Migreer IPS Signature Format 4.x tot 5.x

Inhoud

Inleiding

In Cisco IOS® release 12.4(11)T en hoger biedt Cisco IOS Inbraakpreventiesysteem (IPS) ondersteuning voor de Cisco IPS-softwareversie 5.x-signaalindeling. De 5.x-signatuur is een versie-gebaseerd XML-formaat dat ook wordt gebruikt door andere Cisco op apparaat gebaseerde IPS-producten. Ondersteuning van handtekeningen en signatuur definitiebestanden (SDF's) in Cisco IPS versie 4.x wordt in deze en verdere Cisco IOS T-Train softwarereleases stopgezet.

Klanten die Cisco IOS IPS uitvoeren met versie 4.x SDF's voor kenmerkende onderdelen kunnen Cisco IOS IPS aanpassen om Cisco voorgeprogrammeerde kenmerkende categorieën, basis- en geavanceerde kenmerksets voor handtekeningen te gebruiken, of het Cisco IOS IPS-migratiehulpprogramma om vorige versie 4.x SDF-bestanden te migreren naar Cisco IPS versie 5.x-tekensets.

Dit document beschrijft hoe u kunt migreren van een Cisco IPS 4.x-formaat SDF en hoe u de gemigreerde handtekening kunt inschakelen die is ingesteld in Cisco IOS release 12.4(11)T of hoger. Raadpleeg voor meer informatie over de manier waarop u Cisco IOS IPS in Cisco IOS release 12.4(11)T of hoger kunt configureren Verbeteringen in IPS 5.x ter ondersteuning en bruikbaarheid van signaalindeling.

Opmerking: Cisco raadt u aan de Cisco IOS IPS-migratie uit te voeren voordat u uw upgrade naar een Cisco IOS release 12.4(11)T of een later beeld uitvoert.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS release 12.4(11)T of hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

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

Stappen om bestanden te migreren, versie 4.x SDF

Het migratiemanagement vereist een Cisco IPS 4.x-formaat SDF-bestand en (optioneel) het CLI-configuratiebestand dat Cisco IOS IPS-configuratieinformatie bevat die op een router die eerder dan Cisco IOS release 12.4(11)T wordt gebruikt.

Het migratiescript zoekt naar opdrachten die **IP IPS-handtekeningen** bevatten **<*sigid*> [<*sigsubid*>]** uitgeschakeld in het routerconfiguratiebestand. Als het configuratiebestand deze CLI-opdracht niet bevat, hoeft het migratieteken het CLI-configuratiebestand niet te lezen. De omkering van handtekeningen als zodanig is uitsluitend gebaseerd op SDF.

Als u het migratieteken uitvoert voordat u Cisco IOS IPS upgrade naar Cisco IOS release 12.4(11)T of hoger uitvoert, volgt u het proces in Uitvoer van het Cisco IOS IPS-migratietrift.

Als u het migratietool draait nadat u Cisco IOS IPS naar Cisco IOS release 12.4(11)T hebt geupgrade, voltooid u deze stappen:

1. Controleer de noodzaak om CLI-opdrachten te converteren, **IP-handtekening <*sigid*> [<*sigsubid*>] uitgeschakeld**, zoals hierboven vermeld wordt.
2. Gebruik de opdracht **kopie in werking stellen-configuratieflitser:ipscfg.cfg** om de CLI-configuratie van de router in een bestand op te slaan.Deze opdracht maakt een back-up van de bestaande routerconfiguratie om in een bestand met de naam *ipscfg.cfg* te flitsen. Het migratieproces gebruikt dit bestand voor de volledige conversie van 4.x naar 5.x-formaat.
3. Ga verder naar uitvoering van het Cisco IOS IPS-migratiesCHrift.

Uitvoeren van het Cisco IOS IPS-migratieschrift

Het migratietool is op Cisco.com beschikbaar via deze URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Sla het migratietool op de flitser van de router of op een router-toegankelijke locatie, zoals een TFTP-server (Trial File Transfer Protocol).

