使用ASDM（機箱內管理）在FirePOWER模組中配置基於域的安全智慧（DNS策略）

目錄

簡介
必要條件
需求
採用元件
背景資訊
域清單和源概述
Cisco TALOS提供的域清單和源
自定義域清單和源
配置DNS安全情報
步驟1.配置自定義DNS源/清單（可選）。
手動將IP地址新增到全域性黑名單和全域性白名單
建立黑名單域的自定義清單
步驟2.配置Sinkhole對象（可選）。
步驟3.配置DNS策略。
步驟4.配置訪問控制策略。
步驟5.部署訪問控制策略。
驗證
DNS安全情報事件監控
疑難排解
相關資訊

簡介

本文檔介紹如何使用自適應安全裝置管理器(ASDM)在具有FirePOWER模組的ASA上配置基於域的安全智慧(SI)。

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）防火牆知識
- ASDM（自適應安全裝置管理器）
- FirePOWER模組知識

附註：安全情報過濾器需要保護許可證。

採用元件

本檔案中的資訊是根據以下軟體版本：

- ASA FirePOWER模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)，軟體版本為6.0.0及更高
- ASA FirePOWER模組(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)，軟體版本為6.0.0及更高

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

Firepower系統能夠攔截DNS流量請求並查詢惡意域名。如果Firepower模組發現惡意域，則Firepower會根據DNS策略的配置採取相應操作來緩解請求。

