Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements

First Published: November 17, 2006
Last Updated: November 17, 2006

This feature introduces support for Cisco IOS Intrusion Prevention System (IPS) version 5.0, which is a version-based signature definition XML format. In Cisco IOS Release 12.4(11)T, Cisco IOS IPS 4.x format signatures are replaced by the 5.x format signatures that are used by all other Cisco IPS devices.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS" section on page 59.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

System and Image Requirements for Cisco IOS IPS 5.x

- Cisco IOS IPS signature categories are available in two formats—Basic and Advanced.
- Cisco IOS IPS system requirements depend on the type of deployment, the bandwidth requirements, and security requirements. The larger the number of signatures, the larger the amount of memory consumed.
- You must generate a RSA crypto key and load the public signature on your router for signature decryption.

  This following cisco public key configuration can be cut and pasted directly into your router configuration:

```
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
```

Note You can also access the public key configuration at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup

- You must load one of the following images on your router to install Cisco IOS IPS 5.x: adventerprisek9, advsecurityk9, and advipservicesk9.

Note To check the current system version, use the **show subsys name ips** command.

IPS 4.x uses a version format of 2.xxx.xxx; IPS 5.x uses a version format of 3.xxx.xxx.

Upgrading from Cisco IOS IPS 4.x to Cisco IOS IPS 5.x Signatures

Cisco IOS IPS 5.x format signatures are not backward compatible with Cisco IOS IPS 4.x. You must reconfigure your Cisco IOS IPS features for use with the IPS 5.x signature format command-line interface (CLI) and features.

When reconfiguring Cisco IOS IPS on a router to convert to the 5.x signature format, you must have the following Cisco IOS IPS 4.x information:

- Cisco IOS IPS rule name (which was specified via the **ip ips name** *ips-name* command)
- Interfaces for which the Cisco IOS IPS rule has been applied
- User-created and customized signature definition files (SDFs)

To gather this information, issue the **show ip ips configuration** command, which displays a copy of the existing output.

```
Router# show ip ips configuration
Configured SDF Locations:
disk2:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 05:31:54 MST Sep 20 2003
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 13
Total Inactive Signatures: 0
Signature 50000:0 disable
Signature 50000:1 disable
Signature 50000:2 disable
IPS Rule Configuration
IPS name MYIPS
Interface Configuration
Interface GigabitEthernet0/1
Inbound IPS rule is MYIPS
Outgoing IPS rule is not set
```

Note Detailed or customized changes to specific signatures may be lost. IPS 4.x SDF files will not load under the Cisco IOS IPS 5.x version.

Restrictions for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Warning **Do not enable all IPS signatures. The router may not be able to able to compile all signatures, resulting in high CPU and memory usage, degraded performance, and a system crash.**

Backward Compatibility

Cisco IOS IPS 5.x format signatures are not backward compatible with Cisco IOS IPS 4.x SDFs.

Cisco 870 Series Platform Support

The 870 series platform with Cisco IOS IPS in Cisco IOS Release 12.4(11)T may experience lower performance relative to previous releases (CSCsg57228). The Cisco IOS IPS performance on the 870 series platform will be enhanced in a later 12.4(11)T image rebuild.

On the 870 series platform, Cisco IOS IPS is supported only on the adv-ipservices and the adv-enterprise images. Cisco IOS IPS is the same on both images.

Information About Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Before using Cisco IOS 5.x format signatures with Cisco IOS IPS, you should understand the following concepts:

Cisco IOS IPS Overview

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured via CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

Signature Categories

Cisco IPS appliances and Cisco IOS IPS with Cisco 5.x format signatures operate with signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category. (For a list of supported top-level categories, use your router CLI help (**?**).)

Router Configuration Files and Signature Event Action Processor (SEAP)

As of Cisco IOS Release 12.4(11)T, SDFs are no longer used by Cisco IOS IPS. Instead, routers access signature definition information via a directory that contains three configuration files—the default configuration, the delta configuration, and the SEAP configuration. Cisco IOS accesses this directory via the **ip ips config location** command.

Note You must issue the **ip ips config location** command; otherwise, the configuration files are not saved to any location.

SEAP is the control unit responsible for coordinating the data flow of a signature event. It allows for advanced filtering and signature overrides on the basis of the Event Risk Rating (ERR) feedback. ERR is used to control the level in which a user chooses to take actions in an effort to minimize false positives.

Signatures once stored in NVRAM, will now be stored in the delta configuration file; thus, support for access control lists (ACLs) is no longer necessary.

Additional Risk Rating Algorithims

The ERR characterizes the risk of an attack and allows users to make decisions on the basis of the risk control signature event actions. To help further control signature event actions, the following additional rating categories are now supported:

- Attack Severity Rating (ASR)—Determines the severity of an attack. The attack-severity rating values are hard-coded in Cisco IOS IPS as follows: high, medium, low, and informational. The ASR can be changed via the **alert-rating** command. To change the ASF, see the section "Tuning Signature Parameters."
- Signature Fidelity Rating (SFR)—Determines the confidence level of detecting a true positive. The SFR can be changed via the **fidelity-rating** command. To change the SFR, see the section "Tuning Signature Parameters."
- Target Value Rating (TVR)—Allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS IPS. A host can be a single IP address or a range of IP addresses with an associated target value rating. To configure the TVR, see the task "Setting the Target Value Rating."

