使用 *Panorama* 管理防火牆的最佳做法

10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

December 3, 2020

Table of Contents

將防火牆新增至 *Panorama* 的最佳做法

Panorama™ 管理伺服器是 Palo Alto Networks 網路安全性管理解決方案，用於新世代防火牆的集中管理和可視性。本文件涵蓋的最佳做法包含裝載新的防火牆，或將現有防火牆移轉至 Panorama 以簡化和流暢執行此作業。

> 使用案例 - 將新的新世代防火牆裝載至 Panorama
> 使用案例 - 將新世代防火牆移轉至 Panorama

使用案例 - 將新的新世代防火牆裝載至 Panorama

開始使用 Panorama™ 管理伺服器的第一個使用案例是以受管理裝置形式新增新部署的防火牆至 Panorama。

STEP 1 | **Associate Devices**（關聯裝置）或 **Import**（匯入）多個防火牆，以流暢執行裝載程序。

- 裝置群組、範本堆疊、收集器群組和日誌收集器已成功新增至 Panorama 之後，當您將它們從某個位置新增至 Panorama 時，請將防火牆與它們相關聯，而不是手動關聯防火牆。
- 如果您要新增大量防火牆，則請以 CSV 檔案形式將所有新的防火牆匯入至 Panorama。此 CSV 檔案可讓您將所有防火牆與裝置群組、範本堆疊、收集器群組和日期收集器相關聯，而不是手動關聯它們。如果在手動關聯防火牆時新增大量防火牆需要較長的時間才能完成，則此選項特別有用。

STEP 2 | 啟用 **Auto Push on 1st Connect**（首次連線時自動推送），並設定 **To SW Version**（至 **SW** 版本）以在裝置群組和範本堆疊設定第一次成功連線至 Panorama 並升級受管理防火牆至所選擇的指定 PAN-OS 版本時，將它們自動推送至受管理防火牆。這包含自動安裝 PAN-OS 升級路徑中每個 PAN-OS 版本的所有必要內容更新。

- 如果您要使用 CSV 檔案將所有新的防火牆匯入至 Panorama，則請啟用 **Auto Push on 1st Connect**（首次連線時自動推送），然後在 CSV 檔案中設定 **To SW Version**（至 **SW** 版本）以流暢執行匯入程序。
- 實作基於角色的存取控制時，請利用裝置群組和範本管理員以將防火牆新增至其存取網域內的裝置群組和範本，而不是啟用所有 Panorama 管理員的超級使用者權限。

STEP 3 | 在您成功將防火牆新增至 Panorama 之後，請建立和套用標籤，以簡化受管理防火牆的搜尋和篩選。這可協助您在使用 Panorama 所管理的防火牆數目成長時整理受管理防火牆。

STEP 4 | 如果您要在遠端網站中部署防火牆，而需要 IT 人員極少的幫助，甚至不需要幫助，則請設定零接觸佈建 (ZTP)，藉由自動化新的受管理防火牆裝載，而不需要遠端網站的網路或 IT 管理員的幫助，從而流暢執行初始防火牆部署。

使用案例 - 將新世代防火牆移轉至 Panorama

開始使用 Panorama™ 管理伺服器的第二個使用案例是將現有防火牆轉移至 Panorama。如果可能，請在移轉期間與 Palo Alto Networks 銷售工程師或 Professional Services 工程師合作，確保防火牆設定正確移轉至 Panorama。

STEP 1 | 規劃是重點；在您開始移轉之前，請確定您已瞭解下列各項：

- 檢閱 Palo Alto Networks 相容性矩陣以瞭解跨日誌收集器之 Panorama 與防火牆間的相容性以及內容版本，確保未在移轉期間發生相容性錯誤。
- 使用這種方法規劃裝置群組和範本階層，以減少備援和流暢執行設定管理，而這些設定會在一組防火牆內的所有防火牆之間共用。
- 準備移轉後測試規劃，確認在將防火牆成功移轉至 Panorama 之後驗證重大流量和應用程式流量。

STEP 2 | 當您移轉防火牆至 Panorama 進行管理時，請啟用 **import devices' shared objects into Panorama's shared context**（將裝置共用物件匯入至 **Panorama** 的共用內容）以避免相同設定物件重複。

STEP 3 | 成功移轉之後，請檢閱 **Policies**（政策）來識別任何重複規則。請先刪除所有重複規則，再**Commit**（提交）給 Panorama，以避免提交出錯。

