VM-SERIES 新世代防火牆

世界各地的組織都將本身的雲端和虛擬化計劃擴大到傳統的資料中心和公共雲端部署。新計劃包括作為 NFV 元件或更完整的多租戶解決方案的安全措施。

VM-Series 虛擬化新世代防火牆

支援各種雲端和虛擬化環境，包括：VMware® NSX™、ESXi™、vCloud® Air™、Citrix® Netscaler® SDX™、Microsoft® Azure® 和 Hyper-V®、Amazon® Web Services 以及 KVM，含 OpenStack® 外掛程式的選用支援。

- 識別並控制雲端或虛擬化環境中的應用程式；依照使用者限制應用程式存取，並預防已知和未知的威脅。
- 採用零信任原則隔離任務關鍵應用程式及資料。
- 使工作流程自動化順利進行，讓安全措施跟上雲端變化的速度。
- 集中管理實體和虛擬化防火牆的政策，確保一致的安全態勢。

雲端安全挑戰：公共、私人及混合

採用雲端技術的效益包括提升靈活度、可擴充性，以及因應企業需求的能力。效益相當顯著，不過安全挑戰也相當艱鉅，完全不亞於內部部署的資料中心面臨的挑戰。這些挑戰包括缺乏應用程式可視性和控制，無法預防網路攻擊，以及繁瑣的政策更新程序導致工作負載部署和安全政策更新之間出現延遲。如要獲得成功，組織需要的雲端安全解決方案必須：

- 識別和控制任何連接埠可能使用的應用程式工作負載。
- 依照需求和使用者的認證，控制應該允許哪些使用者使用應用程式並授予存取權。
- 將安全政策一致性從網路擴展到雲端和遠端裝置。
- 阻止惡意軟體進入雲端並橫向 (東西向) 侵擾整個雲端。
- 在虛擬工作負載出現變更時，簡化管理並大幅縮小安全政策落後的差距。

VM-Series 支援與安全設備相同的新世代防火牆和進階的威脅預防功能，能夠讓您保護從網路到雲端的應用程式和資料。

介紹 VM-Series

為了協助客戶因應各種雲端和虛擬化使用案例和不斷增長的提升效能需求，經過優化和擴充的 VM-Series 展現出領先業界的效能，5 種機型的 App-ID™ 等級的防火牆輸送量最高可達到 20Gbps。客戶能夠運用安全功能組保護實體網路，並展現從網路到雲端均一致的安全態勢，藉以保護雲端和虛擬化計劃。VM-Series 機型包括：

- **全新的** VM-50 經過最佳化，佔用最少的資源，可達到 200 Mbps 的 App-ID 等級防火牆效能，適合從虛擬分公司/用戶端設備 (CPE) 到高密度多租戶環境的客戶。
- 經過優化的 VM-100 和 VM-300，將現有混合雲端、區隔和網際網路閘道使用案例的 App-ID 等級防火牆效能分別提升 **2 倍和 4 倍**。
- **全新的** VM-500 和 VM-700 展現出領先業界的效能，App-ID 等級防火牆效能可分別達到 10 Gbps 至 16 Gbps 的，並可在完全虛擬化資料中心和服務供應商環境中部署為 NFV 安全元件。

多樣化的選項和提升的效能可讓您運用從網路到雲端均一致的安全態勢，保護應用程式和資料。

VM-Series：保護任何雲端

VM-Series 能夠讓您採用以雲端為第一優先的部署模式，為貴公司提供更好的支援。在雲端使用 VM-Series 可運用實體網路既有的相同安全態勢保護常駐的應用程式和資料。

VM-Series 可在本機分析單一通道的所有流量，以確定應用程式身分識別、內容以及使用者身分。應用程式、其中的內容和使用者都是安全政策的核心要件，這些都必須加以運用，才能提升可視性、進行報告和事件調查。

更明智的安全決策所需的應用程式可視性

VM-Series 提供所有連接埠的應用程式可視性，這表示您可獲得更相關的 Azure 環境資訊，做出更明智的政策決策。

進行區隔/設定白名單以提高安全性和合規性

現今的網路威脅通常會危害個別的工作站或使用者，然後在網路橫向移動，造成任何位置的任務關鍵應用程式和資料出現風險。運用區隔和白名單政策可讓您控制在不同子網域進行通訊的應用程式，以加強安全性和法規合規性。啟用威脅預防和 WildFire™ 雲端威脅分析服務來強化區隔政策將封鎖已知和未知的威脅，阻止這些威脅在工作負載之間橫向移動。

使用者型政策改善安全態勢

與 Microsoft Active Directory、LDAP 和 Microsoft Exchange 之類的各種使用者儲存庫整合，納入使用者身分成為策略要件，藉由加入存取控制元件來補強應用程式白名單的功能。使用者型政策表示您可以按照使用者認證和個別需求，授予重要應用程式和資料的存取權。Azure 專用 VM-Series 結合端點的 GlobalProtect™ 網路安全進行部署時，能夠讓您將企業安全政策擴大到任何地點的行動裝置和使用者。

預防應用程式層級的進階攻擊

就像許多應用程式一樣，攻擊能夠利用任何連接埠，造成傳統的預防機制失效。Azure 專用 VM-Series 能夠讓您運用威脅預防和 WildFire 實施應用程式特定的威脅預防政策，封鎖企圖造成雲端感染的入侵、惡意軟體和先前未知的威脅 (APT)。

集中管理達到策略一致性

Panorama™ 網路安全管理可讓您管理多個雲端部署的 VM-Series 和實體安全裝置，因此可確保政策的一致性和嚴謹性。多樣化的集中日誌記錄和報告功能提供虛擬化應用程式、使用者和內容的可視性。

