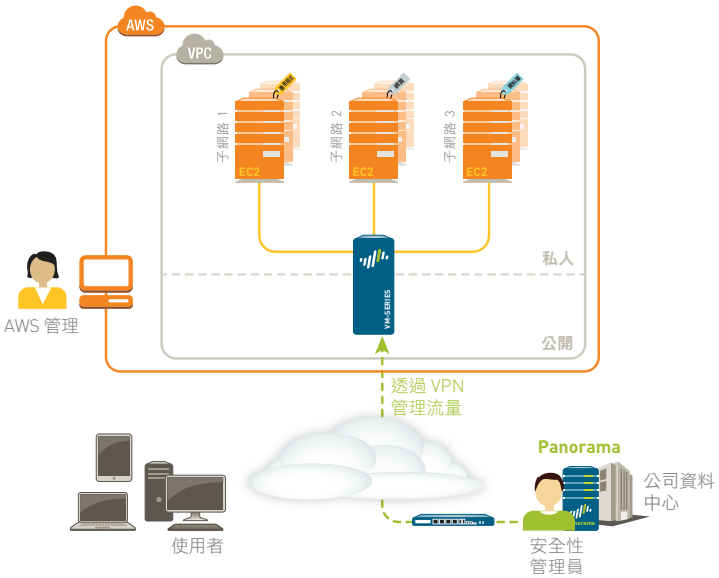
Amazon 網頁服務專用 VM-Series

重要安全性功能：

Palo Alto Networks® 防火牆可為貴組織賦予彈性，在虛擬私有雲 (VPC)、Amazon 網頁服務 (AWS) 內的執行個體上，維護新一代安全性服務。

- 識別並控制進入及通過 VPC 的流量、依使用者限制應用程式存取、封鎖已知及未知威脅。
- 自動化安全性原則更新以與 VPC 中的變更保持同步。
- 使用零信任原則（永不信任、一律驗證）來隔離並區隔業務關鍵應用程式及資料。



Amazon 網頁服務 (AWS) 提供多種全球運算、應用程式、儲存及部署服務，只需在 AWS 內建立虛擬私有雲 (VPC)，便能迅速且有效地延伸雲端運算。當您將業務關鍵應用程式及資料移轉至 VPC 時，應謹慎考量安全性。

具體而言，保護 VPC 需要哪些安全性功能，而彈性雲端運算 (EC2) 執行個體上所部署的虛擬工作負載中出現變更時，這些安全性功能部署是否能與其保持同步？AWS 專用 VM-Series 可利用實體防火牆設備和預設的自動化同步功能（可在您的 EC2 執行虛擬機變更時動態更新安全性原則）所提供的新一代防火牆及進階威脅防護功能來解決這些關鍵挑戰。

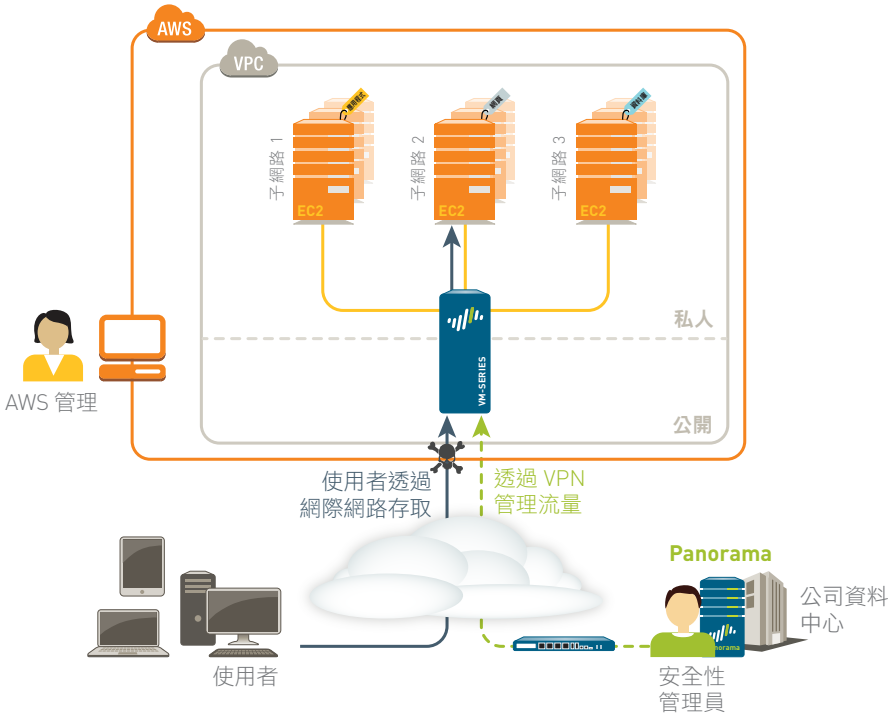
AWS 專用 VM-Series 預設可分析所有流量，以執行應用程式識別、內容以及使用者身分、其內容以及使用者身分。應用程式、內容及使用者身分接著將作為安全性原則的重要元件使用，讓您可隔離業務關鍵應用程式，並保護它們免於已知及未知的網路威脅。

