ترحيل تنسيق توقيع IPS من 4.x إلى 5.x

المحتويات

المقدمة

في الإصدار T(11)12.4 من برنامج Cisco IOS® والإصدارات الأحدث، يوفر نظام Cisco IOS Intrusion Prevention System (IPS) الدعم لتنسيق توقيع برنامج Cisco IPS الإصدار x.5. تنسيق التوقيع x.5 هو تنسيق تعريف التوقيع المستند إلى الإصدار XML المستخدم أيضا من قبل منتجات IPS المستندة إلى جهاز Cisco. يتم إيقاف دعم التوقيعات وملفات تعريف التوقيع (SDFs) في هذا الأمر في Cisco IPS الإصدار x.4 وإصدارات برنامج Cisco IOS T-Train الإضافية.

يمكن للعملاء الذين يقومون بتشغيل نظام منع التسلل (IPS) من Cisco IOS باستخدام الإصدار x.4 من تنسيق التوقيع إعادة تكوين نظام منع التسلل (IPS) من Cisco لنظام Cisco IOS لاستخدام فئات التوقيع المحددة مسبقا أو مجموعات التوقيع الأساسية والمتقدمة أو أداة ترحيل Cisco IOS IPS لترحيل ملفات SDF الإصدار x.4 السابق إلى مجموعات توقيعات الإصدار x.5 من Cisco IPS.

يوضح هذا المستند كيفية الترحيل من تنسيق Cisco IPS 4.x وتمكين مجموعة التوقيعات التي تم ترحيلها في الإصدار T(11)12.4 من Cisco IOS أو الأحدث. للحصول على مزيد من المعلومات حول كيفية تكوين بروتوكول IPS من Cisco IOS في الإصدار T(11)12.4 أو إصدار أحدث، ارجع إلى دعم تنسيق توقيع IPS 5.x وتحسينات قابلية الاستخدام.

ملاحظة: توصي Cisco بتشغيل ترحيل Cisco IOS IPS قبل الترقية إلى الإصدار T(11)12.4 من Cisco IOS أو صورة أحدث.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 12.4(11)T من Cisco IOS أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

خطوات ترحيل ملفات SDF الإصدار x.4

يتطلب البرنامج النصي للترحيل ملف SDF بتنسيق Cisco IPS 4.x و(إختياري) ملف تكوين CLI الذي يحتوي على معلومات تكوين Cisco IOS IPS المستخدمة على موجه تم إصداره قبل الإصدار 12.4(11)T من Cisco IOS.

يبحث البرنامج النصي للترحيل عن الأوامر التي تحتوي على **توقيع *sigsubid*> [<*sigid*> <ip ips** **معطل**] داخل ملف تكوين الموجه. إذا كان ملف التكوين لا يحتوي على أمر CLI هذا، فلا حاجة إلى البرنامج النصي للترحيل لقراءة ملف تكوين CLI. وعلى هذا النحو، فإن تحويل التوقيعات يستند فقط إلى قوات الدفاع عن النفس.

إذا قمت بتشغيل البرنامج النصي للترحيل قبل ترقية Cisco IOS IPS إلى الإصدار 12.4(11)T من Cisco IOS أو إصدار أحدث، فاتبع العملية الموجودة في تنفيذ البرنامج النصي لترحيل Cisco IOS IPS.

إذا قمت بتشغيل البرنامج النصي للترحيل بعد ترقية Cisco IOS IPS إلى Cisco IOS، الإصدار 12.4(11)T أو إصدار أحدث، فقم بإكمال الخطوات التالية:

1. دققت أي حاجة أن يحول CLI أمر، **ip ips توقيع *sigsubid*> [<*sigid*> **يعجز**] [<*sigid*>، كما هو مذكور أعلاه.
2. أستخدم الأمر **copy running-config flash:ipscfg.cfg**لحفظ تكوين واجهة سطر الأوامر (CLI) الخاص بالموجه إلى ملف.يقوم هذا الأمر بإجراء نسخ إحتياطي لتكوين الموجه الحالي إلى ذاكرة Flash (الذاكرة المؤقتة) في ملف باسم *ipscfg.cfg*. تستخدم عملية الترحيل هذا الملف لتحويل تنسيق توقيع x.4 إلى x.5 بالكامل.
3. قم بالمتابعة لتنفيذ البرنامج النصي لترحيل Cisco IOS IPS.

تنفيذ البرنامج النصي لترحيل Cisco IOS IPS

يتوفر البرنامج النصي للترحيل من Cisco.com على عنوان URL هذا: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. قم بحفظ البرنامج النصي للترحيل إلى ذاكرة Flash (الذاكرة المؤقتة) الخاصة بالموجه أو إلى موقع يمكن الوصول إليه بواسطة الموجه، مثل خادم بروتوكول نقل الملفات المبسط (TFTP).

