PANORAMA

安全部署是件複雜的事情，複雜的安全性規則及來自多個來源的海量資料都可能讓 IT 團隊應接不暇。Panorama™ 網路安全管理讓您的操作更加簡便，並且整合了政策產生和集中管理功能的解決方案。利用領先業界的功能以及高效率的規則基礎，集中設定並控制防火牆，對網路流量及威脅進行深度掌控。

主要的安全性功能

管理

- **集中部署企業政策，並可搭配區域性或功能性政策以獲得最大彈性**
- **在區域性層級委派適當的管理控制層級，或以角色為基礎的管理方式進行全域委派**
- **將裝置組成邏輯式、階層式的裝置群組，以獲得更佳的管理彈性**
- **利用範本堆疊來進行簡易的裝置與網路設定**
- **現有的裝置設定能夠輕易匯入 Panorama**

可視性與安全性

- **自動關聯威脅指標，以改善網路中受攻擊主機的可視性和確認**
- **集中分析、檢查與報告網路流量、安全事件以及管理方面的修改**
- **檢視應用程式、使用者、內容以及安全威脅等的高度可自訂圖形摘要**
- **產生能檢視應用程式與威脅流量、SaaS 用量，以及跨設定使用者行為的可行動與可自訂報告**

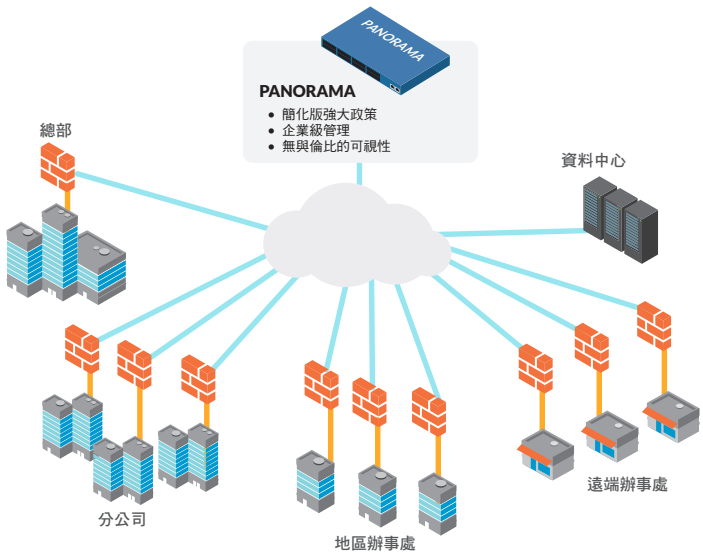

圖 1：Panorama 部署

簡化版強大政策 - Panorama 網路安全管理為不斷變化的網路及威脅情勢提供靜態規則。將單一安全規則基礎用於防火牆、威脅防護、URL 篩選、應用程式感知能力、使用者識別、沙箱、檔案封鎖以及資料篩選來管理您的網路安全。這個關鍵的簡化方案，搭配上動態的安全更新，能減少系統管理員的工作量，同時增進整體安全狀態。

企業級管理 - Panorama 會時刻考慮到企業使用者的需求。從單一主控台便能控制您的網路與資料中心的邊緣，以及您在私有與公共雲端的部署。Panorama 能透過虛擬設備及我們的專用設備進行部署，或者也可以結合兩者進行部署。利用設備來作為 Panorama 的管理單位，或是在階層式部署選項中作為紀錄收集器。隨著網路成長，您只需要新增紀錄收集器，其他的就交給我們吧。

無與倫比的自動化可視性與感知能力 - 自動關聯威脅，搭配預先定義的關聯物件集，能減少巨量資料堆積。它能夠在海量資訊中識別遭到入侵的主機以及相關聯的惡意行為。這進一步減少了嚴重威脅的在您網路中的停留時間。簡潔且可完全自訂的 Application Command Center (應用程式控管中心 - ACC)，能為目前與歷史網路及威脅資料提供全面性的深入見解。

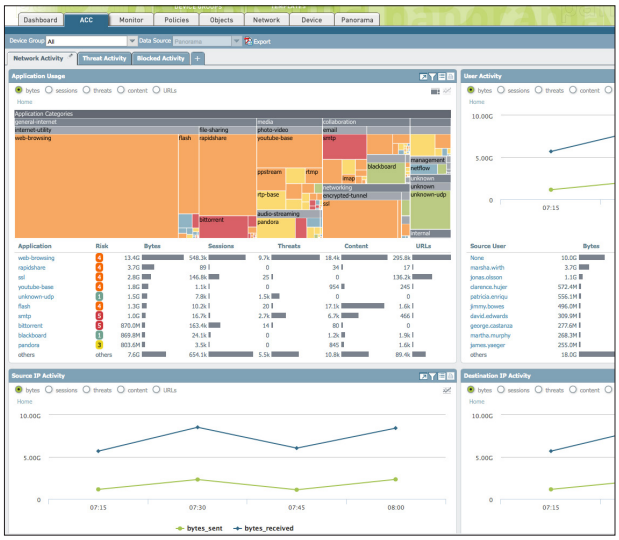

圖 1：ACC

強大的網路可視性：Application Command Center (應用程式控管中心)

