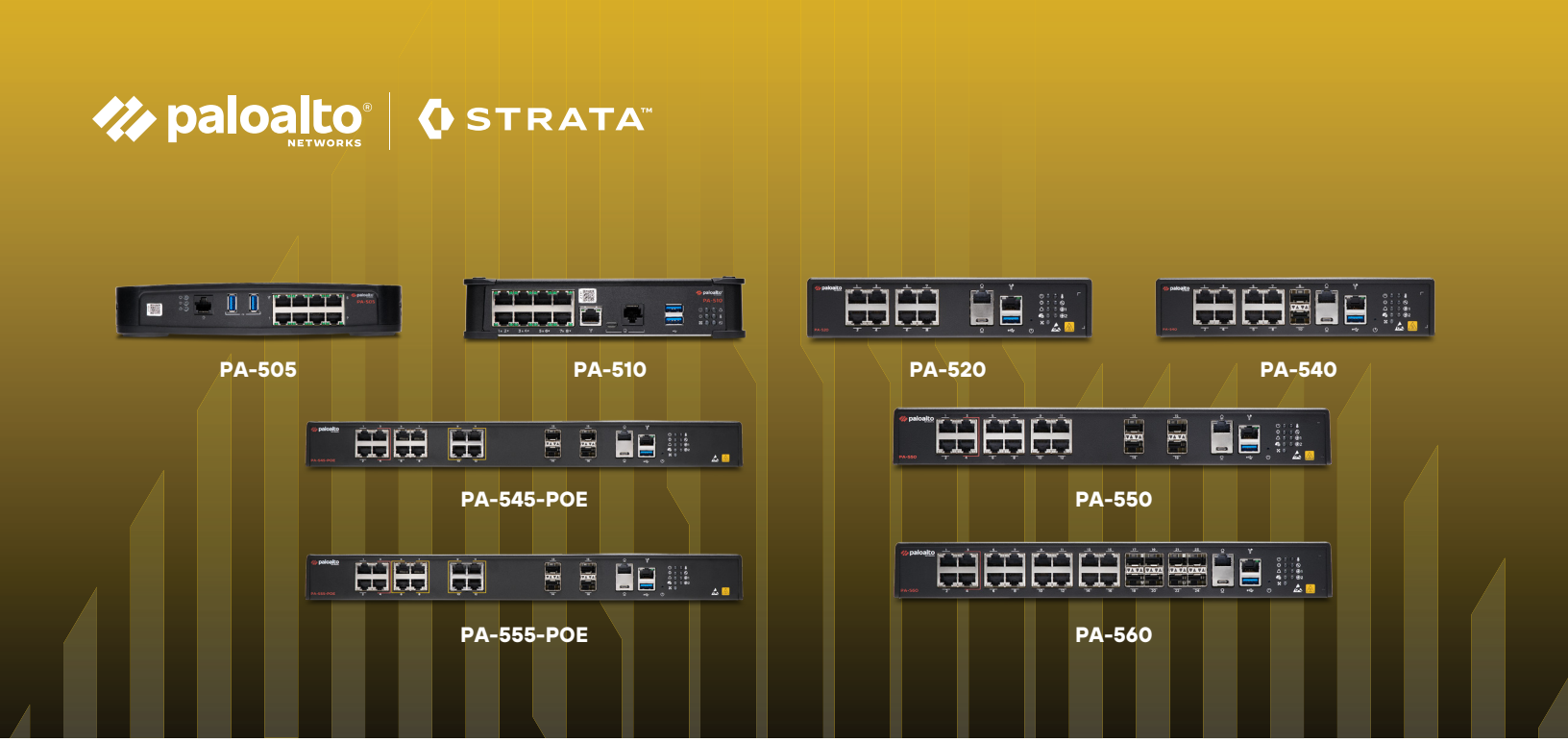

PA-500 Series

Palo Alto Networks PA-500 Series 新世代防火牆 (NGFW) 包括 PA-505、PA-510、PA-520、PA-540、PA-545-POE、PA-550、PA-555-POE 和 PA-560 型號。此系列為分散式企業分公司、零售場所和中型企業提供由 ML 驅動的 NGFW 功能。