新的攻擊方法旨在突破基於IP的情報，濫用DNS負載平衡功能，以隱藏惡意伺服器的實際IP地址。雖然與攻擊相關的IP地址經常被換進和換出，但域名很少被更改。

Firepower能夠將惡意請求重定向到黑洞(Sinkhole)伺服器，該伺服器可以是蜜罐伺服器，用於檢測、轉移或研究對攻擊流量的更多瞭解。

域清單和源概述

域清單和源包含惡意域名的清單，該清單根據攻擊型別進一步分為各種類別。通常，可以將源分為兩種型別。

Cisco TALOS提供的域清單和源

DNS攻擊者：不斷掃描漏洞或試圖利用其他系統的域名的集合。

DNS Bogon：不分配但重新傳送流量的域名集合，也稱為假IP。

DNS殭屍程式：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域名的集合。

DNS CnC：已知殭屍網路識別為控制伺服器的域名集合。

DNS漏洞攻擊包：試圖利用其他系統的域名集合。

DNS惡意軟體：試圖傳播惡意軟體或主動攻擊任何訪問者的域名集合。

DNS Open_proxy：運行Open Web代理並提供匿名Web瀏覽服務的域名集合。

DNS Open_relay：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域名集合。

DNS網路釣魚：域名集合，這些域名會主動嘗試誘騙終端使用者輸入其機密資訊，如使用者名稱和密碼。

DNS響應：重複觀察到參與可疑或惡意行為的域名的集合。

DNS垃圾郵件：標識為傳送垃圾郵件源的域名的集合。

DNS可疑：顯示可疑活動並處於活動調查中的域名的集合。

DNS Tor_exit_node：為Tor匿名程式網路提供退出節點服務的域名的集合。

自定義域清單和源

DNS全域性黑名單：管理員識別為惡意的域名的自定義清單集合。

DNS全域性白名單：由管理員識別為正版的域名的自定義清單的集合。

配置DNS安全情報

配置基於域名的安全情報有多個步驟。

1. 配置自定義DNS源/清單（可選）
2. 配置Sinkhole對象（可選）
3. 配置DNS策略
4. 配置訪問控制策略
5. 部署訪問控制策略

步驟1.配置自定義DNS源/清單（可選）。

有兩個預定義清單可用於向其中新增域。您可以為要阻止的域建立自己的清單和源。

- DNS全域性黑名單
- DNS全域性白名單

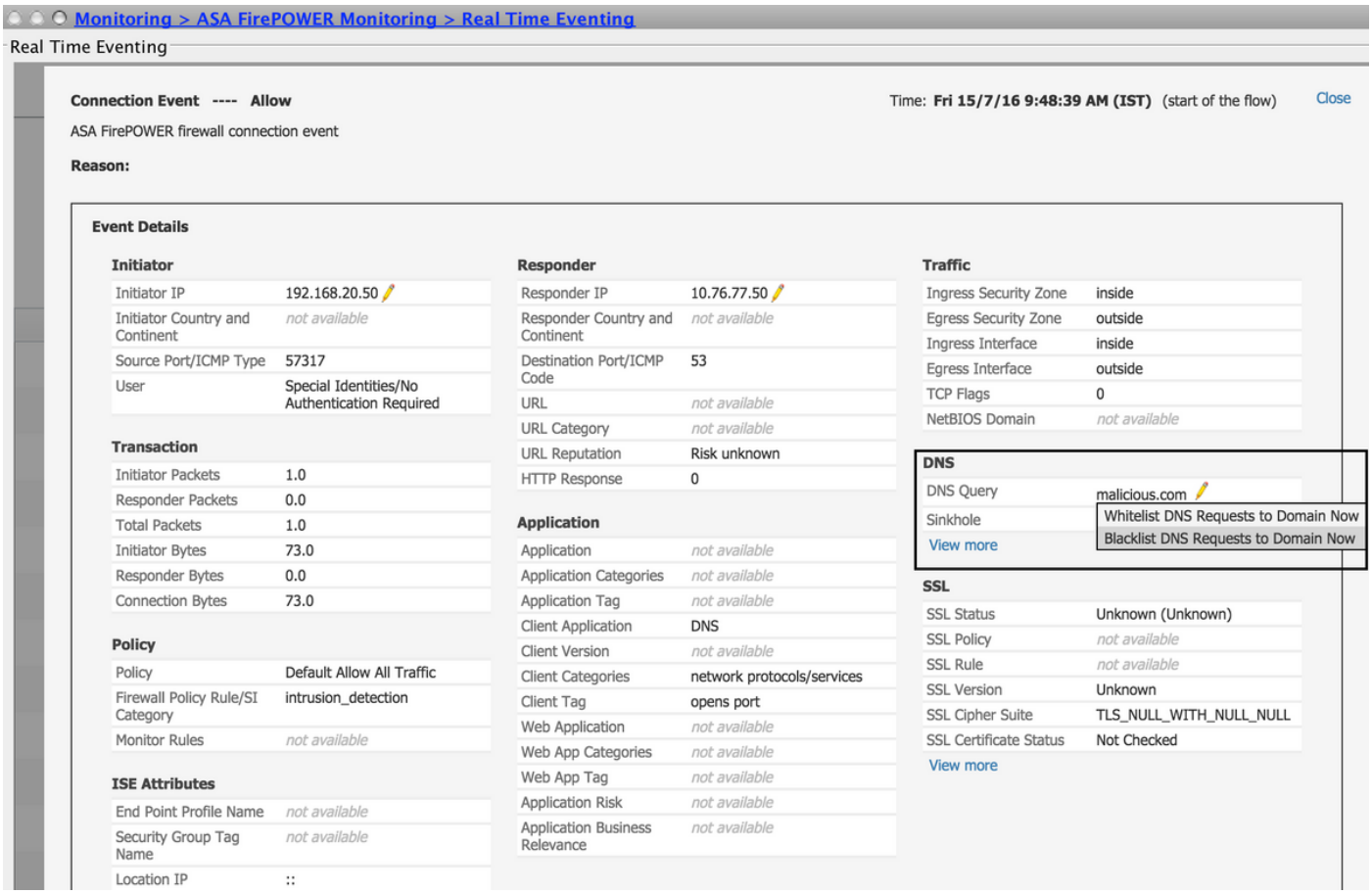
手動將IP地址新增到全域性黑名單和全域性白名單

Firepower模組允許您在知道某些域屬於某些惡意活動時，將其新增到全域性黑名單中。如果希望允許流向被黑名單域阻止的特定域的流量，還可以將域新增到全域性白名單。如果將任何域新增到Global-Blacklist/Global-Whitelist，則無需應用策略即可立即生效。

