Beispiel für die Migration des Signaturformats Intrusion Prevention System Version 4.x auf Version 5.x Signature Format

Inhalt

Einleitung

In Cisco IOS® Version 12.4(11)T und höher unterstützt das Cisco IOS Intrusion Prevention System (IPS) das Signaturformat der Cisco IPS-Software Version 5.x. Das 5.x-Signaturformat ist ein versionsbasiertes SignaturdefinitionsXML-Format, das auch von anderen Cisco Appliance-basierten IPS-Produkten verwendet wird. Die Unterstützung für Signaturen und Signaturdefinitionsdateien (SDFs) in Cisco IPS Version 4.x wird in dieser und weiteren Cisco IOS T-Train-Softwareversionen eingestellt.

Kunden, die Cisco IOS IPS mit SDFs im Signaturformat Version 4.x ausführen, können Cisco IOS IPS für die Verwendung vordefinierter Signaturkategorien, Basic und Advanced-Signatursets oder des Migrations-Utilitys für Cisco IOS IPS neu konfigurieren, um SDF-Dateien der vorherigen Version 4.x in Signatursätze im Format Cisco IPS Version 5.x zu migrieren.

In diesem Dokument wird beschrieben, wie Sie von einem Cisco IPS 4.x-Format-SDF migrieren und den migrierten Signatursatz in Cisco IOS 12.4(11)T oder höher aktivieren. Weitere Informationen zur Konfiguration von Cisco IOS IPS in Cisco IOS 12.4(11)T oder höher finden Sie unter Unterstützung für IPS 5.x-Signaturformat und verbesserte Benutzerfreundlichkeit.

Hinweis: Cisco empfiehlt, die Cisco IOS IPS-Migration vor dem Upgrade auf ein Image der Cisco IOS-Version 12.4(11)T oder höher auszuführen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS-Version 12.4(11)T oder höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Schritte zur Migration von SDF-Dateien der Version 4.x

Das Migrationsskript erfordert eine SDF-Datei im Cisco IPS 4.x-Format und (optional) die CLI-Konfigurationsdatei, die Cisco IOS IPS-Konfigurationsinformationen enthält, die auf einem Router verwendet werden, der vor der Cisco IOS-Version 12.4(11)T veröffentlicht wurde.

Das Migrationsskript sucht nach Befehlen, die die **ip ips-Signatur <*sigid*> [<*sigsubid*>]** enthalten, die in der Router-Konfigurationsdatei **deaktiviert ist**. Wenn die Konfigurationsdatei diesen CLI-Befehl nicht enthält, muss das Migrationsskript die CLI-Konfigurationsdatei nicht lesen. Die Konvertierung von Signaturen als solche basiert ausschließlich auf dem SDF.

Wenn Sie das Migrationsskript ausführen, bevor Sie ein Upgrade von Cisco IOS IPS auf Cisco IOS Release 12.4(11)T oder höher durchführen, folgen Sie dem Prozess unter Ausführen des Cisco IOS IPS-Migrationsskripts.

Wenn Sie das Migrationsskript nach dem Upgrade von Cisco IOS IPS auf Cisco IOS Release 12.4(11)T oder höher ausführen, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie, ob CLI-Befehle konvertiert werden müssen. Die **ip ips-Signatur <*sigid*> [<*sigsubid*>] ist deaktiviert**, wie oben beschrieben.
2. Verwenden Sie den Befehl **copy running-config flash:ipscfg.cfg**, um die CLI-Konfiguration des Routers in einer Datei zu speichern.Mit diesem Befehl wird die vorhandene Router-Konfiguration gesichert, um in einer Datei mit dem Namen *ipscfg.cfg* zu flashen. Der Migrationsprozess verwendet diese Datei für die vollständige Konvertierung des Signaturformats 4.x in 5.x.
3. Führen Sie das Cisco IOS IPS-Migrationsskript aus.

Ausführen des Cisco IOS IPS-Migrationsskripts

Das Migrationsskript steht unter der URL von Cisco.com zur Verfügung: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup Speichern Sie das Migrationsskript im Flash-Speicher des Routers oder an einem für den Router zugänglichen Ort, z. B. einem TFTP-Server (Trivial File Transfer Protocol).