PA-500 Series NGFW 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。無論位置或裝置類型為何，PAN-OS 原生會將所有流量（包括應用程式、威脅和內容）分類，然後將該流量與使用者連結起來。應用程式、內容和使用者（執行您業務的元素）是安全政策的基礎，能夠改善安全態勢與縮短事件回應時間。PAN-OS 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。

重點

- 高效能企業分支 NGFW 系列。
- 由 Precision AI® 提供支援，這是一種突破性的 AI 驅動引擎，可即時分析和預防威脅。
- 較高的連接埠密度，具備最多可達 24 個銅線和光纖介面。
- 最多可達 330W 的乙太網路供電 (PoE) 支援。
- IEEE 802.3bt 支援，每個 PoE 連接埠最大功率為 90W。
- 透過零接觸佈建 (ZTP) 簡化部署。
- 支援主動/主動和主動/被動模式的高可用性。
- 採用單通道架構，可啟用安全服務以提供可預測的效能。
- 採用 Strata™ Cloud Manager 進行管理，這是業界首個由 AI 驅動的網路安全性統一管理和營運解決方案。
- 獲評選為領導者：2025 年 Gartner® 混合網狀防火牆魔力象限™。
- Forrester Wave™ 領導者：企業防火牆解決方案，2024 年第四季。

透過完整的第 7 層檢查進行應用程式識別和分類

App-ID™ 具備完整的第 7 層檢查功能，可隨時識別和分類所有連接埠的所有應用程式，進而支援以下功能：

- 無論使用何種連接埠、通訊協定或加密方法，都能使用通訊協定解碼、啟發式和特徵碼比對等先進技術，準確識別網路上的應用程式。選用的 App-ID 雲端引擎 (ACE) 服務會為 SaaS 應用程式提供隨選 App-ID。
- 提供對各種應用程式相關風險和價值的全面理解，有助於就網路安全政策做出明智的決策。
- 透過在防火牆層級集中識別和控制應用程式，可以有效地實施針對特定應用程式量身打造的安全政策。
- 識別和管理迴避性或自訂應用程式，這類應用程式通常會繞過傳統安全措施。
- 不斷更新其應用程式識別，確保其能夠有效應對最新的應用程式趨勢和手法。
- 使用尖端的 AI 技術，來提高識別和分類由 AI 驅動應用程式的精確度。這些技術可確保即使是最先進和動態的應用程式，也能在網路中加以準確識別和妥善管理。

如需更多資訊，請參閱 App-ID 技術簡介。

使用安全執行

PA-500 Series NGFW 可在任何位置、任何裝置為使用者強制實施安全性，同時根據使用者活動來調整政策。其包括以下能力：

- 依據使用者、群組和 IP 位址啟用可視性、安全政策、報告和鑑識。
- 無論使用者位於何處（辦公室、家中、差旅等）和使用何種裝置，都套用一致的政策。這些裝置包括 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。
- 利用 IP 地理位置自動實施以地理位置為基礎的安全政策，使您能夠減少攻擊面、滿足合規性要求並透過封鎖往返於特定國家或地區的流量來控制應用程式存取。
- 無論使用者身分位於何處以及儲存在何處（雲端和內部部署目錄或兩者），都可以使用雲端身分引擎（以身分為基礎的安全雲端式架構），一致地對使用者進行驗證和授權，進而快速實現零信任安全態勢。
- 使用無密碼驗證保護所有應用程式，無論是內部部署、SaaS 還是混合。
- 透過在防火牆定義雲端動態使用者群組 (CDUG) 來提供以使用者行為為基礎的動態安全措施，以限制可疑或惡意使用者，從而採取以風險為基礎、有時間限制的安全措施，而無需等待將變更套用至使用者目錄。
- 透過在網路層為任何應用程式啟用多因素驗證 (MFA)，完全不需要進行任何變更，就可以同時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。

- 輕鬆與各種儲存庫整合以處理使用者資訊，包括無線 LAN 控制器、VPN、目錄伺服器以及安全資訊和事件管理 (SIEM) 工具。
- 自動化政策建議，可節省時間與減少人為錯誤的可能性。

如需更多資訊，請參閱雲端身分引擎解決方案簡介。

獨特的封包處理方法

PA-500 Series NGFW 使用單通道架構處理封包。透過這種方法，NGFW 就能夠：

- 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)。這大大減少在單一安全裝置中執行多項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，可產生一致且可預測的效能（見表 1）。

