在更新新特徵碼包後如何檢查IPS特徵碼中的行為更改

目錄

簡介

本檔案介紹將思科入侵防禦系統(IPS)更新至新特徵碼包後新特徵碼引入的行為變化。

必要條件

需求

思科建議您瞭解以下主題：

- IPS上的特徵碼更新功能

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IPS 4XXX系列感測器
- ASA 5585-X IPS SSP系列
- ASA 5500-X IPS SSP系列
- ASA 5500 IPS SSM系列

版本7.1(10)E4

版本7.3(4)E4

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題

在IPS上執行特徵碼更新後，某些應用程式可能會出現多種問題，例如丟包和連線問題。若要解決此類問題，如果能夠瞭解在特徵碼更新後活動特徵碼集的更改，將會非常有用。

解決方案

步驟1.

首先需要檢查的是簽名的升級歷史記錄。這將告知在IPS上運行的上一個特徵碼包和當前版本的特徵碼包。

可從**show version**指令的輸出或**show tech**的升級歷史記錄部分找到此內容。此處會提到來自相同內容的片段：

升級歷史記錄

*** IPS-sig-S733-req-E4 19:59:50 UTC週五2015年8月09日**

IPS-sig-S734-req-E4.pkg 19:59:49 UTC週二2015年8月13日

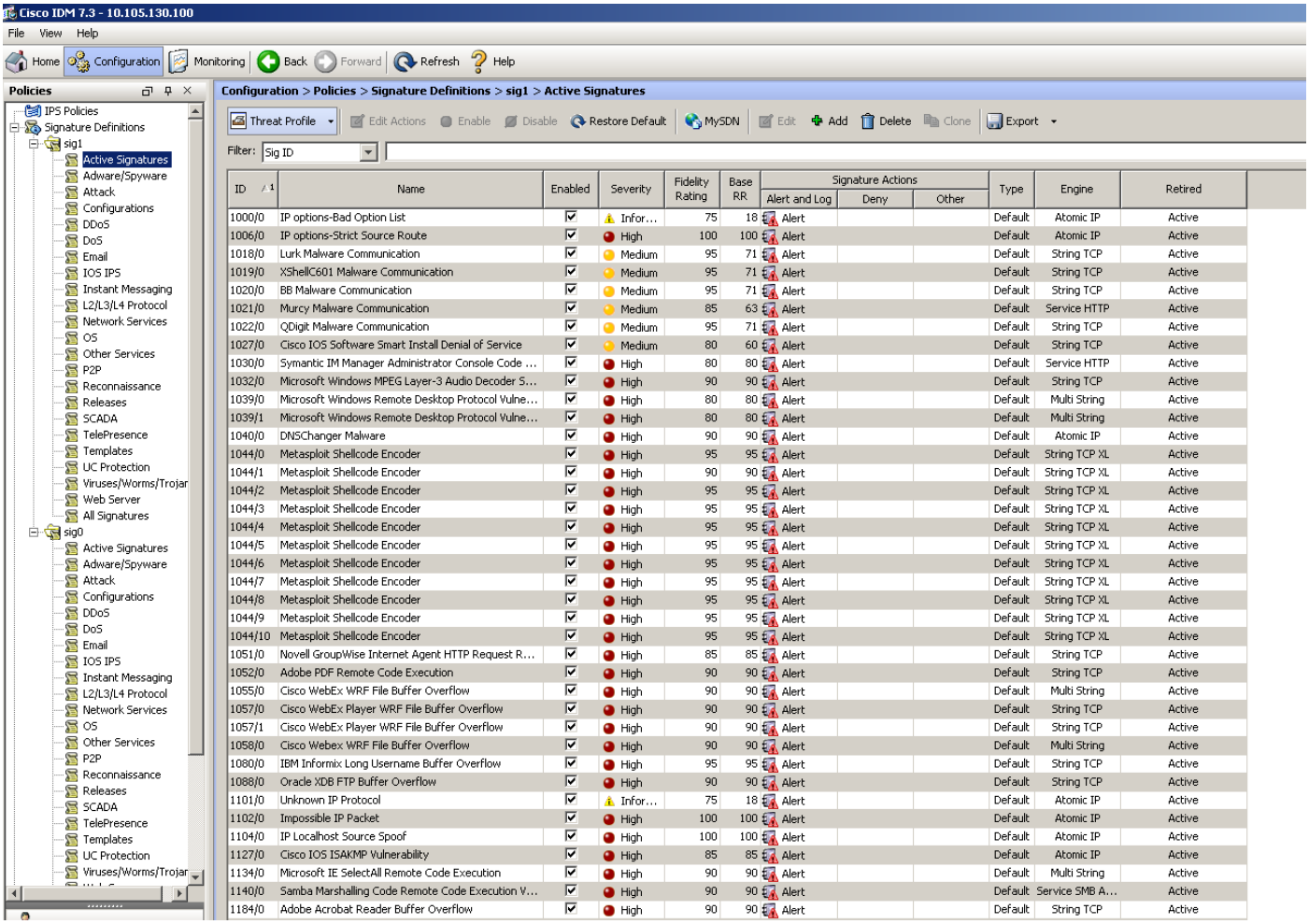
現在，您可以發現IPS上運行的前一個特徵碼包是s733，並且已升級為當前特徵碼包的s734。

步驟2.