為確保安全性能與 VPC 中的變更保持同步，VM 監控、動態位址群組等原生自動化功能可讓您主動監控 EC2 執行個體中的變更、自動將內容直接輸入原則，從而排除虛擬環境基礎結構進行變更時的原則延遲生效的時間，以及變更整合至防火牆安全性原則的時間。

paloalto networks

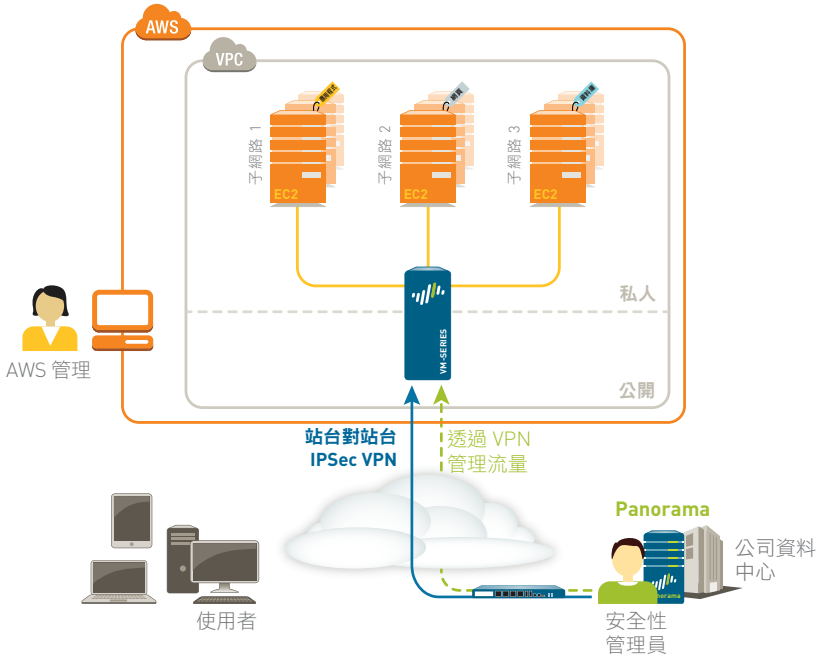
AWS 專用 VM-SERIES 使用案例：周邊閘道

建立 VPC 與建立新的實體網路（包括新的邊際防火牆）之間沒有顯著差異。在本使用案例中，VM-Series 可作為閘道防火牆部署，並以應用程式作為防護 VPC 的基礎，無論連接埠為何、檢查流量是否存在已知或未知威脅，都能同時根據使用者的身分來控制存取。新增或變更 EC2 工作負載時，VM 監控及動態位址群組可讓您的安全性原則與雲端運算變更保持同步。