STEP 4 | 當您 **Export or push device config bundle**（匯出或推送裝置設定包）至受管理防火牆時，請啟用 **Merge with Candidate Config**（與應徵者設定合併）、**Include Device and Network Templates**（包含裝置與網路範本）和 **Force Template Values**（強制範本值）以強制提交防火牆上的任何擱置本機變更、在推送中包含所有裝置群組或範本，以及刪除 Panorama 的裝置群組或範本中沒有的任何本機設定。這確保將 Panorama 所管理的基準線設定推送至所有移轉至 Panorama 的防火牆。

STEP 5 | 執行移轉後測試，確認移轉成功，以及所有事項都如預期運作。在一段時間之後，請視需要最佳化設定。使用 Expedition 這類移轉工具移除任何未用或重複物件來定期評估設定檢疫，以及使用政策最佳化工具來最佳化安全性政策規則庫。

Panorama 上防火牆設定管理最佳做法

防火牆有兩種類型的設定：安全性和網路。Panorama 使用裝置群組來管理安全性設定（例如物件和政策規則），並使用範本和範本堆疊來管理網路設定。

> 管理 Panorama 上的裝置群組設定
> 管理 Panorama 上的範本和範本堆疊設定
> 管理 Panorama 上的範本和範本堆疊變數

管理 Panorama 上的裝置群組設定

裝置群組提供方法來組織和重複使用政策，方法是套用繼承主體以及實作定義良好的裝置群組階層。Panorama 可讓您跨階層的多個裝置群組重複使用相同的裝置群組設定時，您也可以自訂任何本機設定來取代任何繼承的設定。

- 設計裝置群組階層時，請考慮功能或地區需求，以及瞭解預先規則與後續規則的差異。

  例如，在建立安全性後續規則作為任何不符合安全性預先規則之流量的清除時，建立您要受管理防火牆套用的任何安全性預先規則，沒有例外。
- 避免過度使用 **Shared**（共用）裝置群組，讓您不超出較小受管理防火牆的容量限制。管理適當裝置群組層級的設定物件有助於更有效率地最小化未同步防火牆數目，因為修改單一共用設定物件時，所有防火牆都會變成未同步。
- 使用自訂位址物件來指定位址範圍或地理位置，以設定自訂地區。

  企業使用 RFC 1918 位址空間時，管理整個 10.0.0x 網路的政策沒有幫助。而是使用自訂位址物件來指定位址範圍或地理位置，以設定自訂地區。這可讓您建立更精細且相關的政策來減少攻擊面。
- 設定每個裝置群組的**Master Device**（主要裝置），以讓 Panorama 收集使用者群組對應。在裝置群組中設定主要裝置，可在建立政策規則時使用使用者群組。此外，您還可以使用 Panorama 所收集的使用者群組對應來篩選 ACC 和監控頁籤。
- 關聯 **Reference Templates**（參考範本）以參照範本中所含的網路設定物件，而受管理防火牆不屬於該範本，以完成安全性設定。這可讓您跨裝置群組和範本完整利用一般設定物件，而不需要重複使用 **Shared**（共用）裝置群組或是重建相同的網路設定物件。

管理 Panorama 上的範本和範本堆疊設定

使用範本和範本堆疊，以針對一般設定（例如記錄和高可用性 (HA)）跨受管理防火牆重複使用網路和防火牆設定物件，同時仍然讓您可以設定可視需要針對不同範本堆疊中多個受管理防火牆合併使用的模組化範本。

- 使用邏輯設定分組來建立範本以進行模組化，即使設定不完整也是一樣。請記住，設定必須完整，而且所有參考都已在範本堆疊層級進行解析；並非每個範本。您可以重複使用、參考和取代不同範本中的物件，來完成範本堆疊設定。
- 建立模型特定範本（例如，網路介面設定），以及使用案例特定範本（例如，管理員、基於角色的存取控制集）。這可讓您在將正確範本新增至範本堆疊時將它們混合使用和比對。
- 使用您要在範本中取代或在受管理防火牆本機的網路設定，來設定範本堆疊。

