在Firepower模組中配置入侵策略和簽名配置（機箱內管理）

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[組態](#)
[步驟1.配置入侵策略](#)
[步驟1.1.建立入侵策略](#)
[步驟1.2.修改入侵策略](#)
[步驟1.3.修改基本策略](#)
[步驟1.4.使用篩選條選項進行簽名篩選](#)
[步驟1.5.配置規則狀態](#)
[步驟1.6.配置事件過濾器](#)
[步驟1.7.配置動態狀態](#)
[步驟2.配置網路分析策略(NAP)和變數集（可選）](#)
[步驟3:配置訪問控制以包括入侵策略/NAP/變數集](#)
[步驟4.部署訪問控制策略](#)
[步驟5.監控入侵事件](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

簡介

本文檔介紹FirePOWER模組的入侵防禦系統(IPS)/入侵檢測系統(IDS)功能，以及在FirePOWER模組中制定檢測策略的各種入侵策略元素。

必要條件

需求

思科建議您瞭解以下主題：

*瞭解自適應安全裝置(ASA)防火牆、自適應安全裝置管理器(ASDM)。

* 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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FirePOWER IDS/IPS旨在檢查網路流量並識別任何指示網路/系統攻擊的惡意模式（或簽名）。如果ASA的服務策略在監控模式（混雜）下進行了專門配置，則FirePOWER模組在IDS模式下工作，否則它在內聯模式下工作。

FirePOWER IPS/IDS是一種基於簽名的檢測方法，IDS模式下的FirePOWER模組在簽名與惡意流量匹配時生成警報，而IPS模式下的FirePOWER模組生成警報並阻止惡意流量。

: FirePOWER**ProtectConfiguration > ASA FirePOWER Configuration > License**

組態

步驟1.配置入侵策略

步驟1.1.建立入侵策略

要配置入侵策略，請登入自適應安全裝置管理器(ASDM)並完成以下步驟：

步驟1.導航到**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy**。

步驟2.按一下**Create Policy**。

步驟3.輸入入侵策略的**名稱**。

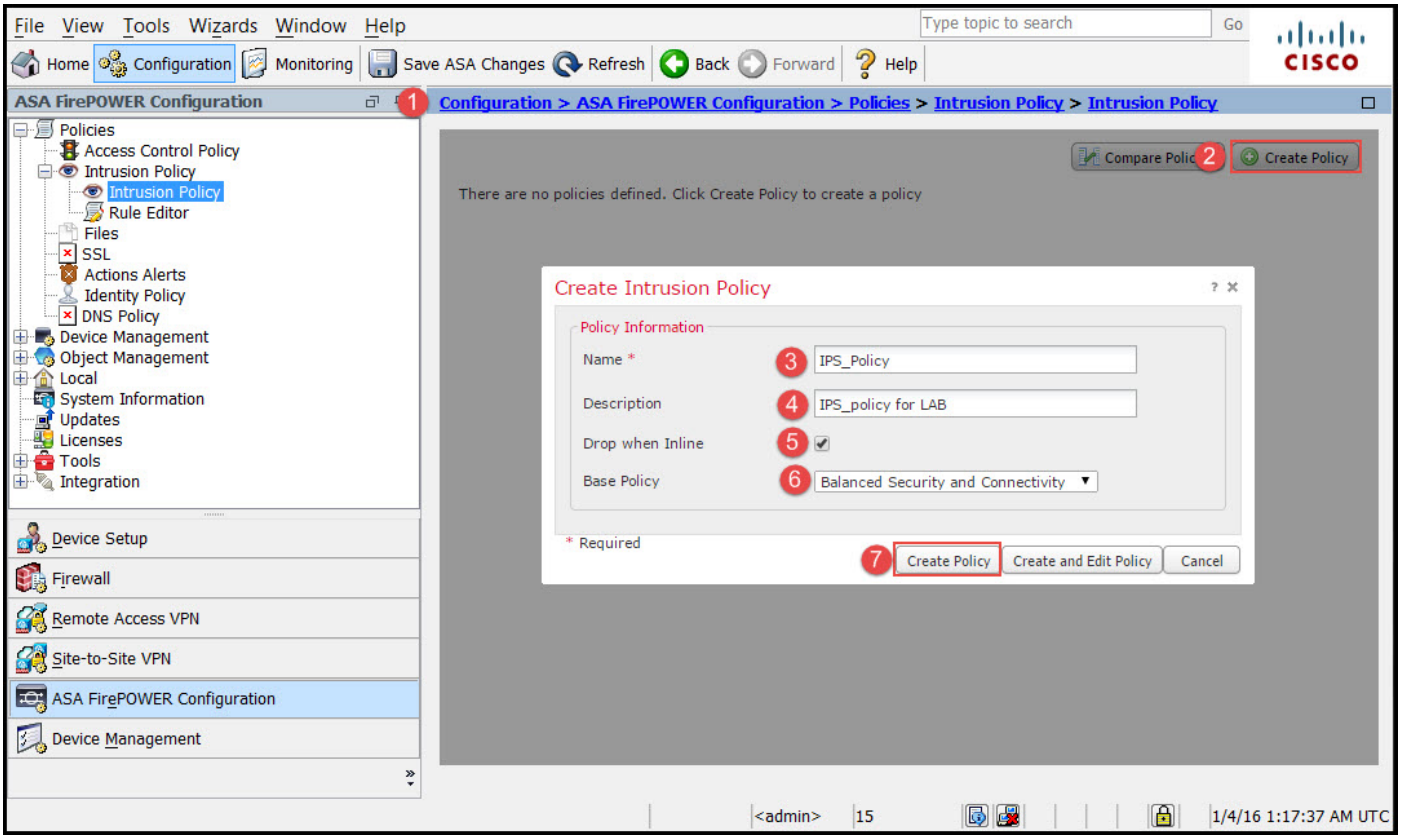
步驟4.輸入**Description** of the Intrusion Policy（可選）。

