如何在更新新签名包后检查IPS签名中的行为更改

目录

简介

本文档介绍将思科入侵防御系统(IPS)更新到新签名包后新签名引入的行为更改。

先决条件

要求

Cisco 建议您了解以下主题：

- IPS上的签名更新功能

使用的组件

本文档中的信息基于以下软件和硬件版本：

- IPS 4XXX系列传感器
- 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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

在IPS上执行签名更新后，可能会出现多个问题，例如丢包和某些应用程序的连接问题。要解决此类问题，请务必了解签名更新后活动签名集中的更改。

解决方案

步骤1:

您首先需要检查签名的升级历史记录。这将告知在IPS上运行的以前的签名包和当前版本的签名包。

这可以从命令**show version**的输出或从show tech的升级历史记录部分中找到。**此处**提到了同一命令的代码片段：

升级历史记录

*** IPS-sig-S733-req-E4 19:59:50 UTC星期五2015年8月09日**

IPS-sig-S734-req-E4.pkg 19:59:49 UTC周二8月13日2015

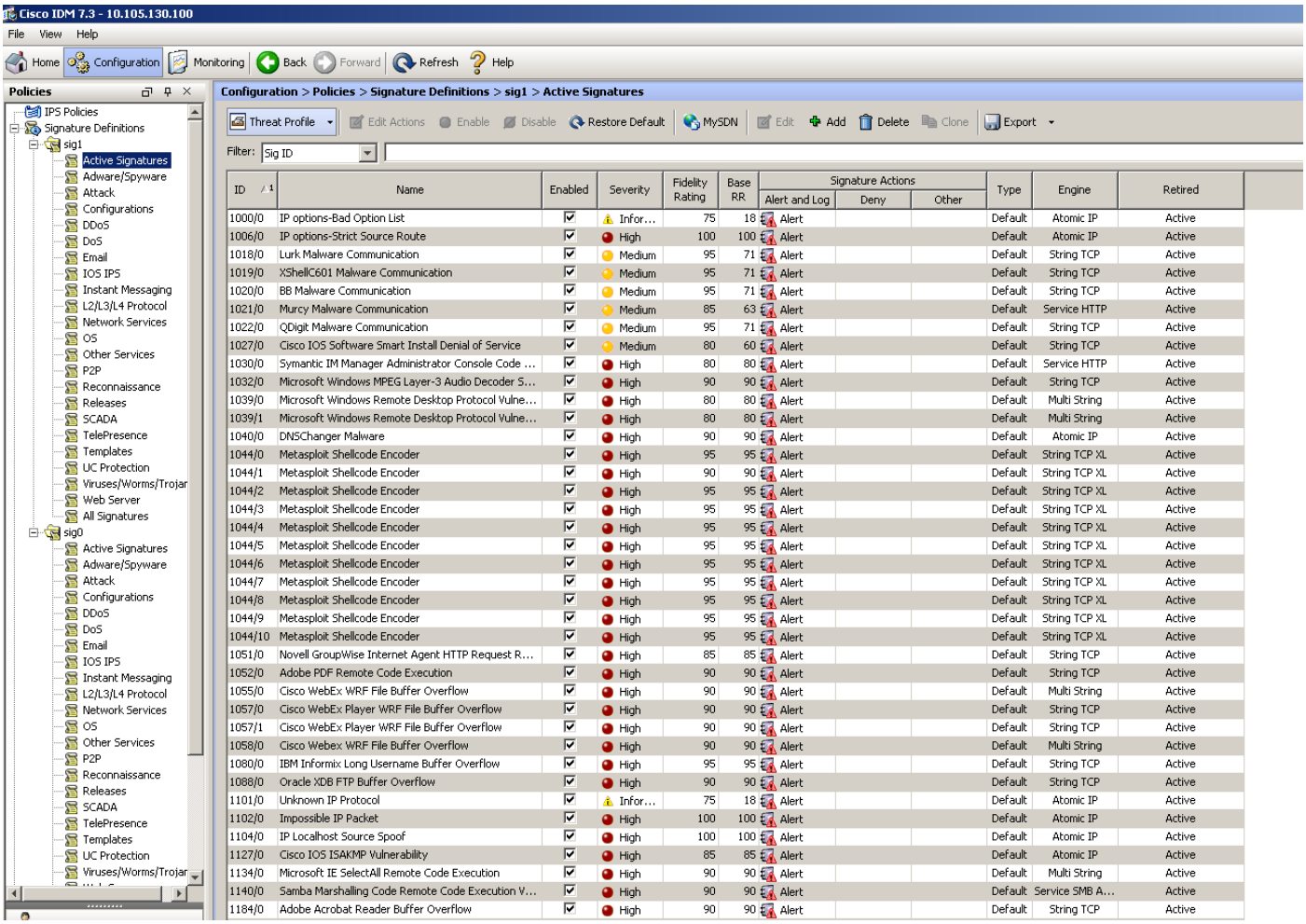
现在，您可以确定在IPS上运行的以前的签名包是s733，并已升级到s734，这是当前的签名包。

