通過ASDM使用思科安全情報時配置IP黑名單（機箱內管理）

目錄

簡介

本檔案介紹思科安全情報/IP位址聲譽以及在使用低聲譽IP位址的自訂/自動饋送時對IP黑名單（封鎖）的組態。

必要條件

需求

思科建議您瞭解以下主題：

- ASA（自適應安全裝置）防火牆、ASDM（自適應安全裝置管理器）知識
- FirePOWER裝置知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本5.4.1及更高版本的ASA FirePOWER模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- 運行軟體版本6.0.0及更高版本的ASA FirePOWER模組(ASA 5515-X、ASA 5525-X、ASA

5545-X、ASA 555-X)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

思科安全情報由幾個定期更新的IP地址集合組成，這些地址被Cisco TALOS團隊確定為信譽不佳。Cisco TALOS團隊會確定是否有惡意活動源自這些IP地址（如垃圾郵件和惡意軟體、網路釣魚攻擊等）時，信譽較低。

Cisco IP Security Intelligence源跟蹤攻擊者、Bogon、Bots、CnC、Dga、ExploitKit、惡意軟體、Open_proxy、Open_relay、網路釣魚、響應、垃圾郵件、可疑的資料庫。Firepower模組確實提供了建立低信譽IP地址的自訂源的選項。