步驟5.指定**Drop when Inline選**項。

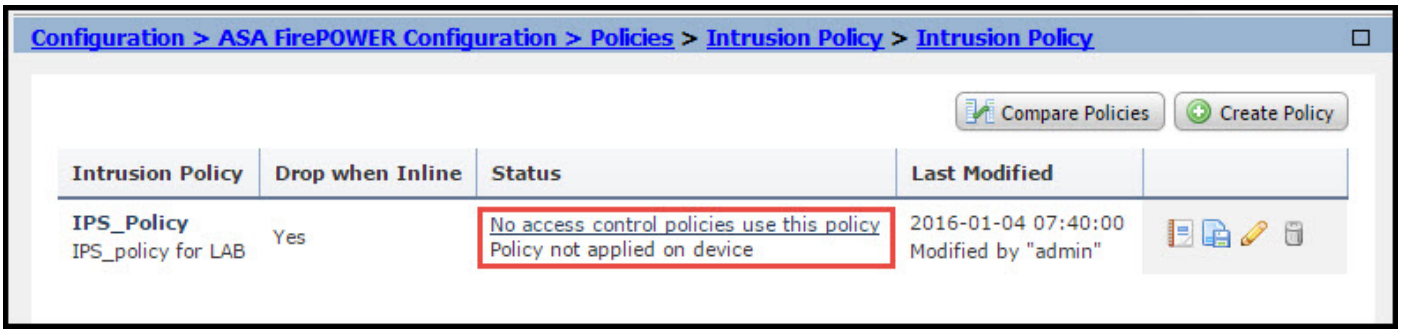
步驟6.從下拉選單中選擇**Base Policy**。

步驟7.按一下**Create Policy**完成入侵策略建立。

: Drop when InlineInline

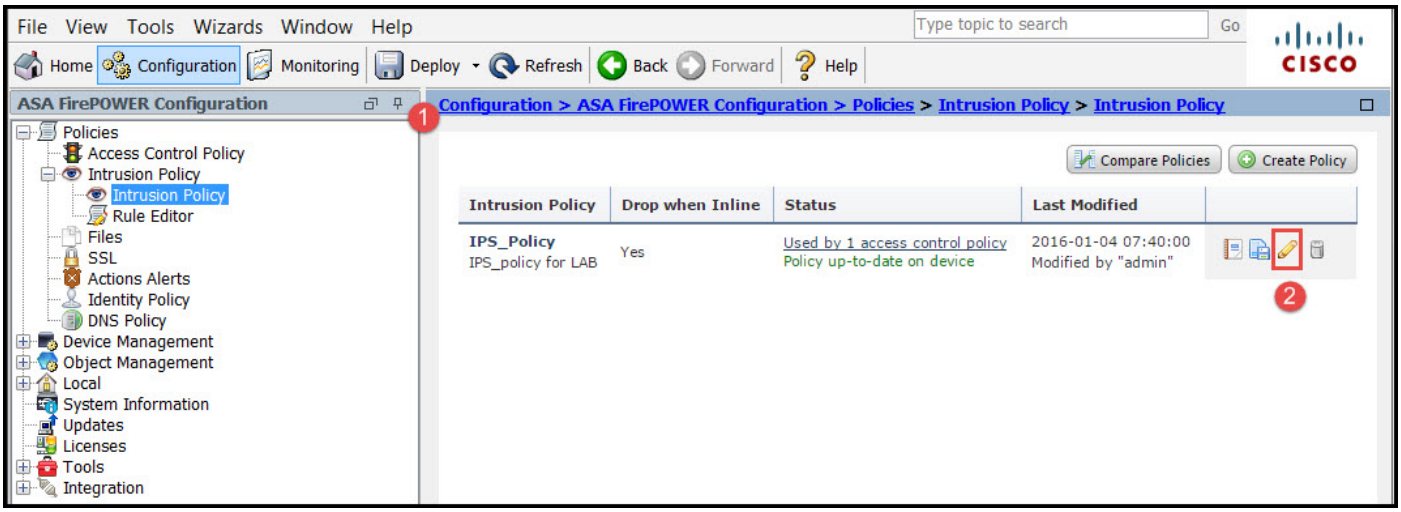


您可以注意到，策略已配置，但未應用於任何裝置。



步驟1.2.修改入侵策略

要修改入侵策略，請導航到Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy，然後選擇Edit選項。

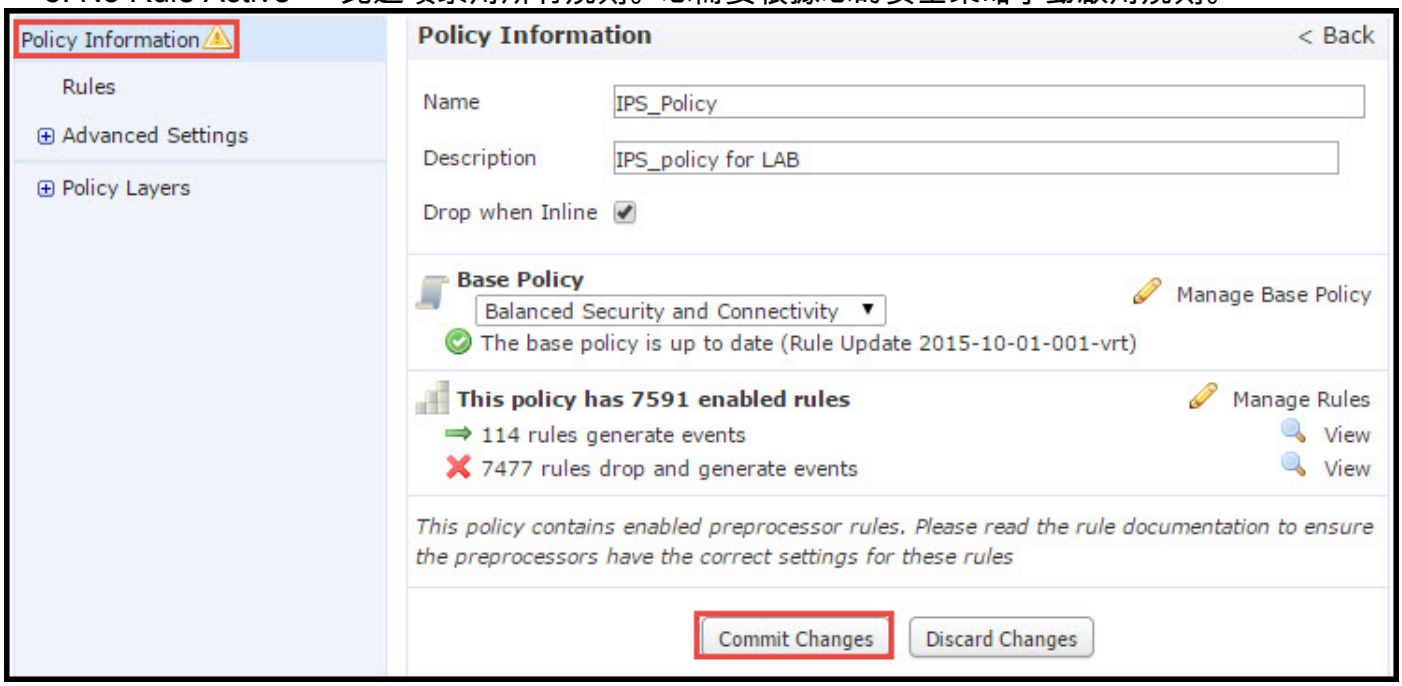


步驟1.3.修改基本策略

Intrusion Policy Management頁面提供了更改Base Policy/Drop when Inline/Save and Discard選項的選項。

基本策略包含一些系統提供的策略，這些策略是內建策略。

1. 平衡的安全和連線：它是安全和連線方面的最佳策略。此策略已啟用約7500個規則，其中有些規則僅生成事件，而有些規則生成事件並丟棄流量。
2. 安全性高於連線性：如果您的偏好是安全性，則可以選擇安全性而非連線策略，這將增加已啟用規則的數量。
3. 連線而非安全：如果您的首選是連線而非安全，則您可以選擇連線而非安全策略，這樣可以減少已啟用規則的數量。
4. Maximum Detection — 選擇此策略可獲得最大檢測。
5. No Rule Active — 此選項禁用所有規則。您需要根據您的安全策略手動啟用規則。



