

sa ipsec

To specify the IP security (IPsec) security association (SA) policy information to be used for a Group Domain of Interpretation (GDOI) group and to enter GDOI SA IPsec configuration mode, use the **sa ipsec** command in GDOI local server configuration mode. To remove the policy information that was specified, use the **no** form of this command.

```
sa ipsec {sequence-number}
```

```
no sa ipsec {sequence-number}
```

| | | |
|---------------------------|---|---|
| Syntax Description | <i>sequence-number</i> | Sequence number of the IPsec SA. |
| Command Default | None | |
| Command Modes | GDOI local server configuration | |
| Command History | Release | Modification |
| | 12.4(6)T | This command was introduced. |
| Usage Guidelines | IPsec and SA policy information must be specified using this command if the traffic encryption key policy has to be defined. | |
| Examples | The following example shows that three IPsec SA policy numbers (1, 2, and 3) have been specified: | |
| | <pre>sa ipsec 1 profile gdoi-p match address ipv4 120 sa ipsec 2 profile gdoi-q match address ipv4 121 sa ipsec 3 profile gdoi-r match address ipv4 122</pre> | |
| Related Commands | Command | Description |
| | crypto gdoi group | Identifies a GDOI group and enters GDOI group configuration mode. |
| | match address | Specifies an IP extended access list for a GDOI registration. |
| | profile | Defines the IPsec SA policy for a GDOI group. |
| | server local | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

sa receive-only

To specify that an IP security (IPsec) security association (SA) is to be installed by a group member as “inbound only,” use the **sa receive-only** command in GDOI local server configuration mode. To remove the inbound-only specification, use the **no** form of this command.

sa receive-only

no sa receive-only

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, IPsec SAs are installed by group members as both inbound and outbound.

Command Modes

GDOI local server configuration (config-local-server)

Command History

| Release | Modification |
|--------------------------|--|
| 12.4(11)T | This command was introduced. |
| Cisco IOS XE Release 2.3 | This command was implemented on the Cisco ASR 1000 series routers. |

Usage Guidelines

This command is configured on a key server. The command may be used to ease in deployment.

Examples

The following example shows that the Group Domain of Interpretation (GDOI) group is instructed by the key server to install the IPsec SAs as “inbound only”:

```
crypto gdoi group gdoi_group
  identity number 1234
server local
  sa receive-only
  sa ipsec 1
  profile gdoi-p
  match address ipv4 120
```

Related Commands

| Command | Description |
|--------------------------|---|
| crypto gdoi gm | Allows group members to change the IPsec SA status. |
| crypto gdoi group | Identifies a GDOI group and enters GDOI group configuration mode. |
| server local | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

save-password

To save your extended authentication (Xauth) password locally on your PC, use the **save-password** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the Save-Password attribute, use the **no** form of this command.

save-password

no save-password

Syntax Description

This command has no arguments or keywords.

Defaults

Your Xauth password is not saved locally on your PC, and the Save-Password attribute is not added to the server group profile.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

| Release | Modification |
|-------------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

Usage Guidelines

Save password control allows you to save your Xauth password locally on your PC so that after you have initially entered the password, the Save-Password attribute is pushed from the server to the client. On subsequent authentications, you can activate the password by using the tick box on the software client or by adding the username and password to the Cisco IOS hardware client profile. The password setting remains until the Save-Password attribute is removed from the server group profile. After the password has been activated, the username and password are sent automatically to the server during Xauth without your intervention.

The save-password option is useful only if your password is static, that is, if it is not a one-time password such as one that is generated by a token.

The Save-Password attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure save password control, use the **save-password** command.

An example of an attribute-value (AV) pair for the Save-Password attribute is as follows:

```
ipsec:save-password=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **save-password** command.



Note

- The Save-Password attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.
 - The attribute can override any similar group attributes.
 - User-based attributes are available only if RADIUS is used as the database.
-

Examples

The following example shows that the Save-Password attribute has been configured:

```
crypto isakmp client configuration group cisco
 save-password
```

Related Commands

| Command | Description |
|---|--|
| acl | Configures split tunneling. |
| crypto isakmp client configuration group | Specifies the DNS domain to which a group belongs. |

scheme

To define the redundancy scheme that is used between two devices, use the **scheme** command in inter-device configuration mode. To disable the redundancy scheme, use the **no** form of this command.

scheme standby *standby-group-name*

no scheme standby *standby-group-name*

Syntax Description

| | |
|---------------------------|--|
| standby | Redundancy scheme. Currently, the standby scheme is the only available scheme. |
| <i>standby-group-name</i> | Specifies the name of the standby group. This name must match the name that was specified via the standby name command. Also, the standby name should be the same on both the active and standby routers. |

Defaults

A redundancy scheme is not specified.

Command Modes

Inter-device configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(8)T | This command was introduced. |

Usage Guidelines

Only the active or standby state of the standby group is used for Stateful Switchover (SSO). The virtual IP (VIP) address of the standby group is not required or used by SSO. Also, the standby group does not have to be part of any crypto map configuration.

Examples

The following example shows how to enable SSO and define the standby scheme that is to be used by the active and standby devices:

```

redundancy inter-device
  scheme standby HA-in
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 10.0.0.1
  remote-port 5000
  remote-ip 10.0.0.2

```

Related Commands

| Command | Description |
|---------------------|---|
| standby name | Configures the name of the standby group. |

secondary-color

To configure the color of the secondary title bars on the login and portal pages of a SSL VPN website, use the **secondary-color** command in webvpn context configuration mode. To remove the color from the WebVPN context configuration, use the **no** form of this command.

secondary-color *color*

no secondary-color *color*

Syntax Description

| | |
|--------------|--|
| <i>color</i> | <p>The value for the <i>color</i> argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a“#”), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):</p> <ul style="list-style-type: none"> • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ <p>The default color is purple.</p> |
|--------------|--|

Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.3(14)T | This command was introduced. |

Usage Guidelines

Configuring a new color overrides the color of the preexisting color.

Examples

The following examples show the three forms in which the secondary color is configured:

```
Router(config-webvpn-context)# secondary-color darkseagreen
Router(config-webvpn-context)# secondary-color #8FBC8F
Router(config-webvpn-context)# secondary-color 143,188,143
```

Related Commands

| Command | Description |
|-----------------------|--|
| webvpn context | Enters webvpn context configuration mode to configure the SSL VPN context. |

secondary-text-color

To configure the color of the text on the secondary bars of an SSL VPN website, use the **secondary-text-color** command in webvpn context configuration mode. To revert to the default color, use the **no** form of this command.

secondary-text-color [**black** | **white**]

no secondary-text-color [**black** | **white**]

Syntax Description

| | |
|--------------|---|
| black | (Optional) Color of the text is black. This is the default value. |
| white | (Optional) Color of the text is white. |

Defaults

The color of the text on secondary bars is black if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.3(14)T | This command was introduced. |

Usage Guidelines

The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

Examples

The following example sets the secondary text color to white:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# secondary-text-color white
Router(config-webvpn-context)#
```

Related Commands

| Command | Description |
|-----------------------|--|
| webvpn context | Enters webvpn context configuration mode to configure the SSL VPN context. |

secret

To associate a command-line interface (CLI) view or a superview with a password, use the **secret** command in view configuration mode.

```
secret {unencrypted-password | 0 unencrypted-password | 5 encrypted-password}
```

Syntax Description

| | |
|-----------------------------|---|
| <i>unencrypted-password</i> | Nonencrypted password. A password can contain any combination of alphanumeric characters. The password is case sensitive. This clear-text password will be encrypted using the Message Digest 5 (MD5) method. |
| 0 | Specifies that an unencrypted password will follow. |
| 5 | Specifies that an encrypted password will follow. |
| <i>encrypted-password</i> | Encrypted password that you enter and that is copied from another router configuration. |

Defaults

User cannot access a CLI view or superview.

Command Modes

View configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.3(14)T | This command was introduced. |

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **secret** command has been issued.



Note

The password cannot be removed, but you can overwrite it.