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**。

您可以將域新增到全域性黑名單/全域性白名單。按一下「**Edit**」部分，然後選擇「**Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now**」，將網域新增到各自的清單

，如下圖所示。



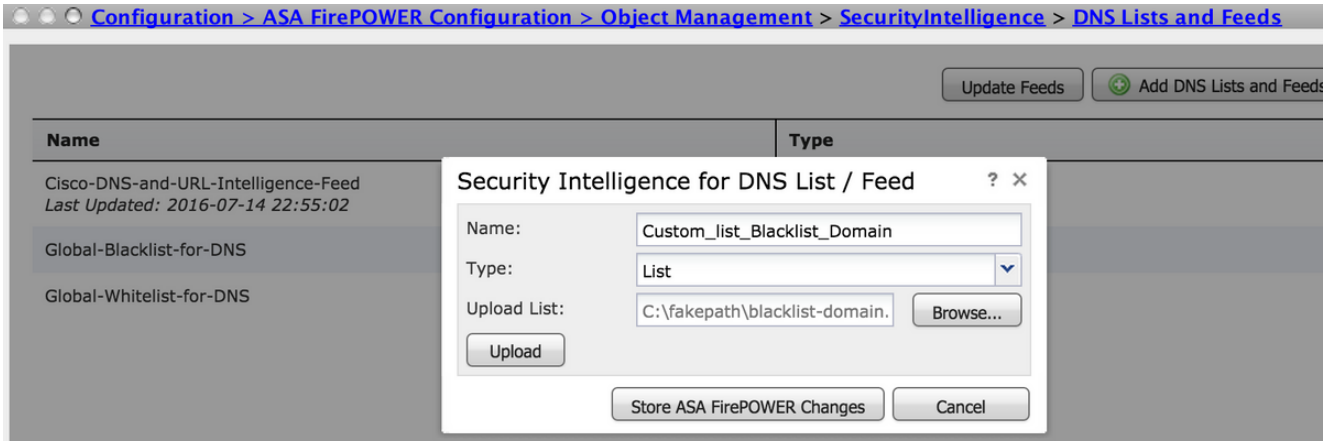
若要驗證是否已將網域新增到全域黑名單/全域白名單，請導覽至**Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds**，然後編輯**DNS的全域黑名單/DNS的全域白名單**。還可以使用「刪除」按鈕從清單中刪除任何域。

建立黑名單域的自定義清單

Firepower允許您建立自定義域清單，該清單可用於通過兩種不同的方法將其列入黑名單（阻止）。

1. 可以將域名寫入文本檔案（每行一個域）並將該檔案上傳到FirePOWER模組。

   若要上傳檔案，請導覽至**Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds**，然後選擇**Add DNS 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**Upload**以上傳檔案。