Benefits of Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Automatic Signature Update

With Cisco IOS IPS 5.0, customers can now configure automatic signature updates from local servers.

Network administrators can either preserve the user's current configuration of signature actions or override the user's current configuration of signature actions with the current IPS configuration.

Auto update can also update the CLI signature package.

If this feature is enabled, signatures are delivered in either a Basic signature file or an Advanced signature file.

Signature Category-Based Configuration

Top-level signature categories help to classify signatures for easy grouping and tuning; that is, group-wide parameters, such as signature event action, can be applied to a group via CLI, so the user does not have to modify each individual signature.

Encrypted Signature Support

Cisco IOS IPS introduces support for encrypted (NDA) signatures.

Signature Update Accessibility

To help detect the latest vulnerabilities, Cisco provides the following signature update options:

- Download the latest signature file package from Cisco.com at the following URL:

  http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup
- Configure automatic signature updates via the **ip ips autoupdate** command. Updates can be configured to run on the basis of a preset time. For more information, see the task "Enabling Automatic Signature Updates."
- Issue the **copy** *url* **idconf** command to instruct the router where to load a signature file. (The file can be saved in a location specified via the **ip ips config location** command.)

How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS

This section contains the following procedures:

Retiring All Signatures and Selecting a Category of Signatures

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-category**
4. **category** *category* [*sub-category*]

5. **retired** {**true** | **false**}
6. **exit**
7. **category** *category* [*sub-category*]
8. **retired** {**true** | **false**}
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips signature-category** **Example:** `Router(config)# ip ips signature-category`	Enters enters IPS category configuration mode.
Step 4	**category** *category* [*sub-category*] **Example:** `Router(config-ips-category)# category all`	Specifies that all categories (and all signatures) will be retired in the following step and enters IPS category action configuration mode.
Step 5	**retired** {**true** | **false**} **Example:** `Router(config-ips-category-action)# retired true`	Specifies that the router should retire all categories (and all signatures). • **true**—Retires all signatures within a given category. • **false** —"Unretires" all signatures within a given category.
Step 6	**exit** **Example:** `Router(config-ips-category-action)# exit`	Exits IPS category action configuration mode.
Step 7	**category** *category* [*sub-category*] **Example:** `Router(config-ips-category)# category ios_ips basic`	Specifies the basic category (and a set of signatures) that are to be "unretired" in the following step.

	Command or Action	Purpose
Step 8	**retired** {**true** | **false**} **Example:** `Router(config-ips-category-action)# retired false`	Specifies that all signatures within the basic category are to be unretired; that is, signatures will be enabled for the basic category.

Step 9	**exit**
	
	Example:
	`Router(config-ips-category-action)# exit`
	`Router(config-ips-category)# exit`
		Exits IPS category action and IPS category configuration modes.

What to Do Next

After you have configured the basic category, you should enable Cisco IOS IPS on your router as shown in the section "Configuring Cisco IOS IPS on Your Router."

You can customize (or tune) the entire category or individual signatures within a category to addresses the needs of your network. For information on tuning signatures, see the section "Tuning Signature Parameters."

Configuring Cisco IOS IPS on Your Router

After you have set up a "load definition" for the signature package file to be copied to the idconf, you must configure an IPS rule name. Use this task to configure an IPS rule name and start the IPS configuration.

You can also use this task to configure a Cisco IOS IPS signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in case the router reboots or IPS is disabled or reenabled. Files, such as signature definition, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

SUMMARY STEPS

1. **enable**
2. **mkdir flash:/ips5**
3. **configure terminal**
4. **ip ips name** *ips-name*
5. **ip ips config location** *url*
6. **interface** *type name*
7. **ip ips** *ips-name* {**in** | **out**}
8. **exit**
9. **show ip ips configuration**
10. **show ip ips signature** *count*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**mkdir flash:/ips5** **Example:** `Router# mkdir flash:/ips5`	Create a directory for which Cisco IOS IPS will save signature information. **Note** The directory location will be specified via the **ip ips config location** command.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**ip ips name** *ips-name* **Example:** `Router(config)# ip ips name myips`	Creates an IPS rule.
Step 5	**ip ips config location** *url* **Example:** `Router(config)# ip ips config location flash:/ips5`	Specifies the location where Cisco IOS IPS will save the signature information, and, if necessary, access the signature configuration information. **Note** You must specify a location; otherwise, the signature package will not be saved. **Note** If the specified location is a URL, such as an FTP server, the user must have writer privileges.
Step 6	**interface** *type name* **Example:** `Router(config)# interface gigbitEthernet 0/0`	Identifies the interface in which to enable Cisco IOS IPS and enters interface configuration mode.
Step 7	**ip ips** *ips-name* {**in** | **out**} **Example:** `Router(config-if)# ip ips MYIPS in`	Applies an IPS rule at an interface and automatically loads the signatures and builds the signature engines. **Note** Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built. Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

	Command or Action	Purpose

Step 8	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)# exit`
		Exits interface and global configuration modes.

Step 9	**show ip ips configuration** **Example:** `Router# show ip ips configuration`	(Optional) Verifies that Cisco IOS IPS is properly configured.
Step 10	**show ip ips signature** *count* **Example:** `Router# show ip ips signature`	(Optional) Verifies the number of signatures that are loaded into each signature micro engine (SME).