安全情報源概述

以下是有關可在安全情報中分類為不同類別的IP地址集合型別的更多資訊。

攻擊者：IP地址集合，這些地址不斷掃描漏洞或試圖利用其他系統。

惡意軟體：試圖傳播惡意軟體或主動攻擊任何訪問者的IP地址集合。

網路釣魚：正在積極嘗試誘騙終端使用者輸入使用者名稱和密碼等機密資訊的主機集合。

垃圾郵件：已確定為傳送垃圾郵件源的主機集合。

機器人：作為殭屍網路的一部分主動參與並由已知殭屍網路控制器控制的主機集合。

CnC:已確定為已知殭屍網路的控制伺服器的主機集合。

OpenProxy:已知運行Open Web代理並提供匿名Web瀏覽服務的主機集合。

OpenRelay:已知提供垃圾郵件和網路釣魚攻擊者使用的匿名電子郵件中繼服務的主機的集合。

TorExitNode:已知為Tor Anonymizer網路提供送出節點服務的主機的集合。

博貢：未分配但正在傳送流量的IP地址的集合。

可疑：顯示可疑活動並處於活動調查中的IP地址集合。

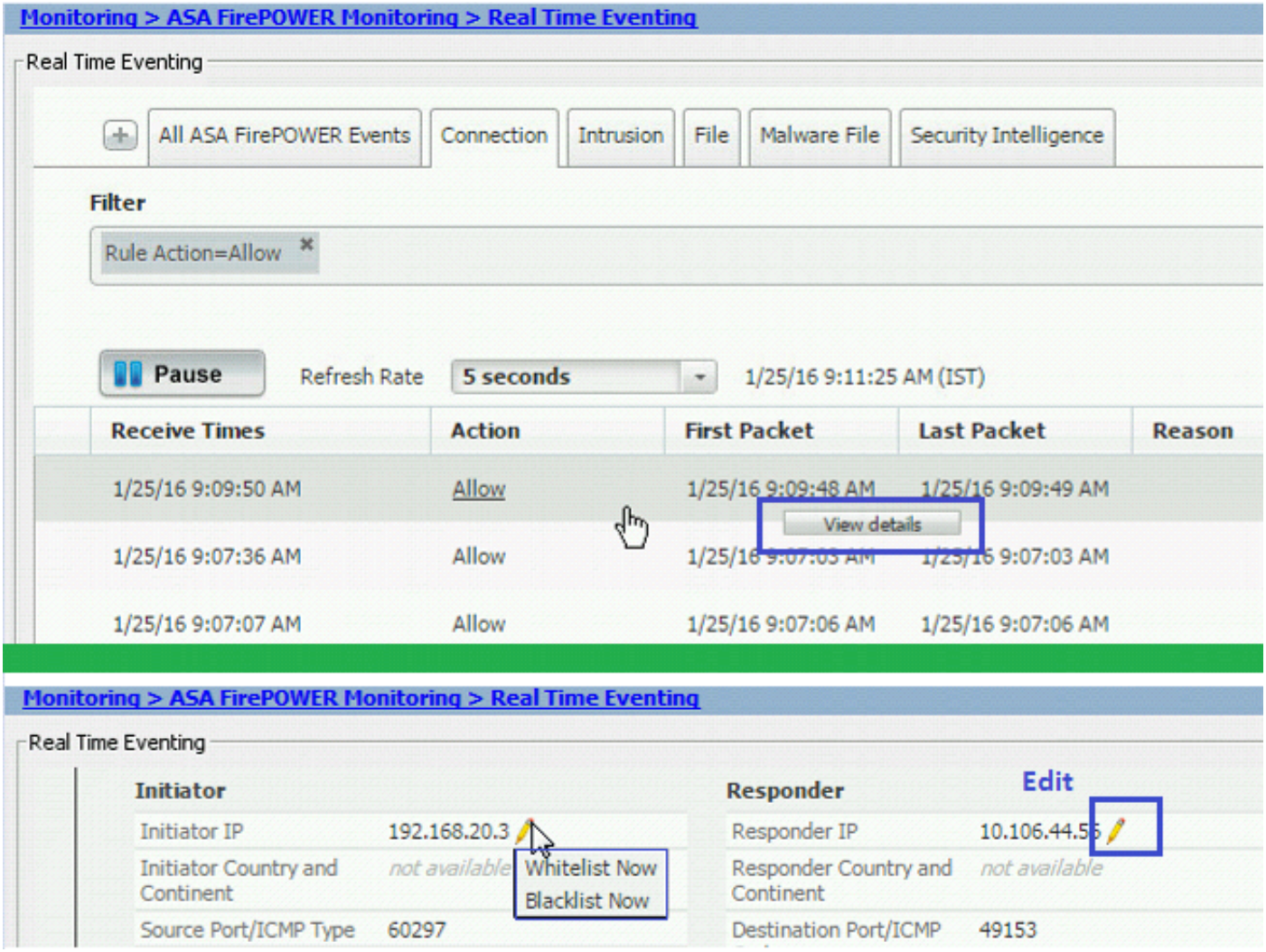
回應：收集重複觀察到的IP地址參與可疑或惡意行為。

手動將IP地址新增到全域性黑名單和全域性白名單

Firepower模組允許您在知道某些IP地址屬於某些惡意活動時，將其新增到全域性黑名單中。如果希望允許流量到達被黑名單IP地址阻止的某些IP地址，也可以將IP地址新增到全域性白名單。如果將任何IP地址新增到Global-Blacklist/Global-Whitelist中，則該地址會立即生效，無需應用策略。

要將IP地址新增到Global-Blacklist/Global-Whitelist，請導航到**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**，將滑鼠懸停在連線事件上，然後選擇**View Details**。

您可以將源IP地址或目標IP地址新增到全域性黑名單/全域性白名單。按一下**Edit**按鈕，然後選擇**Whitelist Now/Blacklist Now**，將IP位址新增到各自的清單，如下圖所示。



若要驗證源或目標IP地址是否已新增到全域性黑名單/全域性白名單，請導航到**Configuration > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds**，然後編輯**Global-Blacklist/全域性白名單**。您還可以使用delete按鈕從清單中刪除任何IP地址。