按一下**Store ASA FirePOWER Changes**以儲存更改。

2. 您可以將任何第三方域用於自定義清單，Firepower模組可以連線第三方伺服器以獲取域清單。

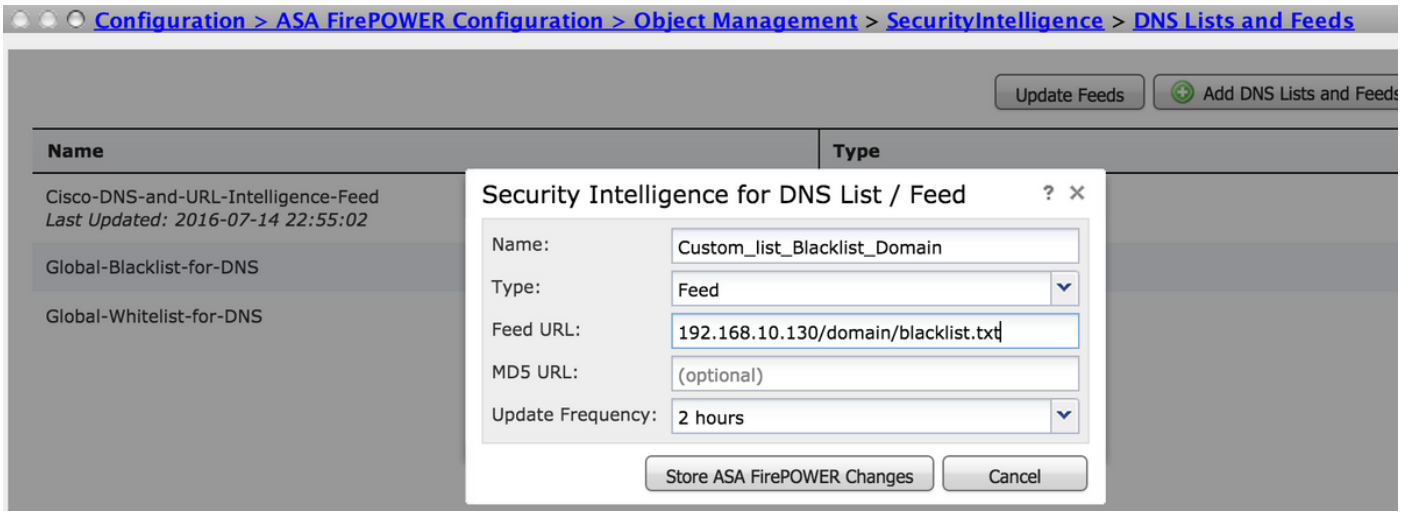
   若要配置此項，請導航到**Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds**，然後選擇**Add DNS Lists and Feeds**
   名稱:指定自定義源的名稱。

   Type:從下拉選單中選擇Feed。

   源URL:指定FirePOWER模組可以連線並下載源的伺服器URL。

   MD5 URL:指定雜湊值以驗證源URL路徑。

   更新頻率：指定模組連線到URL源伺服器的時間間隔。



選擇**Store ASA FirePOWER Changes**以儲存更改。

步驟2.配置Sinkhole對象（可選）。

Sinkhole IP地址可用作對惡意DNS請求的響應。客戶端電腦獲取Sinkhole伺服器的IP地址以進行惡意域查詢，並且終端電腦嘗試連線到Sinkhole伺服器。因此，Sinkhole可以作為蜜罐來檢測攻擊流量。可以將sinkhole配置為觸發危害指示器(IOC)。

要新增Sinkhole伺服器，請**依次選擇Configuration > ASA FirePOWER Configuration > Object Management > Sinkhole**，然後按一下**Add Sinkhole**選項。

