paloalto NETWORKS | STRATA™

PA-3410

PA-3420

PA-3430

PA-3440

PA-3400 Series

Palo Alto Networks PA-3400 Series 機器學習式新世代防火牆包括 PA-3440、PA-3430、PA-3420 和 PA-3410，所有的防火牆均專為高速網際網路閘道部署所設計。PA-3400 Series 設備可以保護所有流量。

亮點

- 全球第一個機器學習式新世代防火牆
- 十一度獲評選 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
- 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應器
- 新世代防火牆的原生網路 Proxy 支援可簡化和整合防火牆和 Proxy 功能的管理
- 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
- 透過 Panorama 網路安全管理支援集中管理
- 運用 Strata™ Cloud Manager 發揮安全投資的最大效益並防止業務中斷

全球第一個機器學習式新世代防火牆 (NGFW) 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-3400 Series 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 (即企業營運中的元件) 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；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 (TLS/SSL)。此外，這也會藉由 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 和 Linux 桌上型電腦和筆記型電腦、Citrix 和 Microsoft VDI，以及終端伺服器)，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 (面向身分式安全性的全新雲端式架構) 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 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憑證的使用，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，例如有固定憑證的應用程式。
- 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 (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)。
- 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。

透過 Strata Cloud Manager 提供 AI 支援的統一管理和營運

- **預防網路中斷**：預測部署健全狀況，並透過預測分析提前七天主動識別容量瓶頸，以主動防止營運中斷。
- **即時加強安全性**：針對業界和 Palo Alto Networks 最佳實務進行 AI 支援的政策分析以及即時合規性檢查。
- **達到簡單且一致的網路安全管理和營運**：跨所有規格來管理設定和安全政策，這些規格包括 SASE、硬體和軟體防火牆以及所有安全服務，以確保一致性並減少營運開支。

透過雲端交付的安全服務偵測和防禦進階威脅

使用孤立安全工具的傳統方法會為企業帶來挑戰，包括安全漏洞、安全團隊的負擔增加，以及企業生產力中斷。而我們的雲端交付安全服務能與我們領先業界的新世代防火牆平台進行無縫整合，可在 65,000 名客戶間共享威脅情報以即時防範所有威脅途徑中的已知及未知威脅。消除整個網路的安全漏洞，並利用內嵌 AI 支援的安全服務，隨處提供即時保護。

服務包括：

- **進階威脅防禦**：透過內嵌的 AI 支援偵測來阻止已知和未知漏洞，以及命令與控制 (C2) 攻擊，而且相較於傳統 IPS 解決方案，其可多阻止 60% 的零時差植入攻擊和 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，以比競爭對手快出 180 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的安全無虞。
- **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% 的惡意網站。
- **DNS Security**：威脅的涵蓋範圍提高 68% 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 安全性**：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性，以快出 20 倍的速度保護每個「物件」並實作零信任裝置安全性。

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。)

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，進而提供絕佳的使用者體驗。

表 1：PA-3400 Series 效能與功能				
	PA-3410	PA-3420	PA-3430	PA-3440
防火牆輸送量 (appmix)*	14 Gbps	19 Gbps	29 Gbps	35 Gbps
Threat Prevention 輸送量 (appmix)†	7.5 Gbps	10 Gbps	15 Gbps	20 Gbps
IPsec VPN 輸送量‡	6.6 Gbps	9.9 Gbps	12 Gbps	14.5 Gbps
並行工作階段數上限§	1.4M	2.2M	2.5M	3M
每秒新工作階段數量‖	145,000	220,000	240,000	268,000
虛擬系統 (基礎/最大)¶	1/11	1/11	1/11	1/11

注意：在 PAN-OS 11.1 上測量結果。

* 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 Security、檔案封鎖和記錄，以 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。

§ 並行工作階段數上限是利用 HTTP 交易所測得。

‖ 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-3400 Series 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
乙太網路點對點通訊協定 (PPPoE)
多點傳送：PIM-SM，PIM-SSM，IGMP v1、v2 與 v3
雙向轉送偵測 (BFD)
IPsec 和 SSL VPN
金鑰交換：手動金鑰、IKEv1 及 IKEv2 (預先共用金鑰、憑證式驗證)
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：4,094/4094
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

* 需要 GlobalProtect 授權。

表 2：PA-3400 Series 網路功能 (續)
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☒ (PA-3440 和 PA-3430)
5G 安全性
GTP 安全性
SCTP 安全性

† 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-3400 Series 硬體規格
I/O
PA-3410：1G/2.5G/5G/10G (12)、1G/10G SFP/SFP+ (10)、25G SFP28 (4)
PA-3420：1G/2.5G/5G/10G (12)、1G/10G SFP/SFP+ (10)、25G SFP28 (4)
PA-3430：1G/2.5G/5G/10G (12)、1G/10G SFP/SFP+ (10)、25G SFP28 (4)、40G/100G QSFP/QSFP28 (2)
PA-3440：1G/2.5G/5G/10G (12)、1G/10G SFP/SFP+ (10)、25G SFP28 (4)、40G/100G QSFP/QSFP28 (2)
管理 I/O
100/1000 頻外管理連接埠 (1) 100/1000 高可用性 (2)、10G SFP+ 高可用性 (1) RJ-45 主控台連接埠 (1)、Micro USB (1)
儲存容量
480 GB SSD
電源 (平均/最大耗電量)
備援 450W AC (133W/190W)
最高 BTU/小時
650
輸入電壓頻率
交流：100–240 VAC (50-60 Hz)
最大電流消耗
交流：1.9 A @ 100 VAC、0.8 A @ 240 VAC
平均無故障時間 (MTBF)
22 年
機架安裝尺寸
1U，19 英吋標準機架 14.15 x 17.15 x 1.70 英吋
重量 (裝置本身/託運時)
15.5 磅/25 磅
安全性
cTUVus、CB
EMI
FCC Class A、CE Class A、VCCI Class A

表 3：PA-3400 Series 硬體規格 (續)
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
非作業溫度：-4°F 至 158°F，-20°C 至 70°C
濕度容限：10% 至 90%
最高海拔：10,000 英呎/3,048 公尺
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-3400-series_022124