移轉至基於應用程式的政策的最佳做法

Version 9.1

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 18, 2019

Table of Contents

移轉至基於應用程式的政策的最佳做法

您不需要犧牲較佳的安全性來獲取應用程式可用性。相反地，請使用 Expedition 和政策最佳化工具自動化和減少下列操作所需的時間和工作：以分段且安全的方式從傳統防火牆上的基於連接埠的安全性政策移轉至 Palo Alto Networks 新世代防火牆或 Panorama 設備上的基於應用程式的安全性政策。

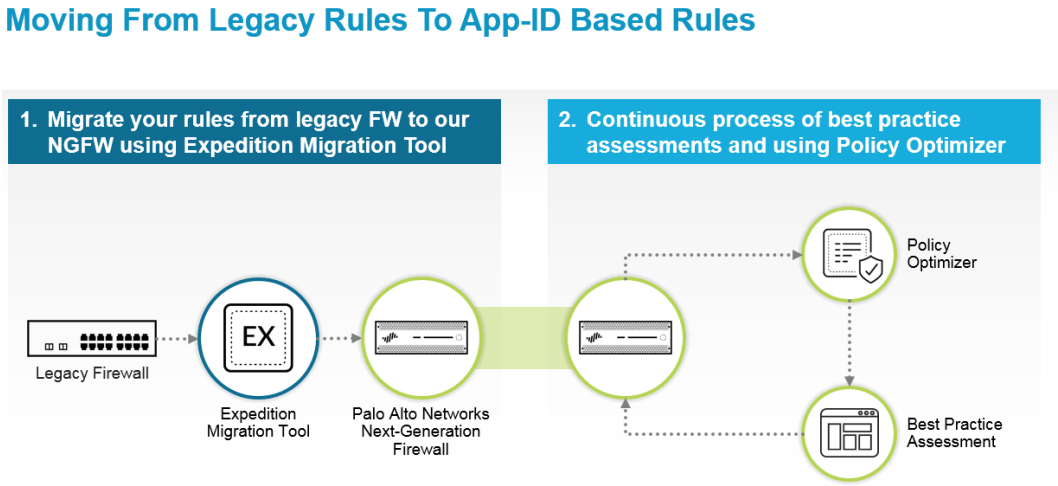
- 使用分段轉換安全地啟用應用程式
- 使用 Expedition 將基於連接埠的政策移轉至 PAN-OS
- 使用政策最佳化工具移轉至基於應用程式的政策
- 採用安全性最佳做法的後續步驟

使用分段轉換安全地啟用應用程式

基於連接埠的安全性政策的明顯弱點眾所周知：您無法看到使用連接埠的應用程式，因此任何惡意應用程式都可以透過開啟的連接埠來存取您的網路，例如連接埠 80 (HTTP) 或連接埠 53 (DNS)。這讓攻擊者可以更輕鬆地安裝惡意軟體、從側面通過整個網路、外洩資料以及危害您的網路，因為您看不到網路上的應用程式，而且無法防止其流量所隱藏的威脅。

相對地，不論連接埠、通訊協定、加密（SSL 或 SSH）或規避行為為何，使用 App-ID™ 的基於應用程式的安全性政策都可以查看應用程式，因此您確切知道網路上的應用程式，而且可以檢查其流量是否有威脅。應用程式特定政策會啟用安全存取，因為您可以設定安全性政策規則，僅允許正確使用者存取正確位置中的正確應用程式，而且您可以將威脅防護設定檔套用至這些規則。使用 App-ID 來分類應用程式可減少攻擊面，因為您僅允許網路上支援您業務所需的應用程式，並自動封鎖不需要的應用程式。允許您想要的應用程式並封鎖其他所有應用程式，會比無止盡嘗試封鎖所有您不想要的個別應用程式還要簡單和安全。

逐階段移轉至 App-ID：



1. 使用 Expedition 匯入傳統規則庫、清除傳統規則庫，以及達成同比移轉至 Palo Alto Networks 新世代防火牆或 Panorama 設備。Expedition 會分送為虛擬機器 (VM)。
2. 在網路生產環境中執行 PAN-OS 防火牆或設備，以了解和分類網路上的應用程式。
3. 在記錄流量至少一週之後，執行最佳做法評估 (BPA) 來設定基準線，然後使用政策最佳化工具開始安全地將基於連接埠的規則轉換為基於應用程式的規則，並保護網路安全。（您可以在大約一週之後轉換一些允許熟知應用程式的簡單規則；針對看到許多應用程式的其他規則（例如一般輸出網際網路存取規則），等待至少 30 天以收集應用程式資訊）。 採用分段方式，根據業務需求和優先順序安全地轉換規則。
4. （選擇性）在您使用政策最佳化工具之後，請將規則庫轉換為 App-ID、將設定重新匯入至 Expedition，並使用規則啟用功能，進一步簡化和調整規則庫。
5. 在您將新的應用程式引進網路時，請維護 App-ID 部署。在第一次轉換通過基於連接埠的規則之後執行 BPA，隨後定期測量進度，並探索其他區域來改善安全性。

從 *PAN-OS 9.0* 開始，提供政策最佳化工具。若您使用 *Panorama* 管理新世代防火牆，不必將受管理防火牆升級至 *PAN-OS 9.0* 即可使用政策最佳化工具。您只需要將 *Panorama* 升級至 *PAN-OS 9.0*，從受管理防火牆傳送流量日誌到執行 *PAN-OS 9.0* 的 *Panorama* 或日誌收集器，並從 *Panorama* 將政策推送至防火牆。受管理防火牆需要執行 *PAN-OS 8.1* 或更新版本，而且，如果它們連線至日誌收集器，則日誌收集器必須執行 *PAN-OS 9.0*。這提供限定資格的快速路徑，讓您可以使用政策最佳化工具，以根據 *App-ID* 來快速採用政策。

PA-7000 系列防火牆支援兩種日誌記錄卡：*PA-7000* 系列防火牆日誌處理卡 *(LPC)* 和高效能的 *PA-7000* 系列防火牆日誌轉送卡 *(LFC)*。與 *LPC* 不同，*LFC* 沒有用於在本機儲存日誌的

磁碟。*LFC* 會將所有日誌轉送至一個或多個外部日誌記錄系統中，例如 *Panorama* 或 *syslog* 伺服器。如果使用 *LFC*，原則最佳化工具的應用程式使用資訊不會顯示在防火牆上，因為流量日誌沒有在本機儲存。如果使用 *LPC*，因為流量日誌儲存在本機防火牆上，所以政策最佳化工具的應用程式使用資訊會顯示在防火牆上。這兩種情況下，只要日誌收集器和 *Panorama* 執行 *PAN-OS 9.0* 或更新版本，*PA-7000* 防火牆便能執行 *PAN-OS 8.1 (*或更新版本*)*。

使用 Expedition 將基於連接埠的政策移轉至 PAN-OS

使用 Expedition 匯入傳統規則庫、清除傳統規則庫，以及達成同比移轉至 Palo Alto Networks 新世代防火牆或 Panorama 設備作為移轉至基於應用程式的安全性政策時的第一個階段。Expedition 是對設定中多個物件執行大量操作的不錯工具，並支援從最主要防火牆廠商匯入傳統設定。

本主題彙總 *Expedition* 工作流程。線上社群支援 *Expedition*，包含如何取得工具以及如何使用工具的詳細文件。

Palo Alto Networks 技術支援 *(TAC)* 不支援 *Expedition*。

如需 Expedition 移轉工作流程詳細資料，請參閱《Expedition 使用者指南》，其中也包含如何使用 CSV 檔案將物件匯入至設定以及如何匯入 Day 1 Iron-Skillet 設定的相關資訊。

如需管理 Expedition，請參閱同時包含部分使用者介面資訊的《Expedition 管理員指南》，以及提供如何保護 Expedition VM 的建議的《Expedition 強化指南》。

在您開始移轉之前，請確定符合下列先決條件：

- 將 Expedition 下載至支援執行 VM 的管理裝置。
- 透過 SSH 和（或）SSL 連線至 Palo Alto Networks Panorama 和您重新移轉至的防火牆。SSH 存取用於連線至 CLI，而 SSL 存取用於連線至 Web 介面以及推送 API 命令。
- Palo Alto Networks Panorama 和您重新移轉至的防火牆的操作存取，以將同比設定推送至 PAN-OS 設備。

Professional Services 具有豐富的移轉經驗。您可以加入 *Professional Services* 團隊，協助您將設定從傳統裝置移至 *Palo Alto Networks* 新世代防火牆和 *Panorama* 設備。

STEP 1 | 檢閱傳統防火牆設定。

了解傳統規則庫的目標。記載您需要知道有關移轉的項目，例如 Juniper SRX 裝置上已停用的介面，或確認具有相同安全性層級之介面間允許流量、確認 IPSec 通道的狀態，以及收集 Cisco ASA 裝置上的預先共用金鑰。

STEP 2 | 將傳統設定匯入至 Expedition，並對設定進行任何必要修改。

STEP 3 | 在 Expedition 中建立新的 **Project**（專案）。

STEP 4 | 將已移轉的來源（傳統）設定匯入至 **Project**（專案）並進行檢查。

檢查檔案格式、是否包含所有必要檔案，以及 Expedition 日誌和事件，確定已正確載入已移轉的設定檔案。必要時，請修改已移轉的來源檔案來修正問題，然後重新檢查。除非修正所有問題，否則請重複此步驟。