名稱:指定sinkhole伺服器的名稱。

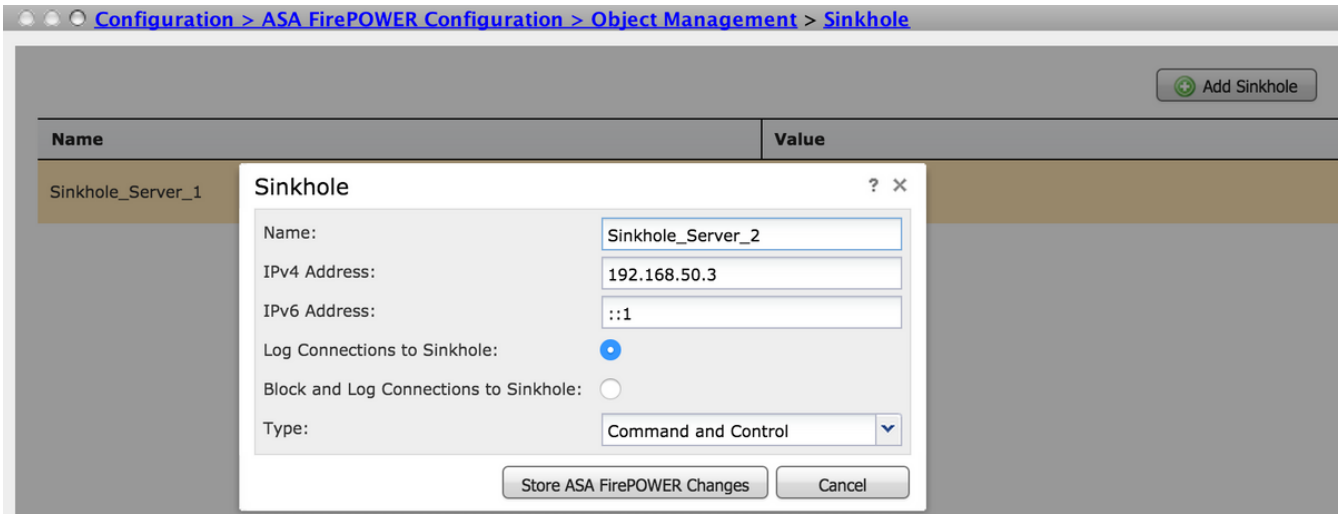
IP 位址:指定sinkhole伺服器的IP地址。

記錄到Sinkhole的連線：啟用此選項可記錄終端和黑洞伺服器之間的所有連線。

阻止並記錄到Sinkhole的連線：啟用此選項可阻止連線並僅在流連線開始時進行記錄。如果沒有物理黑洞伺服器，可以指定任何IP地址，並且可以看到連線事件和IOC觸發器。

Type:從下拉選單中選擇要選擇與sinkhole事件關聯的IOC型別（危害表現）的原始檔。有三種型別的sinkhole IOC可以標籤。

- 惡意軟體
- 命令與控制
- 網路釣魚



步驟3.配置DNS策略。

需要配置DNS策略以確定DNS源/清單的操作。導航到**Configuration > ASA FirePOWER Configuration > Policies > DNS Policy。**

預設DNS策略包含兩個預設規則。第一條 規則**DNS的全域性白名單**包含允許域的自定義清單(Global-Whitelist-for-DNS)。 此規則位於頂端，在系統嘗試匹配任何黑名單域之前，首先匹配。第二條 規則**DNS全域性黑名單**包含阻止域的自定義清單(Global-Blacklist-for-DNS)。

