



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測器
- 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 (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 (SSL/TLS)。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 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 SSL/TLS 加密的傳入和傳出流量，包括使用 TLSv1.3 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，同時減少營運費用。

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。
- **啟用 NetSec 管理和營運：**跨所有規格輕鬆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，以確保一致性並且減少營運開支。

## 新世代防火牆的原生網路 Proxy 支援

- 能夠將防火牆和 Proxy 整合到單一平台，同時透過集中管理平台管理功能以建立政策。
- 能夠透過 PAC 檔案支援明確 Proxy 以及透明 Proxy。
- 明確 Proxy 有助於內部部署 Proxy 部署的無預設路由架構。
- 明確 Proxy 支援使用 Kerberos 和 SAML 進行驗證。
- 不需要 WCCP 或驗證即可簡化透明 Proxy 設定。

## 採用 Precision AI 支援的同級最佳雲端交付安全服務

隨著混合工作模式、雲端、IoT 和 SaaS 的大量採用，一般企業的攻擊範圍隨之大幅增長。此外，由於駭客能夠輕易取得並使用對其活動有利的工具與資源，威脅形勢正迅速加劇。傳統的網路安全解決方案和方法已不再有效。透過 Palo Alto Networks 雲端交付安全服務，客戶都能夠享有同級最佳的即時安全防護，協助保護其網路中的所有使用者、裝置與數據，且不受地理位置限制。

Palo Alto Networks 安全服務運用 Precision AI® 內嵌的強大效能，能保持對於威脅行動者的領先優勢，並可即時阻止前所未見的新型威脅。透過與全球超過 70,000 名客戶的威脅情報共享，他們可以深入了解各種新興威脅並主動採取行動。最後，與新世代防火牆和 SASE 的無縫整合可消除安全漏洞，並為客戶提供單一管理平台來檢視及管理其安全性。

服務包括：

- **進階威脅防禦**：阻止已知和未知入侵、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% 的植入攻擊和 48% 的高迴避性 C2 流量。
- **Advanced WildFire®**：透過業界最大的惡意軟體防禦引擎確保檔案的安全存取，相較於最接近的競爭對手，可以多阻止 22% 的未知惡意軟體，並將偵測轉化為快 180 倍的防禦能力。
- **進階 URL Filtering**：透過業界首次能防範已知和未知網路釣魚攻擊的防禦能力，確保 Web 的安全存取，比傳統篩選數據庫即時多阻止 40% 的威脅，更領先競爭對手至少 48 小時封鎖高達 88% 的惡意 URL。
- **進階 DNS Security**：保護您的 DNS 流量並即時阻止包括 DNS 劫持在內的進階 DNS 層威脅，其 DNS 層威脅涵蓋範圍更比競爭對手多出兩倍。
- **新世代 CASB**：透過對超過 6 萬個 SaaS 應用程式的可視性，在您的網路中探索及控制所有 SaaS 耗用，並利用 28 種以上的 API 整合保護您的數據。
- **IoT Security**：利用業界最全面的零信任 IoT 裝置解決方案確保盲點不會遭到入侵並保護每個連線的裝置，同時在 48 小時內發現 90% 的裝置。

## 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，從而提供絕佳的最終使用者體驗。

**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 11.2 上測量結果。

\* 啟用 App-ID 和記錄，以 appmix 交易測量防火牆輸送量。

† App-ID、IPS、防毒軟體、反間諜軟體、WildFire、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 (預先共鑰金鑰、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)、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                         |
| 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-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                                                                              |
| 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。                                                        |
| 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](https://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 英尺/3,048 公尺

氣流：前進後出



諮詢熱線：0800666326

網址：[www.paloaltonetworks.tw](https://www.paloaltonetworks.tw)

郵箱：[contact\\_salesAPAC@paloaltonetworks.com](mailto: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

© 2025 Palo Alto Networks, Inc. 我們在美國及其他司法管轄區的商標清單可在 <https://www.paloaltonetworks.com/company/trademarks.html> 中找到。本文提及的所有其他標誌皆為其各自公司所擁有之商標。

strata\_ds\_pa-3400-series\_031925