Examples

The following sample output displays the number of signatures that have been loaded into each SME:

```
Router# show ip ips signature count

Cisco SDF release version S247.0
Trend SDF release version V1.2
Signature Micro-Engine: multi-string
Total Signatures: 7
Enabled: 7
Retired: 2
Compiled: 5
Signature Micro-Engine: service-http
Total Signatures: 541
Enabled: 284
Retired: 336
Compiled: 205
Signature Micro-Engine: string-tcp
Total Signatures: 487
Enabled: 332
Retired: 352
Compiled: 135
Signature Micro-Engine: string-udp
Total Signatures: 50
Enabled: 3
Retired: 23
Compiled: 27
Signature Micro-Engine: state
Total Signatures: 26
Enabled: 15
Retired: 23
Compiled: 3
Signature Micro-Engine: atomic-ip
Total Signatures: 140
Enabled: 87
Retired: 93
Compiled: 46
Inactive - invalid params: 1
Signature Micro-Engine: string-icmp
Total Signatures: 2
Enabled: 0
```

```
Retired: 1
Compiled: 1
Signature Micro-Engine: service-ftp
Total Signatures: 3
Enabled: 3
Compiled: 3
Signature Micro-Engine: service-rpc (INACTIVE)
Signature Micro-Engine: service-dns
Total Signatures: 1
Enabled: 1
Retired: 1
Signature Micro-Engine: normalizer
Total Signatures: 9
Enabled: 9
Compiled: 9
Total Signatures: 1266
Total Enabled Signatures: 741
Total Retired Signatures: 831
Total Compiled Signatures: 434
Total Signatures with invalid parameters: 1
```

Loading a Signature File into Cisco IOS IPS

Use this task to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature package is not providing your network with adequate protection from security threats.

Prerequisites

You must enable Cisco IOS IPS (as shown in the task "Configuring Cisco IOS IPS on Your Router") before loading a new signature package.

Flexible Signatures: Ordered and Incremental

Each signature is complied incrementally into the scanning tables at the same time. Thus, Cisco IOS IPS can deactivate signatures that fail to compile. (Prior to Cisco IOS Release 12.4(11)T, Cisco IOS IPS deactivated the entire signature microengine (SME) if a single signature failed to compile.)

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were last released allow Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips config location** *url*
4. **interface** *type name*
5. **ip ips** *ips-name* {**in** | **out**}
6. **exit**
7. **copy** *url* **idconf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips config location** *url* **Example:** `Router(config)# ip ips config location flash:/ips5`	Specifies the location where Cisco IOS IPS will save the signature information, and, if necessary, access the signature configuration information.
Step 4	**interface** *type name* **Example:** `Router(config)# interface gigbitEthernet 0/0`	Identifies the interface in which to enable Cisco IOS IPS.
Step 5	**ip ips** *ips-name* {**in** | **out**} **Example:** `Router(config-if)# ip ips MYIPS in`	Applies an IPS rule at an interface and automatically loads the signatures and builds the signature engines.

Step 6	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)# exit`
		Exits interface and global configuration modes.

Step 7	**copy** *url* **idconf** **Example:** `Router# copy tftp://tftp_server/sig.xml idconf`	Loads a signature package into Cisco IOS IPS. After the package is loaded, all signature information is saved to the location specified via the **ip ips config location** command.

Tuning Signature Parameters

You can tune signature parameters on the basis of a signature ID (for an individual signature), or you can tune signature parameters on the basis of a category (that is, all signatures that are within a specified category). To tune signature parameters, use the following tasks, as appropriate:

- Tuning Signatures Per Signature ID, page 13
- Tuning Signatures Per Category, page 15

Note Some changes to the signature definitions are not shown in the run time config because the changes are recorded in the sigdef-delta.xml file, which can be located via the **ip ips config location** command.

Tuning Signatures Per Signature ID

Use this task to change default signature parameters for a specified signature ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-definition**
4. **signature** *signature-id* [*subsignature-id*]
5. **engine**
6. **event-action** *action*
7. **exit**
8. **alert-severity** {**high** | **medium** | **low** | **informational**}
9. **fidelity-rating** *rating*
10. **status**
11. **enabled** {**true** | **false**}
12. **exit**
13. **show ip ips signature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips signature-definition** **Example:** `Router(config)# ip ips signature-definition`	Enters signature-definition-signature configuration mode.
Step 4	**signature** *signature-id* [*subsignature-id*] **Example:** `Router(config-sigdef-sig)# signature 9000:0`	Specifies a signature for which the CLI user tunings will be changed and enters signature-definition-action configuration mode.
Step 5	**engine** **Example:** `Router(config-sigdef-action)# engine`	(Optional) Enters signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.

	Command or Action	Purpose
Step 6	**event-action** *action* **Example:** `Router(config-sigdef-action-engine)# event-action deny-attacker-inline`	Changes router actions for a specified signature. The *action* argument can be any of the following options: • **deny-attacker-inline** • **deny-connection-inline** • **deny-packet-inline** • **produce-alert** • **reset-tcp-connection** **Note** Signature event actions must be entered on a single line. **Note** You must enter the **engine** command before issuing this command.
Step 7	**exit** **Example:** `Router(config-sigdef-action-engine)# exit`	Exits the signature-definition-action-engine configuration mode. This step is required only if the **engine** and **event-action** commands are issued.
Step 8	**alert-severity** {**high** | **medium** | **low** | **informational**} **Example:** `Router(config-sigdef-action)# alert-severity medium`	(Optional) Changes the alert severity rating for a given signature.
Step 9	**fidelity-rating** *rating* **Example:** `Router(config-sigdef-action)# fidelity-rating`	(Optional) Changes the signature fidelity rating for a given signature.
Step 10	**status** **Example:** `Router(config-sidef-action)# status`	(Optional) Enters the signature-definition-status configuration mode, which allows you to change the enabled status of a signature.
Step 11	**enabled** {**true** | **false**} **Example:** `Router(config-sigdef-status)# enabled true`	(Optional) Changes the enabled status of a given signature or signature category.