您可以新增更多規則來定義Cisco TALOS提供的**域清單和源的各種操作**。要新增新規則，請選擇**新增DNS規則。**

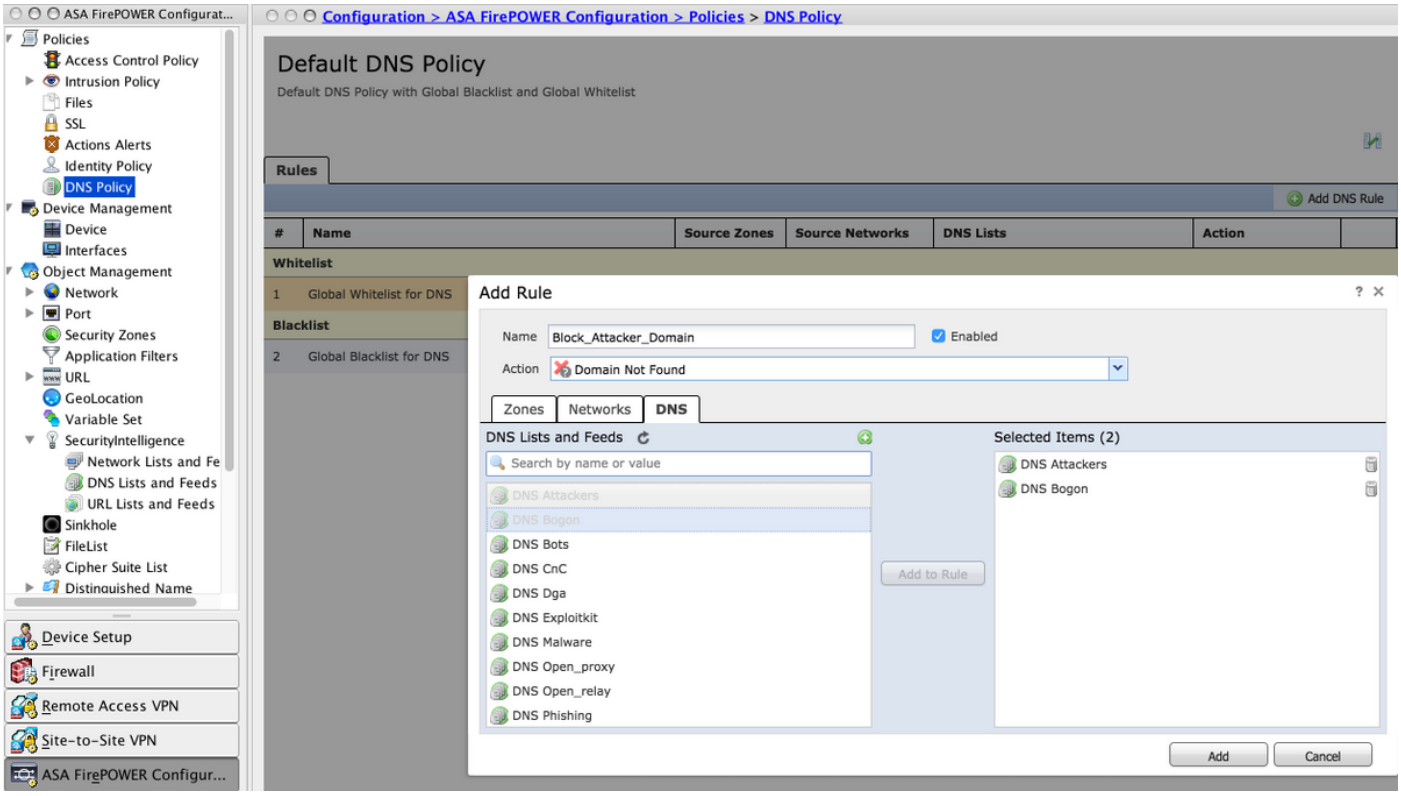
名稱：指定規則名稱。

Action: 指定此規則匹配時要觸發的操作。

- **白名單**：這允許DNS查詢。
- **監視**:此操作會為DNS查詢生成事件，並且流量繼續匹配後續規則。
- **找不到域**：此操作將DNS響應作為未找到域（不存在域）傳送。
- **Drop**:此操作以靜默方式阻止和丟棄DNS查詢。
- **Sinkhole**:此操作將傳送Sinkhole伺服器的IP地址作為對DNS請求的響應。