後量子密碼學就緒

PA-500 Series 是一款後量子密碼學就緒裝置，可協助您透過 PAN-OS 12.1 在硬體和軟體實現量子安全。PA-500 Series NGFW 支援：

- 後量子密碼學 (PQC) 用於 PQC SSL/TLS 解密、PQC VPN 站台到站台、PQC SSL/TLS 密碼轉換代理和用於防火牆管理存取的 PQC SSL/TLS 服務設定檔。
- PQC 演算法，包括 NIST 標準，如 ML-KEM、ML-DSA 和 SLH-DSA，以及預標準 PQC，如 Classic McEliece、BIKE、HQC、Frodo-KEM 和 NTRU-Prime。

防止在加密流量中隱藏的惡意活動

PA-500 Series NGFW 提供以下功能：

- 檢查並將政策套用至 SSL/TLS 加密流量（入站和出站）、使用 SSLv3、TLSv1.1、TLSv1.2 和 TLSv1.3 的流量以及應用程式協定 SMTP、WebSocket、gRPC、HTTP/1.0、HTTP/1.1 和 HTTP/2。
- 使用經典金鑰交換演算法 RSA、ECDHE、DHE 和後量子金鑰交換標準 ML-KEM、HQC 以及實驗性 BIKE 和 Frodo-KEM 解密和檢查 SSL/TLS 工作階段。
- 收集 TLS 流量指標，例如加密流量、SSL/TLS 版本和密碼。
- 支援經典金鑰交換 RSA、ECDHE 和 DHE 等套件，以及後量子金鑰交換 ML-KEM 和 HQC（無需解密），為通過防火牆的所有 SSL/TLS 工作階段的加密資訊帶來額外的可視性。
- 啟用對使用舊式 TLS 通訊協定、不安全和棄用的密碼以及錯誤設定的憑證（包括與憑證通用名稱 (CN) 不符的伺服器名稱指示 (SNI)）的控制，以降低風險。

- 簡化解密部署流程，並讓您運用增強的內建日誌，獨立疑難排解用戶端與伺服器端工作階段中的問題，無論遇到的是中間憑證遺失或固定憑證，皆能提供流暢的疑難排解體驗。
- 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。

此外，此功能提供解密鏡像功能，可讓您建立防火牆解密流量副本，並將其傳送至流量收集工具，以供鑑識、歷史用途或資料遺失防護（DLP）。

閱讀解密：為什麼、在哪裡、如何白皮書了解解密以防止威脅並確保業務安全。

透過 Strata Cloud Manager 的由 AI 驅動的統一管理和營運

使用 Strata Cloud Manager 管理 PA-500 Series NGFW，它使您能夠：

- **取得您整個網路安全性資產的完整可視性：**透過統一介面，實現整個網路安全性環境的即時、全面可視性，包括所有使用者、應用程式、裝置，以及需要注意的最重要威脅。
- **啟用簡單且一致的網路安全性生命週期管理：**管理所有執行點的設定與政策管理，包括 SASE、硬體與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銷。
- **即時強化安全性態勢：**利用 AI 支援的分析來偵測、解決和最佳化政策異常象，例如影子政策和備援政策，以及過度放任或未使用的規則。利用整合式最佳實務建議改善您的安全性態勢，並維持符合業界與 InfoSec 標準。
- **主動解決網路中斷問題並提升使用者體驗：**預測、診斷和解決網路健康問題，例如使用者體驗問題、容量瓶頸、CVE 漏洞、服務連線問題，以及 130 種其他類型的問題，最長可提前 90 天預測、診斷和解決，以確保順暢的營運。
- **即時知識唾手可得，以快速解決問題：**Strata Copilot™ 是由 AI 驅動的輔助工具，以自然語言介面為特色，您可以透過其在安全性與營運挑戰升級之前，快速找到、了解並加以解決。此外，透過其簡化的案例建立功能，您就能在最需要時取得快速支援。