建立黑名單IP地址的自定義清單

Firepower允許您建立可用於黑名單（阻止）的自定義網路/IP地址清單。 有三種方法可以做到這一點：

1. 您可以將IP地址寫入文本檔案（每行一個IP地址）並將檔案上傳到Firepower模組。若要上傳檔案，請導航到**Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds**，然後點選**Add Network Lists and Feeds**
   名稱: 指定自定義清單的名稱。 **Type: 從下拉選單中選擇List。** **上傳清單：** 選擇**Browse**以在系統中查詢文本檔案。選擇選項**Upload**以上傳檔案。
2. 您可以將任何第三方IP資料庫用於自定義清單，Firepower模組會聯絡第三方伺服器以獲取該IP地址清單。要配置此配置，請導航到**Configuration > ASA FirePOWER Configuration >**

Object Management > Security Intelligence > Network Lists and Feeds，然後點選Add Network Lists and Feeds

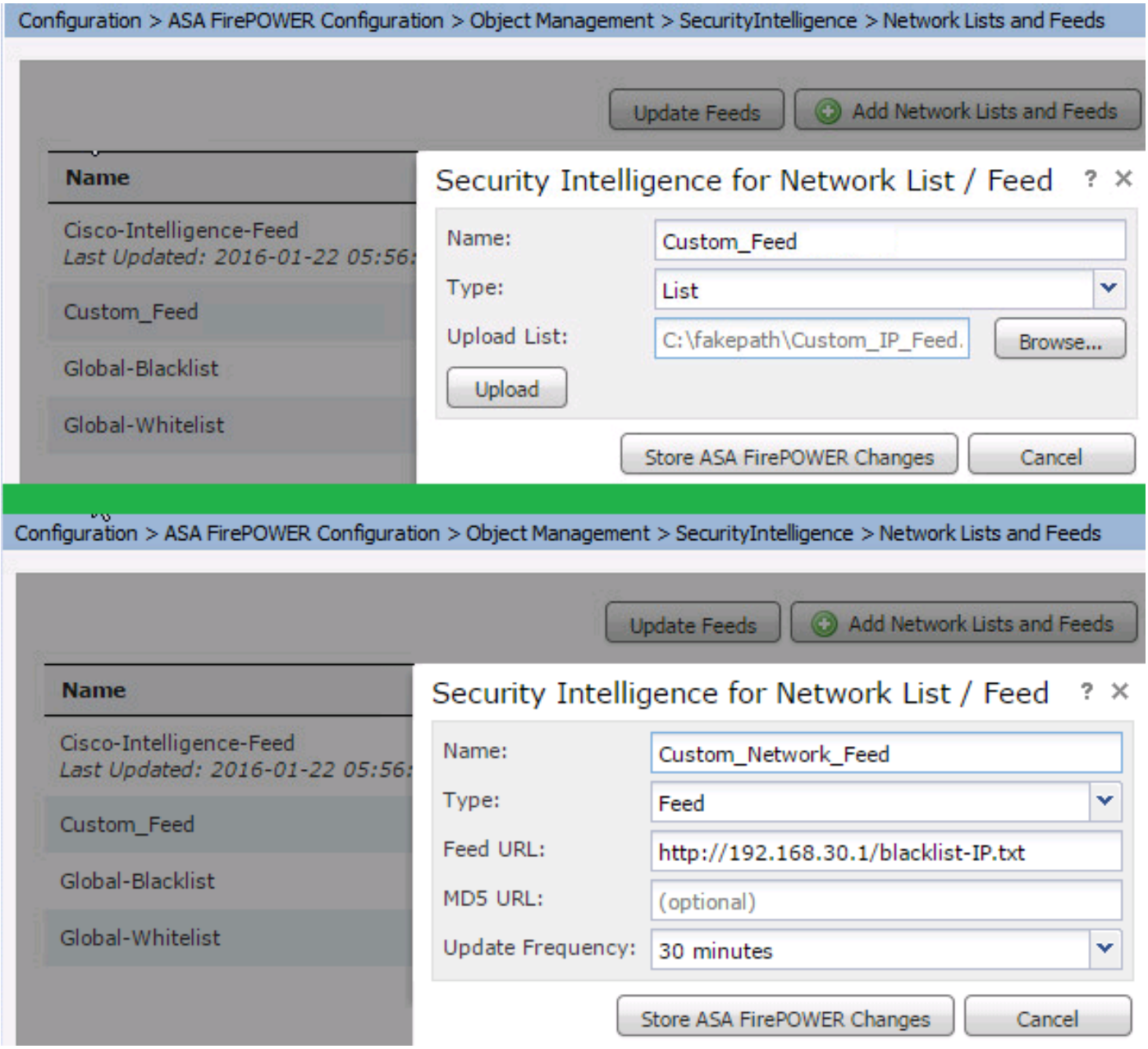
名稱:指定自定義源的名稱。

Type:從下拉選單中選擇Feed選項。