STEP 5 | 將 PAN-OS 設定匯入至 **Project**（專案），以成為進行移轉的基本設定。

取得最新內容更新，然後從現有 PAN-OS 設備（現有設定檔案或原廠預設 PAN-OS 設定檔案）匯入基本設定。

設定檔案應該符合您想要使用的 *PAN-OS* 版本。例如，若要執行 *PAN-OS 9.0*，請匯入 *PAN-OS 9.0* 設定檔案。

STEP 6 | 清除已移轉的設定，以準備將它與基本 PAN-OS 設定合併。

- 移除或取代無效的服務物件。PAN-OS 只會辨識 TCP 和 UDP 服務連接埠，而 Expedition 會自動將 TCP 移轉 UDP 服務物件移轉至應用程式。搜尋基於非 IP 的應用程式和服務（例如 ping 和 ICMP），而部分傳統裝置將其視為服務而非應用程式。將它們取代為 App-ID，以分類為應用程式，並查看、檢查和控制流量。
- 若要簡化設定並減少其大小，請移除或取代其他無效物件和未使用的物件，並合併重複的物件。
- 尋找並移除已停用的規則，讓它們不會弄亂設定。
- 重新命名介面，使其符合 PAN-OS 設備上的介面。已從傳統裝置匯入的介面名稱一般不符合 PAN-OS 命名慣例。
- 當您匯入傳統設定時，Expedition 會自動指派區域名稱。重新命名區域，使其名稱描述您將設定移轉至 PAN-OS 設備時將滿足的用途，並確定將區域正確對應至介面。

  此外，還會檢查靜態路由的虛擬路由器。如果許多靜態路由存在，則請使用 Expedition 將路由移轉至 PAN-OS 設定。如果只有一些靜態路由，則請記下它們，然後在您移轉設定之後手動建立它們。

STEP 7 | 將物件從已移轉的設定拖放至基本設定，以合併已移轉的設定與 PAN-OS 基本設定。

STEP 8 | 檢查合併可能已建立的重複物件的已合併設定，並移除或合併它們。

STEP 9 | 在您將已合併的設定匯出至 PAN-OS 設備之前，請清除連接至 PAN-OS 設備的交換器和路由器以及 PAN-OS 設備上的 ARP 快取來更新其 ARP 表格。

在 PAN-OS 裝置上，使用 **`clear arp all`** CLI 命令。（必要時，您可以使用 **`clear arp <interface>`** CLI 命令以根據介面來清除 ARP 快取）。

STEP 10 | 將已合併的設定匯出至 PAN-OS 設備，並載入已合併的設定。

您使用的方法取決於如何移轉已合併的設定：

- 針對 PAN-OS 設備上的新安裝，**Generate XML & Set Output**（產生 **XML** 並設定輸出），並匯入 XML 檔案（設定），然後將它載入至 PAN-OS 設備。
- 針對現有 PAN-OS 安裝，或者如果您想要一次一個部分地移轉設定，而非同時移轉設定設定，則請 **Generate XML & Set Output**（產生 **XML** 並設定輸出），並匯入 XML 檔案（設定），然後使用 **`load config partial`** CLI 命令來選取要載入之設定的特定部分。您需要有 SSH 存取，才能在 PAN-OS 設備上使用 CLI。
- 如果 PAN-OS 設備連接至 Expedition，則您也可以使用 API 呼叫，將某些部分或整個設定傳送至設備。

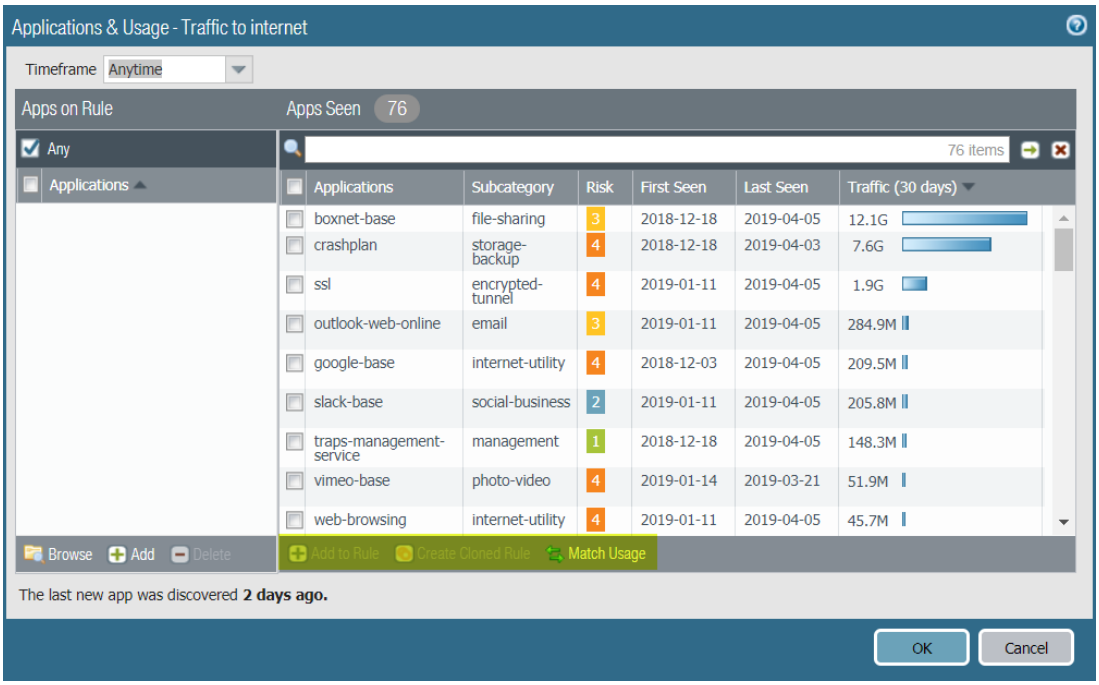
STEP 11 | 在您將已合併的設定匯出至 PAN-OS 設備並載入設定之後，請使用政策最佳化工具將基於連接埠的政策轉換為基於應用程式的政策。

使用政策最佳化工具移轉至基於應用程式的政策

在使用 Expedition 將同比設定移轉至 PAN-OS 設備之後，下個階段是使用政策最佳化工具來簡化移轉至基於 App-ID 的安全性政策規則。政策最佳化工具可讓從傳統基於連接埠的規則的轉換更為簡單，因為它會使用您需要了解資訊的內容來自動呈現每個規則的應用程式資訊，並在單一檢視中建立智慧的基於應用程式的規則。政策最佳化工具：

- 了解並自動記住流量中看到的每個規則的所有應用程式，這不需要徹底搜查和分析日誌資料的擴展。即使翻轉日誌，政策最佳化工具還是會保留應用程式資訊，讓您確信可重新看到規則上的所有應用程式。
- 可讓您安全地移轉至 App-ID，而不危害應用程式可用性。
- 是 PAN-OS 設備上原有和支援的工具，因此您不需要在設備與非原生工具之間移動設定和資料。
- 提供輕鬆且直覺的排序和篩選選項，協助您識別最容易且最安全地先轉換的規則並排定其優先順序。
- 在 Panorama 設備和個別新世代防火牆上執行。如果您管理執行具有 Panorama 的 PAN-OS 8.1 的新世代防火牆，則只需要將 Panorama（和任何連接至受管理防火牆的日誌收集器）升級至 PAN-OS 9.0 以使用並獲得政策最佳化工具的優點，因此您可以比必須限定所有防火牆更快速地限定和採用政策最佳化工具。

這些功能會導致一個易用工具，以節省時間，並防止在將基於連接埠的規則轉換為基於 App-ID 的規則時發生錯誤。政策最佳化工具提供數種方法來轉換規則：



- **Create Cloned Rule**（建立複製的規則）—複製規則可保留原始基於連接埠的規則，並將新的基於 App-ID 的規則放到複製的規則上方。您可以從一個基於連接埠的規則複製多個基於 App-ID 的規則。例如，您可以從一般 Web 瀏覽規則複製多個根據應用程式子類別的 App-ID 規則，以分組需要類似存取和威脅處理的應用程式，而非嘗試使用一個一般且不安全的規則來控制所有位置中所有使用者的所有 Web 存取。

  應用程式可用性沒有風險，因為複製的規則下面的基於連接埠的規則就像安全網。如果基於複製的 (App-ID) 規則不符合所有您需要允許的應用程式，則您會看到這些應用程式符合複製的規則下面的基於連接埠的規則，而且可以進行調整。您想要允許的流量在合理的一段時間不符合基於連接埠的規則時，您可以移除基於連接埠的規則，並完成將該規則轉換至基於 App-ID 的規則。

- **Add to Rule**（新增至規則）—將應用程式新增至規則會將基於連接埠的規則取代為基於 App-ID 的規則，以從規則庫移除基於連接埠的規則，並且不提供複製所提供的安全網。只有當您確定知道您想要規則控制的所有應用程式時，才會使用 **Add to Rule**（新增至規則）。只看到一些應用程式且您確信知道您業務的必要應用程式的規則，是 **Add to Rule**（新增至規則）的候選項目。這可以最安全地複製已看到許多應用程式的規則以及可能看到更多您需要允許的應用程式的規則。如果您未將應用程式新增至規則，則除非另一個規則允許該應用程式，否則會遺失其可用性，而複製規則可保留基於連接埠的規則作為安全網。
- **Match Usage**（比對使用）—比對基於連接埠的規則的使用會將基於連接埠的規則取代為包含該規則上看到的所有應用程式的基於 App-ID 的規則。只有在規則已看到少數具有合法業務用途的熟知應用程式時，才會使用 **Match Usage**（比對使用）。TCP 連接埠 22 是一個很好的範例，只允許 SSH 流量。針對連接埠 22，如果 SSH 是唯一在基於連接埠的規則上看到的應用程式，則您可以安全地 **Match Usage**（比對使用），並將規則轉換為 App-ID 規則。

