كيفية التحقق من التغييرات السلوكية في توقيعات IPS بعد تحديث حزمة توقيع جديدة

المحتويات

المقدمة

يصف هذا المستند التغييرات السلوكية التي أدخلتها التوقيعات الجديدة بعد تحديث نظام منع التسلل (IPS) من Cisco إلى حزمة توقيع جديدة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- ميزة تحديث التوقيع على IPS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- أجهزة الاستشعار IPS 4xxx Series
- سلسلة ASA 5585-X IPS SSP
- سلسلة ASA 5500-X IPS SSP
- سلسلة ASA 5500 IPS SSM

الإصدار 7.1(10)E4

الإصدار 7.3(4)E4

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

المشكلة

قد تكون هناك مشاكل متعددة مثل حالات إسقاط الحزم ومشاكل الاتصال مع تطبيقات معينة بعد إجراء تحديث توقيع على IPS.الاستكشاف أخطاء هذه المشاكل وإصلاحها، سيكون من المفيد جدا إذا كنت قادرا على فهم التغييرات في مجموعة التوقيع النشطة بعد تحديث التوقيع.

الحل

الخطوة 1.

أول شيء تحتاج إلى التحقق منه هو محفوظات الترقية للتوقيع. هذا يخبر حزمة التوقيع السابقة التي كانت تعمل على IPS والإصدار الحالي من حزمة التوقيع.

ويمكنك العثور على ذلك من إخراج الأمر **show version** أو من قسم محفوظات الترقية في **show tech**. يشير هذا إلى جزء مقتطف من نفس المقال:

محفوظات الترقية

*** IPS-SIG-S733-Req-E4 19:59:50 UTC FRI 09 أغسطس 2015**

IPS-SIG-S734-req-E4.pkg 19:59:49 UTC TUE 13 أغسطس 2015

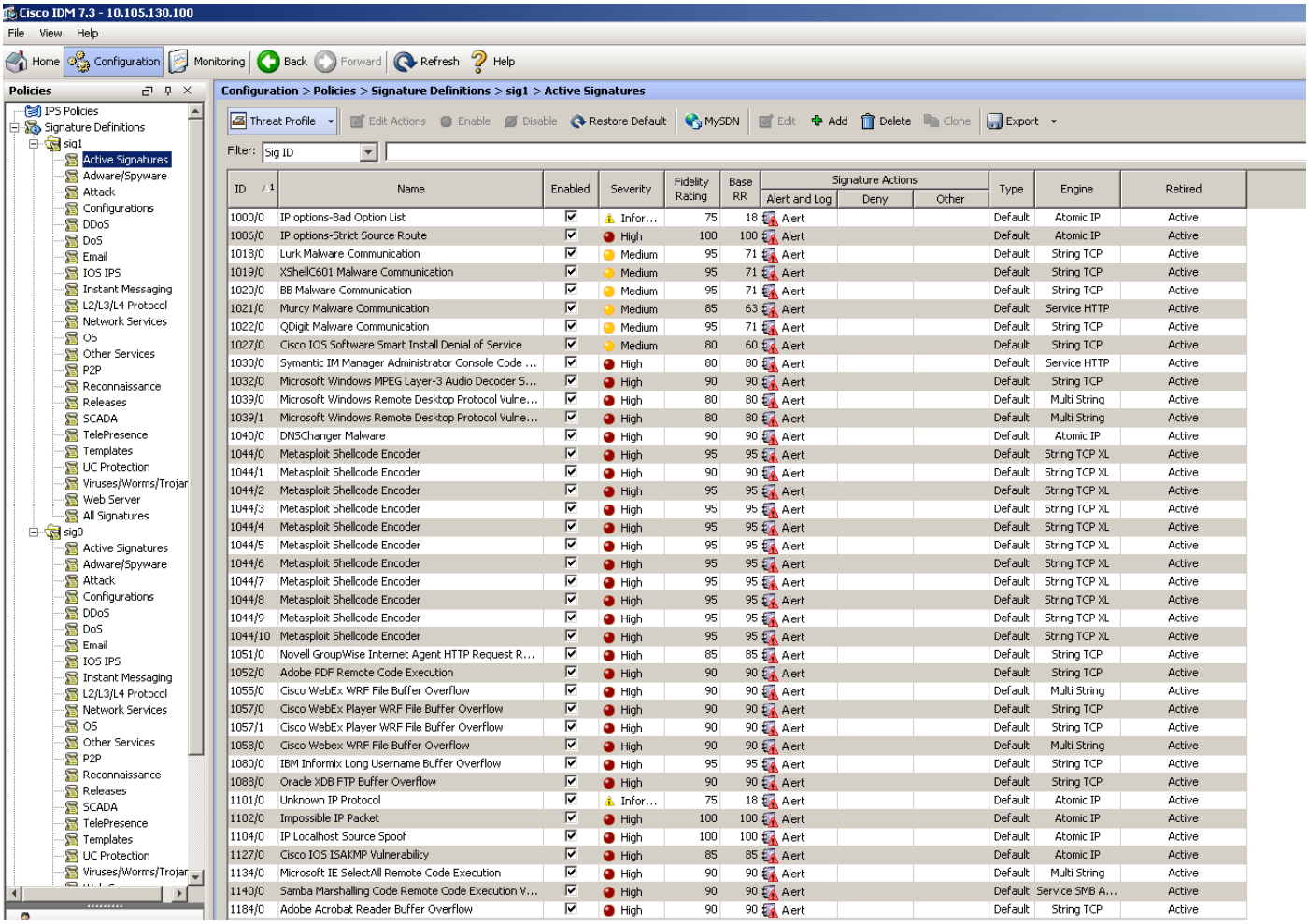
الآن يمكنك أن توضح أن حزمة التوقيع السابقة التي كانت تعمل على IPS كانت s733 وتمت ترقيتها إلى s734 والتي هي حزمة التوقيع الحالية.