	Command or Action	Purpose

Step 12	**exit**
	
	Example:
	`Router(config-sigdef-sta)# exit`
	`Router(config-sidef-action)# exit`
	`Router(config-sidef-sig)# exit`
	`Router(config)# exit`
		Returns to EXEC mode, which allows you to later verify the configuration.

Step 13	**show ip ips signature** **Example:** `Router# show ip ips signature`	(Optional) Verifies the signature changes that have been made.

Tuning Signatures Per Category

Use this task to change default signature parameters for a category of signatures. Categories such as operating systems; Layer 2, Layer 3, or Layer 4 protocols; or service-based categories can be configured to provide wider changes to a group of signatures.

Tip Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures (as shown in the task "Retiring All Signatures and Selecting a Category of Signatures") occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-category**
4. **category** *category* [*sub-category*]
5. **event-action** *action*
6. **alert-severity** {**high** | **medium** | **low** | **informational**}
7. **fidelity-rating** *rating*
8. **enabled** {**true** | **false**}
9. **retired** {**true** | **false**}
10. **exit**
11. **show ip ips signature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips signature-category** **Example:** `Router(config)# ip ips signature-category`	Enters IPS category (config-ips-category) configuration mode.
Step 4	**category** *category* [*sub-category*] **Example:** `Router(config-ips-category)# category attack adware/spyware`	Specifies a category that is to be used for multiple signature actions or conditions and enters IPS category action configuration mode.
Step 5	**event-action** *action* **Example:** `Router(config-ips-category-action)# event-action produce-alert`	Changes router actions for a specified signature category. The *action* argument can be any of the following options: • **deny-attacker-inline** • **deny-connection-inline** • **deny-packet-inline** • **produce-alert** • **reset-tcp-connection** **Note** Event actions associated with a category can be entered separately or on a single line.
Step 6	**alert-severity** {**high** | **medium** | **low** | **informational**} **Example:** `Router(config-ips-category-action)# alert-severity medium`	(Optional) Changes the alert severity rating for a given signature category.
Step 7	**fidelity-rating** *rating* **Example:** `Router(config-ips-category-action)# fidelity-rating`	(Optional) Changes the signature fidelity rating for a signature given category.
Step 8	**enabled** {**true** | **false**} **Example:** `Router(config-ips-category-action)# enabled true`	(Optional) Changes the enabled status of a given signature or signature category.

	Command or Action	Purpose
Step 9	**retired** {**true** | **false**} **Example:** `Router(config-ips-category-action)# retired true`	(Optional) Specifies whether or not the router should retire a signature category.

Step 10	**exit**
	
	Example:
	`Router(config-ips-category-action)# exit`
	`Router(config-ips-category)# exit`
	`Router(config)# exit`
		Returns to EXEC mode, which allows you to later verify the configuration.

Step 11	**show ip ips signature** **Example:** `Router# show ip ips signature`	(Optional) Verifies the signature category changes that have been made.

Setting the Target Value Rating

Use this task to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS IPS. A host can be a single IP address or a range of IP addresses with an associated target value rating.

Note Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips event-action-rules**
4. **target-value** {**mission-critical** | **high** | **medium** | **low**} **target-address** *ip-address* [*/nn* | **to** *ip-address*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips event-action-rules** **Example:** `Router(config)# ip ips event-action-rules`	Enters the config-rule configuration mode, which allows users to change the target value rating.
Step 4	**target-value** {**mission-critical** | **high** | **medium** | **low**} **target-address** *ip-address* [**/***nn* | **to** *ip-address*] **Example:** `Router(config-rul)# target-value medium target-address 10.12.100.53`	Sets the target value rating for a host.
Step 5	**exit** **Example:** `Router(config-rul)# exit`	Exits config-rule configuration mode.

Enabling Automatic Signature Updates

Automatic signature updates allow users to override the existing configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Time can be updated via the hardware clock or the configurable software clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

Use this task to enable Cisco IOS IPS to automatically update the signature file on the system.

Automatic Signature Update Guidelines

When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router's clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined.
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified.
- Optionally, the username and password for which to access the files from the server have been specified.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips auto-update**
4. **occur-at** *min*:*hour date day*
5. **username** *name* **password** *password*
6. **url** *url*
7. **exit**
8. **show ip ips auto-update**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips auto-update** **Example:** `Router(config)# ip ips auto-update`	Enables automatic signature updates for Cisco IOS IPS and enters IPS auto-update configuration mode.
Step 4	**occur-at** *min*:*hour date day* **Example:** `Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5`	(Optional) Defines a preset time for which the Cisco IOS IPS signature files are automatically updated.
Step 5	**username** *name* **password** *password* **Example:** `Router(config-ips-auto-update)# username myips password secret`	(Optional) Defines a username and password for the automatic signature update function.
Step 6	**url** *url* **Example:** `Router(config-ips-auto-update)# url tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml`	(Optional) URL in which the router retrieves the Cisco IOS IPS signature configuration files.