若要 **Create Cloned Rule**（建立複製的規則）或 **Add to Rule**（新增至規則），您必須從 **Apps Seen**（看見的應用程式）選取至少一個應用程式。

如果歷程記錄不夠長，無法擷取其最新活動，則應用程式資訊中可能不會出現僅用於每季或每年事件的應用程式。當您轉換規則時，請注意這些類型的應用程式。

當您將基於連接埠的規則轉換為基於應用程式的規則時，除了將服務轉換為 App-ID 之外，政策最佳化工具不會對規則進行其他變更。在大部分情況下，轉換規則之後，應該將 **Service**（服務）變更為 **application-default**，因此，只有合法使用連接埠的應用程式才能存取它，並使用非標準連接埠來防止具規避性應用程式存取網路。

如果業務需求需要允許特定用戶端與伺服器之間的應用程式（例如非標準連接埠上的內部自訂應用程式），則請將例外僅限制為必要應用程式、來源和目的地。請考慮重新撰寫自訂應用程式，以使用 *application-default* 連接埠。

在您使用政策最佳化工具將基於連接埠的規則轉換為基於 App-ID 的規則之前：

1. 從 Expedition 完成將傳統設定同比移轉至 Palo Alto Networks 新世代防火牆或 Panorama 設備。
2. 您開始將規則轉換為 App-ID 讓設備可以開始了解和分類網路上的應用程式之前，會在生產網路中執行 PAN-OS 9.0 設備大約一週。您可以快速轉換一些簡單規則（例如，連接埠 22 規則只應該允許 SSH 流量且容易轉換），同時需要允許防火牆針對其他規則收集來自流量的應用程式資料較長的一段時間，例如網際網路存取（連接埠 80/433）規則。
3. 執行最佳做法評估 (BPA)，以設定用來比較進度的基準線。
4. 設定實際可行的目標。考慮您想要的最後結果樣子。當您到達目標時，請重新執行 BPA 確認已到達目標，然後重新評估是否可以繼續，而網路速度甚至會更快。使用政策最佳化工具，您不用犧牲可用性來獲取安全性，只需要改善安全性即可。

分段轉換規則。在 PAN-OS 設備只有一週的日誌之後，您可以將一些允許熟知應用程式的簡單基於連接埠的規則轉換為基於 App-ID 的規則（政策最佳化工具會藉由讀取日誌來探索規則上看到的應用程式）。針對看到許多應用程式的其他規則（例如一般 Web 存取規則），等待至少 30 天以收集應用程式資訊。

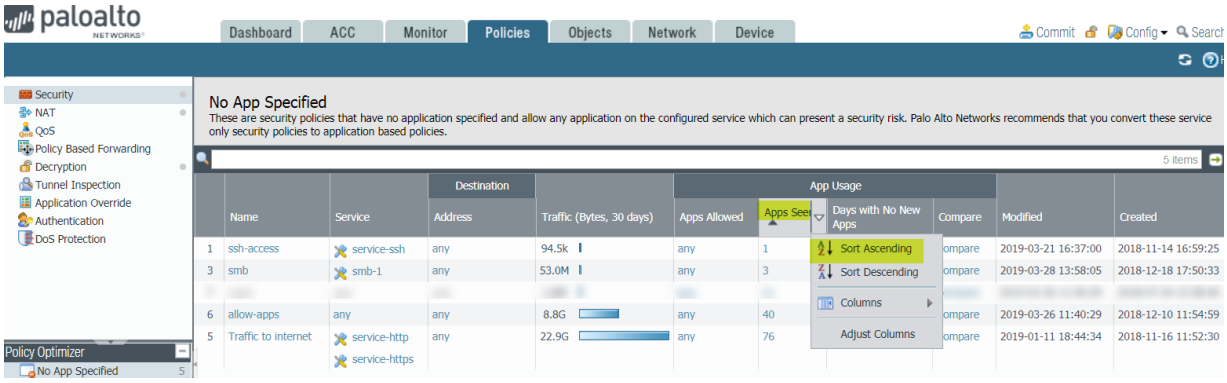
Professional Services 具有豐富的移轉經驗。您可以加入 *Professional Services* 團隊，協助您將設定從傳統設備移至 *Palo Alto Networks* 新世代防火牆和 *Panorama* 設備。

轉換具有一週之後的已知應用程式的簡單規則

在監控生產流量一週之後，您可以安全地開始將簡單基於連接埠的規則轉換為基於 App-ID 的規則。不錯的候選項目包含僅有一個或少數已知應用程式應該合法使用連接埠的規則，因為判定您想要在簡單規則上允許的應用程式相當簡單。範例包含連接埠 21 (FTP)、連接埠 22 (SSH) 和連接埠 53 (DNS)。

先安裝最新內容更新，再開始轉換規則，確定您具有 PAN-OS 設備的最新應用程式特徵碼。此範例顯示您如何排序基於連接埠的規則以找到進行安全轉換的候選項目，以及將基於連接埠的規則直接轉換為基於 App-ID 的規則的選項。

STEP 1 | 在 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）中，選取 **Apps Seen**（看見的應用程式）和 **Sort Ascending**（遞增排序）以找到已看到最少應用程式的基於連接埠的規則。

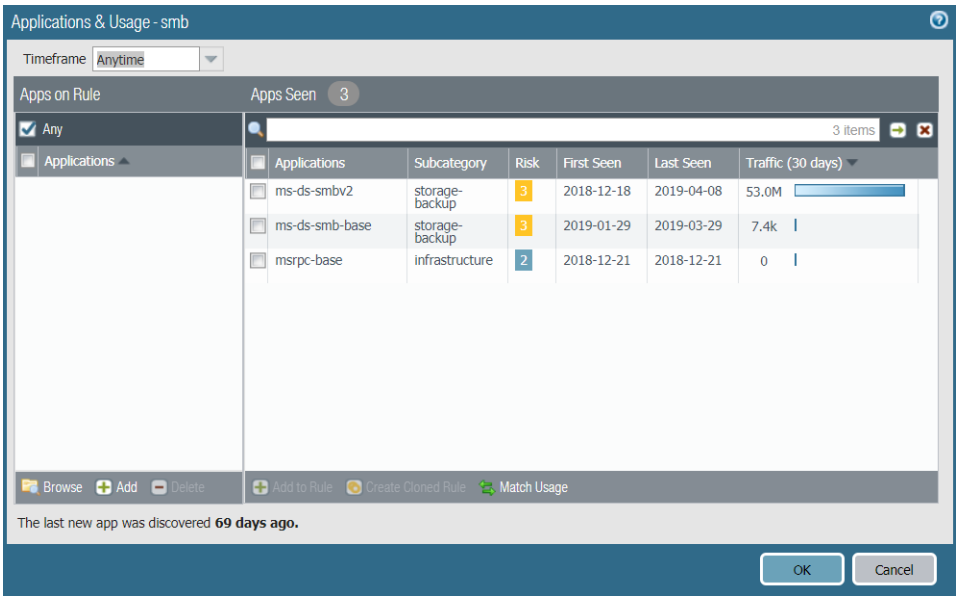


已看到最少應用程式的基於連接埠的規則會位於 **No App Specified**（無指定的應用程式）顯示畫面頂端。您可以將 SSH 這類特定服務的規則安全地直接轉換為基於應用程式的規則，而且可以檢查已有少數應用程式的規則，確認您是否可以安全地轉換它們。

預定允許伺服器訊息區塊 (SMB) 流量的基於連接埠的規則，在將設定移轉至 PAN-OS 設備之後僅看到三個應用程式，因此是進行轉換的候選項目。

STEP 2 | 按一下 **Apps Seen**（看見的應用程式）數目或 **Compare**（比較），以檢查規則上看到的應用程式。

Applications & Usage（應用程式與使用方式）會顯示流量中實際看到且符合規則的應用程式。



STEP 3 | 評估您要允許規則上看到的所有、部分還是零個應用程式，然後選取您想要允許的應用程式。

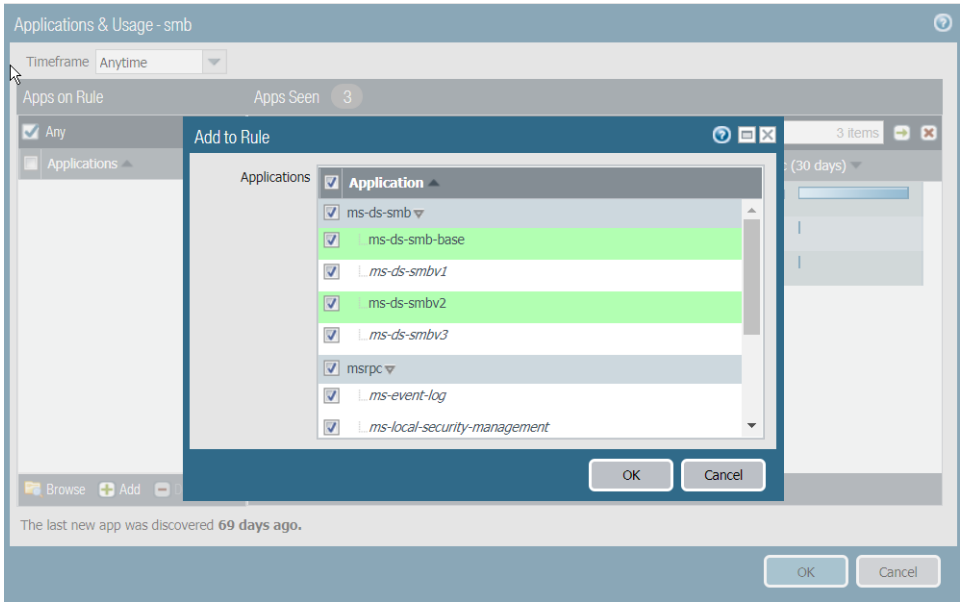
您可以比對規則的確切使用、新增容器應用程式來適應規則，或選取要新增至規則的個別應用程式。