管理 Panorama 上的範本和範本堆疊變數

建立範本和範本堆疊變數，來最大化跨受管理防火牆之網路和裝置設定物件的設定共用和重複使用。

- 適當地使用範本和範本堆疊變數，協助使用較少的範本來管理受管理防火牆設定以及流暢執行設定。

  例如，防火牆的 IP 位址一般會不同。使用範本變數，您可以指定變數來建立所需的設定，而非 IP 位址。將設定推送至受管理防火牆時，Panorama 可以根據每個受管理防火牆所設定的值來填入每個防火牆的正確 IP 位址。
- 建立具有預設值無的變數，確保未意外將不正確的設定推送至受管理防火牆。

  此狀況的顯著例外是 DNS IP 位址。在最佳案例情況下，受管理防火牆應該仍然可以解析 DNS 查詢。

設定變更管理的最佳做法

管理管理員可進行的設定變更，方法是利用基於角色的存取控制 (RBAC) 與分割受管理防火牆的存取權、使用動態結構 (例如外部動態清單 (EDL) 和動態使用者群組 (DAG)) 保留最新的政策規則，以及精細控制管理員可提交和推送至受管理防火牆的設定變更。

- 從 Panorama 管理管理員角色和存取網域
- 簡化 Panorama 所管理的安全性規則
- 大型團隊的設定變更管理
- 提交 Panorama 設定變更
- 推送 Panorama 設定變更

從 Panorama 管理管理員角色和存取網域

動態環境中成功設定管理的重點在於可以指派團隊成員的適當權限。Panorama 提供允許精細角色定義的大量基於角色的存取控制 (RBAC)。RBAC 可以與存取網域一起使用，以加快分割受管理防火牆的存取權。這有助於減少攻擊面，以及避免意外或惡意誤用管理員權限。

如需正確控制 Panorama 和受管理防火牆設定存取權的詳細資訊，請參閱安全性管理存取權的最佳做法。

- 定義管理角色以協助管理員成功管理防火牆，而不需要過度佈建其存取權。
- 如果您有多個滿足不同用途的防火牆子集，則請建立 Panorama 管理員的存取網域。例如，如果由不同的 Panorama 管理員管理您的資料中心防火牆、周邊防火牆和分支防火牆，則請設定和指派只能存取他們所管理防火牆的存取網域。
- 建立裝置群組和範本網域，更恰當地控制存取網域和管理員角色內受管理防火牆的管理存取權。這提供最精細存取權，以允許團隊執行工作而不導致操作問題。

簡化 Panorama 所管理的安全性規則

管理政策規則庫時，管理安全性政策是其中一種最重要的工作。

- 將規則庫設為應用程式感知，方法是組合使用政策最佳化工具與政策規則使用情況以轉移至基於 App-ID 和 User-ID 的安全性政策規則。

  在安全性政策規則中建立使用者群組，讓它們更具效率且更具可讀性。此外，您還可以利用 Expedition 和最佳做法評估 (BPA) 工具，協助逐一查看規則庫修訂，以加強安全性狀態。
- 評估政策規則庫來識別可能已存在的物件或規則時，請利用全域尋找。這將有助於減少設定中的不必要雜亂，而這些雜亂最終會讓 Panorama 上的提交速度變慢。
- 對政策規則進行疑難排解，以測試只需要修改的現有規則是否已處理所提出的政策規則設定變更。這可讓您減少任何重複政策規則，以及防止政策規則庫成長地太快。
- 使用基於標籤的規則群組來識別規則用途、功能、生命週期或其他特性，以快速將規則這類項目排序和群組在一起。基於標籤的規則群組可讓您以視覺方式區別規則庫內以群組形式管理的多組規則，也可以個別修改群組中的單一規則。
- 強制稽核註解進行政策規則建立和修改，以支援重大支援安全性稽核操作功能。具有一系列記載良好稽核註解的規則，可以輕鬆地回應稽核要求，而不是依賴規則說明或外部工具。此外，您還可以在將設定變更提交給 Panorama 時輸入說明，來補充稽核註解。
- 使用外部動態清單、動態位址群組和動態使用者群組這類動態建構，來流暢執行設定以及簡化安全性政策規則庫的維護。隨著您環境的變更，您可以視需要修改這些項目，而不需要提交。
- 建立安全性政策規則時，請避免在 **Target**（目標）頁籤中選取一或多個受管理防火牆，因為它會呈現不可靠的受管理防火牆設定同步狀態。

  這通稱為政策目標。政策目標是在防火牆上進行評估，而不是在 Panorama 上。因此，未將政策規則推送至其中的受管理防火牆可能會錯誤地顯示為未同步。設計裝置群組階層，以最小化或避免目標政策需求。