源URL:指定Firepower模組應連線到的伺服器的URL並下載源。

MD5 URL:指定雜湊值以驗證源URL路徑。

更新頻率：指定系統連線到URL源伺服器的時間間隔。



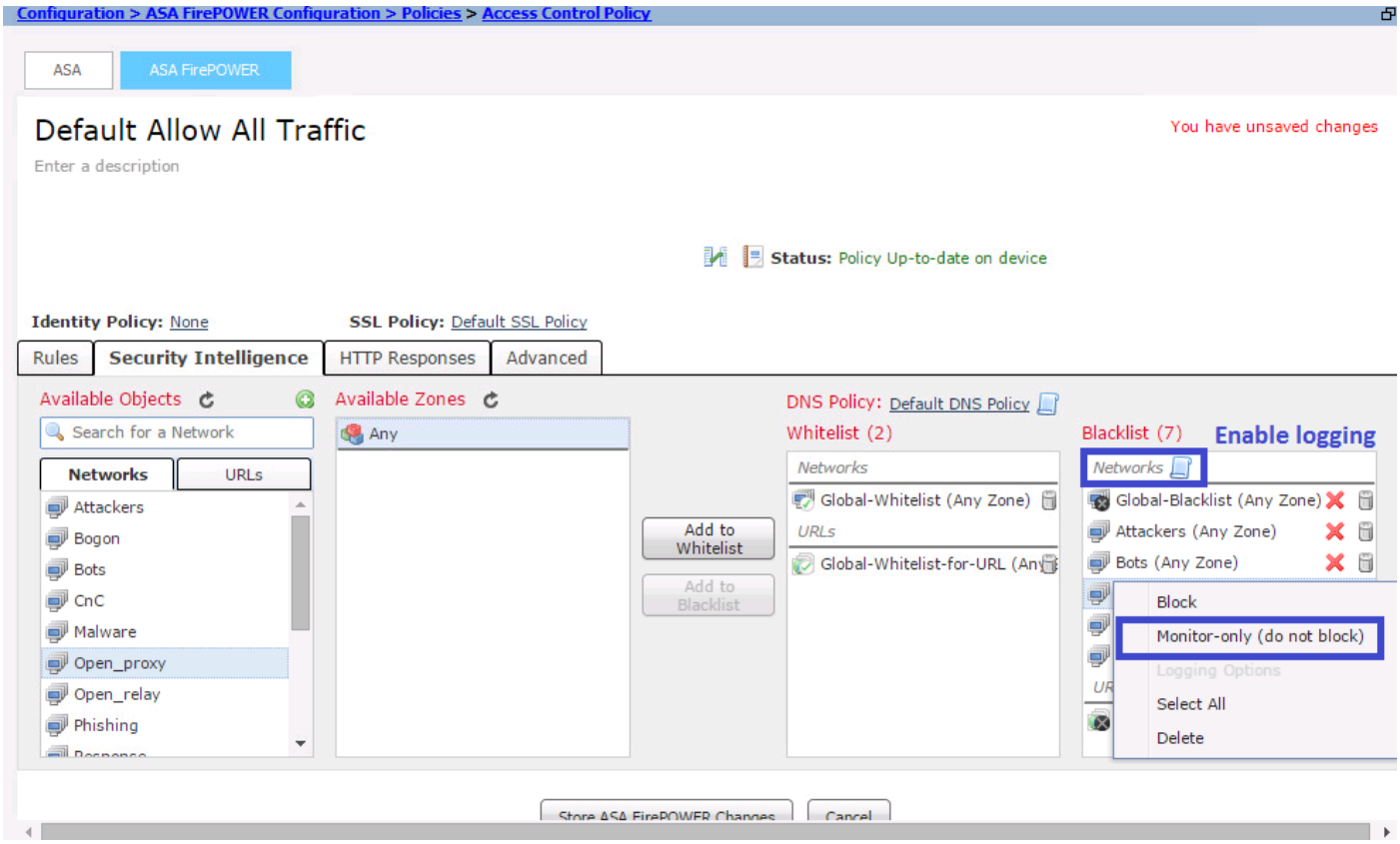
配置安全情報

要配置安全智慧，請導航到**配置> ASA Firepower配置>策略>訪問控制策略，選擇安全智慧**頁籤。

從網路可用對象中選擇源，移動到**白名單/黑名單**列以允許/阻止與惡意IP地址的連線。

您可以點選圖示並啟用日誌記錄，如映像中所指定。

如果您只想為惡意IP連線生成事件，而不是阻止連線，則按一下右鍵源，選擇**Monitor-only(not block)**，如下圖所示：