الخطوة 2.

وتتمثل الخطوة الثانية في فهم التغييرات التي تم إجراؤها والتي يمكن التحقق منها من خلال IME/IDM.

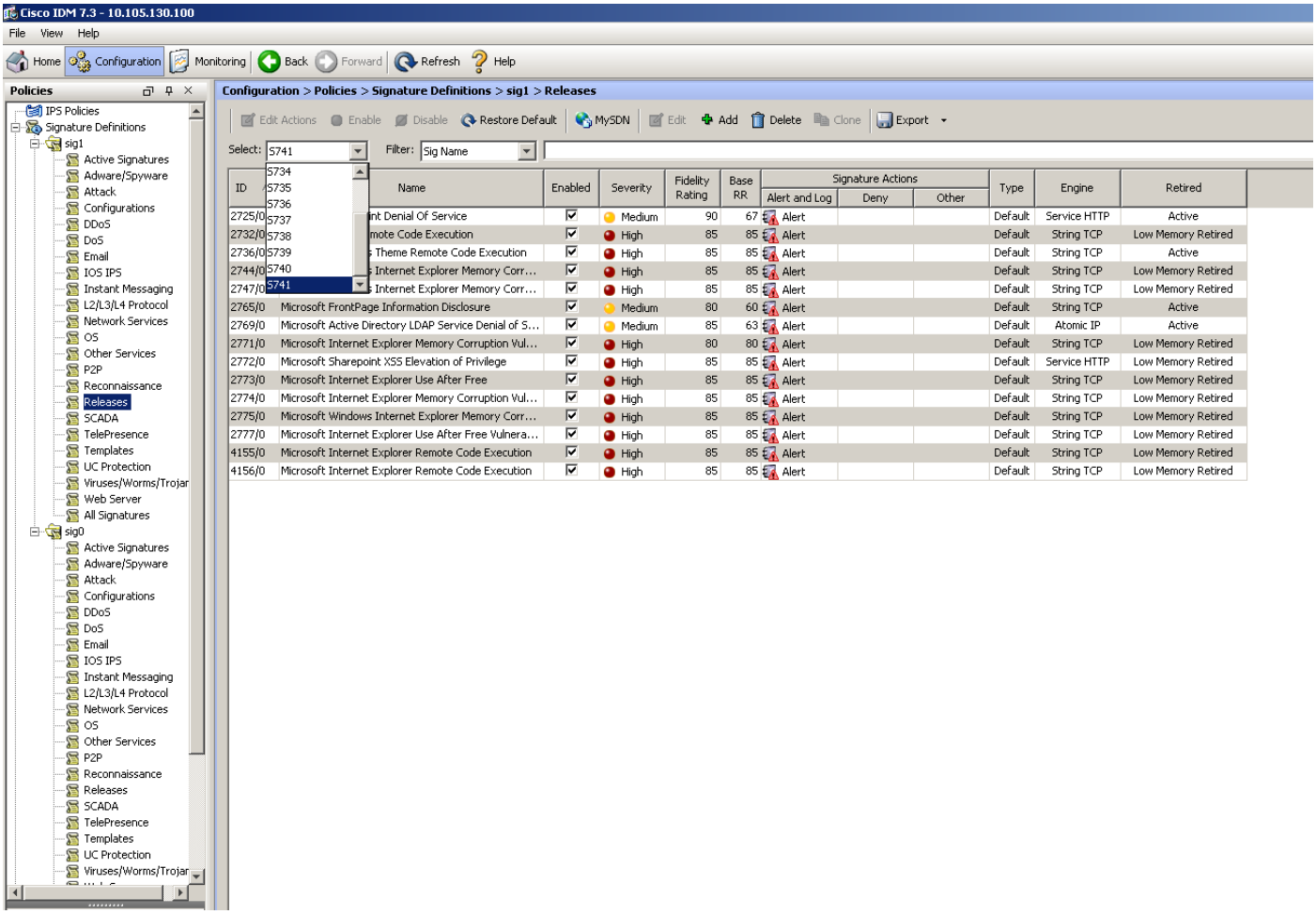
1. يتم عرض علامة التبويب "التوقيع النشط" في IME/IDM في هذه الصورة.

انتقل إلى **التكوين > السياسات > تعريفات التوقيع > SIG1 > التوقيعات النشطة.**



2. توضح هذه الصورة كيفية تحديد إصدار توقيع محدد.

انتقل إلى **التكوين > السياسات > تعريفات التوقيع > SIG1 > الإصدارات.**



باستخدام خيار المرشح الذي حصلت عليه من إصدار معين، يمكنك تصفيتها بناء على المحرك، الدقة، الخطورة، إلى آخره.

من خلال القيام بذلك، يجب أن تكون قادرا على تضييق التغييرات في إصدار التوقيع التي يمكن أن تكون سببا محتملا للمشكلة التي تقوم على أساسها بمحاذاة أستكشاف الأخطاء وإصلاحها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).