PA-5450

Palo Alto Networks PA-5450 機器學習式新世代防火牆 (NGFW) 平台是專為超大規模數據中心、網際網路邊緣與園區區隔部署所設計。它可提供 120 Gbps 的絕佳效能，啟用安全服務，以可擴充、模組化設計為基礎，可隨著您的需求增加同步提升效能。採用單一系統做法進行管理和授權的 PA-5450 能夠提供簡易性。

重點

- 全球第一個基於機器學習的新世代防火牆
- 九度獲選 Gartner 魔力象限® 網路防火牆領導者
- Forrester Wave™：2020 年第三季度企業防火牆領導者
- 2019 NSS 實驗室新世代防火牆測試報告中取得最高的安全效用評分，100% 封鎖迴避
- 在統一及可擴充架構中運作
- 提供內建的 5G 原生安全性以保護服務供應商和企業 5G 轉型與多存取邊緣運算 (MEC)
- 將可視性和安全性延伸至包括未受管理 IoT 裝置在內的所有裝置，且不需要部署額外的感應器。
- 支援主動/主動和主動/被動模式的高可用性
- 藉由安全服務提供可預測的效能

PA-5450

全球第一個機器學習式新世代防火牆能夠透過自動政策建議來防止未知威脅、查看和保護包括物聯網 (IoT) 在內的一切內容，並減少錯誤。PA-5450 的控制元件是 PAN-OS®，這也是執行所有 Palo Alto Networks 新世代防火牆的相同軟體。PAN-OS 能夠在本機將包括應用程式、威脅和內容在內的所有流量分類，並且使該流量與任何地點或裝置類型的使用者相關聯。應用程式、內容與使用者 (即企業營運中的元件) 會成為安全性政策的基礎，藉以改進安全狀況並縮短事件回應時間。

關鍵安全性和連線功能

機器學習式新世代防火牆

- 在防火牆的核心中嵌入機器學習 (ML)，為檔案型攻擊提供內嵌的無特徵碼攻擊防禦，同時識別並立即阻止前所未見的網路釣魚嘗試。
- 運用雲端式 ML 程序，將零延遲特徵碼和指令推送回新世代防火牆。
- 使用行為分析來偵測 IoT 裝置並提出政策建議，構成新世代防火牆上的雲端交付和原生整合服務。
- 自動化政策建議可以節省時間並降低人為錯誤發生的機率。
- 藉由全面的第 7 層檢查，始終可以對所有連接埠上的所有應用程式進行識別和分類

識別周遊網路的應用程式，完全不考慮連接埠、通訊協定、迴避技術或加密 (TLS/SSL)

- 使用應用程式 (而非連接埠) 作為所有安全啟用政策決策的基礎，包括允許、拒絕、排程、檢驗及套用流量調整等政策。
- 能夠為專有應用程式建立自訂 App-ID™ 標籤，或要求 Palo Alto Networks 對於新應用程式進行 App-ID 開發。
- 識別應用程式中的所有承載數據 (例如檔案和數據模式)，藉以阻止惡意檔案並遏止外洩嘗試。
- 建立標準和自訂的應用程式使用狀況報告，包括對於網路上獲批准和未獲批准的所有軟體即服務 (SaaS) 流量提供見解的 SaaS 報告。
- 藉由內建的 Policy Optimizer，可以將舊型第 4 層規則集安全移轉到以 App-ID 為基礎的規則，以便為您提供更安全、更容易管理的規則集。