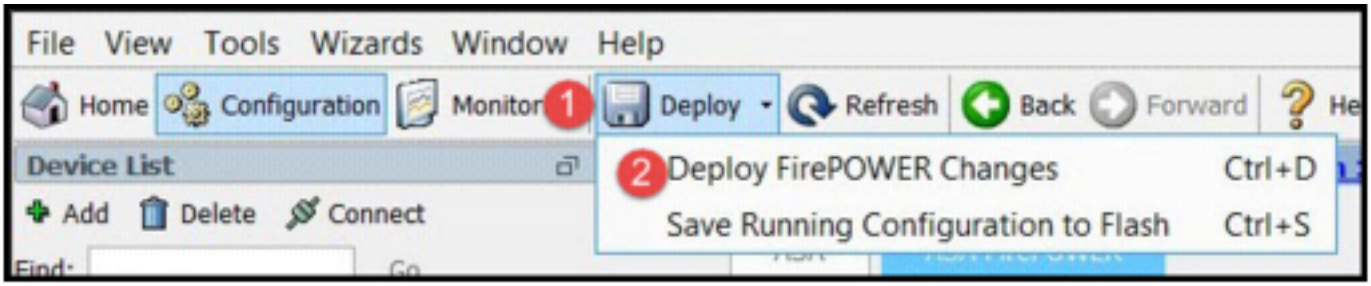


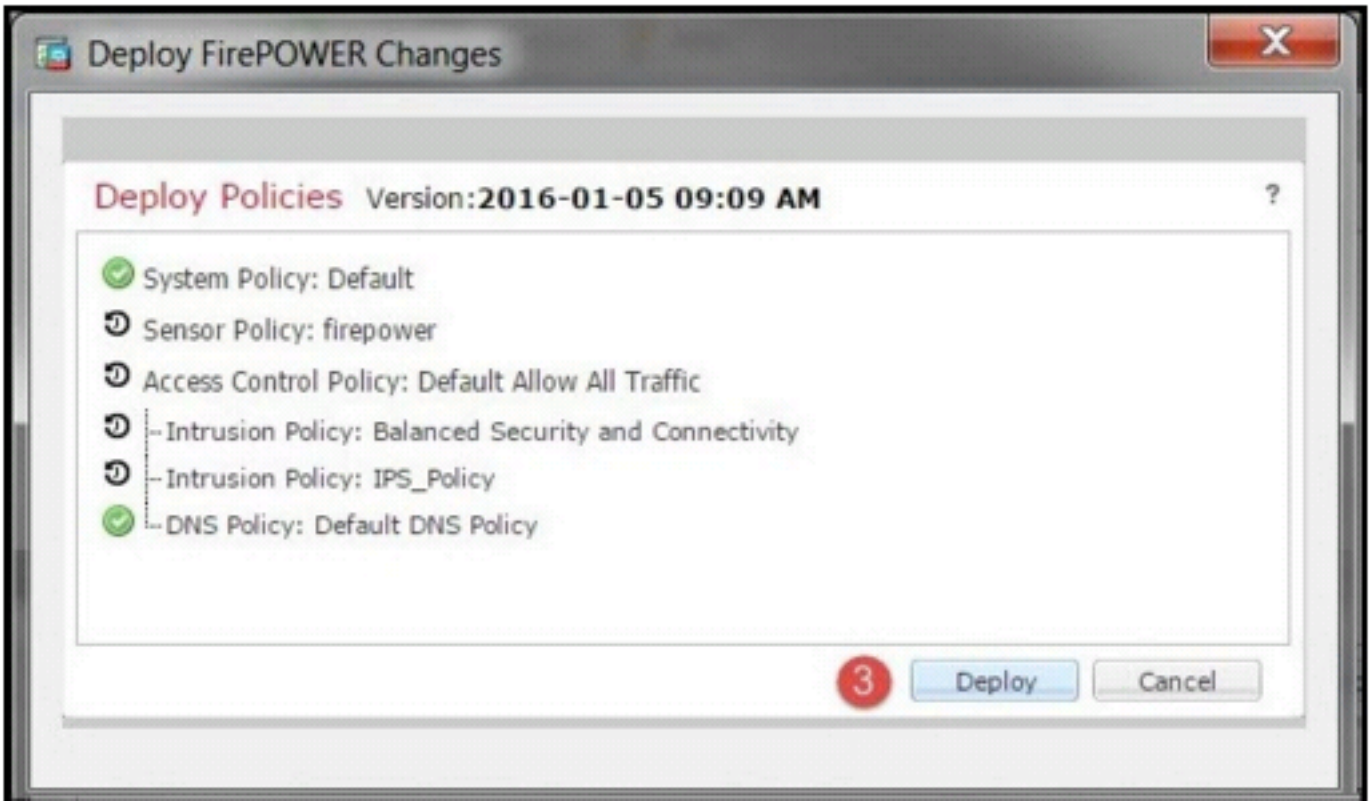
選擇選項Store ASA Firepower Changes以儲存AC策略更改。

部署訪問控制策略

要使更改生效，必須部署訪問控制策略。在應用策略之前，請參閱顯示裝置上的訪問控制策略是否過期的指示。

要將更改部署到感測器，請c按一下**Deploy**並選擇**Deploy FirePOWER Changes**，然後在彈出視窗中選擇**Deploy**以部署更改。