	Command or Action	Purpose

Step 7	**exit**
	
	Example:
	`Router(config-ips-auto-update)# exit`
	`Router(config)# exit`
		Exits IPS auto-update and global configuration modes.

Step 8	**show ip ips auto-update** **Example:** `Router# show ip ips auto-update`	Verifies the automatic signature update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Monitoring Cisco IOS IPS Signatures via Syslog Messages or SDEE

Cisco IOS IPS provides two methods to report IPS intrusion alerts—Cisco IOS logging (syslog) and SDEE. Perform this task to enable SDEE to report IPS intrusion alerts.

To configure syslog messages, see the chapter "Troubleshooting and Fault Management" in the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

SDEE Overview

SDEE is an application-level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers. SDEE is always running, but it does not receive and process events from IPS unless SDEE notification is enabled. If SDEE notification is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

Storing SDEE Events in the Buffer

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

Prerequisites

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not “see” the requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips notify sdee**
4. **ip sdee events** *events*
5. **ip sdee subscriptions** *subscriptions*
6. **ip sdee messages** *messages*
7. **ip sdee alerts** *alerts*
8. **exit**
9. **show ip sdee** {[**alerts**] [**all**] [**errors**] [**events**] [**configuration**] [**status**] [**subscriptions**]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ips notify sdee** **Example:** `Router(config)# ip ips notify sdee`	Enables SDEE event notification on a router.
Step 4	**ip sdee events** *events* **Example:** `Router(config)# ip sdee events 500`	(Optional) Sets the maximum number of SDEE events that can be stored in the event buffer. • Maximum value: 1000 events. **Note** By default, 200 events can be stored in the buffer when SDEE is enabled. When SDEE is disabled, all stored events are lost; a new buffer is allocated when the notifications are reenabled.
Step 5	**ip sdee subscriptions** *subscriptions* **Example:** `Router(config)# ip sdee subscriptions 1`	(Optional) Sets the maximum number of SDEE subscriptions that can be open simultaneously. • Valid value ranges from 1 to 3.
Step 6	**ip sdee messages** *messages* **Example:** `Router(config)# ip sdee messages 500`	(Optional) Sets the maximum number of SDEE messages that can be stored in the buffer at one time.
Step 7	**ip sdee alerts** *alerts* **Example:** `Router(config)# ip sdee alerts 2000`	(Optional) Sets the maximum number of SDEE alerts that can be stored in the buffer at one time.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 9	**show ip sdee** {[**alerts**] [**all**] [**errors**] [**events**] [**configuration**] [**status**] [**subscriptions**]} **Example:** `Router# show ip sdee configuration`	(Optional) Verifies SDEE configuration information and notification functionality.

Examples

The following example shows how to configure and verify SDEE on your router:

```
Router(config)# ip ips notify SDEE
Router(config)# ip sdee event 500
Router(config)# ip sdee subscriptions 1
Router(config)# ip sdee messages 500
Router(config)# ip sdee alerts 2000
router(config)# exit
*Nov 9 21:41:33.171: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router# show ip sdee all
Configured concurrent subscriptions: 1
No currently open subscriptions.
Alert storage: 2000 alerts using 560000 bytes of memory
Message storage: 500 messages using 212000 bytes of memory
SDEE Events
Time Type Description
Router#
```

Troubleshooting Tips

To print out new SDEE alerts on the router console, issue the **debug ip sdee** command.

To clear the event buffer or SDEE subscriptions from the router (which helps with error recovery), issue the **clear ip sdee** command.

Configuration Examples

This section contains the following configuration example:

- Cisco IOS IPS Configuration: Example, page 23

Cisco IOS IPS Configuration: Example

The following example shows how to enable and verify Cisco IOS IPS on your router:

```
Router# mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
```

```
Router(config)#
Router(config)# do show ip interface brief
Interface                IP-Address      OK?    Method  Status                  Protocol
GigabitEthernet0/0       10.0.20.120     YES    NVRAM   up                      up
GigabitEthernet0/1       10.12.100.120   YES    NVRAM   administratively down  down
NVI0                     unassigned      NO     unset   up                      up
Router(config)#
Router(config)# interface gigabits 0/0
Router(config-if)# ip ips MYIPS in
Router(config-if)#
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:17:07 MST Nov 14 2006
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13
engines
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:17:07 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 0 ms
Router(config-if)#
Router(config-if)# ip ips MYIPS out
Router(config-if)#
Router(config-if)#
Router(config-if)#^Z
Router#
*Nov 14 2006 17:17:23 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router# wr
Building configuration...
[OK]
Router#
Router# show ip ips signature count
Cisco SDF release version S0.0

Signature Micro-Engine: multi-string (INACTIVE)
Signature Micro-Engine: service-http (INACTIVE)
Signature Micro-Engine: string-tcp (INACTIVE)
Signature Micro-Engine: string-udp (INACTIVE)
Signature Micro-Engine: state (INACTIVE)
Signature Micro-Engine: atomic-ip
     Total Signatures: 3
       Enabled: 0
       Compiled: 3
Signature Micro-Engine: string-icmp (INACTIVE)
Signature Micro-Engine: service-ftp (INACTIVE)
Signature Micro-Engine: service-rpc (INACTIVE)
Signature Micro-Engine: service-dns (INACTIVE)
Signature Micro-Engine: normalizer (INACTIVE)
Signature Micro-Engine: service-smb-advanced (INACTIVE)
Signature Micro-Engine: service-msrpc (INACTIVE)
     Total Signatures: 3
     Total Enabled Signatures: 0
     Total Retired Signatures: 0
     Total Compiled Signatures: 3
Router#
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms -
packets for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
```

```
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this
signature is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms
Router#
Router#
Router# show ip ips signature count
Cisco SDF release version S258.0

Signature Micro-Engine: multi-string
     Total Signatures: 3
       Enabled: 3
       Retired: 3
Signature Micro-Engine: service-http
     Total Signatures: 611
       Enabled: 159
       Retired: 428
       Compiled: 183
Signature Micro-Engine: string-tcp
     Total Signatures: 864
       Enabled: 414
       Retired: 753
       Compiled: 111
Signature Micro-Engine: string-udp
     Total Signatures: 74
       Enabled: 1
       Retired: 44
       Compiled: 30
```

```
Signature Micro-Engine: state
     Total Signatures: 28
       Enabled: 16
       Retired: 25
       Compiled: 3
Signature Micro-Engine: atomic-ip
     Total Signatures: 252
       Enabled: 56
       Retired: 148
       Compiled: 103
       Inactive - invalid params: 1
Signature Micro-Engine: string-icmp
     Total Signatures: 3
       Enabled: 0
       Retired: 2
       Compiled: 1
Signature Micro-Engine: service-ftp
     Total Signatures: 3
       Enabled: 1
       Compiled: 3
Signature Micro-Engine: service-rpc
            Total Signatures: 75
       Enabled: 44
       Retired: 44
       Compiled: 31
Signature Micro-Engine: service-dns
     Total Signatures: 38
       Enabled: 30
       Retired: 5
       Compiled: 33
Signature Micro-Engine: normalizer
     Total Signatures: 9
       Enabled: 8
       Retired: 5
       Compiled: 4
Signature Micro-Engine: service-smb-advanced (INACTIVE)
Signature Micro-Engine: service-msrpc
     Total Signatures: 22
       Enabled: 22
       Retired: 22
```

Additional References

The following sections provide references related to the Cisco IOS IPS 5.0 Enhancements feature.

Related Documents

Related Topic	Document Title
IPS and firewall	*Cisco IOS Security Configuration Guide*, Release 12.4
IPS and firewall commands	*Cisco IOS Security Command Reference*, Release 12.4T
Loading images and file systems	The chapter "Loading and Managing System Images" in the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new commands only.

- **alert-severity**
- **category**
- **copy idconf**
- **enabled (IPS)**
- **engine (IPS)**
- **event-action**
- **fidelity-rating**
- **ip ips auto-update**

- ip ips config location
- ip ips event-action-rules
- ip ips signature-category
- ip ips signature-definition
- occur-at (ips-auto-update)
- retired (IPS)
- show ip ips auto-update
- signature
- status
- target-value
- url (ips-auto-update)
- username (ips-autoupdate)

alert-severity

To change the alert severity rating for a given signature or signature category, use the **alert-severity** command in signature-definition-action (config-sigdef-action) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

alert-severity {**high** | **medium** | **low** | **informational**}

no alert-severity

Syntax Description

high | **medium** | **low** | **informational**	Alert severity action for a given signature or signature category.

Command Default

No default behavior or values

Command Modes

Signature-definition-action configuration (config-sigdef-action)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **alert-severity** command, you must specify either a signature via the **signature** command or a signature category (such as attack-type) via the **category** command.

Examples

The following example shows how to set the alert severity value to low for signature 5760:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# alert-severity low
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.

category

To specify a signature category that is to be used for multiple signature actions or conditions, use the **category** command in IPS-category configuration mode.

category *category* [*sub-category*]

Syntax Description

category	Category name. For a list of supported top-level categories, use the router CLI help (**?**).
sub-category	(Optional) Category submode. Submode categories are dependent on the category type; that is, submode categories vary from category to category. For a list of supported submode categories, use the router CLI help (**?**)

Command Default

None

Command Modes

IPS-category configuration (config-ips-category)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Cisco IOS Intrusion Prevention System (IPS) 5.x uses signatures and signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category.

Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
ip ips signature-category	Enters IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS IPS signature parameters on the basis of a signature category.

copy idconf

To load a signature package in Cisco IOS Intrusion Prevention System (IPS), use the **copy idconf** command in EXEC mode.

copy *url* **idconf**

Syntax Description

url	Specifies the location from which the router loads the signature file. Available URL locations are as follows: • Local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **copy** *url* **idconf** command to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature file is not providing your network with adequate protection from security threats. After the signature package has been loaded into the router, Cisco IOS IPS saves all signature information to the location specified via the **ip ips config location** command.

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were released enable Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.

Note The **copy** *url* **idconf** command replaces the **copy ips-sdf** command.

Examples

The following example shows how to load a signature package into Cisco IOS IPS from the location "flash:IOS-S258-CLI-kd.pkg":

```
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
```

```
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms -
packets for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this
signature is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms
```

Related Commands

Command	Description
ip ips config-location	Specifies the location in which the router will save signature information.

enabled (IPS)

To change the enabled status of a given signature or signature category, use the **enabled** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

enabled {**true** | **false**}

no enabled

Syntax Description

true	Enables a specified signature or all signatures within a specified category.
false	Disables a specified signature or all signatures within a specified category.

