Hoe gedragsveranderingen in IPS-handtekeningen te controleren Post met een nieuw handtekeningen

Inhoud

Inleiding

Dit document beschrijft de gedragsveranderingen die door de nieuwe handtekeningen zijn geïntroduceerd na het uploaden van Cisco Inbraakpreventiesysteem (IPS) naar een nieuw pakket handtekeningen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Functie voor bijwerken van handtekeningen op IPS

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IPS 4XXX Series sensoren
- ASA 5585-X IPS SSP-serie
- ASA 5500-X IPS SSP-Series Next-Generation
- ASA 5500 IPS IPS SM-serie

versie 7.1(10)E4

Versie 7.3(4)E4

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Probleem

Er zouden meerdere problemen kunnen zijn zoals pakketdruppels en aansluitingsproblemen met bepaalde toepassingen na het uitvoeren van een signatuur update op de IPS.Om dergelijke problemen op te lossen zou het zeer behulpzaam zijn als u de veranderingen in actieve signatuur kunt begrijpen die plaatste post van de signatuur update.

Oplossing

Stap 1.

Het eerste wat je moet controleren is de upgradegeschiedenis voor de handtekening. Dit vertelt het vorige handboekenpakket dat op IPS actief was en de huidige versie van handboekenpakket.

Dit kan worden gevonden in de output van de **opdrachtshow versie** of in het upgradeoverzicht van de **showtechnologie**. Snippet van hetzelfde onderwerp wordt hier genoemd:

Upgradegeschiedenis

*** IPS-sig-S733-req-E4 19:59:50 UTC FRJ augustus 2015**

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

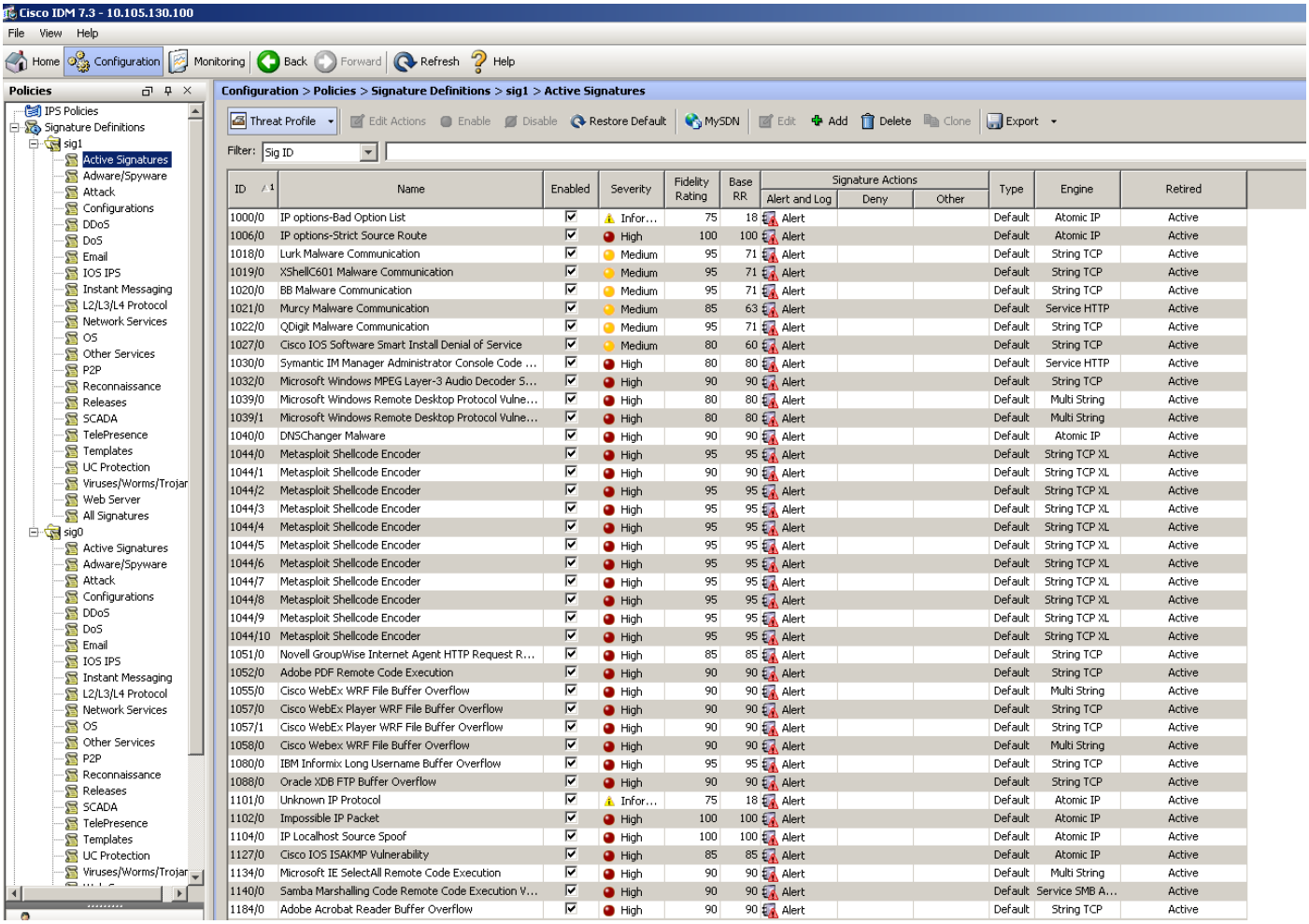
Nu kunt u duidelijk maken dat het vorige signatuur-pakket dat op IPS liep s733 was en opgewaardeerd werd tot s734, wat het huidige handboekje is.

