paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

重點

- 全球第一個機器學習式的新世代防火牆
- 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
- 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
- 藉由選用的零接觸佈建 (ZTP) 簡化大量防火牆的部署
- 透過 Panorama™ 網路安全管理支援集中管理

PA-3200 Series

Palo Alto Networks PA-3200 Series 機器學習式新世代防火牆包括 PA-3260、PA-3250 和 PA-3220，所有的防火牆均專為高速網際網路閘道部署所設計。PA-3200 Series 設備可使用專屬處理器與記憶體，在網路、安全性、威脅防禦及管理方面保護所有流量，包括加密流量。

PA-3260

PA-3250

PA-3220

PA-3200 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 (NGFW) 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，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。

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 類別以及來源和目的地區域、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。

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式威脅時仍可保護自身的安全。服務包括：

- **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** — 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。

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，從而提供絕佳的終端使用者體驗。

表 1：PA-3200 Series 效能與功能

	PA-3260	PA-3250	PA-3220
防火牆輸送量 (HTTP/appmix)*	7.8/8.7 Gbps	5.3/5.8 Gbps	4.3/4.8 Gbps
Threat Prevention 輸送量 (HTTP/appmix)†	3.9/4.7 Gbps	2.6/3.1 Gbps	2.1/2.6 Gbps
IPsec VPN 輸送量‡	4.7 Gbps	2.9 Gbps	2.6 Gbps
最大工作階段數量	2.2M	2M	1M
每秒新工作階段數量§	94,400	63,700	52,800
虛擬系統 (基礎/最大)‖	1/6	1/6	1/6

注意：在 PAN-OS 10.1 上測量結果。

* 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 交易測量 IPSec VPN 輸送量。

§ 使用應用程式覆蓋，以 1 位元組 HTTP 交易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-3200 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

表 2：PA-3200 Series 網路功能 (續)
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

表 2：PA-3200 Series 網路功能 (續)
IPsec 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
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
零接觸佈建 (ZTP)
以 -ZTP SKU 的形式提供 (PA-3260-ZTP、PA-3250-ZTP、PA-3220-ZTP) 需要 Panorama 9.1.3 或更高版本

表 3：PA-3200 Series 硬體規格
I/O
PA-3260：10/100/1000 (12)、1G/10G SFP/SFP+ (8)、40G QSFP+ (4)
PA-3250：10/100/1000 (12)、1G/10G SFP/SFP+ (8)
PA-3220：10/100/1000 (12)、1G SFP (4)、1G/10G SFP/SFP+ (4)
管理 I/O
10/100/1000 頻外管理連接埠 (1)、10/100/1000 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
240 GB SSD
電源 (平均/最大耗電量)
備援 650W 交流或直流 (180/240)
最高 BTU/小時
819
輸入電壓 (輸入頻率)
交流：100-240 VAC (50/60Hz)
直流：-48 V @ 4.7 A、-60 V @ 3.8 A

表 3：PA-3200 Series 硬體規格(續)
最大電流消耗
交流：2.3 A @ 100 VAC、1.0 A @ 240 VAC
直流：-48 V @ 4.7 A、-60 V @ 3.8 A
平均無故障時間 (MTBF)
14 年
機架安裝尺寸
2U，19 英吋標準機架 (3.5 x 20.53 x 17.34 英吋 (高 x 深 x 寬))
重量 (裝置本身/託運時)
29 磅/41.5 磅
安全性
cTUVus、CB
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° 至 122° F，0° 至 50° C
非作業溫度：-4 至 158 °F，-20 至 70 °C
耐濕性：10% 至 90%
最高海拔：10,000 英呎/3,048 米
氣流：前進後出

若要檢視 PA-3200 Series 的特色及相關功能的其他資訊，請前往 paloaltonetworks.com/network-security/next-generation firewall/pa-3200-series。

paloalto NETWORKS

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