步驟1.4.使用篩選條選項進行簽名篩選

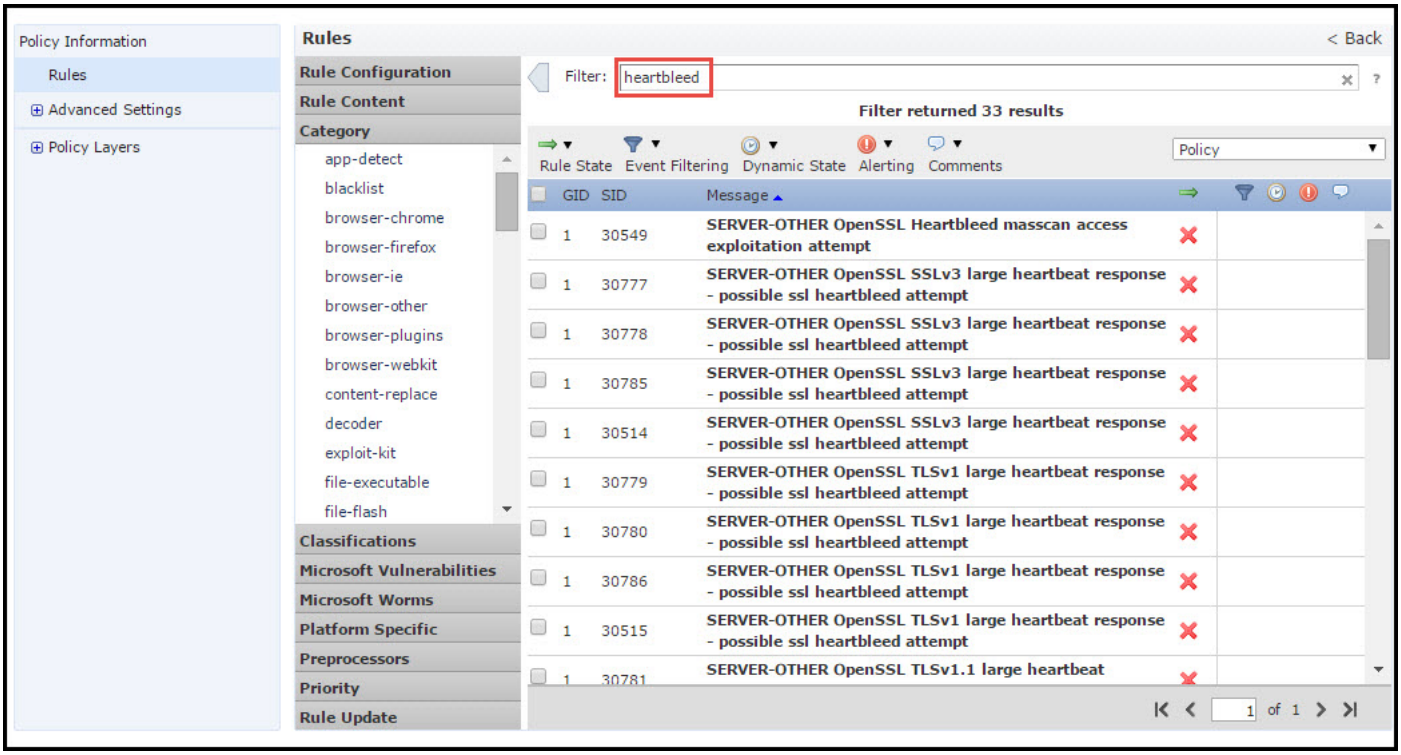
導航到導航面板中的**Rules**選項，然後顯示Rule Management頁面。規則資料庫中有數千個規則。篩選欄提供了一個很好的搜尋引擎選項，以便有效地搜尋規則。

您可以將任何關鍵字插入過濾器欄中，然後系統為您抓取結果。如果要求查詢安全套接字層(SSL)心臟出血漏洞的簽名，您可以在過濾欄中搜尋關鍵字heartbleed，它將獲取心臟出血漏洞的簽名。

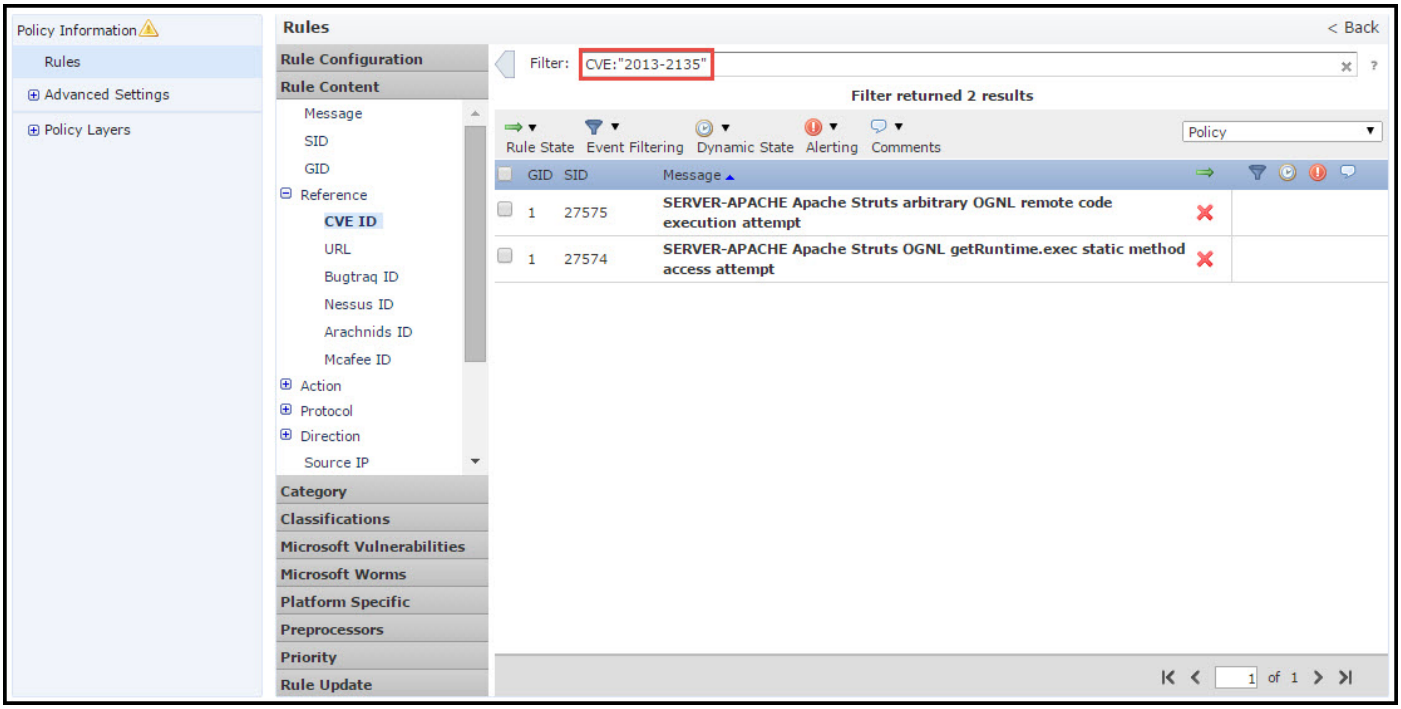
> **提示**：如果在篩選條中使用多個關鍵字，則系統使用AND邏輯組合這些關鍵字以建立複合搜尋。

還可以使用簽名ID(SID)、生成器ID(GID)、類別：dos等

規則被有效地劃分為多種方式，例如基於類別/分類/Microsoft漏洞/Microsoft蠕蟲/特定於平台。這種規則關聯有助於客戶以簡單的方式獲得正確的簽名，並幫助客戶有效地調整簽名。