第二步：

第二步是了解已进行的更改，以及可通过IME/IDM检查的更改。

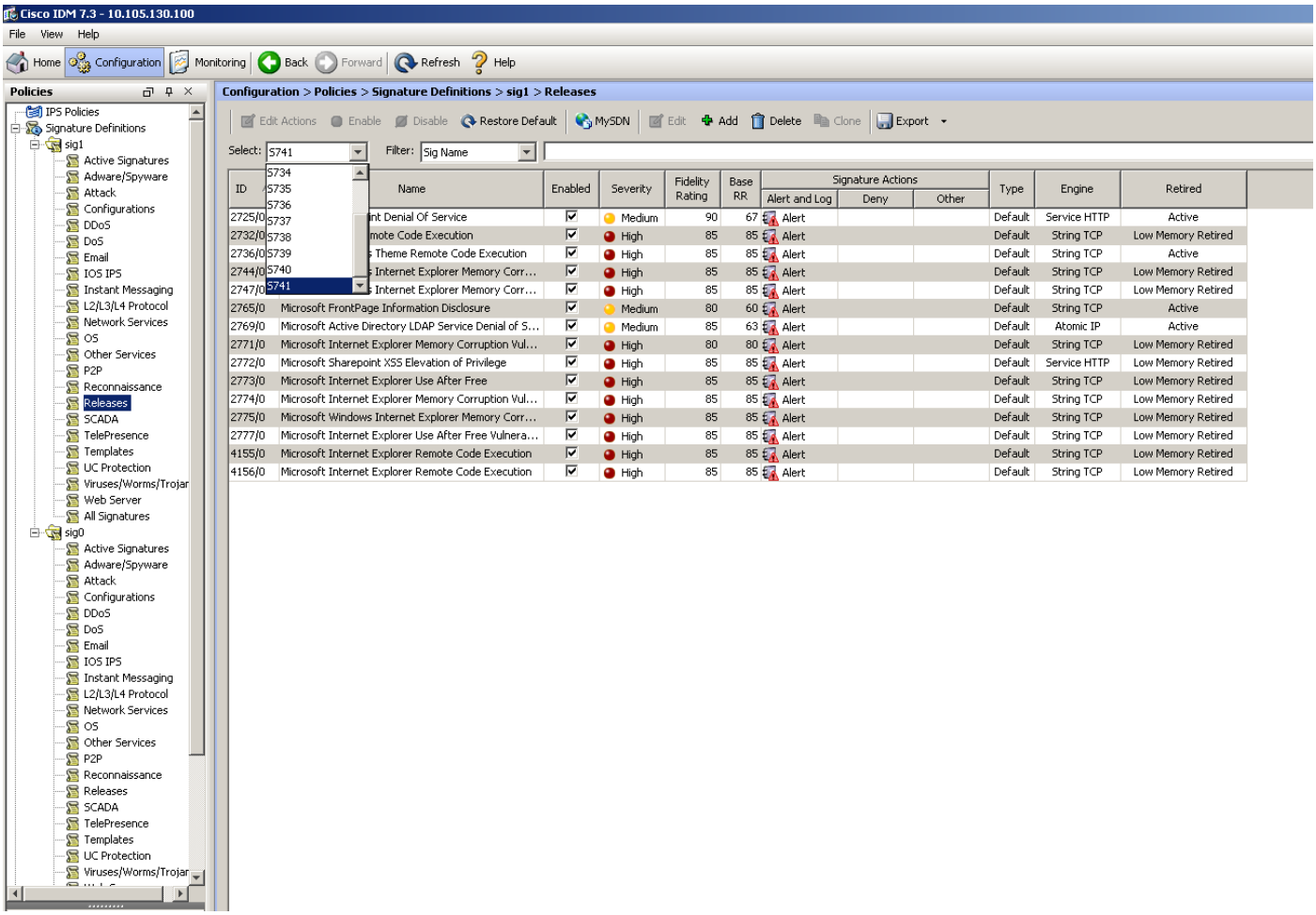
1. IME/IDM上的活动签名选项卡显示在此图像中。

导航至**Configuration > Policies > Signature Definitions > Sig1 > Active Signatures。**



2.此图显示如何选择特定签名版本。

导航至Configuration > Policies > Signature Definitions > Sig1 > Releases。



进一步，使用过滤器选项，您可以根据引擎、保真度、严重性等来过滤从特定版本获取的所有签名。

通过这样做，您必须能够缩小签名版本中的更改范围，这些更改可能会根据您调整故障排除的原因导致问题。