Panorama

安全部署的安全性規則相當複雜以及來自多個來源的數據都可能讓IT團隊應接不暇。Panorama™ 網路安全管理，讓您輕鬆實現整合式的政策建立和集中化管理功能。您可以集中佈建防火牆，並使用業界領先的功能有效建立安全規則，同時對網路流量及威脅進行深入掌控。

主要功能

管理

- 用於組織政策的裝置群組、階層和標籤
- 可重用網路設定的範本堆疊
- 管理員特定的認可以避免意外變更
- 輕鬆的軟體更新及升級
- 分公司的 SD-WAN 連線
- 零接觸佈建 (ZTP) 可簡化遠端網站的防火牆上線和佈建

可視性

- 涵蓋整個基礎結構的集中化可視性
- 可實際運用的相互關聯分析
- 健全狀況分析可增進對於裝置使用情況的瞭解

安全性

- 使用 PAN-OS® 收集的情報將舊版規則輕鬆轉型至應用程式型規則
- 可減少攻擊面並改善安全狀況的規則使用情況分析
- 最新的安全內容更新的集中化部署

自動化

- 第三方系統上的日誌過濾和自動化動作
- 動態環境的自動化政策部署
- 可供輕鬆整合的 XML 型以及 JSON 型 REST API

簡潔而強大的政策

Panorama 是安全管理解決方案，可為不斷變化的網路及威脅形勢提供一致的規則。將單一安全規則基礎套用於防火牆、威脅防禦、URL 篩選、應用程式感知、使用者識別、沙箱、檔案封鎖、存取控制以及數據篩選，整合管理您的網路安全性。關鍵性的簡化以及 App-ID™ 技術型的規則、動態安全更新和規則使用情況分析，可減輕管理上的工作負載並改善您的整體安全狀況。

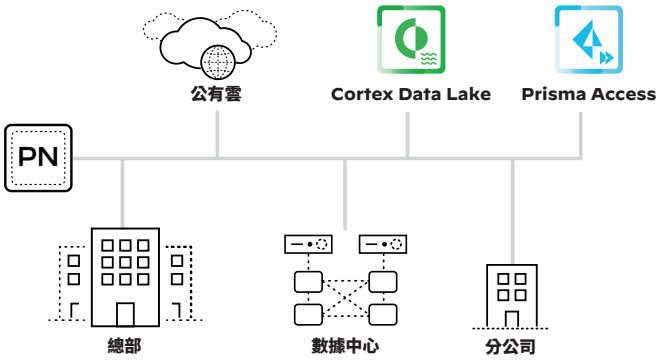

圖 1：Panorama 部署

一致的管理

Panorama 始終考量企業使用者的需求。您可從單一主控台控制您的網際網路邊緣，以及您的私有雲與公有雲部署。無論是在內部部署中託管還是在雲端託管，Panorama 皆能為您提供一致的可視性，以及對南北向和東西向流量的管理。這能夠針對任何形式 (實體、虛擬、雲端交付和容器化) 為所有防火牆群組集中管理裝置和安全設定。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。

集中化可視性和自動化

自動化威脅關聯，可搭配預先定義的關聯物件集，減少巨量數據堆積。並能識別遭到入侵的主機，建立惡意行為之間的關聯性以避免其隱匿在雜訊之中，進而減少您網路中嚴重威脅的停留時間。簡潔且能完全自訂的應用程式控管中心 (ACC)，能為您目前與歷史的網路及威脅數據提供全面性的深入見解。

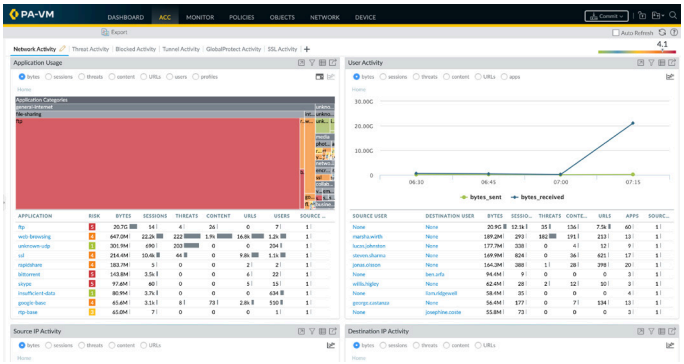

圖 2：應用程式控管中心

無與倫比的規模

運用具備高可用性的一對 Panorama 設備管理最多 5,000 個新世代防火牆，或使用 Panorama 互連外掛程式對於數以萬計的裝置集中進行設定管理和存取控制。