對於在任何位置操作任何裝置的使用者強制實施安全性，同時根據使用者活動調整政策

- 依據使用者和群組 (而不僅依據 IP 位址) 啟用可視性、安全政策、報告和鑑識。
- 輕鬆整合多種儲存庫來運用使用者資訊：無線 LAN 控制器、VPN、目錄伺服器、SIEM、Proxy 等等。
- 可讓您在防火牆中定義動態使用者群組 (DUG)，藉以採取有時限的安全動作，完全不需要等待變更套用於使用者目錄。
- 無論使用者處於什麼位置 (辦公室、家中、差旅等等) 以及使用何種裝置 (iOS 和 Android® 行動裝置、macOS®、Windows®、Linux 桌上型電腦、筆記型電腦；Citrix 和 Microsoft VDI 和終端機伺服器)，都套用一致的政策。
- 透過在網路層為任何應用程式啟用多因素驗證 (MFA)，完全不需要對應用程式進行任何變更，就可以防止公司憑證洩露到第三方網站，並防止重複使用遭竊的憑證。
- 根據使用者行為提供動態安全動作，藉以限制可疑使用者或惡意使用者。

防止在加密流量中隱藏的惡意活動

- 檢查政策並套用於 TLS/SSL 加密的傳入和傳出流量，包括使用 TLS 1.3 和 HTTP/2 的流量。
- 完全不需要解密即可提供對 TLS 流量 (例如，加密流量、TLS/SSL 版本、加密套件等等) 的多樣化可視性。
- 能夠控制對於舊版 TLS 通訊協定、不安全密碼和錯誤設定證書的使用，藉以減輕風險。
- 便於解密的輕鬆部署，並且可讓您使用內建日誌來解決問題，例如有固定證書的應用程式。
- 可讓您按照 URL 類別、來源和目的地區域、位址、使用者、使用者群組、裝置和連接埠，彈性啟用或停用解密，藉以達成隱私權與合規性目的。
- 可讓您從防火牆建立解密流量的副本 (亦即解密鏡像)，並傳送到流量收集工具進行鑑識、用於歷史用途或用於數據遺失防護 (DLP)。

提供集中管理和可視性

- 透過統一使用者介面中的 Panorama™ 網路安全管理，可藉由多個分散式 Palo Alto Networks 新世代防火牆 (無論地點或規模為何) 的集中管理、設定和可視性取得優勢。
- 透過 Panorama 以及範本和裝置群組簡化設定共用，並可隨著記錄需求的增加擴充日誌收集。
- 此外，使用者可透過應用程式控管中心 (ACC) 取得與網路流量和威脅有關的深入可視性和全面性的見解。

偵測和預防進階威脅

現今的網路攻擊者無論在數量和複雜程度上都已大幅提升，可在 30 分鐘內使用多個威脅途徑或進階技術擴充至 45,000 個變體，在

您的企業中產生大量的惡意承載。傳統的孤立安全解決方案已經無法有效地保護企業的使用者、裝置和應用程式，因此對這些企業形成艱鉅的挑戰。它們不僅會形成安全漏洞並增加安全團隊的管理負擔，也會因為不一致的存取和可視性妨礙企業生產力。我們的雲端交付安全服務能夠與業界領先的新世代防火牆平台進行無縫整合，此外還可利用 80,000 名客戶的網路效益以即時協調情報並針對所有的攻擊途徑提供防範措施。它可消除所有企業位置中的涵蓋範圍落差並充分利用平台中一致交付的同級最佳安全性，因此即使在面對最先進的迴避式威脅時仍可保護自身安全。

- **Threat Prevention** — 超越傳統的入侵防禦系統 (IPS)，可針對單一通道的所有流量防禦所有已知的威脅，且無需犧牲任何效能。
- **進階 URL Filtering** — 提供同級最佳的網路防護，並透過業界首部即時網路防護引擎和業界領先的網路釣魚防護達到最大的營運效率。
- **WildFire®** — 透過業界領先的雲端式分析以及超過 42,000 名客戶提供的群眾外包情報，將可自動偵測及防禦未知的惡意軟體以確保檔案安全無虞。
- **DNS Security** — 利用機器學習功能以即時偵測及預防透過 DNS 造成的威脅，讓安全人員掌握情報及脈絡來擬定政策，並快速且有效地回應威脅。
- **IoT Security** — 提供業界最全面的 IoT Security 解決方案，透過單一平台提供機器學習式可視性、防禦和執行。
- **企業 DLP** — 提供業界首部雲端交付的企業 DLP，可持續保護網路、雲端和使用者之間的敏感數據。
- **SaaS 安全性** — 提供整合式 SaaS 安全性，使您能夠以最低的總體擁有成本 (TCO) 監控及保全新的 SaaS 應用程式、保護數據並防範零時差威脅。