您還可以使用CVE編號進行搜尋，以查詢覆蓋這些編號的規則。您可以使用語法**CVE:<cve-number>**。



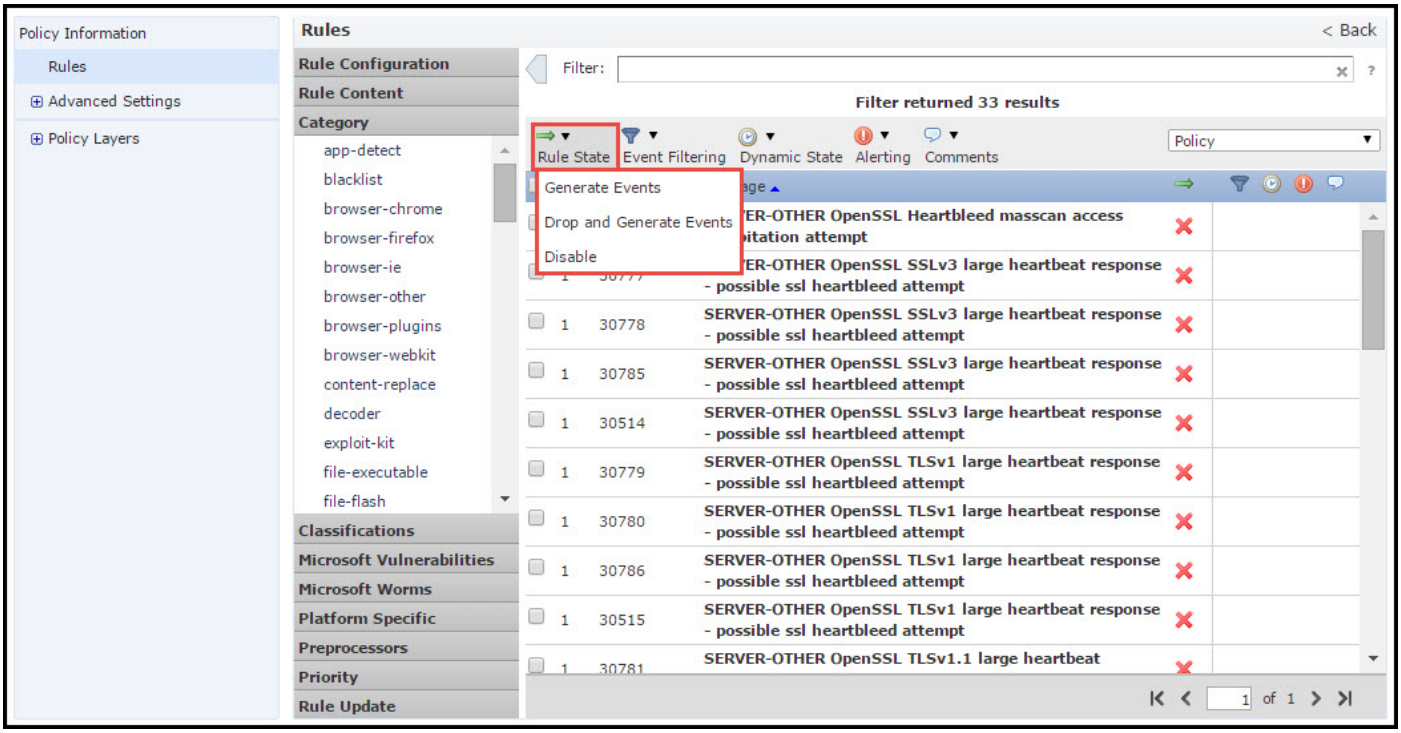
步驟1.5.配置規則狀態

導航至 **規則** 導航面板中的選項，並顯示Rule Management頁面.選擇規則並選擇**規則狀態**選項以配置規則的狀態。可以為規則配置三種狀態：

1. **生成事件**：此選項在規則與流量匹配時生成事件。

2. **Drop and Generate Events**：**該選**項在規則與流量匹配時生成事件並丟棄流量。

3. **Disable**:此選項禁用規則。



步驟1.6.配置事件過濾器

入侵事件的重要性取決於發生頻率，或者源或目標IP地址。在某些情況下，您可能不在乎某事件直到它發生特定次數。例如，如果某人嘗試登入到伺服器，直到其失敗一定次數，您可能不會擔心。在其他情況下，您可能只需要看到幾次規則命中就可以檢查是否存在廣泛的問題。

實現此目標有兩種方式：

1.事件閾值。

2.事件抑制。

事件閾值

您可以設定閾值，根據發生次數指定事件顯示的頻率。您可以根據事件和策略配置閾值。

配置事件閾值的步驟：

步驟1.選**擇要配**置事件閾值的規則。

步驟2.按一下**Event Filtering**。

步驟3.按一下**Threshold**。

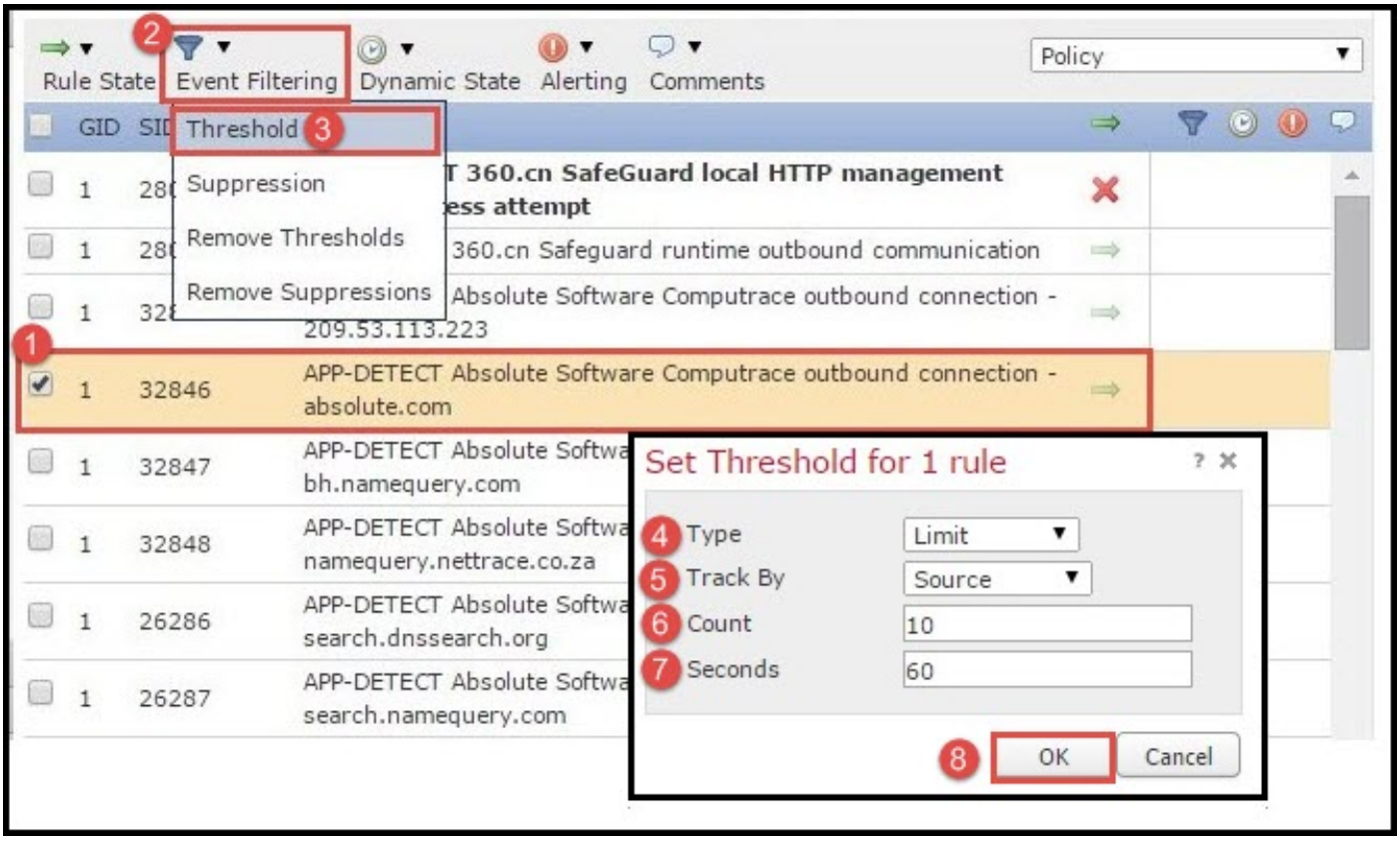
步驟4.從下拉選單中選擇**Type**。（Limit、Threshold或Both）。