第二步是瞭解已經進行的更改以及可以通過IME/IDM檢查的更改。

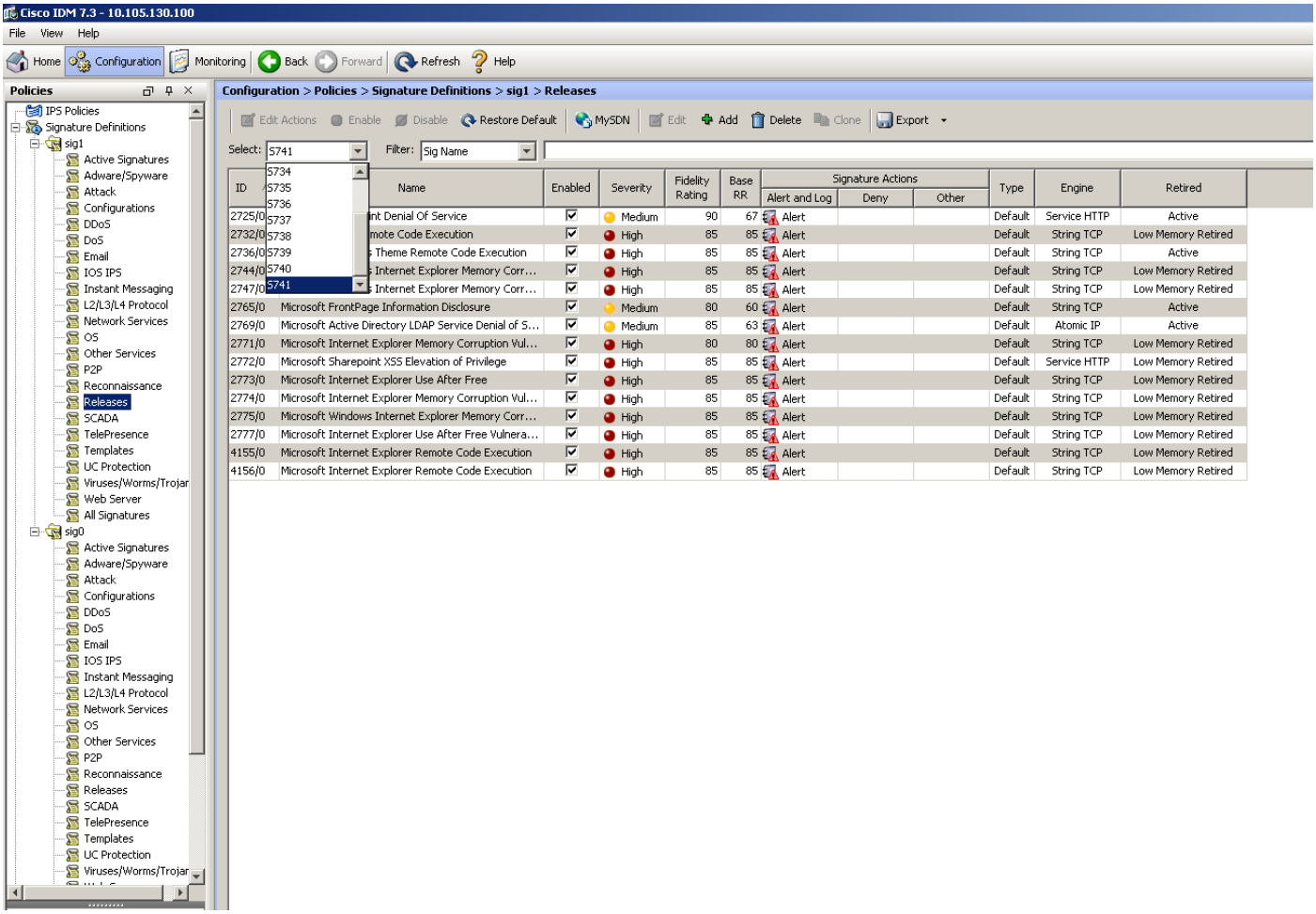
1.此圖顯示了IME/IDM上的活動簽名頁籤。

導航到**Configuration > Policies > Signature Definitions > Sig1 > Active Signatures**。



2.此圖顯示如何選擇特定的簽名版本。

導航到**Configuration > Policies > Signature Definitions > Sig1 > Releases**。



進一步使用filter選項，您可以根據引擎、保真度、嚴重性等過濾特定版本的所有簽名。

通過這樣做，您必須能夠縮小對特徵碼版本所做的更改，這些更改可能是問題發生的潛在原因，您可根據這些原因進行故障排除。