Examples

The following examples show how to configure two CLI views, “first” and “second,” and associate each view with a password:

CLI View “first”

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# parser view first
Router(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Router(config-view)# secret firstpassword
Router(config-view)# secret secondpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
```

```
Router(config-view)# secret 5 invalidpassword
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 5 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.
```

```
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command configure include all ip
Router(config-view)# exit
```

CLI View "second"

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# parser view second
Router(config-view)#
*Dec 30 06:11:52.915: %PARSER-6-VIEW_CREATED: view 'second' successfully created.
Router(config-view)# secret mypasswd
Router(config-view)# commands exec include ping
Router(config-view)# end
```

```
Router# show running-config
```

```
parser view second
 secret 5 $1$Pws8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
```

The following is an example of **show running-config** output for a situation in which the **secret** command has been configured using a level 5 encrypted password:

```
Router: show running-config
```

```
parser view first
 secret 5 $1$jjle$vmYyRbmj5UoU96tT1x7eP1
 commands configure include all ip
 commands exec include configure terminal
 commands exec include configure
 commands exec include show version
 commands exec include show
!
```

Related Commands

| Command | Description |
|--------------------|---|
| parser view | Creates or changes a CLI view and enters view configuration mode. |

secret-key

To configure the policy server secret key that is used to secure authentication requests, use the **secret-key** command in webvpn sso server configuration mode. To remove the secret key, use the **no** form of this command.

secret-key *key-name*

no secret-key *key-name*

| | |
|---------------------------|-------------------------------------|
| Syntax Description | <i>key-name</i> Name of secret key. |
|---------------------------|-------------------------------------|

| | |
|------------------------|---|
| Command Default | A policy server secret key is not configured. |
|------------------------|---|

| | |
|----------------------|---------------------------------|
| Command Modes | Webvpn sso server configuration |
|----------------------|---------------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.4(11)T | This command was introduced. |

Usage Guidelines



Note

- A web agent URL and policy server secret key are required for a Single SignOn (SSO) server configuration. If the web agent URL and policy server secret key are not configured, a warning message is displayed. (See the [Warning Message](#) section in the Examples section below.)
- This is the same secret key that should be configured on the Cisco SiteMinder plug-in.

Examples

The following example shows the policy server secret key is “example.123”:

```
webvpn context context1
  sso-server test-sso-server
    secret-key example.123
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

Related Commands

| Command | Description |
|-----------------------|--|
| webvpn context | Enters webvpn context configuration mode to configure the SSL VPN context. |

secure boot-config

To take a snapshot of the router running configuration and securely archive it in persistent storage, use the **secure boot-config** command in global configuration mode. To remove the secure configuration archive and disable configuration resilience, use the **no** form of this command.

secure boot-config [*restore filename*]

no secure boot-config

Syntax Description

| | |
|-------------------------|--|
| restore filename | (Optional) Reproduces a copy of the secure configuration archive as the supplied filename. |
|-------------------------|--|

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(8)T | This command was introduced. |

Usage Guidelines

Without any parameters, this command takes a snapshot of the router running configuration and securely archives it in persistent storage. Like the image, the configuration archive is hidden and cannot be viewed or removed directly from the command-line interface (CLI) prompt. It is recommended that you run this command after the router has been fully configured to reach a steady state of operation and the running configuration is considered complete for a restoration, if required. A syslog message is printed on the console notifying the user of configuration resilience activation. The secure archive uses the time of creation as its filename. For example, `.runcfg-20020616-081702.ar` was created July 16 2002 at 8:17:02.

The restore option reproduces a copy of the secure configuration archive as the supplied filename (disk0:running-config, slot1:runcfg, and so on). The restore operation will work only if configuration resilience is enabled. The number of restored copies that can be created is unlimited.

The **no** form of this command removes the secure configuration archive and disables configuration resilience. An enable, disable, enable sequence has the effect of upgrading the configuration archive if any changes were made to the running configuration since the last time the feature was disabled.

The configuration upgrade scenario is similar to an image upgrade. The feature detects a different version of Cisco IOS and notifies the user of a version mismatch. The same command can be run to upgrade the configuration archive to a newer version after new configuration commands corresponding to features in the new image have been issued.

The correct sequence of steps to upgrade the configuration archive after an image upgrade is as follows:

- Configure new commands
- Issue the **secure boot-config** command

Examples

The following example shows the command used to securely archive a snapshot of the router running configuration:

```
secure boot-config
```

The following example shows the command used to restore an archived image to the file slot0:rescue-cfg:

```
Router(config)# secure boot-config restore slot0:rescue-cfg  
ios resilience:configuration successfully restored as slot0:rescue-cfg
```

Related Commands

| Command | Description |
|----------------------------|--|
| secure boot-image | Enables Cisco IOS image resilience. |
| show secure bootset | Displays the status of image and configuration resilience. |

secure boot-image

To enable Cisco IOS image resilience, use the **secure boot-image** command in global configuration mode. To disable Cisco IOS image resilience and release the secured image so that it can be safely removed, use the **no** form of this command.

secure boot-image

no secure boot-image

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(8)T | This command was introduced. |

Usage Guidelines

This command enables or disables the securing of the running Cisco IOS image. The following two possible scenarios exist with this command.

- When turned on for the first time, the running image (as displayed in the **show version** command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image from a disk with an Advanced Technology Attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of “hiding” the running image, the image file will not be included in any directory listing of the disk. The **no** form of this command releases the image so that it can be safely removed.
- If the router is configured to boot up with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to the following is displayed at bootup:

```
ios resilience :Archived image and configuration version 12.2 differs from running
version 12.3.
Run secure boot-config and image commands to upgrade archives to running version.
```

To upgrade the image archive to the new running image, reenter this command from the console. A message will be displayed about the upgraded image. The old image is released and will be visible in the **dir** command output.



Caution

Be careful when copying new images to persistent storage because the existing secure image name might conflict with the new image. To verify the name of the secured archive, run the **show secure bootset** command and resolve any name conflicts with the currently secured hidden image.

**Note**

After the Cisco IOS image is secured, the resilient configuration feature will deny any requests to copy, modify, or delete the secure archive and will even survive a disk format operation.

Examples

The following example shows the activation of image resilience.

```
Router(config)# secure boot-image
```

Related Commands

| Command | Description |
|----------------------------|---|
| dir | Displays a list of files on a file system. |
| secure boot-config | Saves a secure copy of the router running configuration in persistent storage. |
| show secure bootset | Displays the status of image and configuration resilience. |
| show version | Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images. |

security (Diameter peer)

To configure the security protocol for the Diameter peer connection, use the **security** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

```
security {ipsec | tls}
```

```
no security {ipsec | tls}
```

| Syntax Description | ipsec | IP security protocol. |
|--------------------|-------|---------------------------|
| | tls | Transport layer security. |

Command Default IP security (IPsec) is the default security protocol for Diameter peer connections.

Command Modes Diameter peer configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(9)T | This command was introduced. |

Usage Guidelines If you dynamically change the security protocol for a Diameter peer, the connection to that peer is broken. When you exit the Diameter peer configuration submode, the connection is reestablished.

Examples The following example shows how to configure IPsec for a Diameter peer:

```
Router (config-dia-peer)# security ipsec
```

| Related Commands | Command | Description |
|------------------|--------------------|--|
| | diameter peer | Configures a Diameter peer and enters Diameter peer configuration submode. |
| | show diameter peer | Displays the Diameter peer configuration. |

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure rate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure rate *threshold-rate* **log**

no security authentication failure rate *threshold-rate* **log**

Syntax Description

| | |
|-----------------------|--|
| <i>threshold-rate</i> | Number of allowable unsuccessful login attempts. The valid value range for the <i>threshold-rate</i> argument is 2 to 1024. The default is 10. |
| log | Syslog authentication failures if the rate exceeds the threshold. |

Defaults

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|---|
| 12.3(1) | This command was introduced. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.3(7)T | The range of the <i>threshold-rate</i> value was changed from 1 through 1024 to 2 through 1024. |

Usage Guidelines

The **security authentication failure rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.



Note

Previous to the Cisco IOS software release 12.3(7)T the *threshold-rate* value range was 1 through 1024. Unsuccessful login attempts will not be logged if a value of 1 is configured. As of Cisco IOS release 12.3(7)T, use a value between 2 and 1024.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

| Command | Description |
|--------------------------------------|--|
| security passwords min-length | Ensures that all configured passwords are at least a specified length. |

security ipsec

To apply a previously configured IP Security (IPSec) profile to the redundancy group communications, use the **security ipsec** command in inter-device configuration mode. To remove the IPSec profile from the configuration, use the **no** form of this command.

security ipsec *profile-name*

no security [**ipsec** [*profile-name*]]

Syntax Description

profile-name Profile name, which was specified via the **crypto ipsec profile** command.

Defaults

The redundancy group is not secured.

Command Modes

Inter-device configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.3(11)T | This command was introduced. |

Usage Guidelines

The **security ipsec** command allows you to secure a redundancy group via a previously configured IPSec profile. If you are certain that the Stateful Switchover (SSO) traffic between the redundancy group runs on a physically secure interface, you do not have to configure this command.



Note

If you configure SSO traffic protection via the **security ipsec** command, the active and standby devices must be directly connected to each other via Ethernet networks.

Examples

The following example shows how to configure SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | crypto ipsec profile | Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers. |
| | redundancy inter-device | Enters inter-device configuration mode. |

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*

no security passwords min-length *length*

| | | |
|---------------------------|---------------|---|
| Syntax Description | <i>length</i> | Minimum length of a configured password. The default is six characters. |
|---------------------------|---------------|---|

| | |
|-----------------|----------------|
| Defaults | Six characters |
|-----------------|----------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|---|------------------------------|
| | 12.3(1) | This command was introduced. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. | |

| | |
|-------------------------|--|
| Usage Guidelines | The security passwords min-length command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length: |
|-----------------|---|