步驟5.從**Track** By下拉框中選擇要**跟蹤的**方式。（源或目標）。

步驟6.輸入**Count**事件以滿足閾值。

步驟7.輸入**Seconds**，在計數重置之前經過。

步驟8.按一下**OK**以完成。



將事件過濾器新增到規則後，您應該能夠看到規則指示旁的過濾器圖示，它表明已為此規則啟用事件過濾。

事件抑制

可以根據源/目標IP地址或按規則來抑制指定的事件通知。

附註：為規則新增事件抑制時。簽名檢查工作正常，但是如果流量與簽名匹配，系統不會生成事件。如果指定特定源/目標，則事件不會僅針對此規則的特定源/目標顯示。如果選擇隱藏完整規則，則系統不會為此規則生成任何事件。

配置事件閾值的步驟：

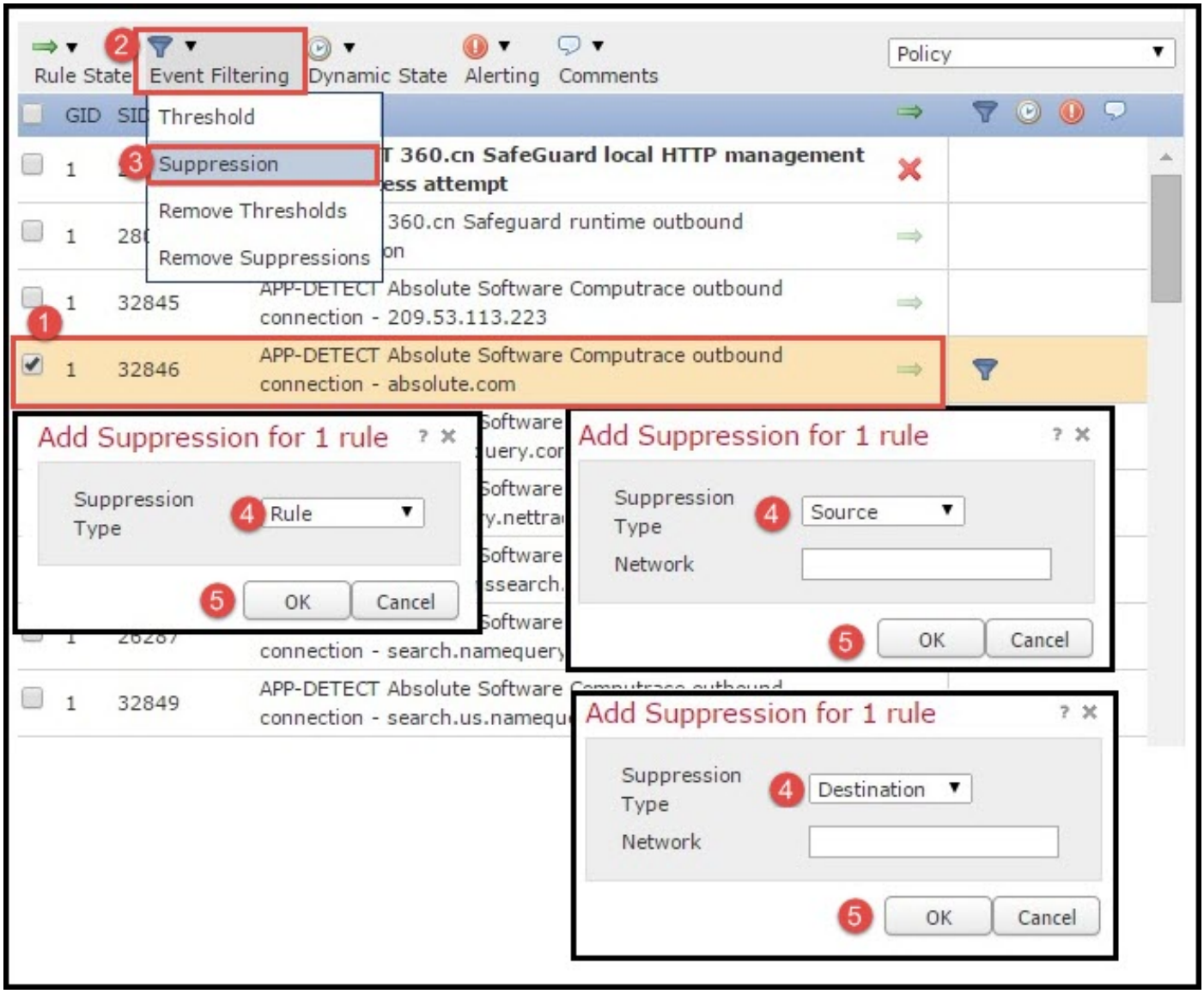
步驟1.選**擇要為其配**置事件閾值的規則。

步驟2.按一下**Event Filtering**。

步驟3.按一下**「Suppression」**。

步驟4.從下拉選單中選擇**Suppression Type。**（規則、源或目標）。

步驟5.按一下**OK**以完成。



將事件過濾器新增到此規則後，您應該能夠看到一個過濾器圖示，在規則指示旁邊顯示計數2，它表明有兩個為此規則啟用的事件過濾器。

步驟1.7.配置動態狀態

此功能可以在指定條件匹配時更改規則的狀態。

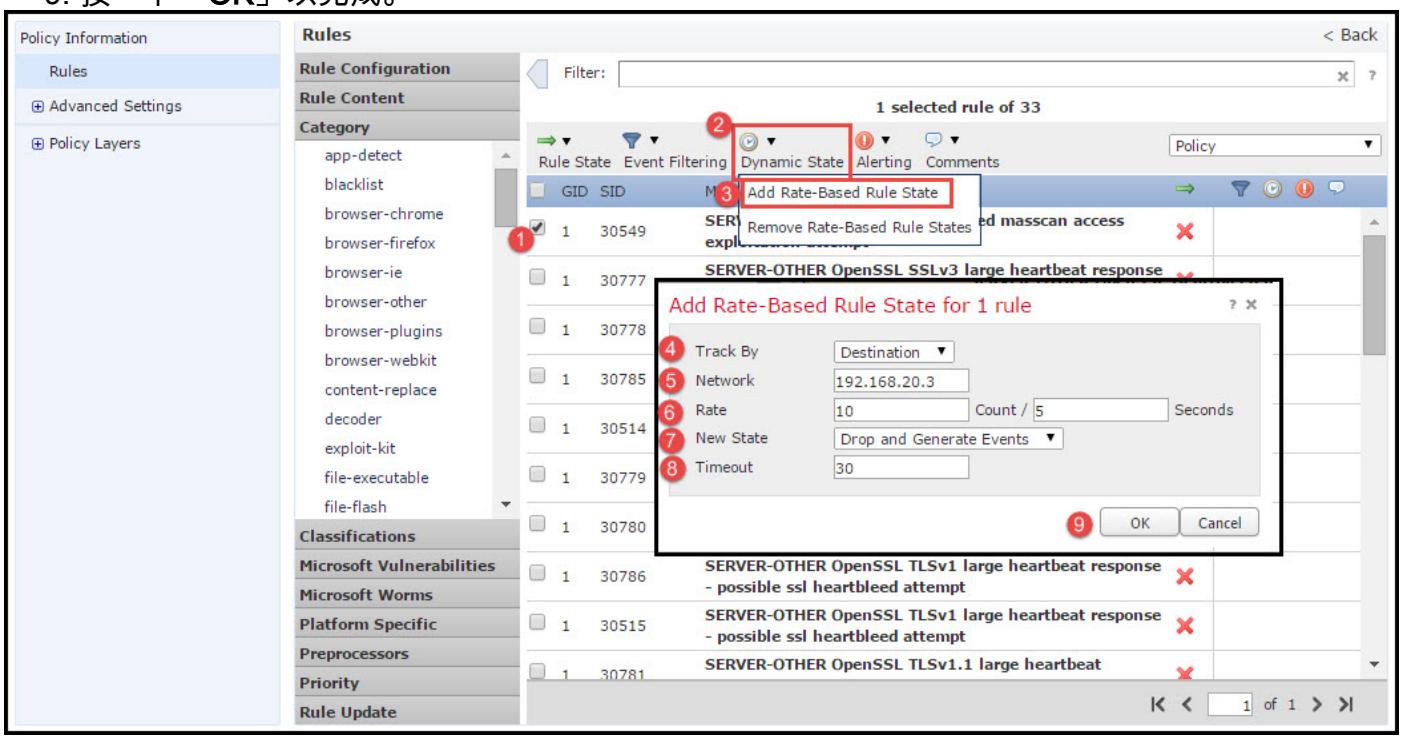
假設有使用暴力攻擊破解密碼的場景。如果簽名檢測到密碼失敗嘗試，則規則操作是生成事件。系統繼續生成密碼失敗嘗試的警報。在這種情況下，可以使用**Dynamic**狀態，其中**Generate Events**的操作可以更改為**Drop and Generate Events**，以阻止暴力攻擊。