Command Default

All commands are enabled.

Command Modes

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **enabled** command to change the status of a signature or signature category to active (true) or inactive (false).

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sig)# signature 9000 0
Router(config-sig-sig)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Changes the enabled or retired status of a given signature or signature category.

engine (IPS)

To enter signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature, use the **engine** command in signature-definition-action configuration mode.

engine

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If you wish to change router actions for a specific signature, you must issue the engine command to enter the appropriate configuration mode, which allows you to issue the **event-action** command and specify any supported action.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
event-action	Changes router actions for a signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.

event-action

To change router actions for a signature or signature category, use the **event-action** command in signature-definition-action-engine or IPS-category-action configuration mode. To revert to the default router action values, use the **no** form of this command.

event-action *action*

no event-action

Syntax Description

action	Router actions for a specified signature or signature category. The *action* argument can be any of the following options: • **deny-attacker-inline** • **deny-connection-inline** • **deny-packet-inline** • **produce-alert** • **reset-tcp-connection** **Note** Event actions for an individual signature must be entered on a single line. However, event actions associated with a category can be entered separately or on a single line.

Command Default

Default values for the signature or signature category will be used.

Command Modes

Signature-definition-action-engine configuration (config-sigdef-action-engine)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Signature-Based Changes

After signature-based changes are complete, Cisco IOS Intrusion Prevention System (IPS) prompts the user to confirm whether or not the changes are acceptable. Confirming the changes instructs Cisco IOS IPS to compile the changes for the signature and modify memory structures to reflect the change. Also, Cisco IOS IPS will save the changes to the location specified via the **ip ips config location** command (for example, flash:ips5/*.xml).

You can issue the **show ip ips signatures** command to verify the event-action configuration. (The **show running-config** command does not show individual signature tuning information.)

Signature Category-Based Changes

After signature category-based changes are complete, the category tuning information is saved in the command-line interface (CLI) configuration.

Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All the tuning information will be applied to all signatures that belong to the adware/spyware signature category.

```
Router(config)# ip ips signature category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
engine	Enters the signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.
ip ips config location	Specifies the location in which the router will save signature information.
signature	Specifies a signature for which the CLI user tunings will be changed.
show ip ips	Displays IPS information such as configured sessions and signatures.

fidelity-rating

To change the signature fidelity rating for a given signature or signature category, use the **fidelity-rating** command in signature-definition-action (config-sigdef-action) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

fidelity-rating *rating*

no fidelity-rating

Syntax Description

rating	Available range: 0 to 100. The higher the number, the more accurate the fidelity rating.

Command Default

The default value is defined in the signature definition XML.

Command Modes

Signature-definition-action configuration (config-sigdef-action)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

A signature's fidelity rating is a rating of the confidence level of detecting a true positive. It can be viewed as a quality rating for the signature.

Examples

The following example shows how to set the fidelity rating to zero for signature 5726:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# fidelity-rating 0
Router(config-sigdef)# ^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.

ip ips auto-update

To enable automatic signature updates for Cisco IOS Intrusion Prevention System (IPS), use the **ip ips auto-update** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips auto-update

no ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is defined in the signature definition XML.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router's clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined (via the **occur-at** command).
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified (via the **url** command).
- Optionally, the username and password in which to access the files from the server has been specified (via the **username** command).

If this feature is enabled, signatures are delivered in either a Basic signature file or an Advanced signature file.

The Default Value

A user or a management station can override the default value via the **category** command or the **signature** command; a value set with either of these commands will be saved as the delta value. The no form of the ip ips auto-update command will remove the delta value and revert back to the default value in the definition XML.

Setting Time for Auto Updates

Cisco IOS time can be updated via the hardware clock or the software configurable clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
occur-at	Defines the frequency in which Cisco IOS IPS obtains updated signature information.
url (ips-autoupdate)	Defines a location in which to retrieve the Cisco IOS IPS signature configuration files.
username (ips-autoupdate)	Defines a username and password in which to access signature files from the server.

ip ips config location

To specify the location in which the router will save signature information, use the **ip ips config location** command in global configuration mode. To remove the specified location, use the **no** form of this command.

ip ips config location *url*

no ip ips config location

Syntax Description

url	Location where the signature file is saved. Available URL options: • Local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml **Note** If the specified location is a URL, such as an FTP server, the user must have writer privileges.

Command Default

No default behavior or values. (Configuration files are saved.)

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before configuring the **ip ips config location** command, you must create a directory for the config location via the **mkdir** command.

The **ip ips config location** command configures a Cisco IOS Intrusion Prevention System (IPS) signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in cases such as router reboots or IPS becoming disabled or reenabled. Files, such as signature definitions, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

Note If a location is not specified, or if a location is removed via the **no** form, no files will be saved.

Note The **ip ips config location** command replaces the **ip ips sdf location** command.

Examples

The following example shows how to instruct the router to save all signature information to the directory "flash:/ips5":