大型團隊的設定變更管理

大型團隊利用 Panorama 進行集中設定管理時，發生設定錯誤。Panorama 允許使用還原、匯入、匯出、載入、合併和取代設定作業的精細操作。這些作業是在裝置群組或範本層級執行。

- 嘗試快速還原 Panorama 設定為先前已知狀態時，請考慮僅還原受影響裝置群組或範本，而不是整個 Panorama 設定。

  這可協助您保留未對受影響裝置群組或範本進行任何設定變更的其他管理員所做的變更。此外，您還是可以匯出設定離線進行修改，然後在您準備好時將它匯回 Panorama。
- 匯出進行中裝置群組和範本設定變更，以將任何緊急設定變更推送至受管理防火牆。在您匯出之後，請還原 Panorama 設定，以進行緊急變更。成功將變更推送至受管理防火牆時，您可以匯入包含進行中設定變更的 Panorama 設定。
- 如果您要合併多個 Panorama 設定，則一般會合併裝置群組和範本設定來合併單一 Panorama 上的設定。

提交 Panorama 設定變更

Panorama 提供多種可讓您控制提交程序的方法。您需要瞭解它們是什麼，並將它們應用於您的日常作業。

- 當您提交 Panorama 設定變更時，請選取 **Commit Changes Made by**（依做成者認可變更）僅提交您自己的變更，而不提交其他管理員所做的設定變更。這確保未將正在進行或尚未核准的其他設定變更錯誤地提交給 Panorama。
- 提交設定變更時，需要管理員**Preview Changes**（預覽變更）以及檢閱變更摘要。設定變更的視覺檢查通常有助於擷取錯誤，以及稍後節省操作維護時間。

推送 Panorama 設定變更

Panorama 提供多種方法來控制如何將設定變更推送至受管理防火牆。您需要瞭解它們是什麼，並將它們應用於您的日常作業。

- 管理員將設定變更推送至受管理防火牆之前，需要他們檢閱推送範圍選取（**Commit**（提交）> **Push to Devices**（推送至裝置）> **Edit Selections**（編輯選取）），確認目標防火牆清單正確。

  即使正確設計裝置群組階層並且完善規劃設定變更，還是會有情況因不同維護時間範圍而不需要在特定時間將設定變更推送至所有防火牆。這一律是最佳做法，用於檢閱目標防火牆清單，確保只將設定變更推出至預定受管理防火牆。
- 謹慎地使用 **Force Template Values**（強制範本值）（**Commit**（提交）> **Push to Devices**（推送至裝置）> **Edit Selections**（編輯選取））設定。啟用此設定的推送會覆寫整個受管理防火牆設定，包含任何本機防火牆設定。

Panorama 上監控和可視性的最佳做法

根據組織需求，設計最佳日誌擷取和儲存的記錄基礎結構。然後，利用 Application Command Center（應用程式控管中心 - ACC）、PDF 摘要報告和自訂報告來識別調查和解決所需的網路活動和威脅。

- 設計記錄基礎結構
- 監控 Panorama 上的應用程式控管中心 (ACC) 和日誌
- 在 Panorama 上產生標準和自訂報告

設計記錄基礎結構

這是在您部署新受管理防火牆之前規劃和設計記錄基礎結構的最佳做法。Panorama 管理伺服器提供多種模式來進行裝置管理和日誌收集。Panorama 模式可讓您管理防火牆設定以及擷取和儲存日誌。如果您要 Panorama 具有單一功能，則設計「日誌收集器」模式只進行日誌擷取和儲存，而設計「僅管理」模式只進行防火牆設定管理。

- 使用 Panorama 大小與設計指南來計算記錄速率，以及決定日誌儲存空間需求。決定日誌收集器的日誌儲存容量時，這十分重要，而且可以根據許多因素（例如法規需求）。

  調整記錄基礎結構大小時，請洽銷售工程師 (SE)。它們將提供判讀和自訂部署所需的技術專業知識，以符合您的需求。
- 如果您因與此模式相關聯的多記錄限制而部署 Panorama 虛擬設備，則請不要使用傳統模式。適合實驗室或示範環境時，請避免在生產環境中以傳統模式使用 Panorama。
- 使用不同介面，在受管理防火牆上進行日誌收集。這可協助您在與 Panorama 通訊時維護管理介面上的效能。作為聲音安全性最佳做法，設定所有介面的允許 IP 清單。

