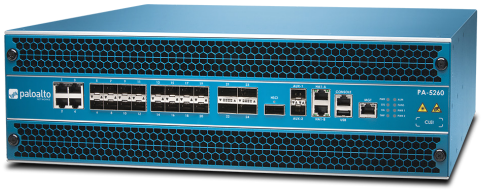
STRATA™
BY PALO ALTO NETWORKS

PA-5200 Series

Palo Alto Networks PA-5200 Series 機器學習式新世代防火牆包括 PA-5280、PA-5260、PA-5250 和 PA-5220，所有這些防火牆均相當適合高速數據中心、網際網路閘道和服務供應商部署。PA-5200 Series 採用專屬處理器與記憶體，能為網路、安全性、威脅防禦及管理等關鍵功能領域提供高達 64 Gbps 的輸送量。



PA-5260

PA-5200 機器學習式新世代防火牆 (NGFW) 的控制元件是 PAN-OS®，它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，並且使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。

關鍵安全性功能

在所有時段對所有連接埠的全部應用程式進行分類

- 識別應用程式，無論連接埠、SSL/SSH 加密方式或所部署的迴避技術為何。
- 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。
- 分類無法識別的應用程式，進行政策控制、威脅鑑識或 App-ID™ 技術開發。
- 充分掌握所有 TLS 加密連線的詳細資訊，並阻止隱藏在加密流量 (包括使用 TLS 1.3 和 HTTP/2 通訊協定的流量) 中的威脅。

針對任何地點的任何使用者執行安全政策

- 對 Windows®、macOS®、Linux、Android® 或 Apple iOS 平台上執行的本機及遠端使用者部署一致的政策。
- 能夠與 Microsoft Active Directory® 和 Terminal Services、LDAP、Novell eDirectory™ 及 Citrix 進行無代理程式整合。
- 輕鬆整合防火牆政策與 802.1X 無線、Proxy、網路存取控制，以及其他任何來源的使用者身分資訊。

透過雲端交付的安全訂閱，將原生保護擴展到所有攻擊途徑

- **Threat Prevention**—檢查所有流量以自動阻擋已知的弱點、惡意軟體、弱點入侵、間諜軟體、命令與控制 (C2)，以及自訂的入侵防禦系統 (IPS) 特徵碼。
- **WildFire® 惡意軟體防禦**—在數秒鐘內針對網路、端點和雲端的大多數新威脅，提供自動化防禦以防範未知的檔案型威脅。
- **URL Filtering**—防止存取惡意網站，並保護使用者免於遭受 Web 型威脅。
- **DNS Security**—透過 DNS 偵測並阻擋已知和未知的威脅，而預測性分析則阻斷使用 DNS 進行 C2 或數據竊取的攻擊。
- **IoT Security**—探索網路中所有未受管理的裝置、識別風險和弱點，以及使用新的 Device-ID™ 政策架構，為機器學習式新世代防火牆自動執行政策。

表 1：PA-5200 Series 效能與功能[1]

	PA-5280	PA-5260	PA-5250	PA-5220
防火牆輸送量 (HTTP/appmix)[2]	58/65 Gbps	58/65 Gbps	38/37 Gbps	16/18 Gbps
Threat Prevention 輸送量 (HTTP/appmix)[3]	29/36 Gbps	29/36 Gbps	19.5/24 Gbps	8.2/10 Gbps
IPsec VPN 輸送量[4]	28 Gbps	28 Gbps	19 Gbps	11 Gbps
最大工作階段數量	6,400 萬	3,200 萬	800 萬	400 萬
每秒新工作階段數量[5]	600,000	600,000	382,000	180,000
虛擬系統 (基礎/最大)[6]	25/225	25/225	25/125	10/20

1. 在 PAN-OS 10.0 上測量結果。
2. 啟用 App-ID 和記錄，以 64 KB HTTP/appmix 交易測量防火牆輸送量。
3. 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 交易測量 Threat Prevention 輸送量。
4. 啟用記錄功能，以 64 KB HTTP 交易測量 IPSec VPN 輸送量。
5. 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。
6. 在基礎數量上新增虛擬系統需要額外購買授權。

表 2：PA-5200 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
基於政策的轉送
動態位址指派支援乙太網路點對點通訊協定 (PPPoE) 和 DHCP
多點傳送：PIM-SM，PIM-SSM，IGMP v1、v2 與 v3
雙向轉送偵測 (BFD)

表 2：PA-5200 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-5200 Series 網路功能 (續)
IPsec VPN
金鑰交換：手動金鑰、IKEv1 及 IKEv (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
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
行動網路基礎結構
GTP 安全
SCTP 安全

表 3：PA-5200 Series 硬體規格
I/O
PA-5280 / PA-5260 / PA-5250：100/1000/10G Cu (4)、1G/10G SFP/ SFP+ (16)、40G/100G QSFP28 (4) PA-5220：100/1000/10G Cu (4)、1G/10G SFP/SFP+ (16)、40G QSFP+ (4)
管理 I/O
PA-5280 / PA-5260 / PA-5250：10/100/1000 (2)、40G/100G QSFP28 高可用性 (1)、10/100/1000 頻外管理 (1)、RJ45 主控台連接埠 (1)
PA-5220：10/100/1000 (2)、40G QSFP+ 高可用性 (1)、10/100/1000 頻外管理 (1)、RJ45 主控台連接埠 (1)

表 3：PA-5200 Series 硬體規格(續)
儲存容量
240 GB SSD、RAID1、系統儲存 2 TB HDD、RAID1、日誌儲存
電源 (平均/最大耗電量)
571/685 W
最高 BTU/小時
2,340
電源 (基礎/最大)
1:1 完全備援 (2/2)
交流輸入電壓 (輸入 Hz)
100–240 VAC (50–60 Hz)
交流電源輸出
1,200 瓦/電源
最大電流消耗
交流：8.5 A @ 100 VAC、3.6 A @ 240 VAC 直流：19 A @ -40 VDC、12.7 A @ -60 VDC
最大湧入電流
交流：50 A @ 230 VAC、50 A @ 120 VAC 直流：200 A @ 72 VDC
直流：200 A @ 72 VDC
9.23 年
安裝機架 (尺寸)
3U，19 英吋標準機架 5.25 x 20.5 x 17.25 英吋 (高 x 深 x 寬)
重量 (裝置本身/託運時)
46 磅/62 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

若要檢視 PA-5200 Series 的特點及相關功能的其他資訊，請前往 paloaltonetworks.com/network-security/next-generation-firewall/pa-5200-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