導航至 **規則** 導航面板中的選項，並顯示Rule Management頁面。選擇要為其啟用Dynamic state的規則，然後選擇**Dynamic State > Add a Rate-base Rule State** 選項。

配置基於速率的規則狀態：

1. 選擇**要為其配**置事件閾值的規則。
2. 按一下**Dynamic State**。
3. 按一下**Add Rate-Based Rule State**。
4. 從**Track By**（跟蹤依據）下拉框中選擇要**跟蹤規則**狀態的方式。(**Rule、Source**或**Destination**)。

5. 輸入**Network**。您可以指定單個IP地址、地址塊、變數或由這些地址塊的任意組合組成的逗號分隔清單。
6. 輸入**事件計數**和時間戳（以秒為單位）。
7. 選擇**要為規**則定義的新狀態。
8. 輸入**Timeout**，在此時間後規則狀態將恢復。
9. 按一下「**OK**」以完成。



步驟2.配置網路分析策略(NAP)和變數集（可選）

配置網路分析策略

網路訪問策略也稱為前處理器。前處理器執行資料包重組和規範化流量。它有助於識別不適當的報頭選項時識別網路層和傳輸層協定異常。

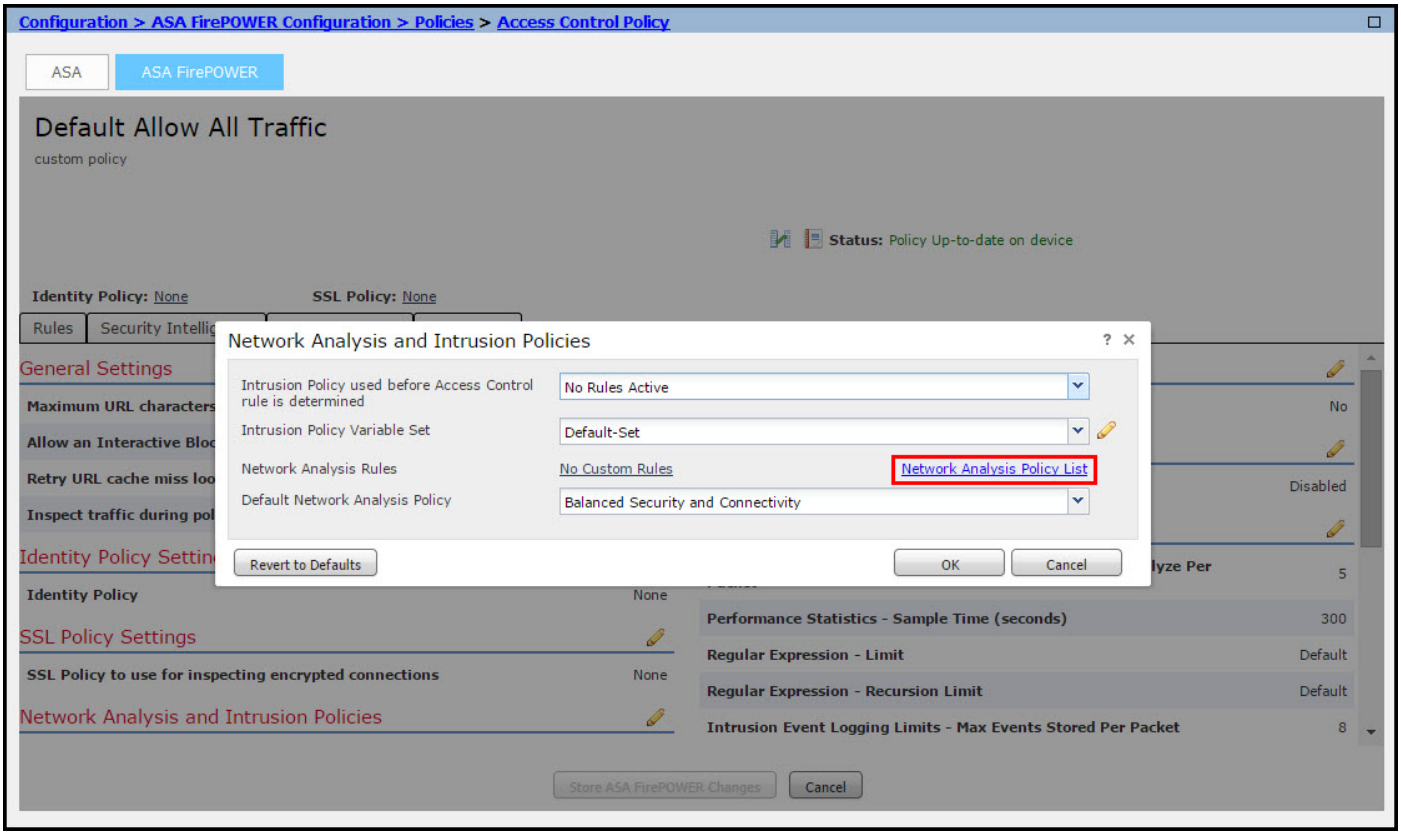
NAP對IP資料包進行碎片整理，提供TCP狀態檢查和流重組以及驗證校驗和。前處理器對流量進行規範化，驗證並驗證協定標準。

每個前處理器都有自己的GID號。它表示資料包觸發了哪個前處理器。

要配置網路分析策略，請導航至**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy > Advanced > Network Analysis and Intrusion Policy**