監控 Panorama 上的應用程式控管中心 (ACC) 和日誌

應用程式控管中心 (ACC) 是一種互動式視覺化工具，設計成協助您快速瞭解網路中的事件。ACC 會從所處環境考慮受管理防火牆日誌，讓您瞭解流量模式以及您可在調查中使用之威脅的可行動資訊。

- 了解如何使用您可在 ACC 中使用的所有資料互動。
  - 使用 ACC 篩選器向下鑽研特定資訊，例如地址或使用者。
  - 套用全域篩選器以依您最重視的詳細資料轉換 ACC 顯示畫面，並排除無關資訊。
  - 如果利用 GlobalProtect，則請檢視 **GlobalProtect Activity**（**GlobalProtect** 活動）Widget 以根據 HIP 比對日誌來檢視 HIP 報告，瞭解可存取網路之終端裝置的安全性狀態。
  - 在您縮小感興趣資訊的範圍之後，請**Export**（匯出）CSV 格式的 ACC 資料或 PDF 格式的 Widget，以與有興趣執行進一步調查或修復的團隊分享。
- 自訂 ACC，確定調整成您有興趣監控的特定網路活動。

  這將協助您改善調查特定使用者或主機時的效率。這可讓您具有完整內容資訊，而不需要切換頁籤或捲動地太遠。
  - 新增 Widget 至 ACC，然後選取 **Content Activity**（內容活動）。
  - 新增 Widget 至 ACC，然後選取 **URL Filtering**（**URL** 篩選）。
  - 依預設，會顯示 **Threat Activity**（威脅活動）Widget。如果未顯示，請新增 Widget，然後選取 **Threat Activity**（威脅活動）。
- 選取 **Objects**（物件）> **Regions**（地區），然後建立具有 IP 位址範圍的自訂地區以用於安全性政策規則。使用自訂地區，以在 ACC 中產生更相關的關聯網路事件。

  例如，您已設定分公司的自訂地區，並注意到，特定 IP 位址負責可能過大的流量。利用自訂地區，您可以建立此可疑網路活動與特定分公司的關聯，並採取步驟來調查和執行修復測量。

在 Panorama 上產生標準和自訂報告

Panorama™ 管理伺服器提供方法，讓您集中並彙總防火牆部署的所有資訊來產生 PDF 報告，以及建立自訂報告。

- 識別組織所使用的所有 SaaS 應用程式，並將其分類為 **Sanctioned**（已認可）或 **Unsanctioned**（未認可）。

  Panorama 和受管理防火牆會將任何沒有認可標籤的應用程式都視為不認可在網路上使用。未認可 SaaS 應用程式可能會導致暴露威脅以及遺失私人和機密資料。最重要的是分類 SaaS 應用程式，更恰當地調查網路活動。

  1. 選取 **Objects**（物件）> **Applications**（應用程式）。
  2. 視需要建立自訂 SaaS 應用程式。
  3. 選取一或多個 SaaS 應用程式，然後選取 **Edit Tags**（編輯標籤）。
  4. 從 [Add Tags（新增標籤）] 下拉式清單中，選取 **Sanctioned**（已認可）或 **Unsanctioned**（未認可）。
  5. 除非視需要標示 SaaS 應用程式，否則請重複步驟 1-4。
  6. 選取 **Commit**（提交）> **Commit and Push**（提交並推送）和 **Commit and Push**（提交並推送）設定變更。
- 設定根據使用者群組的使用者活動報告和 SaaS 應用程式使用報告，以達到更高精細層級的報告。

  例如，您的財務部門將在 GitHub 中儲存大量資料。利用使用者活動和 SaaS 應用程式使用報告中的使用者群組，可讓您更輕鬆地識別這個可疑行為。否則，如果執行整個組織的報告，則可能注意不到這個可疑行為。
- 設定用途驅動和特定自訂報告，以及限制所需的欄數。

  簡明報告參數可讓您更輕鬆地識別需要調查的網路活動。

如果建立自訂報告，則請在可能時使用查詢建立器來快速縮小結果範圍。

例如，某個辦公室位置的目標報告比所有辦公室位置的報告更具效率和行動力。如果您需要包含多個辦公室的報告，則最好執行具有每個辦公室之特定查詢的一些不同報告。