全面可視性和管理

ACC 可讓您以互動性圖形化的方式，檢視在 Palo Alto Networks 防火牆中穿梭通行的應用程式、URL、威脅、數據檔案與模式。ACC 包含索引標籤式的網路活動、威脅活動及封鎖活動檢視內容，而每個頁籤都包含相關 Widget 工具，為網路中的流量模式提供更佳的視覺化效果。您可以建立包含 Widget 工具的自訂索引標籤，讓您能深入掌握系統管理員所需的重要資訊。ACC 提供現有數據及歷史數據可完全自訂的全方位檢視。

有關 URL 類別與威脅的額外數據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，可協助您做出明智的政策決策，快速對潛在安全威脅做出回應。

縮短回應時間

內建於新世代防火牆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。這其中包括關聯物件，可辨識出可疑流量模式或有惡意跡象的一連串行動。有些關聯物件能識別 WildFire® 惡意軟體防禦服務在惡意軟體範本中所觀察到的動態模式。

簡易政策控制

安全啟用應用程式表示允許存取特定應用程式，並透過 Threat Prevention 和存取控制，以及檔案、數據和 URL Filtering 的特定政策進行防護。您可以將大量的舊版規則庫轉型成為直覺式政策，強化安全並大幅節省管理時間。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，同時在區域層級獲得彈性。

易於使用的集中化管理

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。如此便能簡化中央管理，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精簡。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。IT 系統管理員可透過面向所有規則的全域尋找、稽核註解、通用唯一識別碼 (UUID)，以及標籤式規則群組等功能，輕鬆運用網路中的所有資訊。

提升行動工作者可視性和疑難排解

GlobalProtect™ 端點網路安全將新世代防火牆功能擴展到行動工作者。您可以運用 Panorama，在所有階段獲得對於使用者連線失敗的更佳的可視性，使用驗證日誌來協助您解決使用者帳戶的問題，並依據 GlobalProtect 日誌中的特定數據執行存取控制。

流量監控：分析、報告與鑑識

Panorama 會從實體和虛擬化防火牆、Cortex® Data Lake 和 Cortex XDR™ 代理程式中擷取和儲存日誌。在您執行日誌查詢並產生報告時，Panorama 也會從其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 Cortex XDR 代理程式上，您都可藉由按一下儲存格值以使用動態日誌篩選來快速檢視日誌活動，或使用運算式產生器來定義排序準則。您也可以儲存結果以供日後查詢，或是匯出結果執行進一步分析。
- **自訂報告：**預先定義的報告可以直接使用、進行自訂，或者編組為單一報告以符合特定的要求。
- **使用者活動報告：**這些報告可顯示所使用過的應用程式、造訪過的 URL 類別和網站，以及個別使用者在指定期間內造訪過的所有 URL。無論使用者的裝置或 IP，以及保護特定使用者的防火牆為何，Panorama 都能藉由使用者活動的彙總檢視來建立這些報告。
- **SaaS 報告：**軟體即服務 (SaaS) 用量與威脅報告可提供防火牆上所有 SaaS 活動與相關威脅的詳盡可視性。
- **日誌轉送：**Panorama 可以轉送 Cortex XDR 代理程式和 Palo Alto Networks 防火牆的日誌，藉以進行儲存、鑑識、報告等等。可以透過 UDP、TCP 或 SSL 將所有或選取的日誌、SNMP Traps 和電子郵件通知轉送到遠端目標。Panorama 也可以將日誌傳送到 HTTP 式 API 的第三方供應商，例如票證服務或系統管理產品。

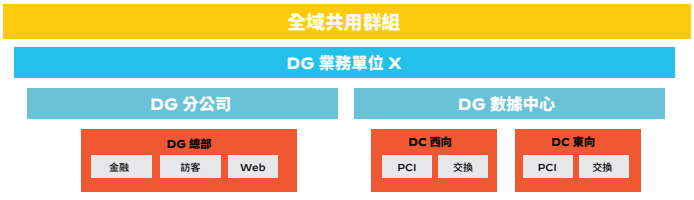

圖 3：裝置群組階層

圖 4：範本堆疊

Panorama 管理架構

Panorama 協助您使用具全域監控與區域性控制的模型來管理您的 Palo Alto Networks 防火牆。Panorama 提供多種全域或集中化管理工具。

