PA-4000 系列

新世代 PA-4000 系列防火牆的關鍵特色：

使用 APP-ID™，在所有時間對全部應用程式、連接埠進行分類。

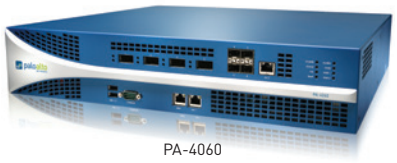
- 識別應用程式，無論連接埠、加密（SSL 或 SSH）或所部署的迴避技術為何。
- 以應用程式為基礎的安全性政策控管，而非單以連接埠進行：允許、拒絕、排程、檢查、套用流量管理。
- 針對未識別的應用程式進行分類，以獲得政策控制、威脅辯論、自訂 App-ID 建立，或 App-ID 開發的封包擷取。

使用 USER-ID™ 與 GLOBALPROTECT™，延伸安全應用程式啟用政策給任何地點的任何使用者。

- 與 Active Directory、LDAP、eDirectory Citrix 及 Microsoft Terminal Services 進行無須安裝代理程式整合。
- 使用 XML API 與 NAC、802.1X 無線網路以及其他非標準使用者容器整合。
- 對在 Microsoft Windows、Mac OS X、Linux、Android 或 iOS 平台上執行的本機及遠端使用者部署一致的政策。

使用 CONTENT-ID™ 及 WILDFIRE™，針對無論是已知或未知的所有威脅提供保護。

- 阻擋一系列已知的威脅，包括在所有連接埠上的入侵、惡意軟體與間諜軟體，無論所採行的常見威脅迴避策略為何。
- 限制未經授權的檔案及敏感資料的傳輸，並控制非工作相關的網路瀏覽。
- 識別未知的惡意軟體，分析超過 100 種惡意行為，在下一個可用的更新中自動建立並提交簽章。



PA-4060

PA-4050

PA-4020

Palo Alto Networks™ PA-4000 系列由三個針對部署高速資料中心與網際網路閘道而設計的高效能平台組成，分別為 PA-4060、PA-4050 與 PA-4020。PA-4000 系列採用專屬的處理能力及記憶體，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 10 Gbps 的吞吐量。

高速骨幹在實體上分為個別的資料及控制骨幹，無論流量負載為何，可藉此確保永遠可以使用管理存取功能 。PA-4000 系列的控制元件為 PAN-OS™，這是一套專為安全性而打造的作業系統，能讓組織安全地使用 App-ID、User-ID、Content-ID、GlobalProtect 及 WildFire 啟用應用程式。

效能與功能[1]	PA-4060	PA-4050	PA-4020
防火牆吞吐量（已啟用 App-ID）	10 Gbps	10 Gbps	2 Gbps
威脅防禦吞吐量	5 Gbps	5 Gbps	2 Gbps
IPSec VPN 吞吐量	2 Gbps	2 Gbps	1 Gbps
每秒新工作階段數量	60,000	60,000	60,000
最大工作階段數量	2,000,000	2,000,000	500,000
IPSec VPN 通道/通道介面數量	4,000	4,000	2,000
GlobalProtect (SSL VPN) 並行使用者數量	10,000	10,000	5,000
SSL 解密工作階段數量	23,000	23,000	7,500
SSL 入埠證書數量	300	300	25
虛擬路由器數量	125	125	20
虛擬系統數量（基礎/最大[2]）	25/125	25/125	10/20
安全性區域數量	500	500	80
最大政策數量	20,000	20,000	10,000

[1] 效能與功能是基於使用 PAN-OS 5.0 在理想測試條件下測得的結果。

[2] 新增虛擬系統到基礎數量需要額外購買授權。

如需新世代 PA-4000 系列防火牆功能組的詳細說明，請瀏覽網站：www.paloaltonetworks.com/literature。

paloalto NETWORKS

the network security company™

硬體規格

I/O

- PA-4060: (4) 10 千兆 XFP、(4) 千兆 SFP
- PA-4050, PA-4020: (16) 10/100/1000、(8) 千兆 SFP

管理 I/O

- (2) 10/100/1000 高可用性、(1) 10/100/1000 頻外管理、(1) DB9 主控台連接埠

儲存容量

- 160GB HDD

電源（平均/最大耗電量）

- 冗餘 400W AC (175W/200W)

最大 BTU/小時

- 682

輸入電壓（輸入頻率）

- 100-240VAC (50-60Hz)

最大電流消耗

- 2.5A@100VACc

平均故障間隔時間 (MTBF)

- 7.18 年

最大浪湧電流

- 50A@230VAC；30A@120VAC

可機架安裝（尺寸）

- 2U、19" 標準機架（3.5" 高 x 16.5" 深 x 17.5" 寬）

重量（獨立裝置/付運時）

- 33磅/40磅

安全

- UL、CUL、CB

EMI（電磁干擾，ELECTROMAGNETIC INTERFERENCE）

- FCC A 級、CE A 級、VCCI A 級、TUV

認證

- FIPS 140 2 級、通用標準 EAL2、ICSA、UCAPL

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

網路功能

介面模式：

- L2、L3、Tap、虛擬線（透通模式）

路由

- 模式：OSPF、RIP、BGP、靜態
- 轉送表格大小（每個裝置/VR 的項目數量）：20,000/20,000（PA-4060、PA-4050），10,000/10,000 (PA-4020)
- 政策式轉送
- 乙太網路點對點通訊協定 (PPPoE)
- Jumbo 框架：最大框架大小：9,210 位元組
- 多點傳送：PIM-SM，PIM-SSM，IGMP v1、v2 與 v3