- 如果您想要規則允許規則上完全相符的所有應用程式：

1. 選取 **Apps Seen**（看見的應用程式）中的所有 **Applications**（應用程式）。
2. 按一下 **Match Usage**（比對使用）。
3. 按一下 **OK**（確定），將基於連接埠的規則轉換為基於 App-ID 的規則。
4. 將 **Service**（服務）設定為 **application-default**，讓具規避性且惡意的應用程式無法使用連接埠。

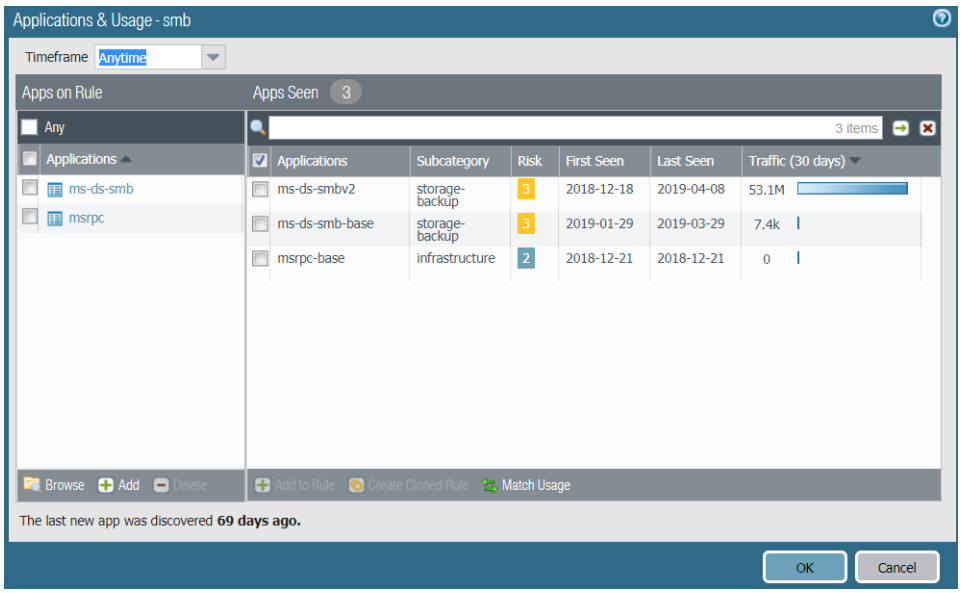
- 如果您想要允許規則上看到的所有應用程式，並新增其容器應用程式來適應規則（因此允許每個容器內的所有應用程式，並自動允許稍後新增至容器應用程式的應用程式）：

1. 保留所有應用程式的選取狀態，並 **Add to Rule**（新增至規則）。



灰色應用程式是容器應用程式。綠色應用程式是規則上看到的應用程式。沒有顏色的應用程式屬於相同的容器應用程式，但未在規則上看不到。

2. 按一下 **OK**（確定）。只有容器應用程式才會出現在 **Apps on Rule**（規則上的應用程式）上，因為它們包含（允許）所含的所有應用程式：

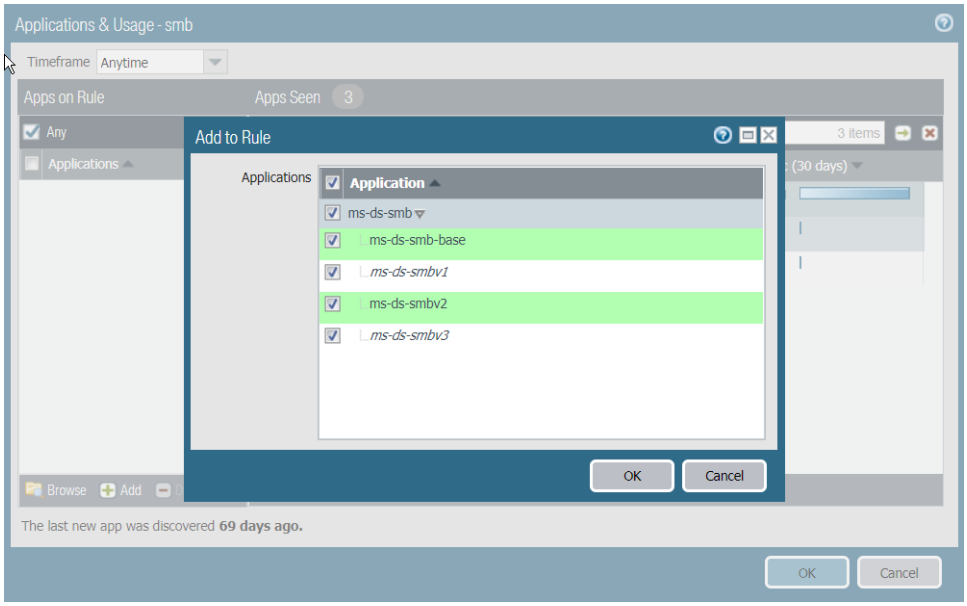


3. 按一下 **OK**（確定）來轉換規則。
4. 將 **Service**（服務）設定為 **application-default**，讓具規避性且惡意的應用程式無法使用連接埠。

- 如果您只想要允許部分應用程式，或想要選取要在容器應用程式內允許的應用程式，則請選取這些應用程式，然後按一下 **Add to Rule**（新增至規則）。例如，如果您決定不允許 msrpc-base、僅選取 ms-ds-smbv2 和 ms-ds-smb-base，並 **Add to Rule**（新增至規則），則政策最佳化工具會顯示容器應用程式中的相關應用程式（ms-ds-smb、灰色），並提供藉由新增這些應用程式來適應規則的機會：

  1. 選取您想要允許的應用程式，然後按一下 **Add to Rule**（新增至規則）。

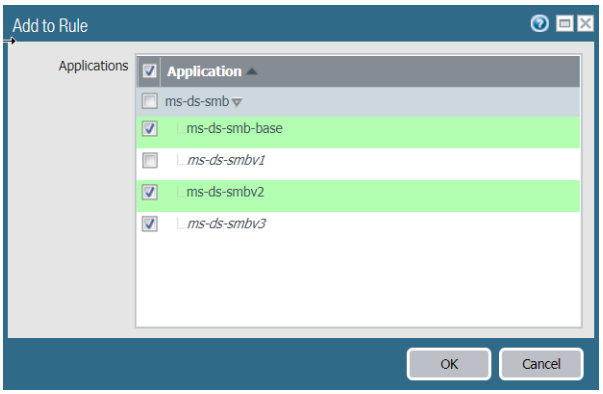
     例如，如果您決定不允許 msrpc-base、僅選取 ms-ds-smbv2 和 ms-ds-smb-base，並 **Add to Rule**（新增至規則），則政策最佳化工具會顯示容器應用程式中的相關應用程式（ms-ds-smb、灰色），並提供藉由新增這些應用程式來適應規則的機會：

     綠色應用程式是規則上看到的應用程式。沒有顏色的應用程式屬於相同的容器應用程式，但未在規則上看不到。在此情況下，您可能會選擇允許 ms-ds-smbv3 適應規則，但不允許 ms-ds-smbv1，因為它是較舊的通訊協定。
  2. 您可以允許所有應用程式，或選取要允許的應用程式。

     若要允許所有應用程式，請按一下 **OK**（確定）。**Apps on Rule**（規則上的應用程式）會顯示選取的應用程式。按一下 **OK**（確定）來轉換規則。

     若只要允許選取的應用程式，請取消選取不需要的應用程式。如果您取消選取容器中的應用程式，則也會取消選取容器應用程式，讓它不會自動允許其子應用程式。

  3. 按一下 **OK**（確定）。**Apps on Rule**（規則上的應用程式）會顯示選取的應用程式。
  4. 按一下 **OK**（確定）來轉換規則。
  5. 將 **Service**（服務）設定為 **application-default**，讓具規避性且惡意的應用程式無法使用連接埠。

在 30 天後開始轉換的規則

在監控生產流量 30 天之後，您可以安全地開始將其餘基於連接埠的規則轉換為基於 App-ID 的規則，並清除規則庫。不錯的開始位置是清除未使用的規則以減少攻擊面。之後，在周邊開始使用輸出網際網路存取（連接埠 80/443）規則將規則轉換為 App-ID，因為該規則可能會看到具有應用程式的流量，而其應用程式和流量都多於任何其他規則，這也表示它是具有最多風險的規則。

先安裝最新內容更新，再開始轉換規則，確定您具有 PAN-OS 設備的最新應用程式特徵碼。

政策最佳化工具提供許多直覺式方式，為要先轉換的規則進行排序、篩選和排定優先順序。在您移除未使用的規則並將 Web 存取規則轉換為 App-ID 之後，選擇排定優先順序的規則取決於業務和安全性需求。下列各節所提供的想法和方法使用簡單但功能強大的排序和篩選選項，來識別要在前 30 天之後轉換的規則並排定其優先順序：