由 Precision AI 提供支援的同級最佳雲端交付安全性服務

PA-500 Series NGFW 透過雲端交付安全服務 (CDSS) 提供同級最佳的安全性。我們的 CDSS 的核心是 Precision AI。與傳統的被動式工具不同，Precision AI 透過主動威脅偵測、內嵌預防和自動化回應來增強防禦能力，甚至可以在最具迴避性、前所未見的攻擊造成損害之前予以阻止。在全球超過 70,000 名客戶威脅情報的支援下，我們的雲端交付服務會不斷學習、適應和發展。CDSS 與 NGFW 和 SASE 平台流暢整合，無論使用者或資料位於何處，都能跨 Web、DNS、電子郵件、應用程式等提供統一的保護。

無論您是進行混合工作、擁抱雲端轉型還是抵禦老練的對手，由 Precision AI 提供支援的 CDSS 都能為您提供可視性、自動化和信心，從而助您保持領先地位。

進階威脅防禦

每天分析多達 6.73 億個新工作階段，並主動即時封鎖 282 億個威脅（包括零日漏洞、惡意軟體、命令與控制 (C2) 流量和迴避性技術），以前所未有的規模提供尖端安全性。

進階 WildFire

利用業界最強大的惡意軟體防護引擎，每天主動阻止多達 45 萬個新威脅。Advanced WildFire® 可在各種進階威脅影響組織之前識別並阻止這些威脅，包括零日惡意軟體、勒索軟體、遠端存取木馬 (RAT)、武器化文件和其他迴避性攻擊技術。

進階 URL Filtering

每天在線上封鎖多達 1.51 億個威脅，同時分析 38 億個新 URL，進而保障網路存取安全。進階 URL Filtering 可防禦網路釣魚、惡意軟體、勒索軟體、C2 通訊和以 Web 為基礎的迴避性攻擊。

進階 DNS 安全性

進階 DNS 安全性提供即時保護，可立即阻止以複雜 DNS 請求和回應為基礎的威脅 - 包括 DNS 劫持、網域產生演算法 (DGA)、DNS 隧道和 C2 回呼。這個功能每天會分析超過 11 億個新網域，識別多達 770 萬個新惡意網域，在線上阻止超過 20 億個威脅。這強大的第一道防線可以識別並阻止 DNS 層的威脅—無論這些威脅來自網路外部還是內部。

裝置安全性

為每個連網裝置提供量身打造的解決方案（涵蓋製造業、零售業、醫療保健、高科技產業及一般企業），實現 48 小時內 90% 的裝置探索率—並提供優先的漏洞與風險評估。此外，您還可以在單一 NetSec 平台上識別異常、取得最低權限存取控制安全性政策建議，並虛擬修補漏洞。

SaaS 安全性

透過對超過 75,000 個 SaaS 應用程式的可視性和針對超過 150 個 SaaS 應用程式的 DLP 控制，來探索和控制所有 SaaS 使用情況。透過對超過 117 個 SaaS 應用程式進行態勢管理以及對 39 個應用程式進行 SaaS 內嵌租用戶控制，來防止 SaaS 設定錯誤。

AI 存取安全性

透過即時查看 GenAI 應用程式、使用者存取控制、資料保護和持續風險監控，實現 GenAI 的安全使用。AI Access Security™ 提供業界領先超過 2,500 個 GenAI 應用程式目錄，其中包括超過 15 個 GenAI 特定的應用程式屬性，可準確識別與降低風險。其包括針對超過 13 個 GenAI 應用程式的態勢管理和針對 11 個應用程式的 SaaS 內嵌租用戶控制。

進階 SD-WAN

只要在具有整合安全性的現有防火牆上啟用 SD-WAN，就可以輕鬆地加以採用。透過使用 SD-WAN 路徑測量和應用程式轉向功能，智慧地將應用程式轉向效能最佳的路徑，就能獲得卓越的最終使用者體驗並確保 SLA。

PA-500 Series 規格

表 1.PA-500 Series NGFW 效能與功能								
	PA-505	PA-510	PA-520	PA-540	PA-545-POE	PA-550	PA-555-POE	PA-560
防火牆輸送量 (appmix)*	1.2 Gbps	1.8 Gbps	2.8 Gbps	3.8 Gbps	5.0 Gbps	6.5 Gbps	7.5 Gbps	8.5 Gbps
Threat Prevention 輸送量 (appmix)†	0.8 Gbps	1.2 Gbps	1.8 Gbps	2.2 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps	6.0 Gbps
IPsec VPN 輸送量‡	0.4 Gbps	0.8 Gbps	1.5 Gbps	2.0 Gbps	3.0 Gbps	4.0 Gbps	4.5 Gbps	5.5 Gbps
並行工作階段數上限§	64K	98K	148K	248K	298K	398K	448K	598K
每秒新工作階段數量‖	10K	15K	25K	50K	55K	70K	75K	100K
虛擬系統（基礎/最大）#	—	—	—	1/2	1/2	1/5	1/5	1/5