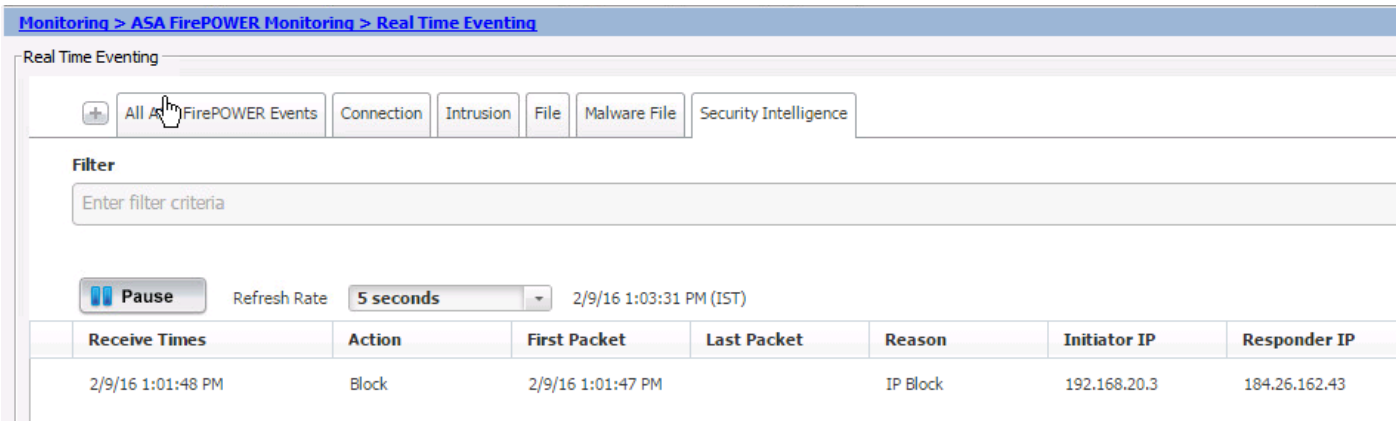


: 5.4.xASA FirePOWER

> ASA Firepower>

安全情報的事件監控

要檢視Firepower模組的安全情報，請導航到**監控> ASA Firepower監控>即時事件**。選擇**Security Intelligence選**項卡。這樣將顯示事件，如下圖所示：

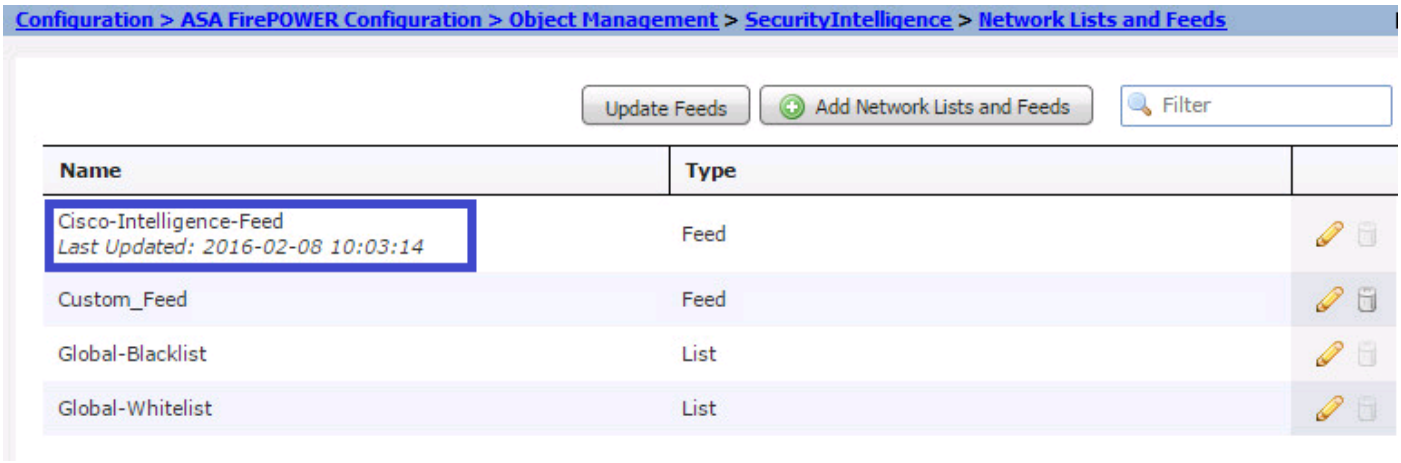


驗證

目前沒有適用於此組態的驗證程序。

疑難排解

為了確保安全情報源是最新的，請導航到Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feed，並檢查上次更新源的時間。可以選擇「編輯」按鈕以設定源更新的頻率。



確保已成功完成訪問控制策略部署。

監控安全情報以檢視流量是否被阻止。

- Cisco ASA FirePOWER
- - Cisco Systems