يحول البرنامج النصي للترحيل SDF من تنسيق Cisco IPS، الإصدار x.4 إلى تنسيق الإصدار x.5. يدعم البرنامج النصي للترحيل معلمات التوقيع التالية فقط:

- الخطورة
- الإجراء
- تمكين

بالإضافة إلى ذلك، يمكن أن يقرأ البرنامج النصي للترحيل أيضا من ملف تكوين IOS IPS وينقل التوقيعات المعطلة التي تم تكوينها بواسطة الأمر **<sigsubid>** <sigid>المعطل ل CLI في الإصدارات الأقدم من الإصدار 12.4(11)T من Cisco IOS.

ملاحظة: لا يتم تحويل التواقيع المخصصة (غير Cisco) باستخدام هذا البرنامج النصي.

يوضح هذا المثال كيفية ترحيل الملف المنسق *sdmips.sdf* IPS 4.x إلى Cisco IOS IPS في الإصدار T(11)12.4 من Cisco IOS IPS 5.x مع دعم تنسيق التوقيع Cisco IOS IPS 5.x.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
.from 4.x format to 5.x format
The migration script will migrate only the following signature
.parameters - severity, action, enabled - for Cisco (non-custom) signatures
Do you want to continue? [y/n] y
.Please choose an IOS config file from which to migrate IOS IPS configuration
[Config File: [startup-config
:The following SDF locations were found configured in startup-config
flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
choice: flash:// sdmips.sdf
:(Migrating following SDF file (this will a take few minutes
flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
C2821-sigdef-delta.xml
C2821#
```

أولا، يعرض النص التنفيذي للترحيل نص مختصر عن وظيفته. بعد ذلك، يوفر البرنامج النصي خيارا لاختيار مكان من حيث تريد قراءة التكوين الحالي (ما قبل الترحيل) ل Cisco IOS IPS. عمليات القراءة الافتراضية من تكوين بدء التشغيل. إذا كنت قد قمت مسبقا بحفظ تكوين إلى خادم TFTP أو ذاكرة Flash الخاصة بالموجه، فحدد الموقع في موجه الأمر.

على سبيل المثال:

أستخدم tftp:// 192.168.1.5/*<تكوين واجهة سطر الأوامر (CLI) للموجه>*لإعلام البرنامج النصي بتحميل تكوين CLI من خادم TFTP 192.168.1.5.

أستخدم flash://*<saved-configuration>*للقراءة من ملف تم حفظه على Flash.

تحميل التوقيعات التي تم ترحيلها في برنامج Cisco IOS IPS في البرنامج Cisco IOS Software، الإصدار T(11)12.4

بعد اكتمال ترحيل التوقيع، قم بترقية صورة الموجه إلى الإصدار T(11)12.4 من Cisco IOS إذا لم تكن قد قمت بذلك بالفعل. بمجرد إعادة تحميل الموجه، أكمل الخطوات التالية.

1. قم بتمكين IOS IPS من Cisco.يوضح هذا الإخراج كيفية تمكين Cisco IOS IPS على موجه Cisco 2821. للحصول على مزيد من المعلومات حول كيفية تكوين Cisco IOS IPS، ارجع إلى دعم تنسيق توقيع IPS 5.x وتحسينات قابلية الاستخدام.

```
C2821#mkdir ips
?[Create directory filename [ips
Created dir flash:ips
C2821#conf t
.Enter configuration commands, one per line. End with CNTL/Z
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
#(C2821(config
```

2. انسخ هذا المفتاح ولصقه في الموجه لتكوين المفتاح العام لتوقيع التشفير.

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 30820122
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36 50437722
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit
exit
exit
```

3. تمكين CISCO IOS IPS على الواجهات كما هو موضح في هذا المثال:

```
#(C2821(config
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```

4. أستخدم الأمر **copy** لتحميل أحدث حزمة توقيع:

```
C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
```

يقوم هذا الأمر بتحميل التوقيعات من حزمة التوقيع *IOS-S253-CLI.pkg* في Cisco IOS IPS.**ملاحظة:** تم تكوين **فئة توقيع IOS-IPS** في الخطوة 1، التي تقوم بإعادة حساب جميع التوقيعات. بعد تحميل حزمة التوقيع بنجاح، لا يتم تحديد وتجميع أي توقيعات.

5. أستخدم هذا الأمر لتحميل ملف XML الذي تم ترحيله إلى Cisco IOS IPS:**<*router-hostname*>-sigdef-delta.xml**على سبيل المثال:

```
copy flash:C2821-sigdef-delta.xml idconf
```

بمجرد أن يقوم الموجه بتحليل ملف التوقيع المنسق للإصدار x.5، يكون الترحيل مكتملا.

6. أستخدم الأمر **show ip ips signature count** للتحقق من حالة ملخص التوقيع، ثم أستخدم الأمر **show ip ips signature details** لعرض تفاصيل محددة على جميع التوقيعات.

معلومات ذات صلة

- نظام Cisco لمنع الاقتحام
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك اكتشاف إقتحام CiscoSecure)
- الدعم الفني - Cisco Systems

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).