

Intrusion Prevention System Version 4.x Signature Format to Version 5.x Signature Format Migration Example

Document ID: 105628

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Steps to Migrate Version 4.x SDF Files

- Execute the Cisco IOS IPS Migration Script

- Load the Migrated Signatures into Cisco IOS IPS in Cisco IOS Software Release

12.4(11)T

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

In Cisco IOS® Release 12.4(11)T and later, Cisco IOS Intrusion Prevention System (IPS) provides support for the Cisco IPS software version 5.x signature format. The 5.x signature format is a version-based signature definition XML format also used by other Cisco appliance-based IPS products. Support for signatures and signature definition files (SDFs) in Cisco IPS version 4.x are discontinued in this and further Cisco IOS T-Train software releases.

Customers that run Cisco IOS IPS with Version 4.x signature format SDFs can reconfigure Cisco IOS IPS to use Cisco predefined signature categories, Basic and Advanced signature sets, or the Cisco IOS IPS migration utility in order to migrate previous version 4.x SDF files into Cisco IPS Version 5.x format signature sets.

This document describes how to migrate from a Cisco IPS 4.x format SDF and enable the migrated signature set in Cisco IOS Release 12.4(11)T or later. For more information on how to configure Cisco IOS IPS in Cisco IOS Release 12.4(11)T or later, refer to IPS 5.x Signature Format Support and Usability Enhancements.

Note: Cisco recommends that you run the Cisco IOS IPS migration before you upgrade to a Cisco IOS Release 12.4(11)T or later image.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco IOS Release 12.4(11)T or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Steps to Migrate Version 4.x SDF Files

The migration script requires a Cisco IPS 4.x format SDF file and (optionally) the CLI configuration file that contains Cisco IOS IPS configuration information used on a router that runs a release earlier than Cisco IOS Release 12.4(11)T.

The migration script searches for commands that contain **ip ips signature <sigid> [<sigsubid>] disabled** within the router configuration file. If the configuration file does not contain this CLI command, there is no need for the migration script to read the CLI configuration file. Conversion of signatures, as such, are based solely on the SDF.

If you run the migration script before you upgrade Cisco IOS IPS to Cisco IOS Release 12.4(11)T or later, follow the process in Execute the Cisco IOS IPS Migration Script.

If you run the migration script after you upgrade Cisco IOS IPS to Cisco IOS Release 12.4(11)T or later, complete these steps:

1. Verify any need to convert CLI commands, **ip ips signature <sigid> [<sigsubid>] disabled**, as mentioned above.
2. Use the command **copy running-config flash:ipscfg.cfg** in order to save the router's CLI configuration to a file.

This command backs up the existing router configuration to flash in a file named *ipscfg.cfg*. The migration process uses this file for full 4.x to 5.x signature format conversion.

3. Proceed to Execute the Cisco IOS IPS Migration Script.

Execute the Cisco IOS IPS Migration Script

The migration script is available from Cisco.com at this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>. Save the migration script to the router's flash or to a router-accessible location, such as a Trivial File Transfer Protocol (TFTP) server.

The migration script converts an SDF from Cisco IPS Version 4.x format to Version 5.x format. The migration script supports only these signature parameters:

- severity
- action
- enabled

In addition, the migration script can also read from an IOS IPS configuration file and migrate disabled signatures that were configured by the CLI **ip ips signature <sigid> <sigsubid> disabled** command in releases earlier than Cisco IOS Release 12.4(11)T.

Note: Custom (non Cisco) signatures are not converted with this script.

This example shows how to migrate the IPS 4.x formatted file *sdmips.sdf* to Cisco IOS IPS in Cisco IOS Release 12.4(11)T with Cisco IOS IPS 5.x signature format support.

```

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#

```

First, the migration script displays a brief text about its function. Next, the script provides an option to choose a location from where to read the current (pre-migration) configuration for Cisco IOS IPS. The default reads from the startup configuration. If you have previously saved a configuration to a TFTP server or the router's flash, specify the location at the prompt.

For example:

Use **tftp:// 192.168.1.5/<router CLI configuration>** in order to notify the script to load a CLI configuration from TFTP server 192.168.1.5.

Use **flash://<saved-configuration>** in order to read from a file saved on flash.

Load the Migrated Signatures into Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T

After signature migration is complete, upgrade the router's image to Cisco IOS Release 12.4(11)T if you have not already done so. Once the router is reloaded, complete these steps.

1. Enable Cisco IOS IPS.

This output shows how to enable Cisco IOS IPS on a Cisco 2821 router. For more information on how to configure Cisco IOS IPS, refer to [IPS 5.x Signature Format Support and Usability Enhancements](#).

```

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. Copy and paste this key into the router in order to configure the crypto signature public key.

```

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. Enable Cisco IOS IPS on interfaces as shown in this example:

```

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. Use the **copy** command in order to load the latest signature package:

```

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

```

This command loads signatures from the signature package *IOS-S253-CLI.pkg* into Cisco IOS IPS.

Note: **ios-ips signature category all** was configured in step 1, which retires all signatures. After the signature package is successfully loaded, no signatures are selected and compiled.

5. Use this command in order to load the migrated XML file to Cisco IOS IPS:

```

<router-hostname>-sigdef-delta.xml

```

For example:

```

copy flash:C2821-sigdef-delta.xml idconf

```

Once the router parses the version 5.x formatted signature file, migration is complete.

6. Use the **show ip ips signature count** command in order to check signature summary status, and then use the **show ip ips signature details** command in order to view specific details on all signatures.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Cisco Intrusion Prevention System**
 - **Security Product Field Notices (including CiscoSecure Intrusion Detection)**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 17, 2008

Document ID: 105628