Het migratietool converteert een SDF van Cisco IPS versie 4.x-formaat naar versie 5.x-formaat. Het migratietool ondersteunt alleen deze kenmerkende parameters:

- ernst
- actie

- ingeschakeld

Bovendien kan het migratieteken ook lezen uit een IOS IPS-configuratiebestand en gehandicapte handtekeningen migreren die door de CLI **ip-handtekening <sigsub> <sigsub> uitgeschakeld** opdracht in releases eerder dan Cisco IOS release 12.4(11)T waren.

Opmerking: Aangepaste (niet-Cisco) handtekeningen worden niet geconverteerd met dit script.

Dit voorbeeld toont hoe u het IPS 4.x geformatteerde bestand *sdmips.sdf* naar Cisco IOS IPS in Cisco IOS release 12.4(11)T kunt migreren met ondersteuning voor Cisco IOS IPS 5.x formaat voor handtekeningen.

```
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#
```

Eerst toont het migratietool een korte tekst over de functie. Daarna biedt het script een optie om een locatie te kiezen waar u de huidige (pre-migratie) configuratie voor Cisco IOS IPS wilt lezen. De standaardinstelling is het resultaat van de opstartconfiguratie. Als u eerder een configuratie aan een TFTP server of de flitser van de router hebt opgeslagen, specificeer de plaats bij de herinnering.

Bijvoorbeeld:

Gebruik **tftp:// 192.168.1.5/<*router CLI-configuratie*>**om het script te laten weten dat het een CLI-configuratie kan laden vanaf TFTP-server 192.168.1.5.

Gebruik **flash://<*opgeslagen-configuratie*>**om te lezen uit een bestand dat op flitser is opgeslagen.

Laad de gedistribueerde handtekeningen in Cisco IOS IPS in Cisco IOS-softwarerelease 12.4(11)T

Nadat de signaalmigratie is voltooid, upgrade van het beeld van de router naar Cisco IOS release 12.4(11)T als u dit nog niet hebt gedaan. Zodra de router opnieuw is geladen, voltooien deze stappen.

1. Cisco IOS IPS inschakelenDeze uitvoer toont hoe om Cisco IOS IPS op een Cisco 2821 router in te schakelen. Voor meer informatie over hoe u Cisco IOS IPS kunt configureren raadpleegt u Verbeteringen in bestandsindeling voor IPS 5.x-handtekeningen en in bruikbaarheid.

   ```
   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. Kopieer en plak deze toets naar de router om de crypto handtekening openbare sleutel te configureren.

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
 key-string
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 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
 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
 F3020301 0001
 quit
 exit
 exit
```

3. Schakel Cisco IOS IPS op interfaces in zoals in dit voorbeeld:

```
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. Gebruik de opdracht **kopie** om het laatste signatuur-pakket te laden:

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

Deze opdracht ladingen handtekeningen van het signatuur-pakket *IOS-S253-CLI.pkg* in Cisco IOS IPS.**Opmerking: ios-ips-signatuurcategorie** werd **allemaal** geconfigureerd in stap 1, die alle handtekeningen terugtrekt. Nadat het signatuur pakket succesvol geladen is, worden geen handtekeningen geselecteerd en samengesteld.

5. Gebruik deze opdracht om het gemigreerde XML bestand naar Cisco IOS IPS te laden:**<*router-hostname*>-sigdef-delta.xml**Bijvoorbeeld:

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

Nadat de router versie 5.x heeft geformatteerd voor de handtekening, is de migratie voltooid.

6. Gebruik de opdracht **IP IP-handtekeningen tellen** om de staat van de handtekening te controleren en gebruik vervolgens de opdracht **om ip IPS-**handtekeningen te **tonen** om specifieke details op alle handtekeningen te bekijken.

Gerelateerde informatie

- Cisco-inbraakpreventiesysteem
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)
- Technische ondersteuning - Cisco-systemen