STRATA™
BY PALO ALTO NETWORKS

PA-220

Palo Alto Networks PA-220 旨在為分散式企業分公司、零售場所和中型企業提供機器學習式新世代防火牆功能。

亮點

- 主動/主動和主動/被動模式的高可用性
- 提升了可靠性的備援電源輸入
- 無風扇設計
- 透過 USB 簡化大量防火牆的部署

PA-220

PA-220 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。

關鍵安全性和連線功能

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。

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-220 效能與功能[1]

防火牆輸送量 (HTTP/appmix)[2]	575/540 Mbps
Threat Prevention 輸送量 (HTTP/appmix)[3]	275/320 Mbps
IPsec VPN 輸送量[4]	540 Mbps
最大工作階段數量	64,000
每秒新工作階段數量[5]	4,300

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。

PA-220 支援各式各樣的網路功能，能夠讓您更輕鬆地將安全功能整合至現有網路。

表 2：PA-220 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
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
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
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

表 2：PA-220 網路功能 (續)
VLAN
每個裝置/介面的 802.1Q VLAN 標籤數量：4,094/4,094
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
故障偵測：路徑監控、介面監控
零接觸佈建 (ZTP)
適用於 -ZTP SKU (PA-220-ZTP)
需要 Panorama 9.1.3 或更高版本

表 3：PA-220 硬體規格
I/O
10/100/1000 (8)
管理 I/O
10/100/1000 頻外管理連接埠 (1) RJ-45 主控台連接埠 (1) USB 連接埠 (1) Micro USB 主控台連接埠 (1)
儲存容量
32 GB eMMC
電源 (平均/最大耗電量)
選用：雙重備援 40 W (21 W / 25 W)

表 3：PA-220 硬體規格 (續)
最高 BTU/小時
102
輸入電壓 (輸入頻率)
100–240 VAC (50–60Hz)
最大電流消耗
防火牆：1.75 A @ 12 VDC 電源 (交流)：1.5A
尺寸
1.62 x 6.29 x 8.07 英吋 (高 x 深 x 寬)
重量 (裝置本身/託運時)
3.0 磅/5.4 磅
安全性
cTUVus、CB
EMI
FCC Class B、CE Class B、VCCI Class B
認證
請參閱 paloaltonetworks.com/company/certifications.html
環境
作業溫度：32° 至 104° F，0° 至 40° C 非作業溫度：-4 至 158 °F，-20 至 70 °C 被動冷卻

若要瞭解 PA-220 的特點及相關功能的詳細資訊，請前往 paloaltonetworks.com/network-security/next-generation-firewall/pa-220。

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

pa-220-ds-071020