使用來自 Panorama 的 Application Command Center (應用程式控管中心 - ACC) 功能，能讓您以高互動性圖形化的方式，檢視在PaloAltoNetworks®防火牆中穿梭的應用程式、URL、威脅及資料 (檔案及形式)。ACC 包含以頁籤檢視網路活動、威脅活動及封鎖活動，而每個頁籤都包含相關 Widget工具，能夠讓您提供網路流量模式的更佳視覺化效果。可以建立自訂頁籤，當中包含許多 Widget 工具，能夠讓您深入考察對系統管理員最重要的資訊。ACC 提供可完全自訂的全方位檢視內容，不僅包括現有資料，也提供歷史資料。

在 URL 類別上的額外資料與威脅則能提供一份完整且全面的網路活動紀錄。ACC 提供的可視性能讓您做出知情的政策決策，並快速對潛在安全威脅做出回應。

縮短回應時間：自動關聯引擎

內建於新世代防火墻中的自動關聯引擎能揭示出可能潛藏於網路中的重大威脅。它包含由 Palo Alto Networks 威脅研究團隊所定義的關聯物件。這些物件能識別有惡意跡象的可疑流量模式或一系列行動。有些關聯物件能識別從 WildFire™ 雲端型威脅分析服務中所觀察到的惡意軟體樣本的動態模式。

簡易政策控制：安全地啟用應用程式

安全啟用應用程式表示允許存取特定應用程式，並且會先透過套用特定的威脅防護、QoS、以及檔案、資料或 URL 篩選政策進行防護。Panorama 讓您能以單一安全規則基礎設定政策，並簡化網路中匯入、複製或修改規則的流程。在政策與物件上結合全域與區域性管理控制功能，可讓您在全域層級獲得一致的安全性，以及在本機層級獲得彈性。

企業級管理

部署階層式裝置群組能確保低階層群組繼承高階層群組的設定。這樣可以簡化集中管理，並讓您依據功能和位置整理裝置，無需重複設定。範本堆疊讓網路與裝置的設定更為簡化。除此之外，新世代防火牆與管理功能使用相同的使用者介面，讓管理變得更加直覺化。全域尋找與標籤式規則群組等功能讓 IT 系統管理員能夠輕鬆利用網路中的所有資訊。

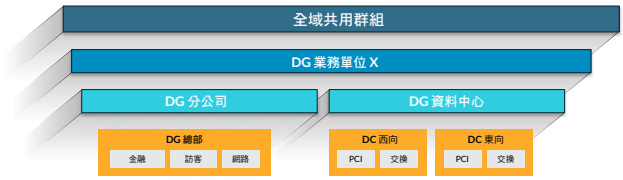

圖 2：裝置群組階層

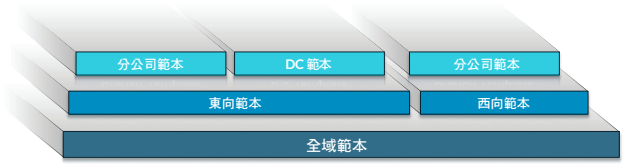

圖 3：範本堆疊

流量監控：分析、報告與鑑識

Panorama 從實體以及 Traps™ 進階端點防護的虛擬防火牆中擷取出日誌，並將其儲存在自身的日誌儲存區中。在您執行紀錄查詢並生成報告時，Panorama 也會從其日誌儲存區中動態擷取出相關日誌，並將結果展示給使用者。

- **日誌檢視器：**無論是在個別裝置、所有裝置或是 Traps 上，您都可藉由點選儲存格值以使用動態日誌篩選來快速檢視日誌活動，或使用表達式建立程式來定義排序規則。可儲存結果以供未來查詢，或者輸出以供未來分析。
- **自訂報告：**預先定義的報告可以依原樣使用，或者群組為單一報告以符合特定的要求。
- **使用者活動報告：**使用者活動報告可顯示所使用過的應用程式、瀏覽過的 URL 類型、網站，以及個別使用者在指定期間內所瀏覽過的所有 URL。Panorama 可藉由使用者活動的彙總檢視來建立報告，無論他們受保護的防火牆為何，或無論他們可能使用的 IP 或裝置為何。