Stap 2.

De tweede stap is het begrijpen van de veranderingen die zijn aangebracht en die kunnen worden gecontroleerd via de IME/IDM.

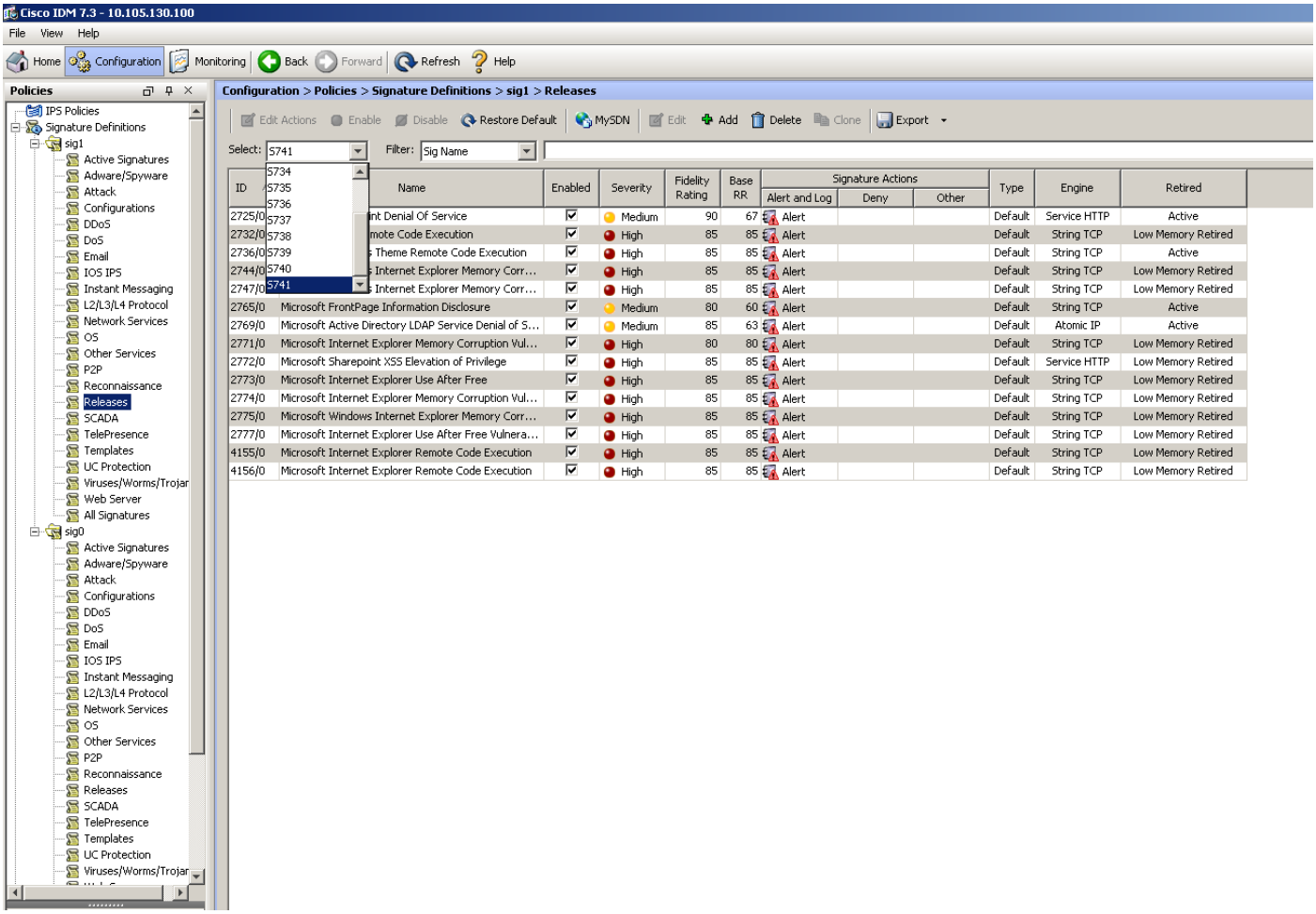
1. Het tabblad actieve handtekening op IME/IDM wordt in deze afbeelding weergegeven.

Navigeer naar **Configuration > Policy > Signature Definitions > Sig1 > Active Signatures.**



2. Deze afbeelding toont hoe een specifieke handmatige release moet worden geselecteerd.

Navigeer naar **Configuratie > Beleid > Definities voor handtekeningen > Sig1 > releases.**



Als u verder de filteroptie gebruikt die u hebt aangeschaft, kunt u alle handtekeningen bij een bepaalde release filteren op basis van motor, trouw, ernst, enz.

Door dit te doen moet u in staat zijn om af te remmen op de veranderingen in de handmatige release die een mogelijke oorzaak voor de kwestie kan zijn op basis waarvan u de probleemoplossing uitlijnen.