- 移除未使用的規則
- 轉換最穩定規則
- 轉換網際網路存取規則
- 轉換看到最大流量的規則
- 轉換某時段看見最少應用程式的規則

移除未使用的規則

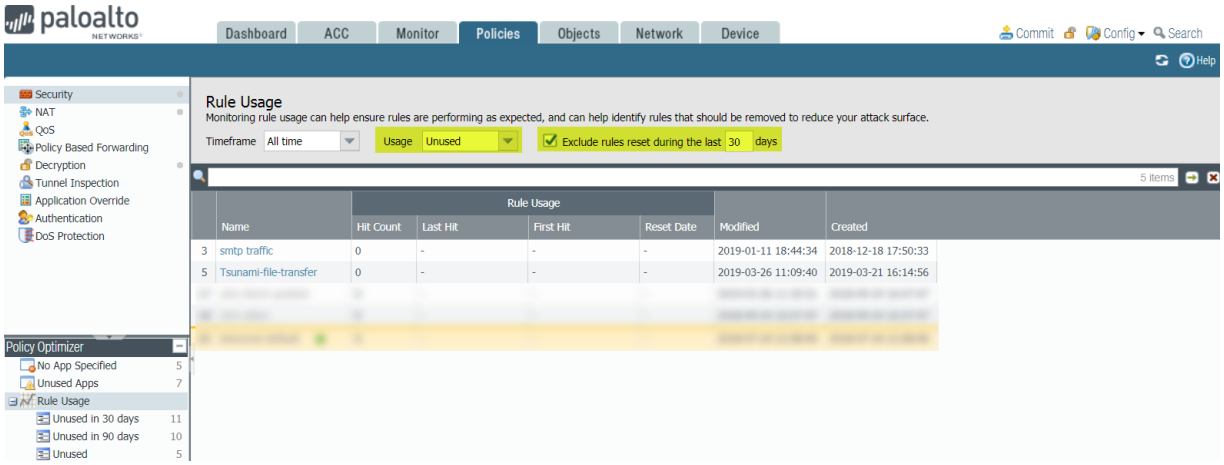
已移轉的規則庫通常會包含未使用的規則，因為應用程式流量不符合這些規則。未使用的規則會弄亂規則庫，並提供對手的攻擊途徑。移除這些規則來清除規則庫並減少攻擊面，或修改它們，以將它們套用至應用程式流量並提供規則庫中的合法用途。

未使用的規則的存在可能有好幾個原因。管理業務已使用但取代為其他應用程式的服務和應用程式的規則，可能在規則庫中。在未使用的規則前面的規則可能會控制符合未使用的規則的應用程式。在部分情況下，未使用的規則是離開公司的管理員所建立的舊規則，而目前管理員不知道規則的目的。

檢視您選擇的任何 **Timeframe**（時間範圍）的規則（**Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **Rule Usage**（規則使用方式））。將 **Usage**（使用方式）設定為 **Unused**（未使用），以篩選出已看到應用程式流量的規則。

STEP 1 | 識別未使用的規則。

在 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **Rule Usage**（規則使用方式）中，將 **Timeframe**（時間範圍）設定為 **All time**（所有時間）、將 **Usage**（使用方式）設定為 **Unused**（未使用）（僅顯示命中數為零的規則），以及 **Exclude rules reset during the last 30 days**（排除在過去 **30** 天重設的規則）（防止顯示最近重設的規則，而這些規則在最後幾天可能看不到流量，但較長的時段可能會看到流量）。結果是在選取的 **Timeframe**（時間範圍）看不到應用程式流量的規則清單。



STEP 2 | 評估看不到流量的規則，並判斷是否需要它們，或您是否可以停用它們。

在此範例中，業務過去使用 Tsunami 檔案傳輸，但調查顯示業務不再使用 Tsunami 並將它取代為其他檔案傳輸應用程式，因此網路上沒有原因需要允許 Tsunami 應用程式流量。

STEP 3 | **Disable**（停用）（或 **Delete**（刪除））規則。

在 **Policies**（政策）> **Security**（安全性）中，選取 Tsunami 檔案傳輸規則。**Disable**（停用）或 **Delete**（刪除）規則。

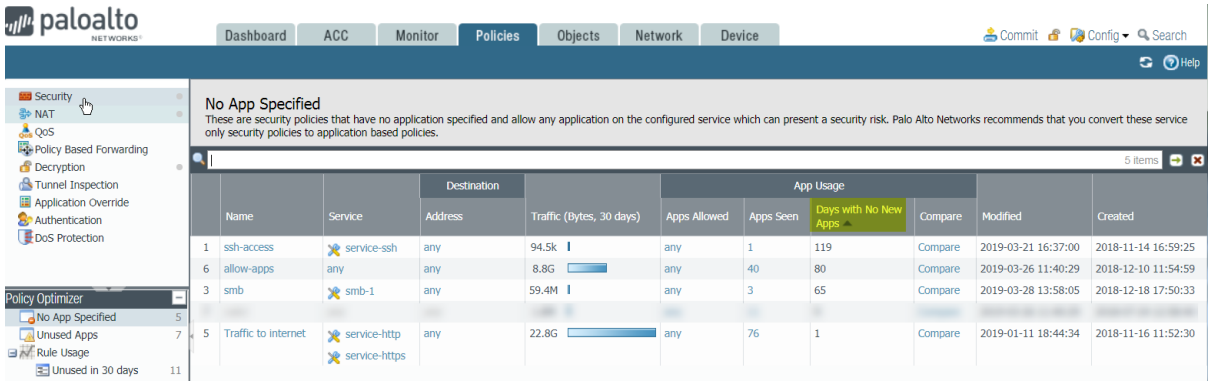
如果後來您的業務需要應用程式，則停用規則比較安全，即使看不到任何流量也是一樣。（如果您在調查業務是否使用應用程式時未考慮到每季和年度事件，或者承包商或合作夥伴需要其流量只會定期存取網路的應用程式，則會發生這種情況）。 在合理的一段時間之後，您可以刪除您稍早停用的未使用的規則。

轉換最穩定規則

轉換合理的一段時間看不到新應用程式的基於連接埠的規則，表示規則趨於穩定，而且您較不可能在其上看到新的應用程式。複製這些規則，確定如果稍後有更多應用程式符合規則，則只要安全網需要，基於連接埠的規則就會保留在規則庫中。

當您評估新的應用程式是否符合規則時，請考量僅用於每季、年度和其他定期事件的應用程式。

STEP 1 | 在 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）中，排序規則（遞減），以將具有最高數目的 **Days with No New Apps**（沒有新應用程式的天數）的規則顯示在清單頂端。

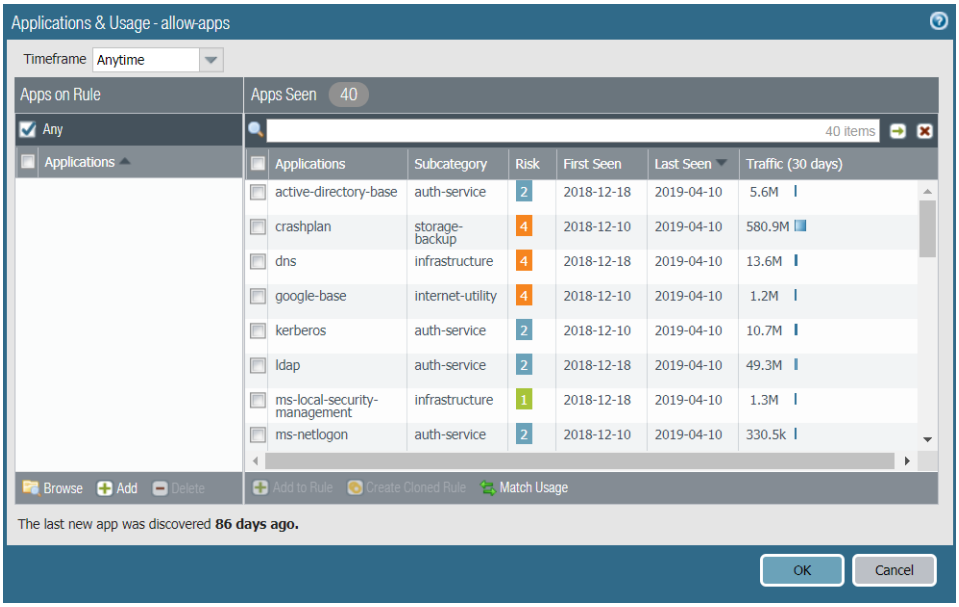


前三個規則在相當長的一段時間都看不到新的應用程式，因此是轉換為應用程式 ID 的候選項目。（轉換具有一週之後的已知應用程式的簡單規則描述如何轉換具有少數 **Apps Seen**（看見的應用程式）的規則（例如 smb 規則），讓此範例聚焦於允許應用程式規則）。

檢查 *Modified*（已修改）日期，因為有一段長時間未修改的規則可能也較為穩定。最近修改的規則可能看不到所有符合規則的應用程式。

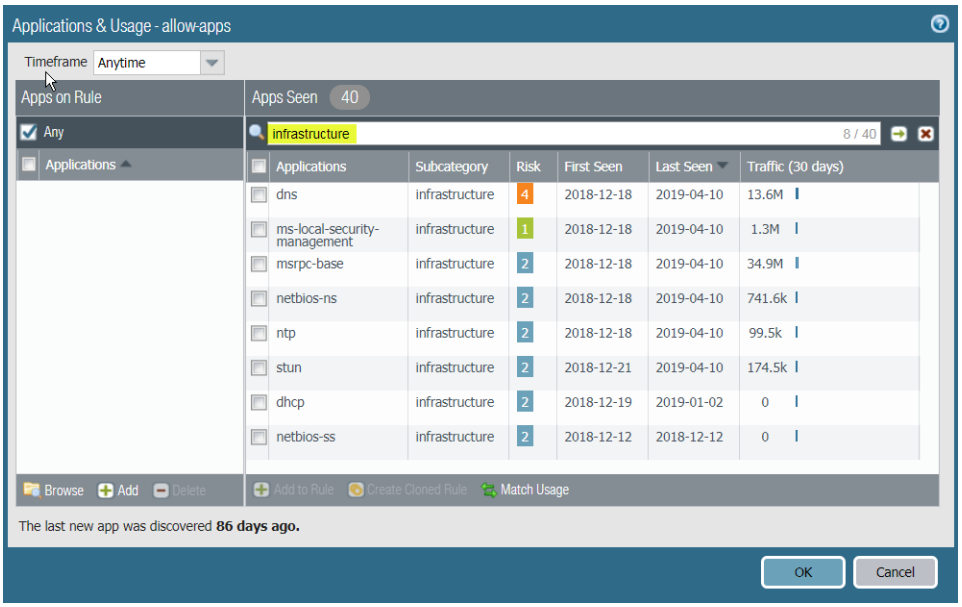
因為已在規則上看到多個應用程式，所以會複製規則，而不是將它直接轉換為基於 App-ID 的規則。