- **SaaS 報告：**SaaS 用量與威脅報告能提供所有防火牆 SaaS 活動與相關威脅的詳盡可見度。
- **日誌轉送：**Panorama 能將所有從 Palo Alto Networks 防火牆處收集的日誌轉寄至遠端目的地，用作長期儲存、鑑識與合規報告等目的。Panorama 能轉寄所有或特定日誌、SNMP 設陷以及電子郵件通知至遠端紀錄目的地，如 syslog 伺服器 (透過 UDP、TCP 或 SSL)。除此之外，Panorama 能開始工作流程，並將日誌寄送至提供 HTTP 式 API 的第三方服務，例如票券服務或系統管理產品等。

Panorama 管理架構

Panorama 可讓組織使用全域監控與區域性控制的模型來管理其 Palo Alto Networks 防火牆。Panorama 提供數種全域或集中化管理工具：

- **範本/範本堆疊：**Panorama 可以透過範本來管理通用的裝置與網路組態。可使用範本以集中方式管理組態，然後推送變更到受管理的防火牆。這種方法可以避免在眾多裝置上，對個別的防火牆重複進行相同的變更。為了讓過程更加簡便，範本可以在裝置與網路設定期間進行堆疊，並作為建置組塊使用。
- **階層式裝置群組：**Panorama 可透過階層式裝置群組管理通用的政策與物件。多層級的裝置群組可用於集中管理許多具有共同要求的部署位置政策。裝置群組階層能根據地理位置 (例如：歐洲、北美和亞洲)、職責 (例如：資料中心、主園區和分公司)、兩者混合或其他標準來建立。這可允許在裝置上的不同虛擬系統間分享通用的政策。

您可以使用通用的政策來進行全域控制，同時提供區域防火牆系統管理員依照其需求做出特定調整的自主性。在裝置群組層級，您可以建立被定義為是第一組規則 (預先規則) 以及最後一組規則 (後續規則) 的共用政策，以便針對配對規則進行評估。可以在受管理的防火牆上檢視預先規則與後續規則，但是只能在已經被定義的管理角色的範圍內，從 Panorama 進行編輯。裝置規則 (介於預先與後續規則之間的規則) 可以由區域防火牆系統管理員編輯，或者由已經切換成防火牆裝置範圍內的 Panorama 管理員編輯。此外，組織可以使用由 Panorama 管理員所定義，可被區域管理的裝置規則參照的共用物件。

- **以角色為基礎的管理：**以角色為基礎的管理是用於委派功能層級的管理存取，包括不同員工成員的資料可用性 (啟用、唯讀，或停用與隱藏檢視)。

特定個人可獲得與其工作相關的任務所需的適當存取權限，同時使其他權限為隱藏或唯讀。管理員可以不受其他管理員所做的變更所影響，獨立交付或還原他們在 Panorama 設定中所進行的變更。

軟體、內容與授權更新管理：由於部署的規模會越來越大，因此您可能必須確保能以有序的方式將更新傳送到下游裝置內。例如，安全團隊可能偏好以集中方式驗證軟體更新，然後透過 Panorama 將更新傳送到所有防火牆產品。透過 Panorama，可以使用集中方式來管理軟體更新、內容 (應用程式更新、防毒特徵碼、威脅特徵碼、URL 篩選資料庫等) 與授權。

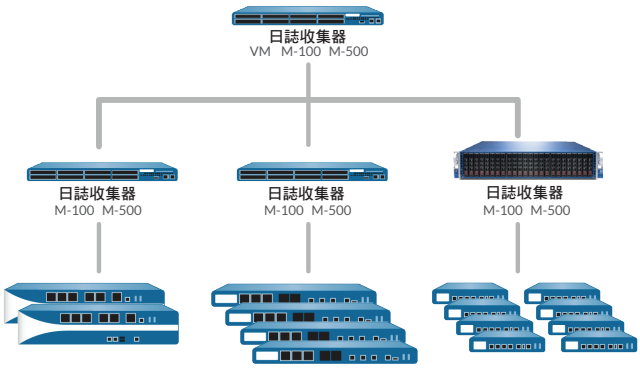

圖 3：Panorama 架構

使用範本、裝置群組、以角色為基礎的管理方式與更新管理，您可以在全域及區域層級委派適當的存取權限給所有管理職能、視覺化工具、政策建立、報告與紀錄。

部署彈性

組織可以將 Panorama 搭配硬體設備部署或作為虛擬設備部署。

硬體設備

Panorama 能部署於 M-100 或 M-500 管理設備上，而個別管理與紀錄組件能以分散方式區隔，以配合大量的紀錄資料。在這些設備上執行的 Panorama 可以使用以下方式部署：