```
security password min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

| Related Commands | Command | Description |
|---|---|--|
| | enable password | Sets a local password to control access to various privilege levels. |
| security authentication failure rate | Configures the number of allowable unsuccessful login attempts. | |

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

```
self-identity {address | address ipv6} | fqdn | user-fqdn user-fqdn}
```

```
no self-identity {address | address ipv6} | fqdn | user-fqdn user-fqdn}
```

| Syntax Description | Parameter | Description |
|--------------------|----------------------------|---|
| | address | The IP address of the local endpoint. |
| | address ipv6 | The IPv6 address of the local endpoint. |
| | fqdn | The fully qualified domain name (FQDN) of the host. |
| | user-fqdn user-fqdn | The user FQDN that is sent to the remote endpoint. |

Command Default If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes ISAKMP profile configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.2(15)T | This command was introduced. |
| | 12.4(4)T | The address ipv6 keyword was added. |

Examples The following example shows that the IKE identity is the user FQDN “user@vpn.com”:

```
crypto isakmp profile vpnprofile
self-identity user-fqdn user@vpn.com
```

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | crypto isakmp profile | Defines an ISAKMP profile and audits IPsec user sessions. |

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [none]

no serial-number

Syntax Description

| | |
|-------------|--|
| none | (Optional) Specifies that a serial number will not be included in the certificate request. |
|-------------|--|

Defaults

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(8)T | This command was introduced. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) command was introduced. |

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the “root” certificate request:

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  ip-address none
  fqdn none
  serial-number none
  subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US
```

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  serial-number
```

Related Commands

| Command | Description |
|-----------------------------|--|
| crypto ca trustpoint | Declares the CA that your router should use. |

serial-number (pubkey)

To define the serial number for the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **serial-number** command in pubkey configuration mode. To remove the manual key that was defined, use the **no** form of this command.

serial-number *serial-number*

no serial-number *serial-number*

| | | |
|---------------------------|----------------------|---|
| Syntax Description | <i>serial-number</i> | Device serial number. The value is from 0 through infinity. |
|---------------------------|----------------------|---|

| | |
|-----------------|-------------------------------|
| Defaults | No default behavior or values |
|-----------------|-------------------------------|

| | |
|----------------------|----------------------|
| Command Modes | Pubkey configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.2(15)T | This command was introduced. |

Examples The following example shows that the public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# serial-number 1000000
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

| | | |
|-------------------------|-------------------------|--|
| Related Commands | Command | Description |
| | address | Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure. |
| | key-string (IKE) | Specifies the RSA public key of a remote peer. |

server (application firewall policy)

To configure a set of Domain Name System (DNS) servers for which the specified instant messenger application will be interacting, use the **server** command in the appropriate configuration mode. To change or remove a configured set of DNS servers, use the **no** form of this command.

```
server {permit | deny} {name string | ip-address {ip-address | range ip-address-start
ip-address-end}}
```

```
no server {permit | deny} {name string | ip-address {ip-address | range ip-address-start
ip-address-end}}
```

Syntax Description

| | |
|--|---|
| permit | Inspects all traffic destined for a specified server, and the applicable policy is enforced. |
| deny | Blocks all traffic destined for a specified, denied server. TCP connections are denied by dropping all packets bound to the specified server. |
| name string | Name of DNS server for which traffic will be permitted (and inspected) or denied. The same server name cannot appear under two different instant messenger applications; however, the same name can appear under two different policies within the same instant messenger application. Each entry will accept only one DNS name. |
| ip-address | Indicates that at least one IP address will be listed. |
| <i>ip-address</i> | IP address of the DNS server for which traffic will be permitted (and inspected) or denied. |
| range ip-address-start ip-address-end | Range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied. |

Command Default

If this command is not issued, instant messenger application polices cannot be enforced.

