Cómo verificar cambios de comportamiento en firmas IPS después de actualizar un nuevo paquete de firma

Contenido

Introducción

Este documento describe los cambios de comportamiento introducidos por las nuevas firmas después de actualizar Cisco Intrusion Prevention System (IPS) a un nuevo paquete de firma.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Función de actualización de firma en IPS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Sensores IPS de la serie 4XXX
- ASA serie 5585-X IPS SSP
- Serie ASA 5500-X IPS SSP
- ASA serie 5500 IPS SSM

Versión 7.1(10)E4

Versión 7.3(4)E4

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema

Puede haber varios problemas, como caídas de paquetes y problemas de conectividad con ciertas aplicaciones después de realizar una actualización de firma en el IPS. Para solucionar tales problemas, sería muy útil que comprendiera los cambios en el conjunto de firmas activo después de la actualización de la firma.

Solución

Paso 1.

Lo primero que debe comprobar es el historial de actualización de la firma. Esto indica el paquete de firmas anterior que se estaba ejecutando en IPS y la versión actual del paquete de firmas.

Esto se puede encontrar en la salida del comando **show version** o en la sección del historial de actualizaciones de **show tech**. Un fragmento de lo mismo se menciona aquí:

Historial de actualización

*** IPS-sig-S733-req-E4 19:59:50 UTC 09 de agosto de 2015**

IPS-sig-S734-req-E4.pkg 19:59:49 UTC Tue 13 de agosto de 2015

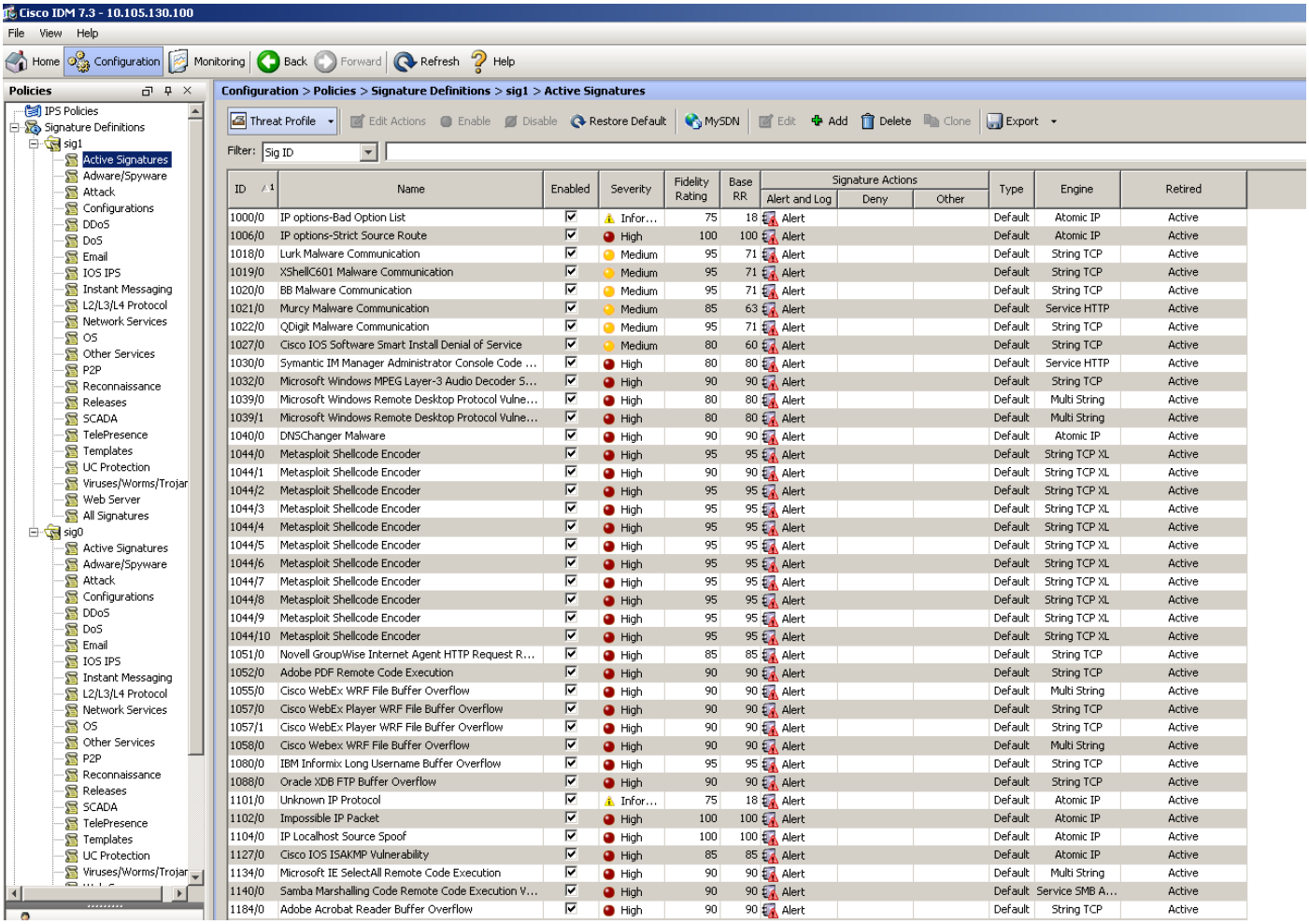
Ahora puede saber que el paquete de firmas anterior que se ejecutaba en el IPS era s733 y se ha actualizado a s734, que es el paquete de firmas actual.

