PA-7500

PA-7500

Palo Alto Networks PA-7500 機器學習式新世代防火牆 (NGFW) 可讓具有企業規模的組織與服務供應商在高效能環境中部署安全工具，例如大型數據中心和高頻寬網路周邊。這些系統的設計是為了滿足應用程式、使用者和裝置產生之數據不斷增長的輸送量需求，並提供絕佳效能和防禦功能來抵禦進階的網路攻擊，透過高輸送量解密來阻擋隱匿於加密背後的威脅。PA-7500 旨在將安全處理的資源使用率提升到最高，並在獲得新運算能力時自動擴充，採用單一 UV 做法進行管理和授權，以此來實現簡單易用性。

亮點

- 全球第一個機器學習式新世代防火牆
- 十一度獲選 Gartner 魔力象限網路防火牆領導者
- Forrester Wave：2022 年第四季度企業防火牆領導者
- 在統一及可擴充架構中運作
- 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，而且不需要部署額外的感測器
- 透過叢集解決方案支援高可用性
- 藉由安全服務提供可預測的效能
- 透過 Panorama 網路安全管理支援集中管理
- 運用 AIOps 發揮安全投資的最大效益並防止業務中斷

PA-7500 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，並且讓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 (企業營運中的元件) 會成為安全政策的基礎，藉以改進安全狀況、縮短事件回應時間，並降低目前在高度動態環境中保持安全政策的相關管理開支。

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物聯網 (IoT) 裝置並提出政策建議；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，可以一直對所有連接埠上的全部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 (SSL/TLS)。
- 藉由 SaaS 安全訂閱自動探索及控制新的應用程式以
- 因應 SaaS 激增。
- 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數據外洩嘗試。
- 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且更容易管理的規則集。

參閱 App-ID 技術簡介了解詳細資訊。

對於任何位置的使用者裝置強制實施安全性，同時根據使用者活動來調整政策

- 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。
- 無論使用者處於任何位置 (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 和終端伺服器)，都可套用一致的政策。

- 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，並且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。
- 無論使用者身分實際位於何處，它都能藉由雲端身分引擎 (面向身分式安全的全新雲端式架構) 透過一致的方式驗證和授權使用者，快速朝向零信任安全狀況持續前進。

參閱雲端身分引擎解決方案簡介了解詳細資訊。

防止在加密流量中隱藏的惡意活動

- 檢查政策並套用於 SSL/TLS 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、SSL/TLS 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、裝置和連接埠等，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 (即解密鏡像)，並且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)。
- 可讓您使用網路封包代理以智慧化的方式將所有流量 (解密 TLS、非解密 TLS 和非 TLS) 轉送到第三方安全工具，並且達到最佳的網路效能，並且減少營運費用。

參閱此解密白皮書以了解何時、何地以及如何解密來防禦威脅並保護企業的安全。

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以簡化設定共用，並且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。

運用 AIOps 發揮安全投資的最大效能並且防止業務中斷

- 新世代防火牆的 AIOps 針對您的獨特部署提供客製化持續性最佳實務建議，藉以加強您的安全狀況，並且充分發揮安全投資的效益。
- 依據進階遙測數據支援的機器學習以智慧化的方式預測防火牆健全狀況、效能和容量問題。這也提供可採取行動的見解來解決預測的中斷情況。

透過雲端交付的安全服務偵測和防禦進階威脅

如今網路攻擊的複雜度大幅提升，可在 30 分鐘內使用多個威脅途徑和進階技術擴充 45,000 個變體，在您的企業中產生大量的惡意承載。傳統而孤立的安全措施為企業帶來挑戰，因為這會形成安全漏洞、增加安全團隊的管理負擔，以及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我們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性威脅時仍可保護自身安全。

服務包括：

- **進階威脅防禦：**阻止已知入侵、惡意軟體、間諜軟體和命令與控制 (C2) 威脅，同時利用業界首創的零時差攻擊防禦措施，相較於傳統 IPS 解決方案，可以多阻止 60% 的未知植入攻擊和 48% 的高迴避性命令與控制流量。
- **Advanced WildFire®：**透過業界最大的威脅情報和惡意軟體防禦引擎，以快 60 倍的速度自動防禦已知、未知和高迴避性惡意軟體以確保檔案安全無虞。
- **進階 URL Filtering：**透過業界首創已知和未知威脅即時防禦解決方案確保網際網路的安全存取，並且多阻止 40% 的 Web 型攻擊，能夠比其他廠商至少提前 48 小時阻止 88% 的惡意 URL。
- **DNS Security：**威脅的涵蓋範圍提高 40% 並阻止 85% 濫用 DNS 進行命令與控制或數據竊取的惡意軟體，而不需要變更基礎結構。
- **企業 DLP：**將數據洩露風險降到最低、阻止違反政策的數據傳輸並在您的企業中啟用一致的合規性，此外還能為任何雲端交付的企業 DLP 提供 2 倍大的涵蓋範圍。
- **SaaS 安全：**透過業界唯一的新世代 CASB 以自動查看並保護所有通訊協定的任何應用程式，藉以因應不斷激增的 SaaS。
- **IoT Security：**透過業界最聰明的智慧裝置安全，以快 20 倍的速度保護每個「物件」並實作零信任裝置安全。