STEP 2 | 按一下 **Apps Seen**（看見的應用程式）數目，以開啟 **Applications & Usage**（應用程式與使用方式）對話方塊。



STEP 3 | 排序和篩選規則上的 **Apps Seen**（看見的應用程式），以判定如何處理應用程式。

依子類別進行排序或篩選可協助您了解看到多個應用程式之規則上看到的流量。例如，您可以依基礎結構子類別進行篩選來查看所有基礎結構應用程式，並複製基於 App-ID 的規則來控制它們。



STEP 4 | 遵循轉換網際網路存取規則中的步驟 4-7，以建立複製的規則來控制您想要以類似方式處理的應用程式的每個子類別（或相關子類別）。

轉換網際網路存取規則

網際網路存取規則可控制連接埠 80 (HTTP) 和連接埠 443 (HTTPS) 的流量。此規則通常會看到最大數目的應用程式及最大流量（位元組）。基於連接埠的網際網路存取規則可以允許您不想要在網路上的應用程式，並暴露它受到攻擊，因此您需要在這些連接埠上控制和安全地啟用您允許的應用程式。

當您將網際網路存取規則從基於連接埠的規則轉換為基於應用程式的規則時，需要了解您公司基於業務使用而認可的應用程式，以及您公司基於其他用途而容忍的應用程式。

轉換網際網路存取規則的不錯方法是分組相同規則中需要類似處理的應用程式，而非為每個應用程式建立單獨規則，以協助防止規則庫太滿。使用政策最佳化工具以依應用程式子類別來排序規則上看到的應用程式，讓您可以看到規則上特定子類別的所有應用程式，並選取您業務所使用的應用程式，然後複製規則以控制這些應用程式。政策最佳化工具提供許多排序和篩選選項來組織和分析規則上看到的應用程式。

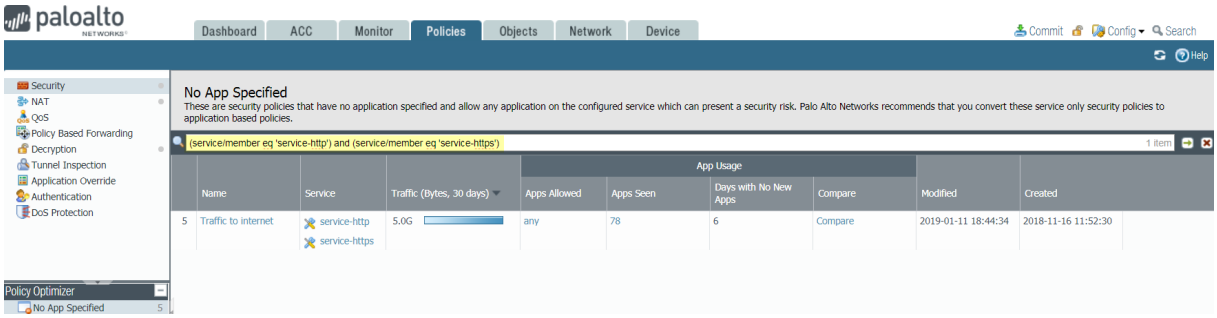
請複製規則，而非直接轉換它來確定應用程式可用性。複製規則會保留原始基於連接埠的規則，並將複製的基於應用程式的規則直接放在安全性規則庫中基於連接埠的規則上方。這可讓您建立與您想要以不同方式處理之應用程式群組的原始基於連接埠的規則不同的網際網路存取規則，而不危害應用程式可用性。您可以輕鬆地看到與複製的規則相符的應用程式，以及篩選整個原始基於連接埠的規則並視需要調整規則的應用程式。如果您想要允許的應用程式有夠長的一段時間不符合基於連接埠的規則，確信您已考量業務所需的所有應用程式，則可以停用（或刪除）基於連接埠的規則，以完成轉換，而不危害應用程式可用性。

您可以使用相同的方法來轉換已看到更多已知應用程式的其他規則。使用 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）資訊，在您轉換網際網路存取規則之後，協助您排定要轉換的規則優先順序。例如，您可以依最多 **Apps Seen**（看見的應用程式）與過去 30 天的最大流量（**Traffic (Bytes, 30 days)**（流量（位元組，30 天））的組合來排定優先順序以轉換最常用的規則，也可以查看 **Days with No New Apps**（沒有新應用程式的天數）和 **Modified**（已修改）日期以找到已看到許多應用程式同時也較穩定的規則。

此範例顯示如何從基於連接埠的網際網路存取規則複製可控制電子郵件應用程式的基於應用程式的規則。您可以使用相同的複製程序，為不同的子類別以及任何基於連接埠的規則上看到的個別應用程式安全地建立基於應用程式的規則。

STEP 1 | 導覽至 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式），並找到可控制網際網路存取的基於連接埠的規則。

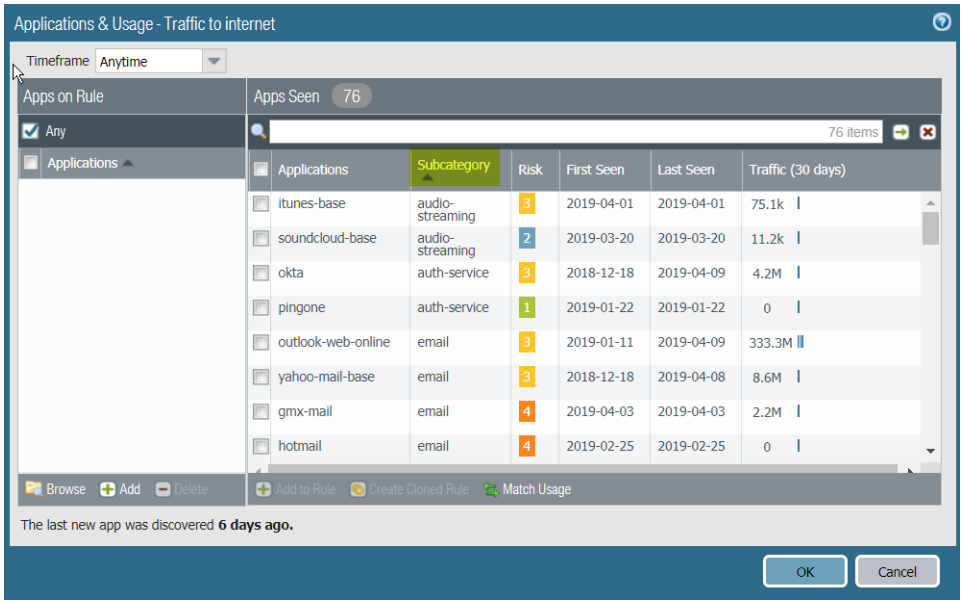
使用 `(service/member eq 'service-http') and (service/member eq 'service-https')` 篩選，以找到已設定 **service-http** 和 **service-https** 網際網路存取規則的基於連接埠的規則。



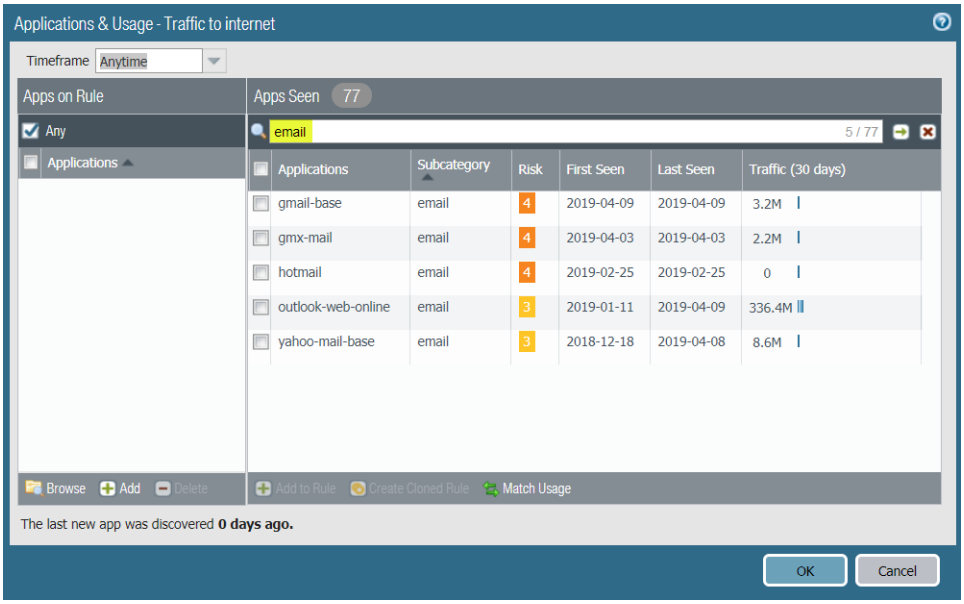
STEP 2 | 按一下 **Compare**（比較）或 **Apps Seen**（看見的應用程式）數目，以開啟 **Applications & Usage**（應用程式與使用方式）對話方塊。