指定區**域/網路**以定義規則條件。在DNS頁籤中，選擇**DNS清單和源**，並移至**Selected Items**選項，您可以在其中應用已配置的操作。

您可以根據組織需要，使用不同的操作為不同的DNS清單和源配置多個DNS規則。

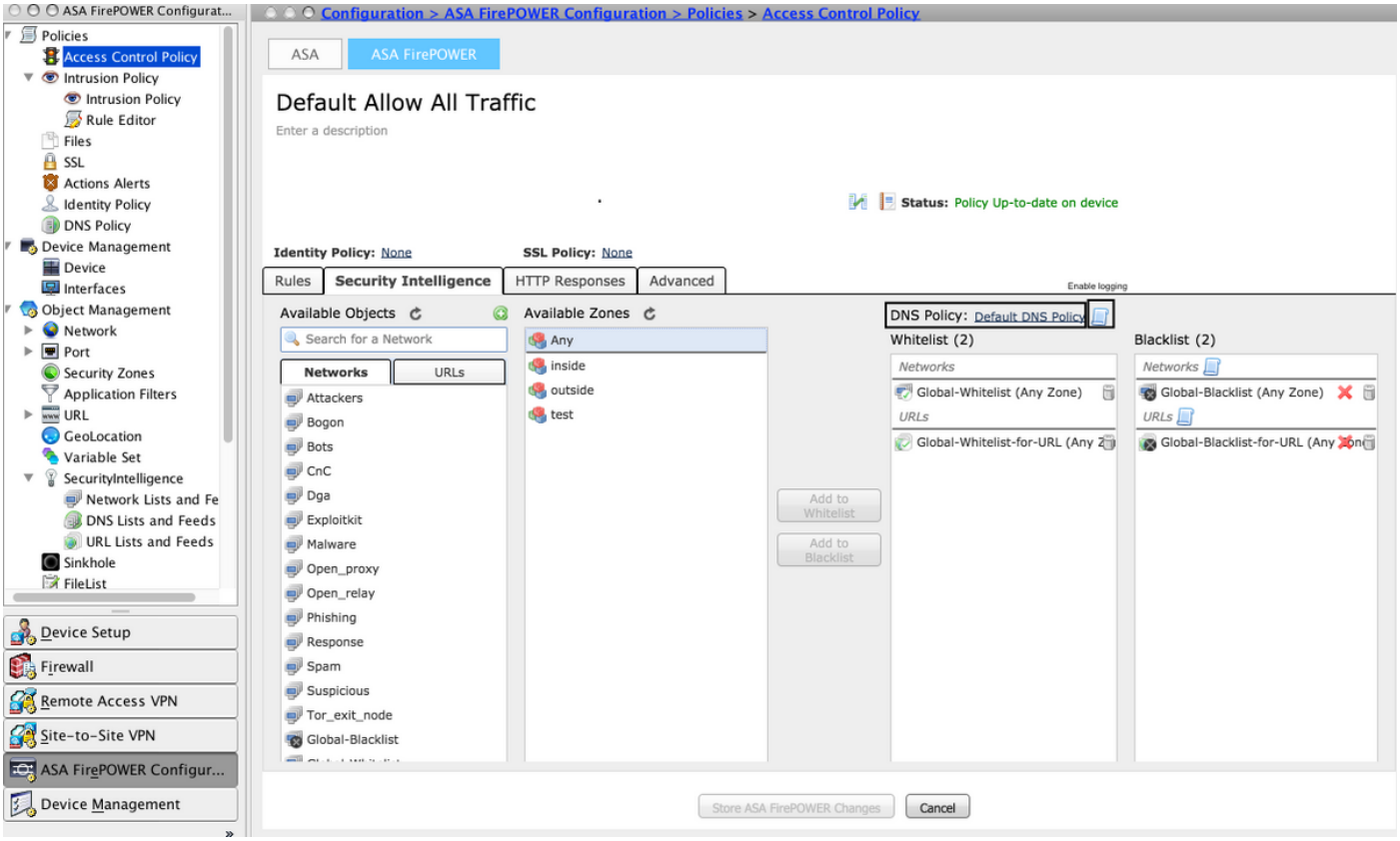


按一下**Add**選項新增規則。

步驟4.配置訪問控制策略。

要配置基於DNS的安全智慧，請導航至**配置> ASA Firepower配置>策略>訪問控制策略，選擇安全智慧**頁籤。

確保配置了DNS策略，或者，您也可以在按一下日誌圖示時啟用日誌，如下圖所示。



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

步驟5.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。

> **附註**：在5.4.x版本中，要將訪問策略應用到感測器，需要按一下**應用ASA FirePOWER更改**。

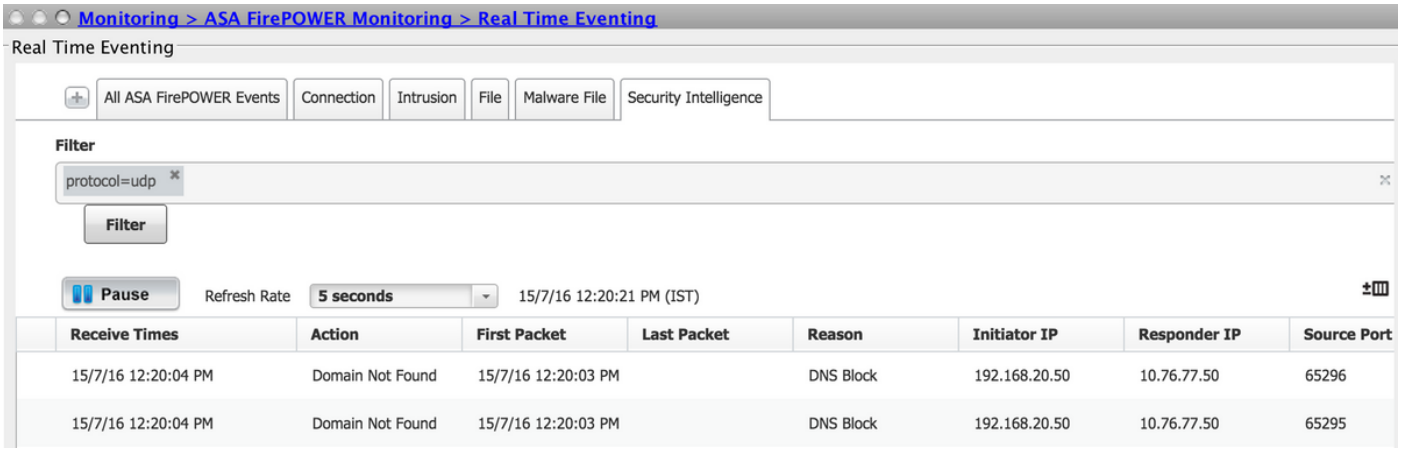
> **附註**：導航到**監控> ASA Firepower監控>任務狀態**。確保任務已完成，以確認配置更改。