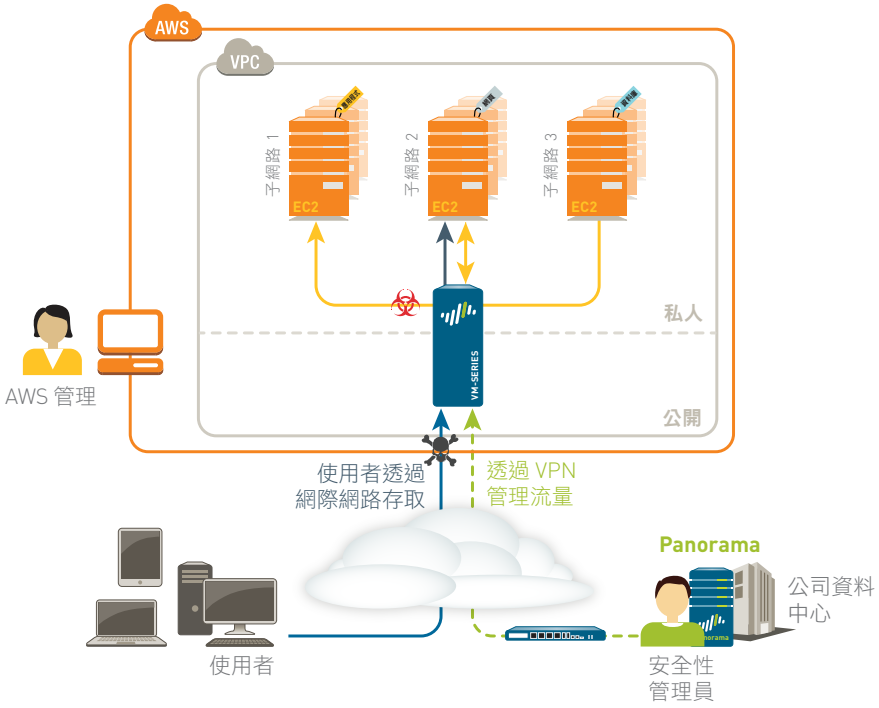
AWS 專用 VM-SERIES 使用案例：IPSEC VPN 到公司網路

VPC 是公司運算環境的延伸，讓您可以迅速擴充，同時將資本及作業費用降到最低。在本使用案例中，VM-Series 所能支援的功能，與實體防火牆設備完全相同，包括標準的點對點 IPSec VPN。您可將 VM-Series 設定為建立 IPSec VPN 連線，根據應用程式、個別內容及使用者身分來控制存取。實際上，您可將控制公司網路的相同原則延伸至 VPC。同樣地收集動態、內容變更的自動化功能可用於虛擬及實體防火牆設備，使原則與應用程式環境中的任何變更保持同步。



AWS 專用 VM-SERIES 使用案例：VM 至 VM 安全性

近期幾宗知名的威脅事件指出，網路罪犯習慣於繞過邊界控制，便藏身於明顯之處，之後便能肆意在網路中移動。在實體網路中，您可以使用零信任原則（永不信任、一律驗證）來區隔網路以保護應用程式及資料。在您的 VPC 中，您可使用 VM-Series 實施相同的零信任原則，以根據應用程式及使用者控制 IP 子網路間的流量，同時檢查是否存在網路威脅。在此情況下，自動化功能可監控 EC2 執行個體變更，將內容輸入原則以動態保持安全性最新狀態。



摘要

AWS 專用 VM-Series 可讓您利用新一代防火牆及進階威脅防護服務來保護您的 VPC。進入及通過您 AWS 部署的流量將根據應用程式識別並加以保護，接著檢查是否存在已知及未知網路威脅。原生 VM-Series 自動化功能可協助確保安全性原則與 VPC 中的任何內容虛擬機變更保持同步，而 Panorama 可讓您集中管理整個 Palo Alto Networks 實體及虛擬設備部署。

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

主要電話： +1.408.753.4000
銷售專線： +1.866.320.4788
支援專線： +1.866.898.9087

www.paloaltonetworks.com