

# VM-系列

新世代 VM-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。**

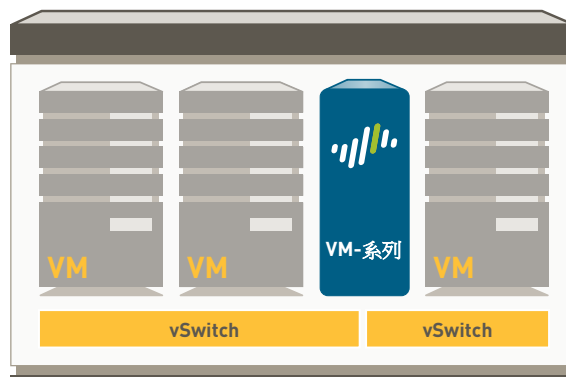
- 識別應用程式，無論連接埠、加密方式（SSL 或 SSH），或所部署的迴避技術為何。
- 在所有安全機制政策決定中以應用程式為基礎，而非單以連接埠進行：允許、拒絕、排程、檢查、套用流量管理。
- 針對未識別的應用程式進行分類，以獲得政策控制、威脅鑑識、自訂 App-ID 建立，或針對進一步調查所進行的封包擷取。

**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、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 平台上執行的使用者部署一致的政策，無論其位置為何。

**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保護功能。



VM-系列虛擬防火牆

Palo Alto Networks™ VM-系列可將安全應用程式功能延伸到虛擬化環境，同時解決重要的虛擬化安全性挑戰：使用動態定址物件來追蹤虛擬機器動作的安全政策，並使用功能強大的 XML 管理 API 來整合系統。

VM-系列由三部高效能機型組成，分別為 VM-100、VM-200 與 VM-300，它們全部都使用單通道軟體架構，可將資料中心環境下的延遲降至最低。透過硬體分離的方式來區隔使用者管理介面與資料骨幹應用，使用者可指派專屬的 CPU 給每一個管理介面使用，以此確保管理存取永遠處於可用的狀態，且無關乎於網路流量負載。VM-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，能讓組織安全無疑地使用 App-ID、User-ID、Content-ID、GlobalProtect 及 WildFire 啟用應用程式。

| 一般功能 <sup>1</sup>               | VM-300   | VM-200  | VM-100 |
|---------------------------------|----------|---------|--------|
| 最大工作階段數量                        | 250,000  | 100,000 | 50,000 |
| IPSec VPN 通道/通道介面數量             | 2,000    | 500     | 25     |
| GlobalProtect (SSL VPN) 並行使用者數量 | 500      | 200     | 25     |
| SSL 解密工作階段數量                    | 1,024    | 1,024   | 1,024  |
| SSL 入埠證書數量                      | 25       | 25      | 25     |
| 虛擬路由器數量                         | 3        | 3       | 3      |
| 安全性區域數量                         | 40       | 20      | 10     |
| 最大政策數量                          | 5,000    | 2,000   | 250    |
| 位址物件數量                          | 10,000   | 4,000   | 2,500  |
| <b>效能<sup>1</sup></b>           |          |         |        |
| 防火牆吞吐量（已啟用 App-ID）              | 1 Gbps   |         |        |
| 威脅防禦吞吐量                         | 600 Mbps |         |        |
| IPSec VPN 吞吐量                   | 250 Mbps |         |        |
| 每秒新工作階段數量                       | 8,000    |         |        |

<sup>1</sup> 效能與功能是基于使用 PAN-OS 5.0 與 4 CPU 核心在理想測試條件下測得的結果。

**虛擬化規格**

HyperVisor  
網路驅動程式  
CPU 核心數量  
記憶體（最小）  
磁碟機容量（最小/最大）

**VM-300      VM-200      VM-100**

VMware ESXi 4.1 與 ESXi 5.0  
VMXNet3  
2、4 或 8  
4GB  
40GB/2TB

**網路功能****介面模式：**

- L2、L3、Tap、虛擬線（透過模式）

**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）：5000/5000 (VM-300)、1,250/1,250 (VM-200)、1000/1000 (VM-100)
- 政策式轉送
- 多點傳送：PIM-SM、PIM-SSM、IGMP v1、v2 與 v3

**高可用性**

- 模式：主動/被動（無工作階段同步）
- 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（透過模式）
- 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：2,000 (VM-300)、500 (VM-200)、100 (VM-100)

**NAT/PAT**

- 最大 NAT 規則數量：1,000 (VM-300)、1,000 (VM-200)、125 (VM-100)
- 最大 NAT 規則數量 (DIPP)：200 (VM-300)、200 (VM-200)、125 (VM-100)
- 動態 IP 與連接埠集區：254
- 動態 IP 集區：32,000
- 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）：2 (VM-300)、1 (VM-200)、1 (VM-100)
- NAT64

**虛擬線**

- 最大虛擬線數量：1000 (VM-300)、250 (VM-200)、50 (VM-100)
- 對應至虛擬線的介面類型：實體介面與子介面

**L2 轉送**

- ARP 表格大小/裝置：2,500 (VM-300)、500 (VM-200)、500 (VM-100)
- MAC 表格大小/裝置：2,500 (VM-300)、500 (VM-200)、500 (VM-100)
- IPv6 芳鄰表格大小：1,000 (VM-300)、500 (VM-200)、500 (VM-100)

**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：6（VM-300、VM-200），4（VM-100）

**SSL VPN/遠端存取 (GLOBALPROTECT)**

- GlobalProtect 閘道
- GlobalProtect 入口網站
- 透過模式：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、Netflow v9 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 VM-系列防火牆功能組的詳細說明，請瀏覽網站：[www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature)。