驗證

僅當觸發事件時才能驗證配置。為此，您可以在電腦上強制DNS查詢。但是，當已知的惡意伺服器被攻擊時，請小心後果。生成此查詢後，您可以在「即時事件」**部分中檢視**事件。

DNS安全情報事件監控

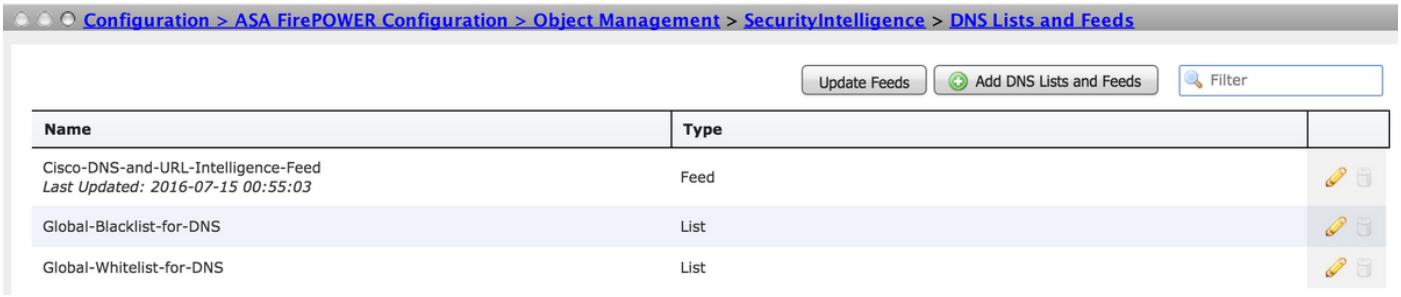
要檢視Firepower模組的安全情報，請導航到**監控> ASA Firepower監控>即時事件**。選擇**Security Intelligence選**項卡。如下圖所示顯示事件：



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

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 > DNS Lists and Feed**，並檢查上次更新源的時間。可以選擇**編輯**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Security Intelligence Real Time Eventing頁籤，檢視流量是否被阻止。

相關資訊

- [Cisco ASA FirePOWER模組快速入門手冊]
- [技術支援與文件 - Cisco Systems]