預設網路分析策略是平衡安全性和連線，這是最佳推薦策略。還有另外三個系統提供的NAP策略可以從下拉選單中進行選擇。

選擇選項**Network Analysis Policy** List以建立自定義NAP策略。



配置變數集

在入侵規則中使用變數集來標識源、目標地址和埠。當變數更準確地反映網路環境時，規則會更有效。變數在效能調節中起著重要作用。

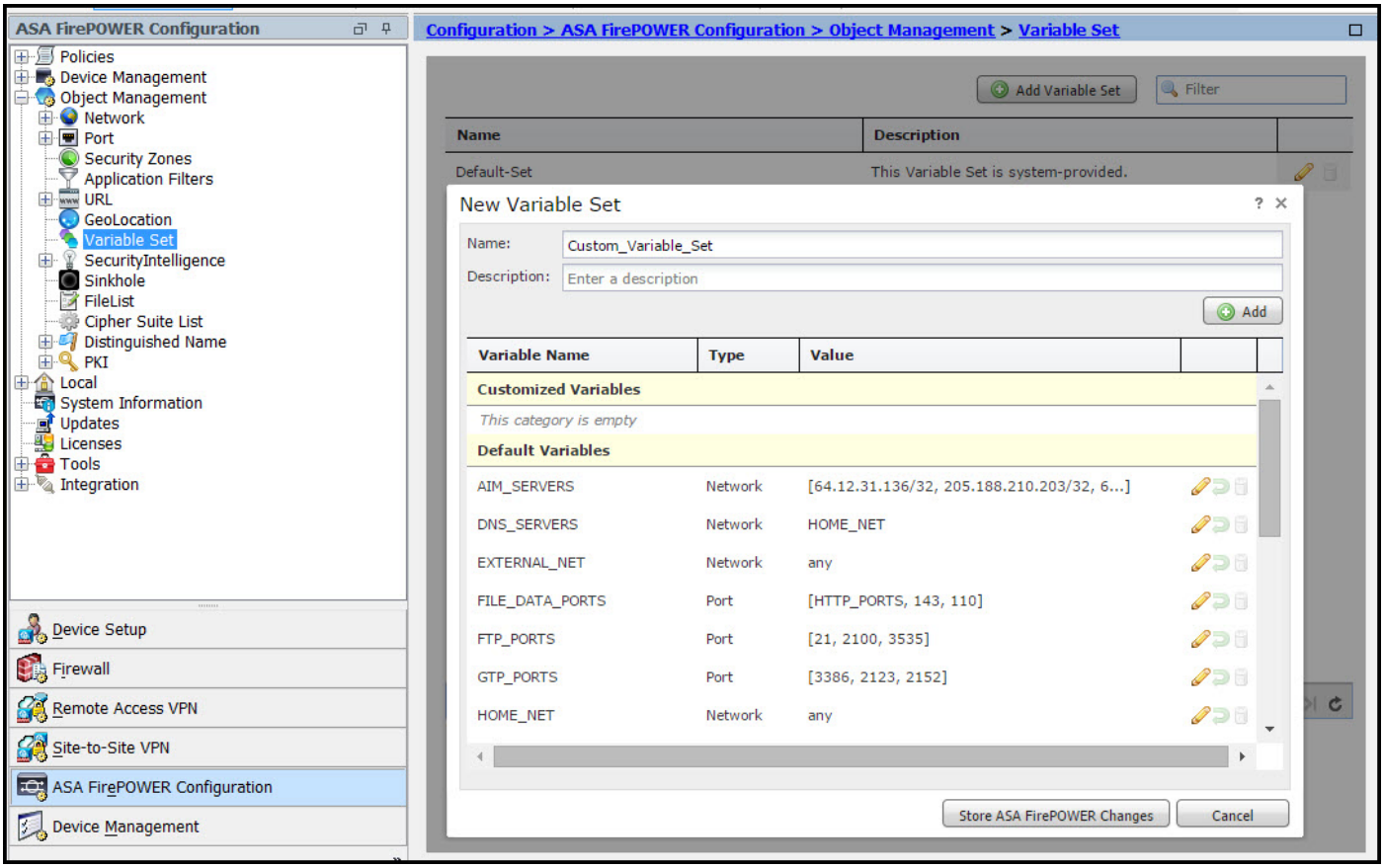
已使用預設選項（網路/埠）配置變數集。 如果要更改預設配置，請新增新的變數集。

要配置變數集，請導航到**配置> ASA Firepower配置>對象管理>變數集**。選擇選項Add Variable Set以新增新變數集。輸入**變數集**的名稱並指定**說明。**