Command Modes

cfg-appfw-policy-aim configuration
 cfg-appfw-policy-ymsgsr configuration
 cfg-appfw-policy-msnmsgsr configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.4(4)T | This command was introduced. |

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize the port-hopping instant messenger traffic and to enforce the security policy for that instant messenger application; thus, if this command is not issued, the security policy cannot be enforced if IM applications use port-hopping techniques.

To deploy IM traffic enforcement policies effectively, it is recommended that you issue the appropriate **server** command.

**Note**

If a router cannot identify a packet as belonging to a particular instant messenger policy, the corresponding policy cannot be enforced.

To configure more than one set of servers, you can issue the **server** command multiple times within an instant messenger's application policy. Multiple entries are treated cumulatively.

The server name Command

The **server** command (with the **name** keyword) internally resolves the DNS name of the server. This command sends DNS queries multiple times to gather all possible IP addresses for the IM servers, which return different IP addresses at different times in response to DNS queries of the same names. It uses the Time to Live (TTL) field found in DNS responses to refresh its cache. After a certain period, the DNS cache in IM applications stabilize. It is recommended that you allow a couple of minutes for the DNS cache to populate with the IM server IP addresses before the IM traffic reaches the Cisco IOS firewall. All existing IM application connections are not subjected to IM policy enforcement.

Denying Access to a Particular Instant Messenger Application

You can deny traffic to a particular instant messenger application in one of the following ways:

- Issue the **server deny** command and list all the server names and IP addresses to which you want to deny access.

**Note**

The first option is the preferred method because it performs slightly better than the second option.

- Issue the **server permit** command and list all the server names and IP addresses that you want inspected; thereafter, issue the **service default reset** command, which will deny access to all services.
- Issue **server deny** command to block access to any site given its DNS name. For example, to block all access to a gambling site, you can configure **server deny name www.noaccess.com**.

Examples

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
  application http
    port-misuse im reset
  !
  application im yahoo
    server permit name scs.msg.yahoo.com
    server permit name scsa.msg.yahoo.com
    server permit name scsb.msg.yahoo.com
    server permit name scsc.msg.yahoo.com
    service text-chat action allow
    service default action reset
  !
  application im aol
    server deny name login.cat.aol.com
  !
```

■ server (application firewall policy)

```
application im msn
server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
description Inside interface
ip inspect test in
```

Related Commands

| Command | Description |
|----------------|---|
| service | Specifies an action when a specific service is detected in the instant messenger traffic. |

server

To associate a Diameter server with a Diameter authentication, authorization, and accounting (AAA) server group, use the **server** command in Diameter server group configuration submode. To remove a server from the server group, enter the **no** form of this command.

server *name*

no server *name*

Syntax Description

| | |
|-------------|--|
| <i>name</i> | Character string used to name the Diameter server. |
| Note | The name specified for this command should match the name of a Diameter peer defined using the diameter peer command. |

Command Default

No server is associated with a Diameter AAA server group.

Command Modes

Diameter server group configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.4(9)T | This command was introduced. |

Usage Guidelines

The **server** command allows you to associate a Diameter server with a Diameter server group.

Examples

The following example shows how to associate a Diameter server with a Diameter server group:

```
Router (config-sg-diameter)# server dia_peer_1
```

Related Commands

| Command | Description |
|----------------------------------|--|
| aaa accounting | Enables AAA accounting of requested services for billing or security purposes. |
| aaa authentication login | Set AAA authentication at login. |
| aaa authorization | Sets parameters that restrict user access to a network. |
| aaa group server diameter | Configures a server group for Diameter. |

server (parameter-map)

To configure a set of Domain Name System (DNS) servers for which a given instant messenger application will be interacting, use the **server** command in parameter-map configuration mode. To remove a server from the parameter map, use the **no** form of this command.