啟用 SD-WAN 功能

- 只要在現有的防火牆上啟用 SD-WAN，就可以讓您輕鬆地加以採用。
- 可讓您安全地實作 SD-WAN，其與我們業界領先的安全產品進行原生整合。
- 將延遲、抖動和封包遺失降至最低，從而提供絕佳的終端使用者體驗。

提供藉由單通道架構進行封包處理的獨特方法

- 在單通道中執行網路連線、政策查詢、應用程式和解碼以及特徵碼比對 (針對所有威脅和內容)。這能夠顯著減少在一台安全裝置中執行多種功能所需的處理開銷。
- 使用基於串流的統一特徵碼比對，在單通道中掃描所有特徵碼的流量，藉以避免導致延遲。
- 啟用安全訂閱後，可達到一致且可預測的效能。(在表 1 中，「Threat Prevention 輸送量」是在啟用多個訂閱情況下所測量的結果。)PA-5450 架構

PA-5450 架構

PA-5450 採用可擴充架構，能夠應用適當類型及規模的處理能力，進行網路連線、安全及管理等關鍵功能作業。該裝置是一套統一管理的系統，可讓您輕鬆引導所有可用資源，以保護您的數據。PA-5450 將處理需求巧妙地分散到三個子系統上，每個子系統都具備大量的運算能力和專用記憶體：網路卡 (NC)、數據處理卡 (DPC) 和管理處理卡 (MPC)。

PA-5450 提供總共 6 個適用於 NC 和 DPC 的插槽。

表 1：PA-5450 效能與功能

	PA-5450 已設定系統*	單一 PA-5400-DPC-A
防火牆輸送量 (HTTP/appmix)***	200/200 Gbps	72/68 Gbps
Threat Prevention 輸送量 (HTTP/appmix)†	125/150 Gbps	31/37 Gbps
IPsec VPN 輸送量‡	95 Gbps**	19 Gbps
最大工作階段數量	100M	20M
每秒新工作階段數量§	4M	830000
虛擬系統 (基礎/最大)‖	25/225	—

* 除非另有說明，所有測試都是使用已插入的 2 個網路卡 + 4 個數據處理卡所執行
** 此測試是使用已插入的 1 個網路卡 + 5 個數據處理卡所執行
*** 啟用 App-ID 和記錄，以 64 KB HTTP/appmix 交易來測量防火牆輸送量。
† 啟用 App-ID、IPS、防毒軟體、反間諜軟體、WildFire、檔案封鎖和記錄，以 64 KB HTTP/appmix 交易來測量 Threat Prevention 輸送量。
‡ 啟用記錄功能，以 64 KB HTTP 交易來測量 IPSec VPN 輸送量。
§ 使用應用程式覆蓋，以 1 位元組 HTTP 交易來測量每秒新工作階段數量。
‖ 在基礎數量上新增虛擬系統需要額外購買授權。

網路卡

為了實現網路連線，PA-5450 至少需要一個 NC (PA-5400-NC-A)。第二個 NC 需要至少兩個安裝在系統中的 DPC。最多可安裝兩個 NC。NC 專門用於執行中的封包傳入與傳出任務。

每個 PA-5400-NC-A 都可提供多個連接埠，如表 3 所示：100/1000/10G Cu (4)、1G/10G SFP/SFP+ (12) 和 40G/100G QSFP28 (2)。