如果任何自定義應用程式在特定埠上運行，則在Port number欄位中定義埠號。配置網路引數。

$Home_NET指定內部網路。

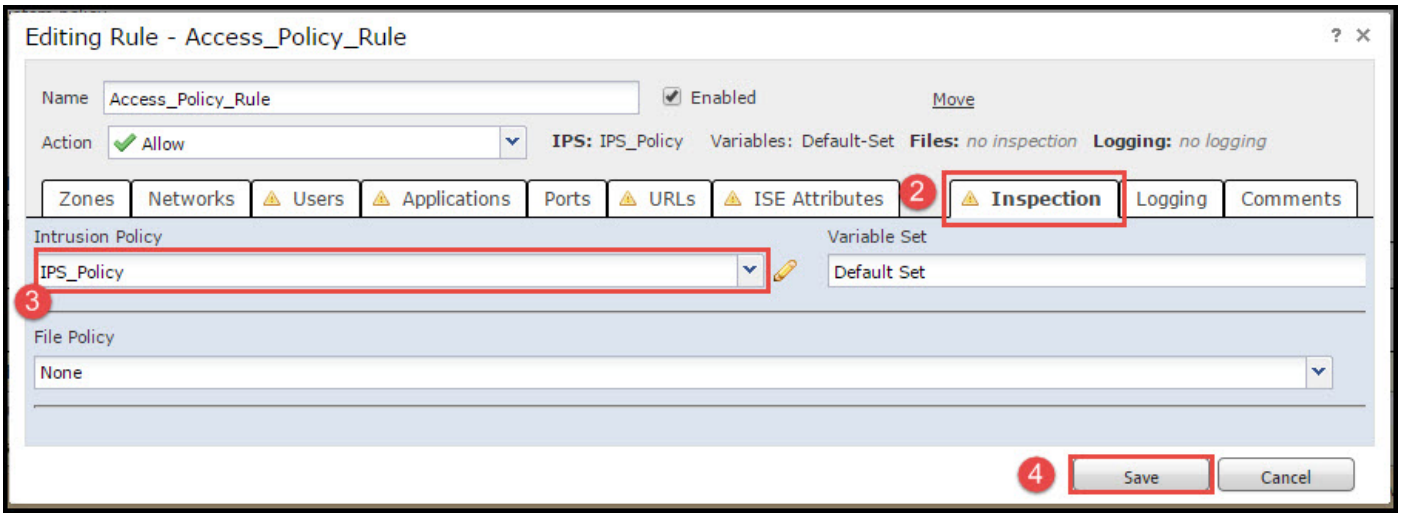
$external_NET指定外部網路。



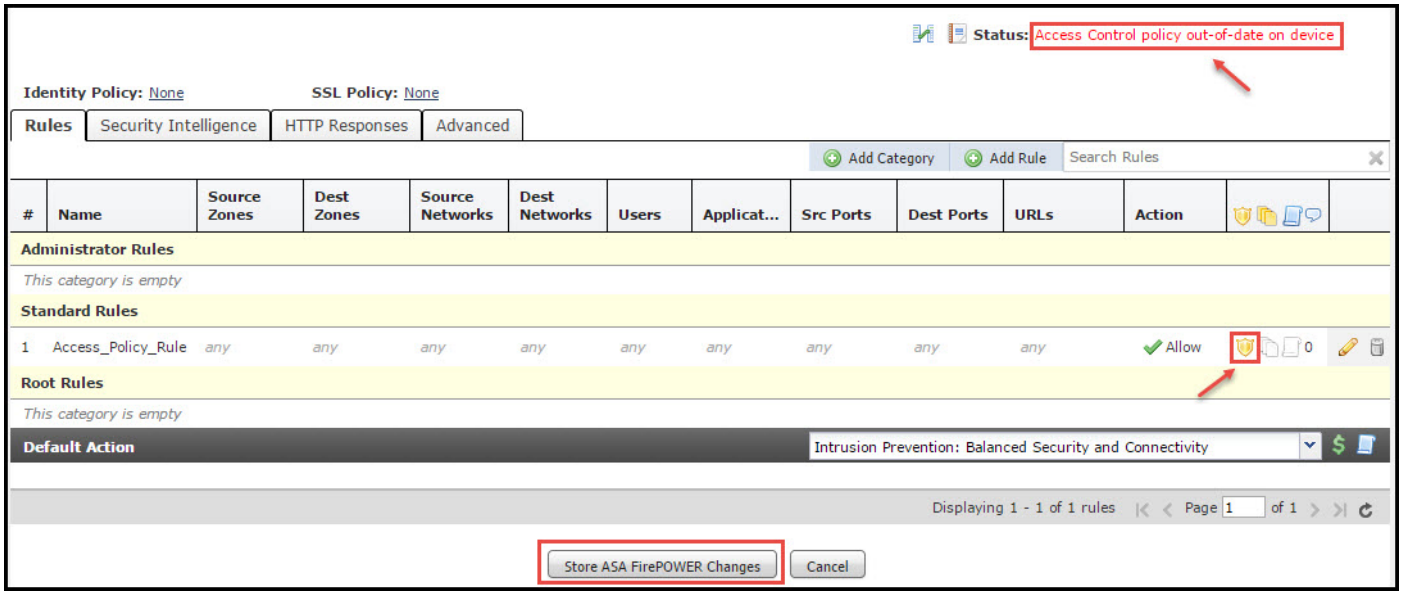
步驟3:配置訪問控制以包括入侵策略/NAP/變數集

導航到Configuration > ASA Firepower Configuration > Policies > Access Control Policy。您需要完成以下步驟：

1. 編輯要在其中分配入侵策略的訪問策略規則。
2. 選擇Inspection頁籤。
3. 從下拉選單中選擇Intrusion Policy，然後從下拉選單中選擇Variable Sets
4. 按一下「Save」。



因為入侵策略已新增到此訪問策略規則。您可以在Golden Color中看到指示已啟用入侵策略的遮蔽圖示。

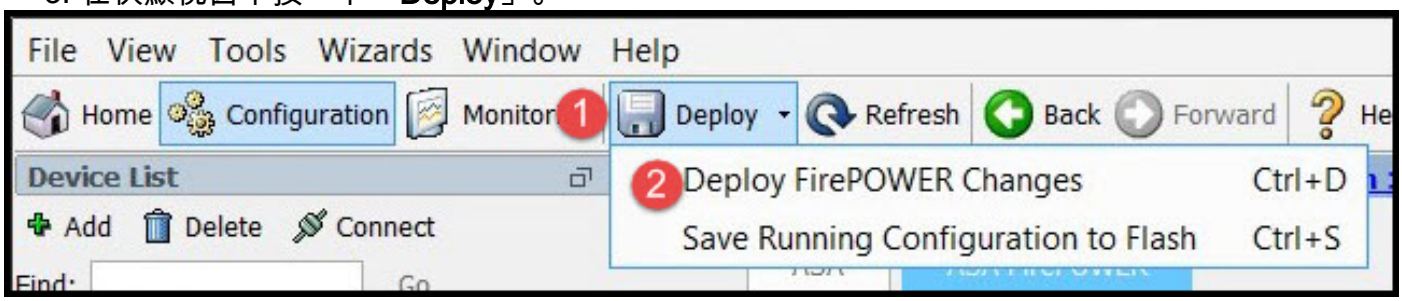


按一下Store ASA FirePOWER changes以儲存更改。

步驟4.部署訪問控制策略

現在，您必須部署訪問控制策略。在應用策略之前，您將看到裝置上的訪問控制策略已過期的指示。要將更改部署到感測器：

1. 按一下「Deploy」。
2. 按一下Deploy FirePOWER Changes。
3. 在快顯視窗中按一下「Deploy」。

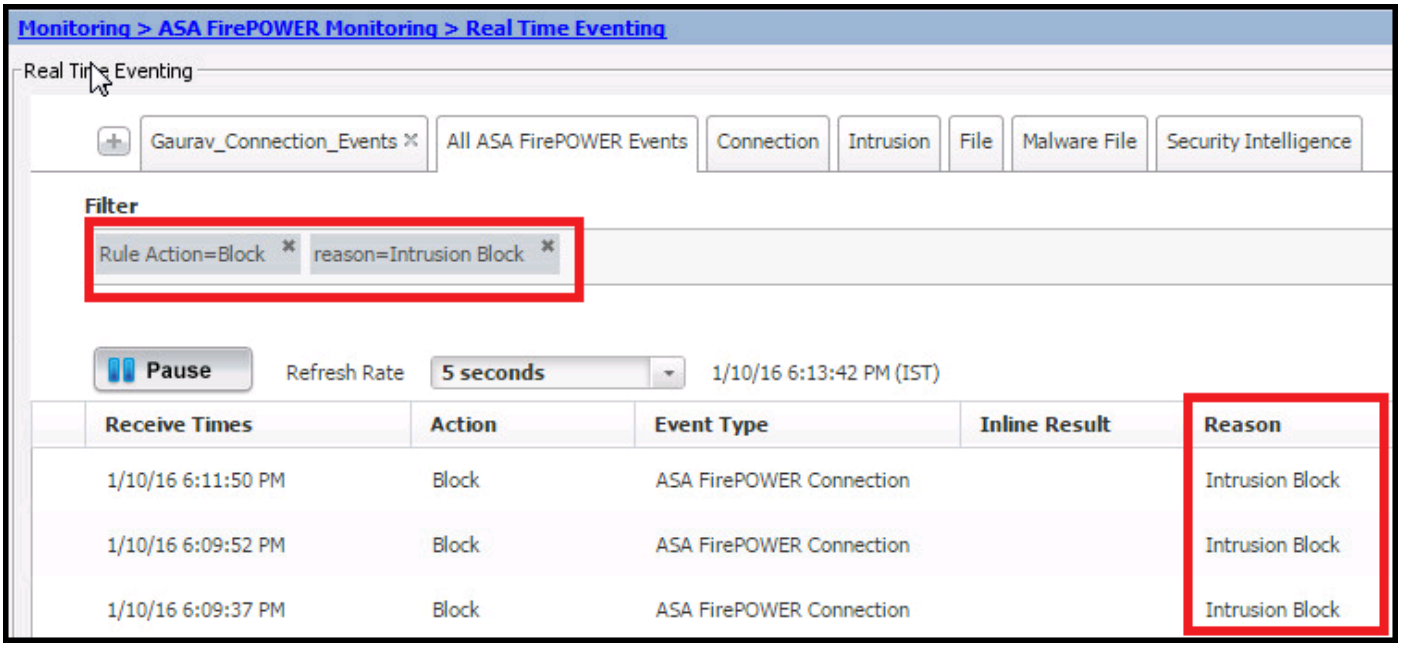


: 5.4.xApply ASA FirePOWER Changes

> ASA Firepower>

步驟5.監控入侵事件

要檢視FirePOWER模組生成的入侵事件，請導航至 **監控> ASA FirePOWER監控>即時事件。**



驗證

目前沒有適用於此組態的驗證程序。

疑難排解

步驟1.確保正確配置規則的規則狀態。

步驟2.確保訪問規則中包含正確的IPS策略。

步驟3.確保變數集配置正確。如果變數集配置不正確，簽名將與流量不匹配。

步驟4.確保訪問控制策略部署成功完成。

步驟5.監控連線事件和入侵事件以驗證資料流是否達到正確的規則。

- **Cisco ASA FirePOWER**
- **- Cisco Systems**