STEP 3 | 依應用程式子類別來排序 **Apps Seen**（看見的應用程式），以分組相同安全性政策規則中可能適合控制的類似應用程式。

依 **Subcategory**（子類別）進行排序，以分組規則上看到的應用程式：

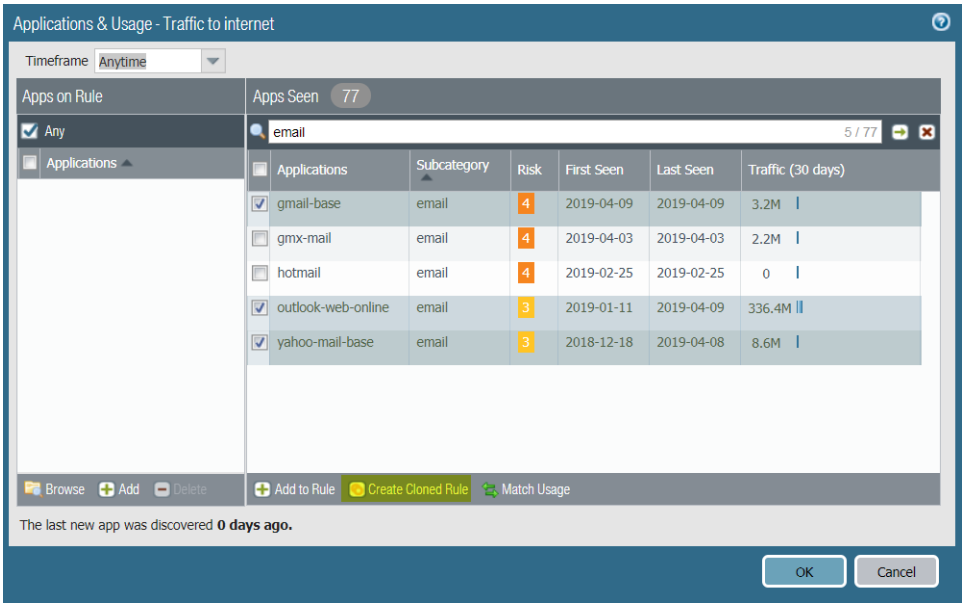


您也可以依特定子類別進行篩選，僅查看屬於該子類別的應用程式。在此範例中，若要建立基於 App-ID 的規則來控制電子郵件應用程式，請進行篩選，僅檢視規則上看到的電子郵件應用程式：

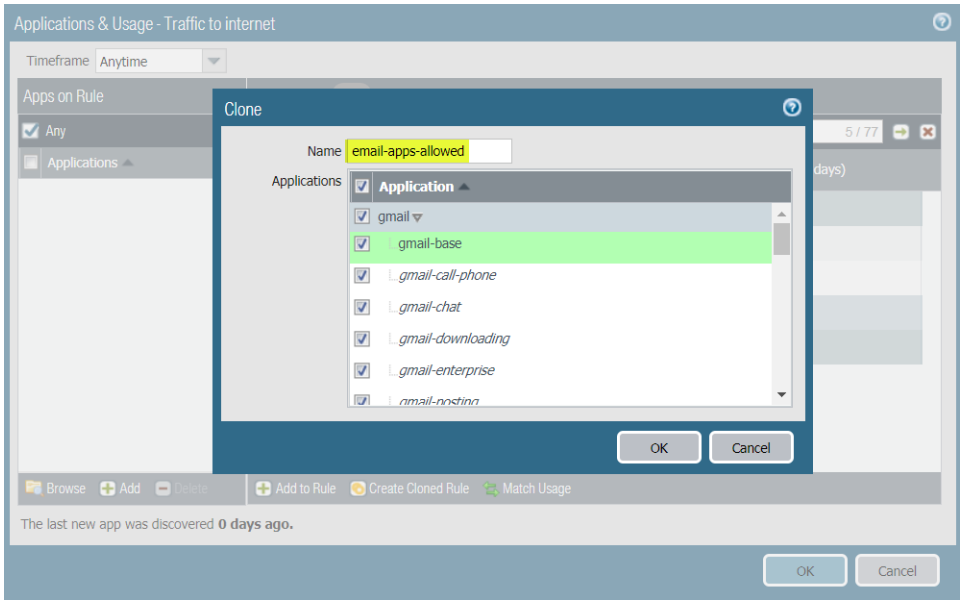


STEP 4 | 選取您想要允許的應用程式，然後 **Create Cloned Rule**（建立複製的規則），以從基於連接埠的規則複製新的基於應用程式的規則。

例如，如果您的公司認可在公司內使用 Gmail 和 Outlook，並容忍將 Yahoo 電子郵件作為個人使用，但選擇不允許 GMX 郵件或 Hotmail：

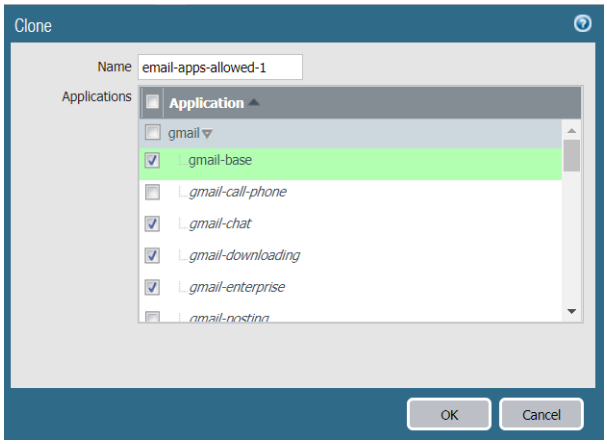


STEP 5 | 在 **Clone**（複製）對話方塊中，選取與您想要允許的每個應用程式相關聯的應用程式。



提供新規則的 **Name**（名稱），而此名稱可描述其用途。決定是否想要僅允許每個電子郵件應用程式的特定功能，或是否想要允許容器應用程式。如果您允許容器應用程式，則允許容器中的所有應用程式。這藉由在將新的應用程式新增至容器應用程式時自動允許它們來適應規則，並協助確定應用程式可用性。預設會選取所有應用程式。每個應用程式的容器應用程式都會加上灰色、已在規則上看到的應用程式會加上綠色，而容器應用程式中未在規則上看到的應用程式會加上斜體而且不會加上顏色。

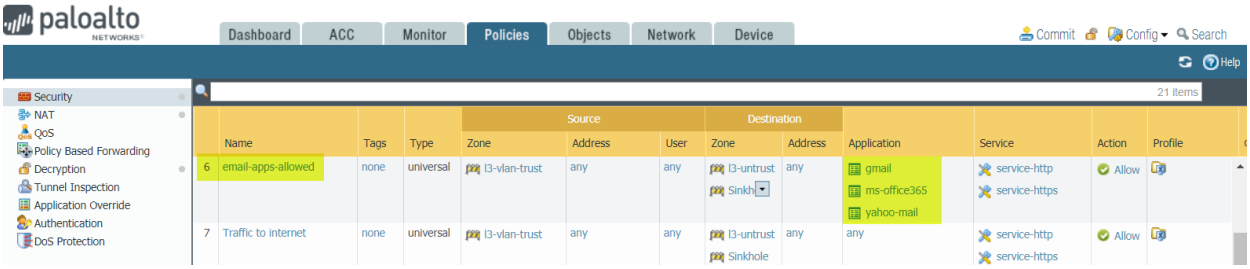
如果您選擇不允許容器應用程式中的部分應用程式，則也會取消選取容器應用程式，而且規則只會包含您選取的特定應用程式。



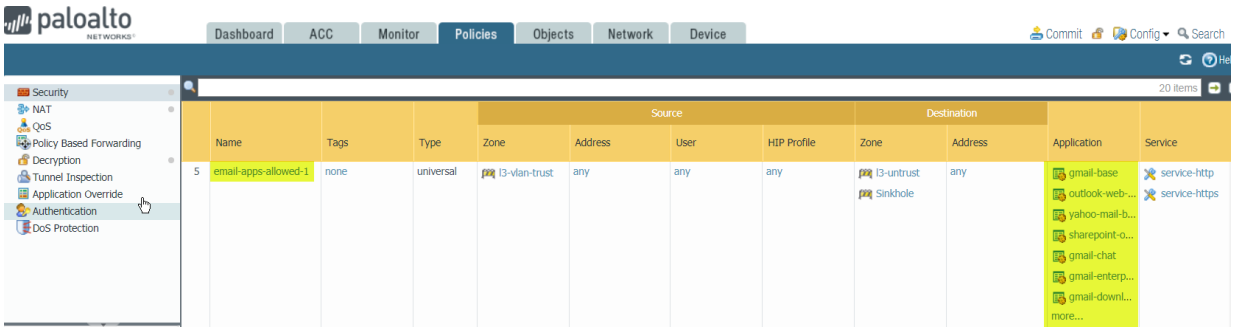
取消選取 gmail-call-phone 和 gmail-posting 應用程式，也會取消選取 gmail 容器應用程式。

STEP 6 | 按一下 **OK**（確定）來建立規則，而此規則放在安全性政策規則庫中基於連接埠的規則上方（**Policies**（政策）> **Security**（安全性））。