Paso 2.

El segundo paso consiste en comprender los cambios que se han realizado y que se pueden comprobar a través de IME/IDM.

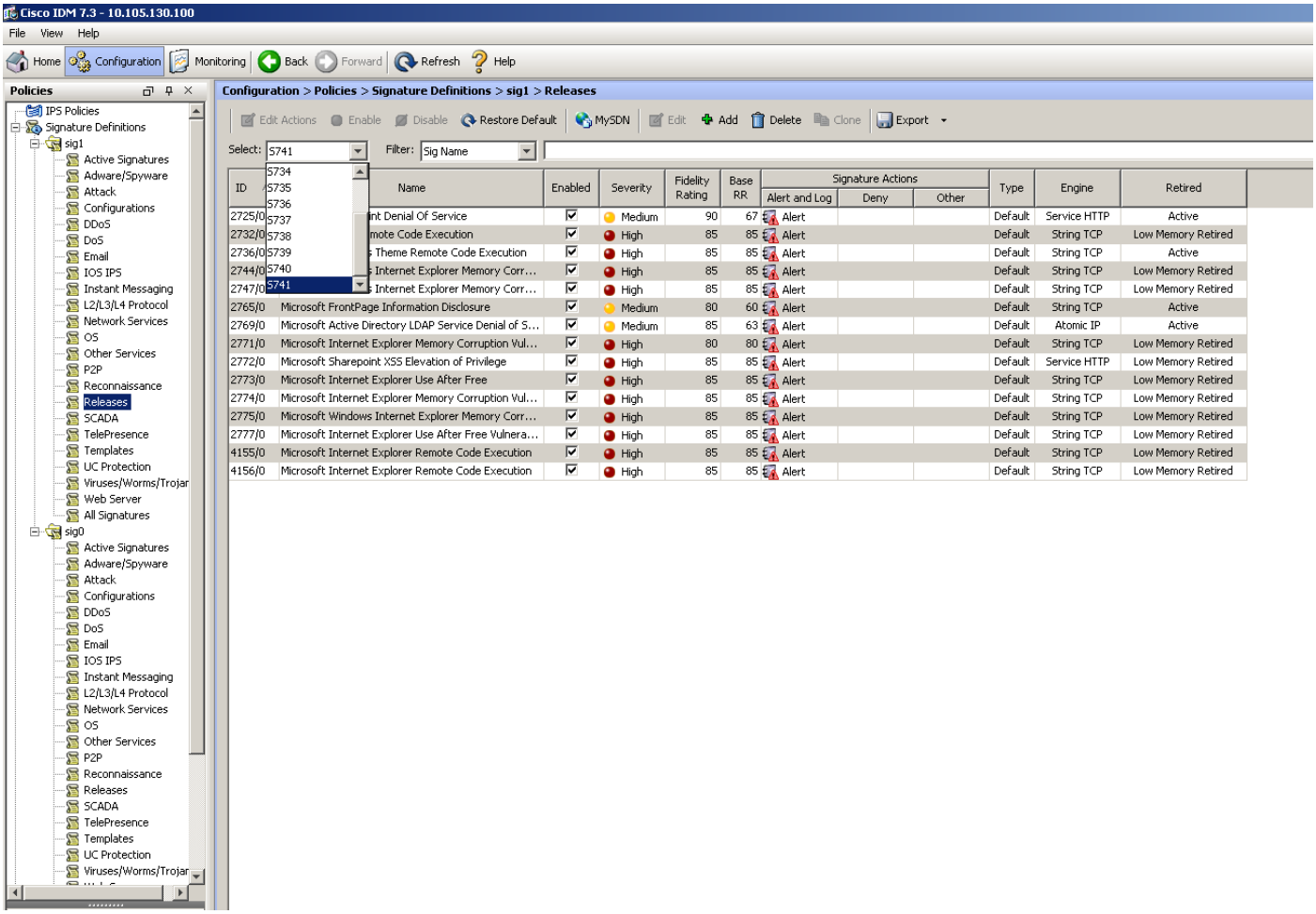
1. En esta imagen se muestra la ficha de firma activa de IME/IDM.

Navegue hasta **Configuración > Políticas > Definiciones de firma > Sig1 > Firmas activas.**



2. Esta imagen muestra cómo seleccionar una versión de firma específica.

Vaya a **Configuración > Políticas > Definiciones de firma > Sig1 > Versiones.**



Con la opción de filtro que ha obtenido todas las firmas de una versión en particular, puede filtrarlas en función del motor, la fidelidad, la gravedad, etc.

Al hacer esto, debe ser capaz de limitar los cambios en la versión de firma que pueden ser una causa potencial para el problema en función del cual alinee su solución de problemas.