Migrazione del formato della firma IPS da 4.x a 5.x

Sommario

Introduzione

In Cisco IOS® versione 12.4(11)T e successive, Cisco IOS Intrusion Prevention System (IPS) supporta il formato della firma del software Cisco IPS versione 5.x. Il formato della firma 5.x è un formato XML di definizione della firma basato sulla versione utilizzato anche da altri prodotti IPS basati su appliance Cisco. Il supporto per le firme e i file di definizione delle firme (SDF) in Cisco IPS versione 4.x non è più disponibile in questa e in altre versioni del software Cisco IOS T-Train.

I clienti che eseguono Cisco IOS IPS con SDF in formato firma versione 4.x possono riconfigurare Cisco IOS IPS in modo da utilizzare le categorie di firma predefinite, i set di firme di base e avanzati o l'utility di migrazione IPS di Cisco IOS in modo da migrare i file SDF della versione precedente nella versione 5.x dei set di firme in formato Cisco IPS.

In questo documento viene descritto come eseguire la migrazione da un SDF in formato Cisco IPS 4.x e abilitare il set di firme migrato in Cisco IOS versione 12.4(11)T o successive. Per ulteriori informazioni su come configurare IPS Cisco IOS in Cisco IOS versione 12.4(11)T o successive, fare riferimento alla sezione Supporto del formato della firma IPS 5.x e miglioramenti della facilità d'uso.

Nota: Cisco consiglia di eseguire la migrazione a Cisco IOS IPS prima di eseguire l'aggiornamento a un'immagine Cisco IOS versione 12.4(11)T o successive.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco IOS versione 12.4(11)T o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Procedura per la migrazione dei file SDF versione 4.x

Lo script di migrazione richiede un file SDF in formato Cisco IPS 4.x e (facoltativamente) il file di configurazione CLI che contiene le informazioni di configurazione IPS di Cisco IOS utilizzate su un router con una versione precedente a Cisco IOS versione 12.4(11)T.

Lo script di migrazione cerca i comandi che contengono la **firma ip ip <*sigid*> [<*sigsubid*>] disabilitata** nel file di configurazione del router. se il file di configurazione non contiene questo comando CLI, non è necessario che lo script di migrazione legga il file di configurazione CLI. La conversione delle firme, in quanto tale, si basa esclusivamente sull'SDF.

Se si esegue lo script di migrazione prima di aggiornare Cisco IOS IPS alla versione 12.4(11)T o successive, seguire il processo illustrato in Esecuzione dello script di migrazione IPS di Cisco IOS.

Se si esegue lo script di migrazione dopo aver aggiornato Cisco IOS IPS alla versione 12.4(11)T o successive, attenersi alla seguente procedura:

1. Verificare se è necessario convertire i comandi CLI. **ip ips signature <*sigid*> [<*sigsubid*>] disabilitato**, come indicato in precedenza.
2. Per salvare la configurazione CLI del router in un file, usare il comando **copy running-config flash:ipscfg.cfg**.Questo comando esegue il backup della configurazione del router esistente per la memorizzazione nella memoria flash di un file denominato *ipscfg.cfg*. Il processo di migrazione utilizza questo file per la conversione completa del formato di firma da 4.x a 5.x.
3. Procedere all'esecuzione dello script di migrazione IPS Cisco IOS.

Esegui script di migrazione IPS Cisco IOS

Lo script di migrazione è disponibile all'indirizzo Cisco.com al seguente URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Salvare lo script di migrazione nella memoria flash del router o in una posizione accessibile dal router, ad esempio un server TFTP (Trivial File Transfer Protocol).

Lo script di migrazione converte un SDF dal formato Cisco IPS versione 4.x al formato versione 5.x. Lo script di migrazione supporta solo i seguenti parametri di firma:

- gravità
- azione
- attivato

Inoltre, lo script di migrazione può anche leggere da un file di configurazione IPS di IOS ed eseguire la migrazione delle firme disabilitate configurate dal comando CLI **ip ips signature <sigid> <sigsubid>** disabled nelle versioni precedenti a Cisco IOS versione 12.4(11)T.

Nota: le firme personalizzate (non Cisco) non vengono convertite con questo script.

Nell'esempio viene mostrato come eseguire la migrazione del file formattato IPS 4.x *sdmips.sdf* a Cisco IOS IPS nella versione 12.4(11)T con supporto del formato della firma 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#
```

Innanzitutto, lo script di migrazione visualizza un breve testo sulla sua funzione. Successivamente, lo script fornisce un'opzione per scegliere un percorso da cui leggere la configurazione corrente (pre-migrazione) per Cisco IOS IPS. Il valore predefinito viene letto dalla configurazione di avvio. Se la configurazione è stata salvata in precedenza su un server TFTP o sul flash del router, specificare il percorso al prompt.

Ad esempio:

Utilizzare **tftp:// 192.168.1.5/<*router CLI configuration*>** per notificare allo script il caricamento di una configurazione CLI dal server TFTP 192.168.1.5.

Usare **flash://<*saved-configuration*>** per leggere da un file salvato nella memoria flash.

Caricamento delle firme migrate nel software Cisco IOS IPS versione 12.4(11)T

Al termine della migrazione della firma, aggiornare l'immagine del router a Cisco IOS versione 12.4(11)T, se non è già stato fatto. Dopo aver ricaricato il router, procedere come segue.

1. Abilitare Cisco IOS IPS.Questo output mostra come abilitare Cisco IOS IPS su un router Cisco 2821. Per ulteriori informazioni su come configurare IPS Cisco IOS, fare riferimento a Supporto del formato della firma IPS 5.x e miglioramenti della facilità d'uso.

   ```
   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. Copiare e incollare questa chiave nel router per configurare la chiave pubblica della firma crittografica.

```
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. Abilitare Cisco IOS IPS sulle interfacce come mostrato nell'esempio:

```
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. Utilizzare il comando **copy** per caricare l'ultimo pacchetto di firma:

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

Questo comando carica le firme del pacchetto di firma *IOS-S253-CLI.pkg* in Cisco IOS IPS.**Nota: la categoria di firma ios-ips all** è stata configurata nel passaggio 1, che prevede il ritiro di tutte le firme. Dopo il caricamento del pacchetto di firma, non verrà selezionata e compilata alcuna firma.

5. Utilizzare questo comando per caricare il file XML migrato in Cisco IOS IPS:**<*nomehost-router*>-sigdef-delta.xml**Ad esempio:

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

Una volta che il router ha analizzato il file di firma formattato versione 5.x, la migrazione è completa.

6. Usare il comando **show ip ips signature count** per controllare lo stato del riepilogo della firma, quindi usare il comando **show ip ips signature details** per visualizzare i dettagli specifici di tutte le firme.

Informazioni correlate

- Cisco Intrusion Prevention System
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure Intrusion Detection)
- Supporto tecnico – Cisco Systems