高可用性

- 模式：主動/主動、主動/被動
- 故障偵測：路徑監視、介面監視

位址分配

- 裝置位址分配：DHCP 用戶端/PPPoE/靜態
- 使用者位址分配：DHCP 伺服器/DHCP 轉送/靜態

IPV6

- L2、L3、Tap、虛擬線（透通模式）
- 功能：App-ID、User-ID、Content-ID、WildFire 與 SSL 解密

VLANS

- 每個裝置/介面的 802.1q VLAN 標籤數量：4,094/4,094
- 最大介面數量：4,096（PA-4060、PA-4050），2,048 (PA-4020)
- 彙總介面 (802.3ad)

NAT/PAT

- 最大 NAT 規則數量：4,000（PA-4060、PA-4050），1,000 (PA-4020)
- 最大 NAT 規則數量 (DIPP)：250（PA-4060、PA-4050），200 (PA-4020)
- 動態 IP 與連接埠集區：254
- 動態 IP 集區：16,234
- NAT 模式：1:1 NAT、n:n NAT、m:n NAT
- DIPP 過度訂閱（每個源連接埠與 IP 的唯一目的地 IP）：8（PA-4060、PA-4050），4 (PA-4020)
- NAT64

虛擬線

- 最大虛擬線數量：2,048（PA-4060、PA-4050），1,024 (PA-4020)
- 對應至虛擬線的介面類型：實體與子介面

L2 轉送

- ARP 表格大小/裝置：20,000（PA-4060、PA-4050），10,000 (PA-4020)
- MAC 表格大小/裝置：20,000（PA-4060、PA-4050），10,000 (PA-4020)
- IPv6 芳鄰表格大小：5,000（PA-4060、PA-4050），2,000 (PA-4020)

安全性

防火牆

- 針對應用程式、使用者和內容進行政策式管控
- 分散封包保護
- 偵察掃描保護
- 阻斷服務 (DoS)/分散式阻斷服務 (DDoS) 保護
- 解密：SSL（入埠和出埠）、SSH

WILDFIRE

- 針對 100 餘種惡意行為辨識並分析具針對性的和未知的檔案
- 透過特徵碼更新針對新發現的惡意軟體生成並自動提供保護
- 特徵碼更新可在 1 小時內完成；整合記錄/報告；可存取 WildFire API 從而以程式設計方式每日提交多達 100 個範本以及透過檔案雜湊每日提交多達 1,000 個報告查詢（需要訂閱）

檔案與資料篩選

- 檔案傳輸：針對 60 餘種獨特檔案類型進行雙向控制
- 資料傳輸：針對未經授權的 CC 號碼和 SSN 傳輸進行雙向控制
- 偷渡式下載防護

使用者整合 (USER-ID)

- Microsoft Active Directory、Novell eDirectory、Sun One 和其他基於 LDAP 的目錄
- Microsoft Windows Server 2003/2008/2008r2、Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services、Citrix XenApp
- 方便與非標準使用者存放庫整合的 XML API

IPSEC VPN（站點對站點）

- 金鑰交換：手動金鑰、IKE v1
- 加密：3DES、AES（128 位元、192 位元、256 位元）
- 驗證：MD5、SHA-1、SHA-256、SHA-384、SHA-512
- 動態 VPN 通道建立 (GlobalProtect)

威脅防禦（需要訂閱）

- 應用程式、作業系統漏洞入侵保護
- 針對病毒（包括嵌入在 HTML、Javascript、PDF 中的與壓縮的）、間諜軟體和蠕蟲提供串流式保護

URL 篩選（需要訂閱）

- 預先定義和自訂 URL 類別
- 最近存取過的 URL 的裝置快取
- 作為部分安全性政策的 URL 類別
- 瀏覽時間資訊

服務品質 (QOS)

- 針對應用程式、使用者、來源、目的地、介面、IPSec VPN 通道等進行政策式流量調整
- 8 個擁有保證、最大和優先頻寬參數的流量級別
- 即時頻寬監視
- 根據政策區分服務標記
- 支援 QoS 的實體介面數量：12

SSL VPN/遠端存取 (GLOBALPROTECT)

- GlobalProtect 閘道
- GlobalProtect 入口網站
- 透通模式：IPSec 及 SSL Fall-back
- 驗證：LDAP、SecurID 或本機 DB
- 用戶端作業系統：Mac OS X 10.6、10.7（32/64 位元）、10.8（32/64 位元）、Windows XP、Windows Vista（32/64 位元）、Windows 7（32/64 位元）
- 第三方用戶端支援：Apple iOS、Android 4.0 和更高版本、用於 Linux 的 VPNC IPSec

管理、報告、可見度工具

- 整合式 Web 介面、CLI 或中央管理 (Panorama)
- 多語言使用者介面
- Syslog 和 SNMP v2/v3
- 基於 XML 的 REST API
- 應用程式、URL 類別、威脅和資料的圖形化摘要 (ACC)
- 檢視、篩選和匯出流量、威脅、WildFire、URL 與資料篩選記錄檔
- 完全可自訂的報告

如需新世代 PA-4000 系列防火牆功能組的額外資訊，請瀏覽網站：www.paloaltonetworks.com/literature。

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com