備註：在 PAN-OS 12.1 上測量結果。

* 啟用 App-ID 和記錄，使用 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-500 Series 網路功能
介面模式
L2 模式（MC-LAG 彙總介面上不可用）、L3、Tap 和虛擬線路（透明模式）。
路由
具有平滑重新啟動、RIP 和靜態路由的 OSPFv2/v3 和 MP-BGP。
政策式轉送。
支援 PPPoE 和 DHCP 用戶端，可同時為 IPv4 和 IPv6 進行動態位址指派。
DHCPv4 伺服器。
多播：PIM-SM、PIM-SSM、IGMPv2 和 v3。
進階 SD-WAN
路徑品質測量（抖動、封包遺失和延遲）。
頻寬監控。
金鑰交換：手動金鑰、IKEv1 及 IKEv2（預先共用金鑰、憑證式驗證）。
後量子 PPK。
SD-WAN 覆蓋範圍的多 VR 和 LR 支援。
Prisma® Access 中心（混合 SASE）。
自主數位體驗管理 (ADEM)，可供 NGFW 支援之用。
IPv6
L2、L3、Tap 和虛擬線路模式（透明模式）中的 IPv6 檢查。
支援雙堆疊和僅 IPv6 網路。
功能：IPv6 地理定位、OSPFv3、MP-BGP、NAT64 和 NPTv6。
具有前綴委派 (PD) 支援的 DHCPv6 用戶端。無狀態位址自動設定 (SLAAC) 伺服器支援。

表 2.PA-500 Series 網路功能（續）
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 和 AES（128 位元、192 位元和 256 位元）。
驗證：MD5、SHA-1、SHA-256、SHA-384 和 SHA-512。
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/每個介面的 802.1Q VLAN 標籤：4,094/4,094。
彙總介面 (802.3ad) 和 LACP。

* 需要 GlobalProtect 授權。

表 3.PA-500 Series 硬體規格
I/O
PA-505：1G RJ45 (7) PA-510：1G RJ45 (8) PA-520：1G RJ45 (8) PA-540：1G RJ45 (8)、1G SFP (2) PA-545-POE：1G RJ45 (8)、1G/2.5G (4)/PoE、1G SFP (4) PA-550：1G RJ45 (12)、1G SFP (2)、1G/10G SFP/SFP+ (2) PA-555-POE：1G RJ45 (4)、1G RJ45 (4)/PoE、1G/2.5G (4)/PoE、1G SFP (2)、1G/10G SFP/SFP+ (2) PA-560：1G RJ45 (16)、1G SFP (4)、1G/10G SFP/SFP+ (4)
管理 I/O
PA-505：10/100/1000 頻外管理連接埠 (1)、USB 連接埠 (2) 和 RJ45 主控台連接埠 (1) PA-510：10/100/1000 頻外管理連接埠 (1)、USB 連接埠 (2)、RJ45 主控台連接埠 (1) 和 Micro USB 主控台連接埠 (1) PA-520、PA-540、PA-545-POE、PA-550、PA-555-POE、PA-560：10/100/1000 頻外管理連接埠 (1)、USB 連接埠 (1)、RJ45 主控台連接埠 (1) 和 USB-C 主控台連接埠 (1)
儲存容量
PA-505、PA-510：128 GB PA-520、PA-540、PA-545-POE、PA-550、PA-555-POE：120 GB PA-560：240 GB
可信任平台模組 (TPM)
與 TPM 整合，可實現安全啟動、硬體信任根和保護系統密碼。
乙太網路供電
PA-545-POE PoE 預算總計：181W，PoE 連接埠 (4)，單一連接埠最大負載：90W PA-555-POE PoE 預算總計：330W，PoE 連接埠 (8)，單一連接埠最大負載：90W
耗電量

模型	最大功耗
PA-505	23W
PA-510	34.3W
PA-520 或 PA-540	30W
PA-545-POE*	336W（含 181W PoE 輸出）
PA-550	57W
PA-555-POE*	503W（含 332W PoE 輸出）
PA-560	106W

