的業務需求和安全狀態提供更加精細化的控制。

Forcepoint—提供最直接的企業價值

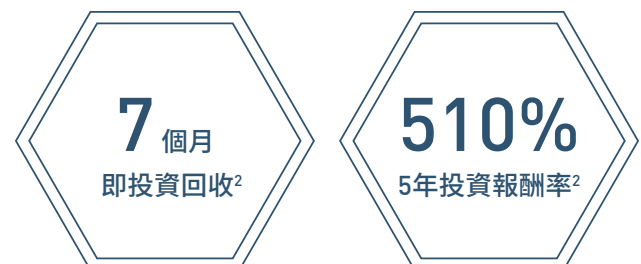
Forcepoint對於防護企業安全採取一種新的方式:Stop the bad,Free the good。Forcepoint NGFW是屢獲殊榮的次世代防火牆,能阻擋惡意攻擊並在基礎架構轉型時避免資料與智慧財產遭竊且增加維運效率。

提高企業生產力 – Forcepoint NGFW網路安全解決方案專為需要連線不中斷的企業而設計,可以讓分散各地的員工安全存取重要資料以協助企業創新。

降低總持有成本(TCO)負擔 – Forcepoint NGFW獨特的高可用性架構、多功能平台與自動化中央管理功能,可降低維運成本、延長使用壽命並且較不需要特別進行訓練或特殊專長。

降低IT風險 – Forcepoint NGFW能在潛在威脅、資料外洩與盜竊演變成財務損失之前將其阻擋下。

簡化法規遵循 – Forcepoint NGFW能兼顧業務需求與安全控制,讓你快速回應事件並修復缺失,以符合重要的法規遵循與稽核要求。



參考資料

¹ Gartner

² Forcepoint NGFW Business Value Snapshot,
IDC Research, March 2017.



「Forcepoint滿足了我們受託客戶所有的需求，包括安全、法規遵循與成本。它有彈性、非常安全，而且可以任意擴充，沒有其他防火牆能將安全做到這麼好。」

— Netprotocol資深安全顧問



關於FORCEPOINT

Forcepoint顛覆傳統的資安思維，透過瞭解人們的意圖，來保護企業的使用者及資料安全，尤其當他們在存取營業秘密或智慧財產的時候，無論資料位於何處皆可受到保護。我們安全穩固的系統使企業能夠充分保護使用者的安全，讓員工可以安全無虞地存取機密資料，同時保護企業的智慧財產安全，以及簡化法規遵循的程序。Forcepoint總部位於美國德州奧斯丁，Forcepoint服務全球超過2萬個組織。更多Forcepoint訊息，請上網查詢 www.Forcepoint.com 或在Twitter 關注我們@ForcepointSec。

聯絡方式

886-8758-2970 fkuo@forcepoint.com

www.forcepoint.com/contact

©2017 Forcepoint。Forcepoint與FORCEPOINT都是Forcepoint的商標。Raytheon是Raytheon公司的註冊商標，此份文件所使用的所有其他商標是各別持有人的財產。

[BROCHURE_NGFW_OVERVIEW_ENUS] 400013.101017