範本/範本堆疊

Panorama 透過範本來管理通用的裝置與網路設定，如此便可集中管理設定，並將變更推送至受管理的防火牆。此方法可避免在眾多裝置上對個別的防火牆重複進行相同變更的作業需要。為了讓過程更加簡便，範本可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所有部署位置的政策。裝置群組階層的建立可根據地理位置 (例如：歐洲、北美和亞洲)、職責 (例如：數據中心、主園區和分公司)、結合兩者，或依據其他準則，藉此在裝置上的不同虛擬系統間共用常見政策。

您可以使用共同政策來進行全域控制，同時允許區域防火牆管理員依照其需求自主做出特定調整。在裝置群組層級，您可以分別建立定義為第一組以及最後一組的規則 (即預先規則和後續規則) 的共用政策，以便針對比對規範進行評估。可以在受管理的防火牆上檢視預先規則與後續規則，但是只能在已經定義的管理角色的範圍內，通過 Panorama 對其進行編輯。

裝置規則 (介於預先與後續規則之間的規則) 可以由區域防火牆管理員編輯，或者由已經切換到防火牆裝置範圍內的 Panorama 管理員編輯。此外，企業可以使用由 Panorama 管理員所定義、且區域管理的裝置規則可參照的共用物件。

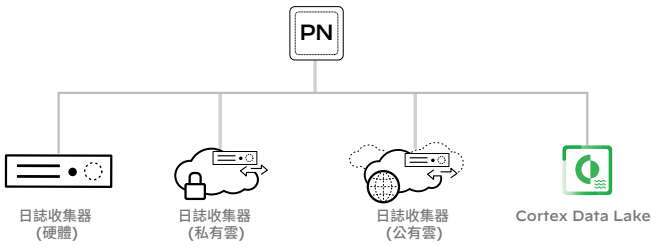

圖 5：Panorama 日誌管理

依據角色進行的管理

依據角色進行的管理用於委派功能層級的管理存取，包括不同員工成員的數據可用性，例如啟用、唯讀，或停用與隱藏檢視。

您可以授予特定個人存取與其工作相關之任務所需的適當權限，並將其他權限設為隱藏或唯讀。管理員可以不受其他管理員所做的變更影響，獨立交付或還原他們在 Panorama 設定中所進行的變更。

軟體、授權更新，以及內容管理

隨著部署持續擴展，您需要確保能以有序的方式將更新傳送到下游裝置內。例如，安全團隊可能偏好集中驗證軟體更新，然後透過 Panorama 將更新傳送到所有防火牆產品。Panorama 可讓您集中管理軟體更新、授權和內容的更新程序，包括應用程式更新、防毒特徵碼、威脅特徵碼、URL Filtering 數據庫項目等。

您可以運用範本、裝置群組、依據角色進行的管理方式與更新管理，在全域及區域層級為所有管理職能、視覺化工具、政策建立、報告與記錄委派適當的存取權限。

部署彈性

您可以將 Panorama 部署為硬體設備或是虛擬設備。

硬體設備

Panorama 可以部署為 M-200 或 M-600 管理設備。

虛擬設備

Panorama 可以在下列位置部署為虛擬設備：VMware ESXi™、KVM、Nutanix、OCI 和 Microsoft Hyper-V®；在包括 Google Cloud Platform (GCP®)、Amazon Web Services (AWS®)、AWS GovCloud、Alibaba Cloud、Microsoft Azure® 和 Azure GovCloud 等公有雲環境中。

部署模式

您可以使用部署模式，將 Panorama 的管理功能與記錄功能分開。支援的三種部署模式包括：

1. **僅用於管理：**Panorama 會管理受管理裝置的設定，但並不收集或管理日誌。
2. **Panorama：**Panorama 會控制所有受管理裝置的政策和日誌管理功能。
3. **日誌收集器：**Panorama 會收集並管理受管理裝置的日誌。此時將假設其他 Panorama 部署在「僅用於管理」模式中作業。

部署規模

Panorama 互連外掛程式可連接多個 Panorama 執行個體，將防火牆管理擴展到數萬個防火牆。Panorama 控制器會利用外掛程式讓您同步設定、快速將防火牆上線，並從單一集中位置排程內容更新 (見圖 6)，進而簡化所有防火牆的管理，無論其位於內部部署或雲端位置。