- **集中式：**此情況下，所有 Panorama 管理及紀錄功能都將集中在單一裝置內處理 (具備高可用性選項)。
- **分散式：**您可將多個裝置的管理和記錄功能分開，並將管理器和記錄收集器功能分隔。
- **Panorama 管理員：**Panorama 管理員負責在所有受管理裝置上處理與政策及裝置設定相關的所有工作。管理員並不會在本機儲存記錄資料，而是使用個別的日誌收集器來處理記錄資料。管理員分析儲存在日誌收集器內的資料以進行集中化報告。
- **Panorama 日誌收集器：**擁有龐大紀錄量與紀錄保留需求的組織可以部署專屬的 Panorama 日誌收集器裝置，這些裝置將從多個受管理的防火牆彙總日誌資訊。

將管理與日誌收集分隔後，可以讓您最佳化 Panorama 的部署方式，以符合規模彈性、組織及地理的需求。

虛擬設備

您也可以在 VMware® ESXi™ 上將 Panorama 部署成為虛擬設備，並允許組織支援其虛擬化提案，與壓縮資料中心內有時有限又昂貴的機櫃空間。

虛擬設備可當成 Panorama 管理員使用，並負責在所有受管理裝置上處理與政策及裝置設定相關的所有工作。可以使用兩種方式來進行部署：

- **集中式：**將所有 Panorama 管理及紀錄功能都將壓縮到單一虛擬裝置內 (具備高可用性選項)。
- **分散式：**Panorama 分散式日誌收集功能需要混用各種硬體與虛擬設備。

注意：虛擬設備不得用作 Panorama 日誌收集器。Panorama 日誌收集器 (M-100 或 M-500 設備) 要負責分載密集的日誌收集與處理任務。

擁有硬體或虛擬化設備的選擇，以及結合或分隔 Panorama 功能的選擇，提供您在分散式網路環境下管理多部 Palo Alto Networks 防火牆的最大彈性。

Panorama 規格
支援的裝置數量
• 最多 1,000
高可用性
• 主動/被動
管理員驗證
• 本機資料庫 • RADIUS
管理工具和 API
• 圖形化使用者介面 (GUI) • 命令列介面 (CLI) • 基於 XML 的 REST API

虛擬設備規格
最低伺服器需求
• 81 GB 硬碟 • 8 CPU 核心 • 16 GB RAM
VMware 支援
• VMware ESX 3.5、4.0、4.1、5.5、6.5
支援瀏覽器
• IE v7 或更高版本 • Firefox v3.6 或更高版本 • Safari v5.0 或更高版本 • Chrome v11.0 或更高版本
日誌儲存
• VMware 虛擬磁碟：最大 24 TB

M-100 Panorama 設備

M-500 Panorama 設備

M-100 設備
I/O
• (4) 10/100/1000、[1] DB9 主控台序列埠、(1) USB
儲存空間
• 最高設定：RAID：8 x 2 TB RAID 認證 HDD，用於 8 TB 的 RAID 儲存
電源/最大耗電量
• 500W/500W
最高 BTU/小時
• 1,705 BTU/小時
輸入電壓 (輸入頻率)
• 100-240 VAC (50-60Hz)
最大電流消耗
• 10A @ 100 VAC
平均故障間隔 (MTBF)
• 14.5 年
機架安裝 (尺寸)
• 1U，19" 標準機架 (1.75" 高 x 23" 深 x 17.2" 寬)
重量
• 26.7 磅
安全性
• UL、CUL、CB
EMI
• FCC Class A、CE Class A、VCCI Class A
環境
• 作業溫度：40 至 104 °F，5 至 40 °C • 非作業溫度：-40 至 149 °F，-40 至 65 °C

M-500 設備
I/O
• (4) 10/100/1000、(1) DB9 主控台序列埠、(1) USB 連接埠、(2) 10 GigE 連接埠
儲存空間
• 最高設定：RAID：24 x 2 TB RAID 認證 HDD，用於 24 TB 的 RAID 儲存 • 預設的出貨設定：4 TB：8 x 1TB RAID 認證 HDD，用於 4 TB 的 RAID 儲存
電源/最大耗電量
• 雙電源、熱交換備援 • 1200W/493W (全系統)
最高 BTU/小時
• 1,681 BTU/小時
輸入電壓 (輸入頻率)
• 100-240 VAC (50-60 Hz)
最大電流消耗
• 4.2A @ 120 VAC
平均故障間隔 (MTBF)
• 6 年
機架安裝 (尺寸)
• 2U，19" 標準機架 (3.5" 高 x 21" 深 x 17.5" 寬)
重量
• 42.5 磅
安全性
• UL、CUL、CB
EMI
• FCC Class A、CE Class A、VCCI Class A
環境
• 作業溫度 50 至 95 °F，10 至 35 °C • 非作業溫度 -40° 至 158 °F，-40° 至 65 °C

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

panorama-ds-121216