如果您選取容器應用程式，則政策最佳化工具只會將包含所有應用程式的容器應用程式新增至規則。



如果您從 **Clone**（複製）對話方塊選取個別應用程式，而非容器應用程式，則政策最佳化工具只會將選取的應用程式新增至新的基於 App-ID 的規則。



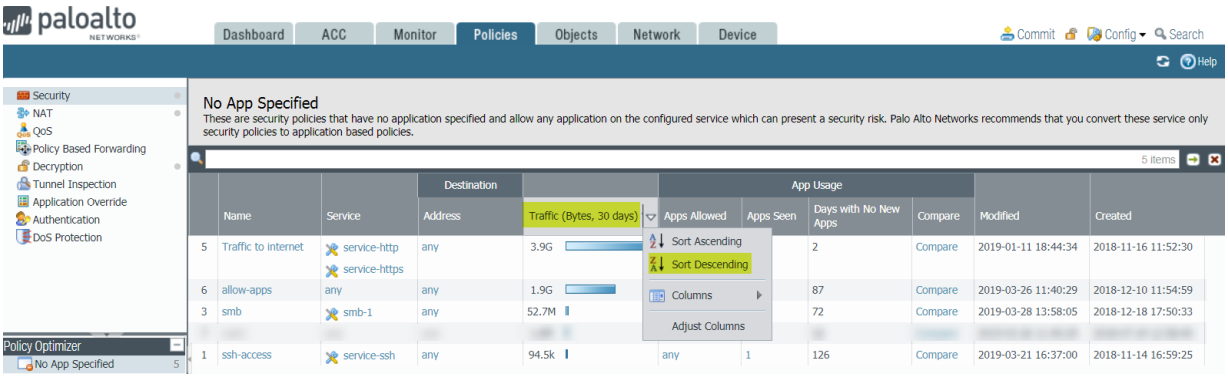
STEP 7 | 按一下規則 **Name**（名稱）或 **Service**（服務），並將 **Service**（服務）變更為 **application-default** 以防止在非標準連接埠上存取具規避性應用程式。

轉換看到最大流量的規則

排序已看到過去 30 天最大流量（**Traffic (Bytes, 30 days)**（流量（位元組，30 天））的規則，會顯示您目前最活躍規則。（較長的時間範圍可能會藉由強調因具有大的累計總計而保留在清單頂端的較舊規則來誤導您，即使不再看到太多流量也是一樣）。 將這些規則轉換為基於 App-ID 的規則，可防衛您工作的最大流量。

如果多個規則看到大量流量，則請使用 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）資訊，協助為要先轉換的規則排定優先順序。例如，您可以為具有最多 **Apps Seen**（看見的應用程式）的規則排定優先順序（可能是風險最高的規則），或為具有最多 **Days with No New Apps**（沒有新應用程式的天數）和最舊 **Modified**（已修改）日期的規則排定優先順序（最穩定高流量規則）。

STEP 1 | 在 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）中，依 **Traffic (Bytes, 30 days)**（流量（位元組，30 天））遞減排序規則，以將最近的活躍規則放在清單頂單。



STEP 2 | 選取規則以開始轉換，然後按一下 **Apps Seen**（看見的應用程式）數目。

STEP 3 | 在 **Applications & Usage**（應用程式與使用方式）對話方塊中，排序和篩選規則上的 **Apps Seen**（看見的應用程式），以判定如何處理應用程式。

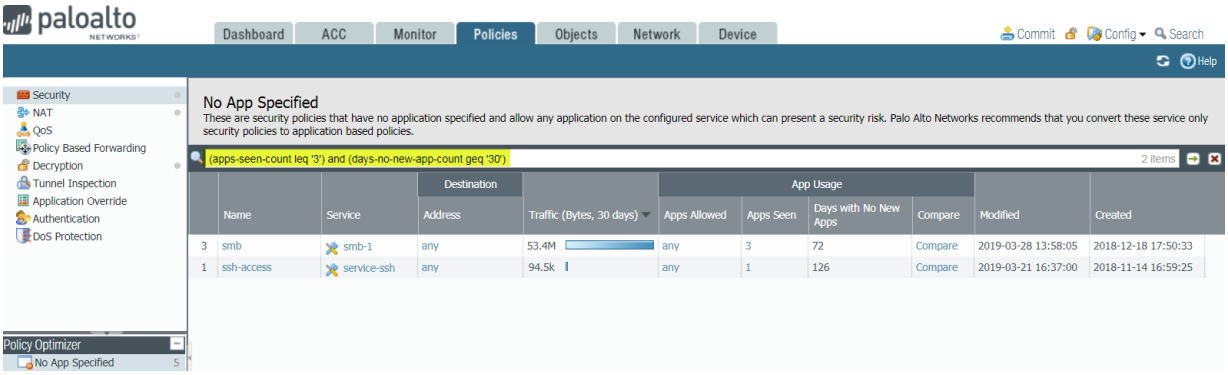
依應用程式子類別進行排序或篩選，以分組可能需要類似處理且可以使用一個基於應用程式的規則所控制的應用程式。根據 **Traffic (30 days)**（流量（30 天））排序，以查看個別應用程式的最近流量來排定目前最活躍應用程式的優先順序。

STEP 4 | 遵循轉換網際網路存取規則中的步驟 4-7，以建立複製的規則來控制您想要以類似方式處理的應用程式的每個子類別（或相關子類別）。

轉換某時段看見最少應用程式的規則

具有相當少 **Apps Seen**（看見的應用程式）且在夠長的時段未看見新應用程式的規則，可以輕鬆轉換、相當穩定，而且可以使用篩選輕鬆識別。

STEP 1 | 在 **Policies**（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）> **No App Specified**（無指定的應用程式）中，篩選規則，僅顯示具有少數 **Apps Seen**（看見的應用程式）且未在特定時段看到應用程式的規則。



此範例會篩選已看到三個以下應用程式的規則 **(apps seen count leq '3')**，以及至少 30 天未看到應用程式的規則 **(days no new app count geq '30')**。

STEP 2 | 選取要轉換的規則，然後按一下 **Apps Seen**（看見的應用程式）數目。

STEP 3 | 在 **Applications & Usage**（應用程式與使用方式）對話方塊中，決定是否想要允許所有應用程式，以及它們是否應該位於相同的規則中；亦即決定應用程式是否需要對存取和安全性進行類似的處理。

如果您想要允許所有應用程式，而且它們需要類似的處理，則可以 **Match Usage**（比對使用），並將基於連接埠的規則取代為新的基於 App-ID 的規則。

如果您想要允許所有應用程式，但它們需要不同的處理，則請為每組需要不同處理的應用程式複製規則。例如，如果基於連接埠的規則允許三個應用程式，但其中兩個是電子郵件應用程式，而一個是基礎結構應用程式，則建議您為電子郵件應用程式複製一個規則，並為基礎結構應用程式建立另一個規則。

如果您想要允許某些應用程式，但拒絕其他應用程式：

- 為您想要保留的應用程式複製一個或多個規則，並監控原始基於連接埠的規則，確定您不想要保留的應用程式是唯一符合該規則的應用程式。如果過了足夠的時間，確信沒有您想要允許的應用程式符合基於連接埠的規則，則您可以停用或刪除它。轉換網際網路存取規則中的步驟 4-7 顯示如何建立複製的規則。
- 如果您確信知道想要允許的應用程式以及想要封鎖的應用程式：
  - 如果您想要允許的應用程式需要類似的處理，則請使用 **Add to Rule**（新增至規則）以將基於連接埠的規則取代為僅允許您新增至規則的應用程式的基於應用程式的規則。除非您在另一個規則中允許您未新增至規則的應用程式，否則會封鎖它們。
  - 如果您想要允許的應用程式需要不同的處理，則請透過基於連接埠的規則為您想要允許的應用程式複製基於應用程式的規則。如果您仍然確信可以封鎖其餘應用程式，則可以停用（或刪除）基於連接埠的規則。

採用安全性最佳做法的後續步驟

在您第一次通過將基於連接埠的規則轉換為基於應用程式的規則之後，請考慮使用下列步驟來加強安全性政策規則庫，並改善網路安全性：

- 使用 Expedition 的規則啟用功能，以使用機器學習來檢查和合併政策設定。
- 定期執行最佳做法評估 (BPA)，以測量達成 App-ID 採用目標的進度，以及識別其他弱點。當您到達目標時，請使用 BPA 識別您可繼續改善採用並進一步防衛網路的區域。
- 政策最佳化工具會將基於連接埠的規則轉換為基於 App-ID 的規則，但不會變更規則的其他所有項目。在您將傳統規則轉換為基於 App-ID 的規則之後，請加強規則以減少攻擊面並提高可見度：
  - 將 **Service**（服務）設定為 **application-default**，以防止應用程式使用非標準連接埠。針對內部自訂應用程式，定義預設連接埠，然後套用 **application-default**。
  - 在周邊（網際網路閘道），針對 Web 應用程式，使用 URL 篩選類別來防止存取具風險的網站。
  - 設定 User-ID 來控制誰可以存取應用程式。
  - 設定日誌轉送來集中管理來自多個 PAN-OS 設備的日誌、將特定警示的電子郵件警示傳送給特定管理員或群組，以及保留日誌來進行歷程記錄分析。
  - 設定防毒、反間諜軟體、弱點保護、檔案封鎖和 WildFire 分析的最佳做法安全性設定檔，然後將它們套用至 App-ID 安全性政策規則。
  - 請考慮使用 GitHub 上的 Iron-Skillet 範本來開始使用，以及啟動初始最佳做法設定。
- 維護 App-ID 部署。在您新增新應用程式的規則（包含內部自訂應用程式）時，請建立基於 App-ID 的規則，以協助維持您網路的安全。請不要回復為使用讓您無法查看應用程式流量或讓您無法檢查和控制它的基於連接埠的規則。深入了解 PAN-OS 管理員指南中的 App-ID。
- 在您加強安全性政策規則庫時，請考慮將其他保護套用至網路，例如解密流量以及 DoS 和區域保護的最佳做法。

如果您需要協助將傳統裝置設定移轉至 Palo Alto Networks 設備，請聯絡 Palo Alto Networks 的 Professional Services 群組，此群組具有豐富的移轉經驗，可用來達成成功移轉和成功轉換至 App-ID。