注意：*僅於 M-600 設備或具備類似資源的 VM 上支援 Panorama 互連。*

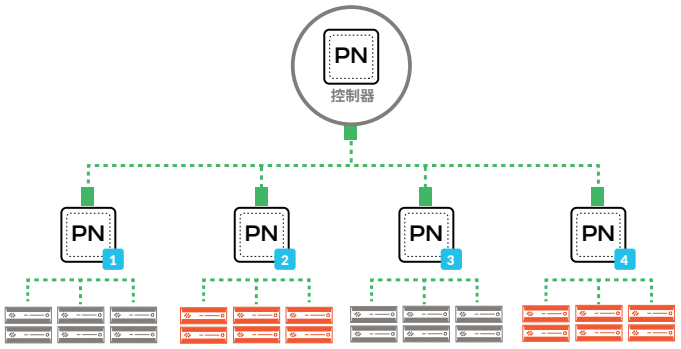

圖 6：所有防火牆的同步設定

表 1：Panorama 設備硬體規格

	M-200	M-600
I/O	10/100/1000 (4)、DB9 主控台序列埠 (1)、USB 連接埠 (1)	10/100/1000 (4)、DB9 主控台序列埠 (1)、USB 連接埠 (1)、10 個 GigE 連接埠 (2)
儲存	最高設定：8 TB RAID 認證 HDD (4)，用於 16 TB RAID 儲存 預設的出貨設定：8 TB RAID 認證 HDD (4)，用於 16 TB RAID 儲存	最高設定：8 TB RAID 認證 HDD (12)，用於 48 TB RAID 儲存 預設的出貨設定：8 TB RAID 認證 HDD (4)，用於 16 TB RAID 儲存
電源/最大耗電量	雙電源、熱插拔備援設定 750 W/300 W	雙電源、熱插拔備援設定 750 W/486 W (全系統)
最高 BTU/小時	1,114 BTU/小時	1,803 BTU/小時
輸入電壓 (輸入頻率)	100–240 VAC (50-60 Hz)	100–240 VAC (50-60 Hz)
最大電流消耗	9.5 A @ 110 VAC	4.5 A @ 220 VAC
平均無故障時間 (MTBF)	10 年	8 年
安裝機架 (尺寸)	1U，19 英吋標準機架 (1.7 x 29 x 17.2 英吋 (高 x 深 x 寬))	2U，19 英吋標準機架 (3.5 x 28.46 x 17.2 英吋 (高 x 深 x 寬))
重量	26 磅	36 磅
安全	UL、CUL、CB	UL、CUL、CB
EMI	FCC Part 15、EN 55032、CISPR 32	FCC Part 15、EN 55032、CISPR 32
環境	作業溫度：41° 至 104° F，5° 至 40° C 非作業溫度：-40° 至 140° F，-40° 至 60° C	作業溫度：41° 至 104° F，5° 至 40° C 非作業溫度：-40° 至 140° F，-40° 至 60° C

表 2：其他 Panorama 規格
支援的裝置數量
• M-200 - 多達 1,000
• M-600 - 多達 5,000
高可用性
• 主動/被動
管理員驗證
• 本機數據庫
• RADIUS
• SAML
• LDAP
• TACACS+
管理工具和 API
• 圖形使用者介面
• 命令列介面
• XML 型以及 JSON 型 REST API

表 3：Panorama 虛擬設備系統要求			
	僅用於管理模式	Panorama 模式	日誌收集器模式
支援的核心（最小）	16 個 CPU	16 個 CPU	16 個 CPU
記憶體（最小）	32 GB	32 GB	32 GB
系統磁碟	預設值：81 GB 已升級：224 GB	預設值：81 GB 已升級：224 GB	預設值：81 GB
日誌儲存容量	不支援本機日誌儲存	2 TB 至 24 TB	2 TB 至 24 TB

表 4：支援的公有雲
Alibaba Cloud、Azure、Azure GovCloud、AWS、AWS GovCloud、GCP 和 OCI

表 5：支援的私有雲
Hyper-V、KVM、Nutanix、VMware ESXi 和 vCloud Air

paloalto NETWORKS
諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓

strata_ds_panorama_042021