*配備一或多個提供的 AC 轉接器。

表 3.PA-500 Series 硬體規格 (續)
最大 BTU/小時
PA-505：78 PA-510：117 PA-520 或 PA-540：102 PA-545-POE：1145（含 181W PoE 輸出） PA-550：195 PA-555-POE：1715（含 332W PoE 輸出） PA-560：361
輸入電壓（輸入頻率）
100–240 VAC (50-60 Hz)
最大電流消耗
PA-505：2 A @ 12 VDC PA-510：2.5 A @ 12 VDC PA-520 或 PA-540：4 A @ 12 VDC PA-545-POE：6 A @ 54 VDC PA-550：5 A @ 12 VDC PA-555-POE：9 A @ 54 VDC PA-560：8 A @ 12 VDC
尺寸
PA-505：1.63 x 6.42 x 9.53 英吋（高 x 深 x 寬）（43.9 x 163 x 242 公釐（高 x 深 x 寬）） PA-510：1.74 x 8.83 x 8.07 英吋（高 x 深 x 寬）（43.9 x 224 x 205 公釐（高 x 深 x 寬）） PA-520 或 PA-540：1.74 x 10.4 x 8 英吋（高 x 深 x 寬）（43.9 x 265 x 203 公釐（高 x 深 x 寬）） PA-550 或 PA-560：1.74 x 12.1 x 13 英吋（高 x 深 x 寬）（43.9 x 37 x 330 公釐（高 x 深 x 寬）） PA-545-POE 或 PA-555-POE：1.75 x 12.6 x 16.1 英吋（高 x 深 x 寬）（43.9 x 314 x 409 公釐（高 x 深 x 寬））
重量（獨立裝置/出貨時）
PA-505：3.1 磅/5.9 磅 PA-510：5.0 磅/7.8 磅 PA-520 或 PA-540：5.8 磅/8 磅 PA-545-POE：13.5 磅/19.8 磅 PA-550：11.2 磅/15.6 磅 PA-555-POE：13.5 磅/20.2 磅 PA-560：11.2 磅/15.6 磅
安全
cTUVus、CB
EMI
PA-505、PA-510：FCC B 類、CE B 類和 VCCI B 類 PA-520、PA-540、PA-545-POE、PA-550、PA-555-POE、PA-560：FCC A 類、CE A 類和 VCCI A 類
認證
請參閱我們的合規頁面。
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 被動冷卻：PA-505、PA-510、PA-520、PA-540、PA-545-POE、PA-550 和 PA-555-POE 主動冷卻：PA-560

表 4.PA-500 Series 訂購資訊		
配件	**簡短描述**	**模型**
PAN-PWR-25W-AC	25W 備用電源轉接器	PA-505
PAN-PWR-50W-AC*	50W 備用電源轉接器*	PA-510
PAN-PWR-150W-12V-AC-A	150W 備用電源轉接器	PA-520、PA-540、PA-550 和 PA-560
PAN-PWR-350W-54V-AC-A	350W 備用電源轉接器	PA-545-POE
PAN-PWR-550W-54V-AC-A	550W 備用電源轉接器	PA-555-POE
PAN-PA-400-RACKTRAY*	適用於以下項目的 1RU 4 柱機架安裝： 兩個 PA-510 和四個電源轉接器	PA-510
PAN-1RU-4POST-RACK-11	適用於以下項目的 1RU 4 柱機架安裝： 一個 PA-560 和兩個電源轉接器， 一個 PA-550 和兩個電源轉接器， 兩個 PA-540 和四個電源轉接器， 兩個 PA-520 和四個電源轉接器。	PA-520、PA-540、PA-550 和 PA-560
PAN-1RU-4POST-RACK-12	適用於以下項目的 1RU 4 柱機架安裝： 一個 PA-555-POE 和兩個電源轉接器， 一個 PA-545-POE 和兩個電源轉接器	PA-545-POE 和 PA-555-POE

* 需分開報價。

3000 Tannery Way
Santa Clara, CA 95054

總部： +1.408.753.4000
銷售： +1.866.320.4788
支援： +1.866.898.9087

www.paloaltonetworks.com

strata_ds_pa-500-series_090825