數據處理卡

針對封包和安全處理，PA-5450 可使用 DPC (PA-5400-DPC-A)，最少一個 DPC，最多 5 個 DPC，可以置於所提供的六個插槽中。

管理處理卡

MPC 子系統 (PAN-PA-5400-MPC-A) 是專屬接觸點，可控制 PA-5450 的所有層面。

表 2：PA-5450 網路功能
介面模式
L2、L3、旁接、虛擬線路 (透通模式)
路由
具備非失誤性重新啟動功能的 OSPFv2/v3 與 BGP、RIP、靜態路由
基於政策的轉送
動態位址指派支援乙太網路點對點通訊協定 (PPPoE) 和 DHCP
多點傳送：PIM-SM，PIM-SSM，IGMP v1、v2 與 v3
雙向轉送偵測 (BFD)
SD-WAN
路徑品質測量 (抖動、封包遺失、延遲)
初始路徑選取 (PBF)
動態路徑變更
IPv6
L2、L3、旁接、虛擬線路 (透通模式)
功能：App-ID、User-ID、Content-ID、WildFire 與 SSL 解密
SLAAC
IPsec VPN
金鑰交換：手動金鑰、IKEv1 及 IKEv (預先共用金鑰、證書式驗證)
加密：3DES、AES (128 位元、192 位元、256 位元)
驗證：MD5、SHA-1、SHA-256、SHA-384、SHA-512
用於簡化設定和管理的 GlobalProtect 大規模 VPN

表 2：PA-5450 網路功能 (續)
VLAN
每個裝置/介面的 802.1Q VLAN 標籤數量：4,094/4,094
彙總介面 (802.3ad)、LACP
網路位址轉譯
NAT 模式 (IPv4)：靜態 IP、動態 IP、動態 IP 和連接埠 (連接埠位址轉譯)
NAT64、NPTv6
其他 NAT 功能：動態 IP 保留、可調整的動態 IP 及連接埠超額訂閱
高可用性
模式：主動/主動、主動/被動、高可用性叢集
故障偵測：路徑監控、介面監控
行動網路基礎結構*
GTP 安全
SCTP 安全

*如需詳細資訊，請參閱適用於 5G 的機器學習式新世代防火牆型錄。

表 3：PA-5450 硬體規格
PA-5400-NC-A 網路 I/O
100/1000/10G Cu (4)、1G/10G SFP/ SFP+ (12)、40G/100G QSFP28 (2)；每個系統最少 1 個 NC，最多 2 個 NC；2 個 NC 需要至少安裝 2 個 DPC
PAN-PA-5400-MPC-A 管理 I/O
10/100/1000 (2)、40G/100G QSFP28 高可用性 (2)、10/100/1000 頻外管理 (2)、RJ45 主控台連接埠 (1)、USB 主控台連接埠 (1)
儲存容量
480 GB SSD、RAID1、系統儲存 4 TB SSD，日誌儲存 (選用)
最高 BTU/小時
8828
電源 (基礎/最大)
2/4
交流輸入電壓 (輸入頻率)
100–120 VAC 與 200–240 VAC (50–60 Hz)
交流電源輸出
2,200 瓦/電源
最大電流消耗
交流：100–120 VAC，每個輸入最多大約 14 A；200–240 VAC 每個輸入最多大約 12.5 A
直流：48–60 VDC，每個輸入最多 52 A

表 3：PA-5450 硬體規格 (續)
最大湧入電流
交流：35 A @ 230 VAC、35 A @ 120 VAC
直流：50 A @ 72 VDC
安裝機架 (尺寸)
5U，19 英吋標準機架 8.75 x 30.25 x 17.38 英吋 (高 x 深 x 寬)
最大無故障時間 (MTBF)
視設定而定；請聯絡 Palo Alto Networks 代表瞭解 MTBF 詳細資料。
安全性
cTUVus、CB
EMI
FCC Class A、CE Class A、VCCI Class A、KCC Class A、BSMI Class A
認證
請參閱 paloaltonetworks.com/company/certifications.html
環境
作業溫度：32° 至 122° F，0° 至 50° C
非作業溫度：-4 至 158 °F，-20 至 70 °C

若要檢視 PA-5450 的特色及相關功能的其他資訊，請前往 paloaltonetworks.com/network-security/next-generation-firewall/pa-5450。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