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-7500 架構

PA-7500 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。

PA-7500 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-7500 機箱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：網路處理卡 (PA-7500-NPC-A)、數據處理卡 (PA-7500-DPC-A) 和管理處理卡 (PA-7500-MPC-A)。PA-7500 提供九個插槽來安裝這些處理卡，每種卡片至少需要有一張以符合最低設定要求。此外，其後方還安裝一個或兩個具有選擇性備援的交換結構卡 (PAN-PA-7500-SFC-A)，以用於正交匹配。

表 1：PA-7500 Series 效能與功能

	PA-7500-DPC-A	PA-7500*
防火牆輸送量 (appmix)†	310 Gbps	1,500 Gbps
Threat Prevention 輸送量 (appmix)‡	250 Gbps	1,440 Gbps
並行工作階段數上限§	73M	440M
IPsec VPN 輸送量‖	67 Gbps	407 Gbps
每秒新工作階段數量#	1.2M	7.2M
虛擬系統 (基礎/最大)**	—	25/225

注意：在 PAN-OS 11.1 上測量結果。

* 本列的結果源自於使用六張 PA-7500-DPC-A 卡和兩張 PA-7500-NPC-A 卡的設定。

† 啟用 App-ID 和記錄，以 appmix 交易測量防火牆輸送量。

‡ 啟用 App-ID、IPS、防毒軟體、反間諜軟體、WildFire、DNS 安全性、檔案封鎖和記錄，以 appmix 交易來測量 Threat Prevention 輸送量。

§ 並行工作階段數上限是利用 HTTP 交易所測得。

‖ 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。

表 2：PA-7500 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
以政策為基礎的轉送
動態位址指派支援 DHCP
多點傳送：PIM-SM，PIM-SSM，IGMP v1、v2 與 v3
雙向轉送偵測 (BFD)
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 和 SSL VPN
金鑰交換：手動金鑰、IKEv1 及 IKEv2 (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*
使用 GlobalProtect 閘道與入口網站，透過 IPsec 和 SSL VPN 通道進行安全存取*
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) 卡內和/或卡間，以及 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
新世代防火牆叢集

* 需要 GlobalProtect 授權。

表 3：PA-7500 Series 硬體規格
I/O (各 PA-7500-NPC-A)
QSFP-DD (8)—支援 400 Gbps/100 Gbps/40 Gbps，以及支援分向複製模式的硬體 SFP-DD (12)—100 Gbps/25 Gbps/10 Gbps 連接埠
管理 I/O (各 PA-7500-MPC-A)
QSFP28 記錄連接埠 (2)—100 Gbps/40 Gbps QSFP-DD 高可用性連接埠 (2)—400 Gbps/100 Gbps SFP28 管理連接埠 (2)，支援 1 Gbps/10 Gbps/25 Gbps 組合 RJ-45 主控台連接埠 (1)、Micro USB 主控台連接埠 (1)、USB (1)
信賴平台模組 (TPM)
與 TPM 的整合可進行安全開機、提供硬體信任根並保護系統密碼。

表 3：PA-7500 Series 硬體規格 (續)
BTU
設定：SFC (2)、NPC (2)、DPC (6)、MPC (1) 最大 BTU 31142 (總功率 — 風扇功率以 BTU 為單位)
電源 (閒置/一般/最大耗電量)
設定：SFC (2)、NPC (2)、DPC (6)、MPC (1) 6.3 KW/8.2 KW/10 KW @ 25C @ 海平面 7.3 KW/9.2 KW/11.5 KW @ 40C @ 海拔高度 2000 英呎
電源 (基礎/最大)
N+M 備援 (最多 10 個可負載共用的電源供應器)
交流輸入電壓
100–240 VAC (50-60 Hz)
交流電源額定輸入電流
20 A
交流電源輸出
每個電源供應器 3600 @ 高線 (180V、200/240V、305V) 每個電源供應器 1800 @ 低線 (90V、110/120V、132V)
直流輸入電壓
-48V 直流電源
直流電源額定輸入電流
83A @ -48 V 直流電源
直流電源輸出
3600 W/電源
最大電流/電源
20A 交流電源、83 A 直流電源
機架安裝尺寸
14U 24.4 x 31.0 x 17.4 英吋 (高 x 深 x 寬)
安全性
cMETus、CB、噪音等級符合 NEBS
EMI
FCC Class A、CE Class A、VCCI Class A
認證
請參閱 paloaltonetworks.com/company/certifications.html。
環境
作業溫度：32°F 至 104°F，0°C 至 40°C 濕度容限：5% 至 90% 無凝露 氣流：前進後出

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 6F-1

strata_ds_pa-7500_032725