Das Migrationsskript konvertiert ein SDF aus dem Format Cisco IPS Version 4.x in das Format Version 5.x. Das Migrationsskript unterstützt nur folgende Signaturparameter:

- schweregrad
- aktion
- aktiviert

Darüber hinaus kann das Migrationsskript auch aus einer IOS IPS-Konfigurationsdatei lesen und deaktivierte Signaturen migrieren, die mit dem Befehl CLI **ip ips signatur <sigid> <sigsubid> disabled** in Versionen vor Cisco IOS Release 12.4(11)T konfiguriert wurden.

Hinweis: Benutzerdefinierte Signaturen (nicht von Cisco) werden mit diesem Skript nicht konvertiert.

In diesem Beispiel wird gezeigt, wie die mit IPS 4.x formatierte Datei *sdmips.sdf* in Cisco IOS IPS 12.4(11)T mit Unterstützung des Signaturformats Cisco IOS IPS 5.x migriert wird.

```
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#
```

Zunächst zeigt das Migrationsskript einen kurzen Text über seine Funktion an. Als Nächstes bietet das Skript die Option, einen Speicherort auszuwählen, von dem aus die aktuelle (vor der Migration) Konfiguration für Cisco IOS IPS gelesen werden kann. Der Standardwert lautet aus der Startkonfiguration. Wenn Sie zuvor eine Konfiguration auf einem TFTP-Server oder im Flash-Speicher des Routers gespeichert haben, geben Sie den Speicherort an der Eingabeaufforderung an.

Beispiele:

Verwenden Sie **tftp:// 192.168.1.5/<*CLI-Konfiguration des Routers*>**, um das Skript darüber zu benachrichtigen, dass eine CLI-Konfiguration vom TFTP-Server 192.168.1.5 geladen wird.

Verwenden Sie **flash://<*save-configuration*>**, um aus einer im Flash gespeicherten Datei zu lesen.

Laden der migrierten Signaturen in Cisco IOS IPS in Version 12.4(11)T der Cisco IOS-Software

Nachdem die Signaturmigration abgeschlossen ist, aktualisieren Sie das Image des Routers auf Cisco IOS Release 12.4(11)T, falls Sie dies noch nicht getan haben. Führen Sie nach dem erneuten Laden des Routers diese Schritte aus.

1. Aktivieren Sie Cisco IOS IPS.Diese Ausgabe zeigt, wie Cisco IOS IPS auf einem Cisco 2821 Router aktiviert wird. Weitere Informationen zur Konfiguration von Cisco IOS IPS finden Sie unter Unterstützung von IPS 5.x-Signaturformaten und Verbesserungen bei der Benutzerfreundlichkeit.

```
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. Kopieren Sie diesen Schlüssel, und fügen Sie ihn in den Router ein, um den öffentlichen Schlüssel für die Krypto-Signatur zu konfigurieren.

```
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. Aktivieren Sie Cisco IOS IPS auf Schnittstellen, wie in diesem Beispiel gezeigt:

```
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. Verwenden Sie den Befehl **copy**, um das neueste Signaturpaket zu laden:

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

   Dieser Befehl lädt Signaturen aus dem Signaturpaket *IOS-S253-CLI.pkg* in Cisco IOS IPS.**Hinweis: Die ios-ips-Signaturkategorie** wurde **alle** in Schritt 1 konfiguriert, in der alle Signaturen außer Kraft gesetzt werden. Nachdem das Signaturpaket erfolgreich geladen wurde, werden keine Signaturen ausgewählt und kompiliert.
5. Verwenden Sie diesen Befehl, um die migrierte XML-Datei in Cisco IOS IPS zu laden:**<*router-hostname*>-sigdef-delta.xml**Beispiele:

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

   Nachdem der Router die Signaturdatei im Format Version 5.x analysiert hat, ist die Migration abgeschlossen.

6. Verwenden Sie den Befehl **show ip ips signature count** (Anzahl der Signaturen anzeigen), um den Status der Signaturzusammenfassung zu überprüfen, und verwenden Sie dann den Befehl **show ip ips signature details**, um spezifische Details aller Signaturen anzuzeigen.

Zugehörige Informationen

- Cisco Intrusion Prevention System
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- Technischer Support – Cisco Systems