自動進行安全部署和政策更新

VM-Series 包含多種管理功能，可讓您將安全措施整合於以雲端為第一優先的開發專案。

- 啟動載入會運用以授權和訂閱強化的作業組態來佈建防火牆，然後自動向 Panorama 註冊。
- 為了在工作負載變動時自動進行政策更新，全面文件記錄的 XML API 和 Dynamic Address Group (動態位址群組 - DAG) 能夠讓 VM-Series 使用標籤形式的外部資料，以便動態進行政策更新。

部署新應用程式和工作負載時，會自動同時部署新世代安全措施，確保安全性跟上企業的腳步。

以雲端為中心的可擴充性和可用性

在任何雲端或虛擬化環境中，必須使用傳統的資料中心做法或以雲端為中心的做法因應可擴充性和可用性需求。以雲端為中心的做法運用既有的雲端基礎設施服務因應可擴充性和可用性需求。在 AWS® 和 Azure 中運用既有的應用程式閘道和負載平衡器服務，能夠讓 VM-Series 支援企業關鍵應用程式所需的可擴充性和可用性需求。

部署彈性

可以在各種雲端和虛擬化環境中部署 VM-Series。

VMware NSX 專用 VM-Series

NSX 專用 VM-Series 是緊密整合式解決方案，結合 VM-Series新世代防火牆、Panorama 及 VMware NSX，可發揮軟體定義式資料中心的效用。深入瞭解 **NSX 專用 VM-Series**。

VMware ESXi 專用 VM-Series

ESXi 伺服器上的 VM-Series 非常適合網絡環境，虛擬形式有助於簡化並提升彈網路的彈性。常見的部署情況包括實體空間有限的環境，以及很難運送硬體的遠端地點。深入瞭解 **ESXi 專用 VM-Series**。

Microsoft Hyper-V 專用 VM-Series

Hyper-V 專用 VM-Series 能夠使用 Hyper-V 安全地啟用資料中心內部署的應用程式。深入瞭解 **Hyper-V 專用 VM-Series**。

Microsoft Azure 專用 VM-Series

Azure 專用 VM-Series 能夠讓您將採用 Microsoft 堆疊 (Windows® Server、SQL Server、.NET Framework) 建立的應用程式安全地延伸到公共雲端。深入瞭解 **Azure 專用 VM-Series**。

Amazon Web Services 專用 VM-Series

Amazon® Web Services (AWS) 專用 VM-Series 能夠運用新世代防火牆和進階威脅預防功能保護 AWS 部署。深入瞭解 **AWS 專用 VM-Series**。

Citrix SDX 專用 VM-Series

Citrix NetScaler SDX 專用 VM-Series 將安全和應用程式傳遞控制器 (ADC) 功能整合於單一平台，提供全面的雲端服務來提升應用程式的可用性、安全和效能。深入瞭解 **vCloud Air** 專用 VM-Series。

KVM 專用 VM-Series

核心虛擬機器 (KVM) 專用 VM-Series 能夠讓服務供應商和企業將新世代防火牆和進階威脅預防功能加入 Linux® (CentOS/RHEL 和 Ubuntu®) 虛擬化和雲端計劃中。

深入瞭解 **KVM 專用 VM-Series**。

VMware vCloud Air 專用 VM-Series

vCloud Air 專用 VM-Series 可讓您使用保護 ESXi 型私人雲端所用的相同安全應用程式啟用政策，保護 VMware 型公共雲端。深入瞭解 **vCloud Air** 專用 VM-Series。

VM-Series 效能與功能

虛擬機器大小、指派的核心數和專用記憶體容量之類的許多因素都會影響效能。下列的效能和功能都是在受控制的實驗室條件下使用支援的最大核心數，透過以下的測試條件測得：

防火牆輸送量和 IPsec VPN 是在啟用 App-ID™ 應用程式識別技術和 User-ID™ 使用者識別技術的情況下，進行 64K HTTP 交易時測得。

- 在啟用 App-ID、User-ID、IPS、防毒和反間諜軟體功能的情況下，進行 64K HTTP 交易時測得的威脅防護輸送量。
- 每秒連線數是以 4K HTTP 交易測得。

建議另行在您的環境中測試，以確保符合功能需求。如需所有 VM-Series 功能和能力的完整清單，請造訪 www.paloaltonetworks.com/comparefirewalls。

型號	VM-50 (2 個核心)	VM-100 (2 個核心)	VM-300 (4 個核心)	VM-500 (8 個核心)	VM-700 (16 個核心)
防火牆輸送量 (啟用 App-ID)	不適用	2 Gbps	4 Gbps	4 Gbps	4 Gbps
威脅防護輸送量	不適用	1 Gbps	2 Gbps	4 Gbps	4 Gbps
IPsec VPN 輸送量	不適用	1 Gbps	2 Gbps	3.5 Gbps	3.5 Gbps
每秒新工作階段數量	不適用	9K	9K	20K	40K
最大工作階段數量	不適用	250K	800K	2M	10M
系統需求					
支援的核心 (最小/最大)	不適用	0.4/2	2/4	2/8	2/16
記憶體 (最小)	不適用	6.5GB	9GB	16GB	56GB
磁碟機容量 (最小/最大)	不適用	60GB	60GB	60GB	60GB

4401 Great America Parkway
Santa Clara, CA 95054

總部辦公室：+1.408.753.4000
銷售專線：+1.866.320.4788
支援專線：+1.866.898.9087

www.paloaltonetworks.com

© 2017 Palo Alto Networks, Inc. Palo Alto Networks 是 Palo Alto Networks 的註冊商標。您可在以下網址檢視我們的商標名單：http://www.paloaltonetworks.com/company/trademarks.html。本文提及的所有其他商標可能是其各自公司的商標。pan-vm-series-next-generation-firewall-ds-011117