```
Router# mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
Router(config)#
```

ip ips event-action-rules

To enter config-rule configuration mode, which allows users to change the target value rating, use the **ip ips event-action-rules** command in global configuration mode.

ip ips event-action-rules

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

You must issue the **ip ips event-action-rules** command to define the target value rating via the **target-value** command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

Related Commands

Command	Description
target-value	Defines the target value rating for a host.

ip ips signature-category

To enter IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS Intrusion Prevention System (IPS) signature parameters on the basis of a signature category, use the **ip ips signature-category** command in global configuration mode.

ip ips signature-category

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **ip ips signature-category** command if you want to tune signature parameters per category.

Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.

ip ips signature-definition

To enter signature-definition-signature configuration mode, which allows you to define a signature for command-line interface (CLI) user tunings, use the **ip ips signature-definition** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips signature-definition

no ip ips signature-definition

Syntax Description

This command has no arguments or keywords.

Command Default

Signature parameters cannot be defined and default values are used.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **ip ips signature-definition** command to enter signature-definition-signature configuration mode, which allows you to issue the **signature** command. The **signature** command is used to specify a signature whose CLI user tunings are to be customized. After you issue the **signature** command, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to “produce alert” and “reset tcp connection”:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

occur-at (ips-auto-update)

To define the frequency in which Cisco IOS Intrusion Prevention System (IPS) obtains updated signature information, use the **occur-at** command in IPS-auto-update configuration mode.

occur-at *min*:*hour date day*

Syntax Description

min:*hour date day*	Frequency (in minutes: hour, date, and day) in which automatic signature updates occur.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, issue the **occur-at** command to define how often the Cisco IOS IPS signature files should be automatically updated.

Examples

The following example shows how to configure automatic signature updates and set the frequency in which updates are made. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
   hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
```

```
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

retired (IPS)

To specify whether or not a retired signature or signature category definition should be saved in the router memory, use the **retired** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

retired {**true** | **false**}

no retired

Syntax Description

true	Retires all signatures within a given category.
false	"Unretires" all signatures within a given category.

Command Default

Signature or signature category definitions are not saved in the system.

Command Modes

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

Examples

The following example shows how to retire all signatures and configure the Basic "ios_ips" category:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
enabled	Changes the enabled status of a given signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Enters the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature.

show ip ips auto-update

To display the automatic signature update configuration, use the **show ip ips auto-update** command in EXEC mode.

show ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **show ip ips auto-update** command to verify the auto update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
   hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
```

```
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

signature

To specify a signature for which the command-line interface (CLI) user tunings will be changed, use the **signature** command in signature-definition-signature (config-sigdef-sig) configuration mode. To remove the CLI user tunings and revert to the default values, use the **no** version of this command.

signature *signature-id* [*subsignature-id*]

no signature *signature-id* [*subsignature-id*]

Syntax Description

signature-id [*subsignature-id*]	Signature number. If a subsignature is not specified, the default is 0. For example, if signature 1105 is specified without a subsignature, the router will interpret the signature as 1105:0.

Command Default

Default signature parameters cannot be changed.

Command Modes

Signature-definition-signature configuration (config-sigdef-sig)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **signature** command to specify a signature whose CLI user tunings are to be customized. Thereafter, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to "produce alert" and "reset tcp connection":

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
ip ips signature-definition	Enters signature-definition-signature configuration mode, which allows you to define a signature for CLI user tunings.

status

To enter the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature, use the **status** command in signature-definition-action configuration mode. To return to the default action, use the **no** form of this command.

status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **status** command, you must specify at least one signature via the **signature** command.

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 9000 0
Router(config-sigdef-action)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

target-value

To define the target value rating for a host, use the **target-value** command in configuration rule configuration mode. To change the target value rating or revert to the default value, use the **no** form of this command.

target-value {**mission-critical** | **high** | **medium** | **low**} **target-address** *ip-address* [*/nn* | **to** *ip-address*]

no target-value {**mission-critical** | **high** | **medium** | **low**} **target-address** *ip-address* [*/nn* | **to** *ip-address*]

Syntax Description

mission-critical | **high** | **medium** | **low**	Rates how important the system is to the network.
target-address *ip-address* [*/nn* | **to** *ip-address*]	A host, which can consist of a single IP address or a range of IP addresses.

Command Default

medium

Command Modes

Configuration rule configuration (config-rul)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **target-value** command to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS Intrusion Prevention System (IPS). A host can be a single IP address or a range of IP addresses with an associated target value rating.

Note Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location** command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

url (ips-auto-update)

To define a location in which to retrieve the Cisco IOS Intrusion Prevention System (IPS) signature configuration files, use the **url** command in IPS-auto-update configuration mode.

url *url*

Syntax Description

url	Location in which the router retrieves the latest signature files.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Examples

In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

username (ips-autoupdate)

To define a username and password in which to access signature files from the server, use the **username** command in IPS-auto-update configuration mode.

username *name* **password** *password*

Syntax Description

name	Username required to access the latest updated signature file package.
password *password*	Password required to access the latest updated signature file package.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, you can optionally issue the **username** command to specify a username and password to access signature files.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration:

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update
```

```
IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Feature Name	Releases	Feature Information
Cisco IOS IPS 5.x Signature Format and Usability Enhancements	12.4(11)T	This feature introduces support for Cisco IOS Intrusion Prevention System (IPS) version 5.0, which is a version-based signature definition XML format. Cisco IOS IPS 4.x format signatures are replaced by the 5.x format signatures that are used by all other Cisco IPS devices.