```
server {name string [snoop] | ip {ip-address | range ip-address-start ip-address-end}}
```

```
no server {name string [snoop] | ip {ip-address | range ip-address-start ip-address-end}}
```

Syntax Description

| | |
|---|---|
| name <i>string</i> | Name of DNS server for which traffic will be permitted (and inspected) or denied. |
| snoop | (Optional) Enables DNS snooping. |
| ip | Indicates that at least one IP address will be listed. |
| <i>ip-address</i> | IP address of the DNS server for which traffic will be permitted (and inspected) or denied. |
| range <i>ip-address-start ip-address-end</i> | Range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied. |

Command Default

If at least one server instance is not configured, the parameter map will not have any definitions to enforce; that is, the configured instant messenger policy cannot be enforced.

Command Modes

Parameter-map configuration

Command History

| Release | Modification |
|-----------|---|
| 12.4(9)T | This command was introduced. |
| 12.4(20)T | The snoop keyword was added. Support for the I Seek You (ICQ) and Windows Messenger IM Protocols was added. |

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize the instant messenger traffic and to enforce the configured policy for that instant messenger application.

Before you can issue the **server** command, you must issue the **parameter-map type** command, which allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.



Note

To enable name resolution to occur, you must also enable the **ip domain name** command and the **ip name-server** command.

To configure more than one set of servers, you can issue the **server** command multiple times within an instant messenger's parameter map. Multiple entries are treated cumulatively.

DNS Snooping

In Cisco IOS Release 12.4(20)T, users can now enable DNS snooping on an access router to easily obtain address names. When DNS snooping is enabled, the Cisco IOS firewall that is running on the access router can “snoop” DNS responses that are going through the access router. The firewall can obtain the necessary addresses from DNS responses because the DNS inspection engine decodes DNS response packets and returns a list of addresses back to the address database.

Also, when using DNS snooping, network administrators no longer have to give a complete address, such as `abcd.msg.yahoo.com`; instead, they can specify a partial address with a “wildcard character,” such as `*.msg.yahoo.com`.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and AOL traffic is allowed to pass through, while all MSN Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and AOL traffic on a more granular level.

```
! Define Layer 7 class-maps.
class-map type inspect ymsgr match-any l7-cmap-ymsgr
  match service text-chat
!
class-map type inspect aol match-any l7-cmap-aol
  match service text-chat
  match service any
!
! Define Layer 7 policy-maps.
policy-map type inspect im l7-pmap-ymsgr
  class-type inspect ymsgr l7-cmap-ymsgr
  allow
  alarm
!
!
policy-map type inspect im l7-pmap-aol
  class-type inspect aol l7-cmap-aol
  allow
  alarm
!
!
! Define parameter map.
parameter-map type protocol-info ymsgr
  server name sdsc.msg.yahoo.com
  server ip 10.1.1.1
!
parameter-map type protocol-info aol
  server name sdsc.msg.aol.com
  server ip 172.16.1.1.
```

The following example shows how to configure an access router to block ICQ and Yahoo IM applications while allowing only text chat with Windows Messenger. In this example, snooping is enabled to obtain addresses for all IM applications.

```
! Define the servers for ICQ.
parameter-map type protocol-info icq-servers
  server name *.icq.com snoop
  server name oam-d09a.blue.aol.com

! Define the servers for Windows Messenger.
parameter-map type protocol-info winmsgr-servers
  server name messenger.msn.com snoop
```

■ server (parameter-map)

```

! Define servers for yahoo.
parameter-map type protocol-info yahoo-servers
  server name scs*.msg.yahoo.com snoop
  server name c*.msg.yahoo.com snoop

! Define class-map to match ICQ traffic.
class-map type inspect icq-traffic
  match protocol icq icq-servers

! Define class-map to match windows Messenger traffic.
class-map type inspect winmsgr-traffic
  match protocol winmsgr winmsgr-servers
!

! Define class-map to match text-chat for windows messenger.
class-map type inspect winmsgr winmsgr-textchat
  match service text-chat
!

Define class-map to match default service
class-map type inspect winmsgr winmsgr-defaultservice
  match service any
!

! Define a Layer 7 IM policy-map to permit text-chat and block everything else.
policy-map type inspect im im-policy
  class type inspect winmsgr winmsgr-textchat
    allow
  !
  class type inspect winmsgr winmsgr-defaultservice
    reset
  !
!

! Define the Layer 4 policy to block ICQ and Yahoo Messenger and allow yahoo text-chat
! with Windows Messenger
policy-map type inspect firewall-policy
  class type inspect winmsgr-traffic
    inspect
    service-policy type inspect im im-policy
  !
  class type inspect icq-traffic
    drop
  !
  class type inspect yahoo-traffic
    drop

```

Related Commands

| Command | Description |
|---------------------------|---|
| ip domain lookup | Enables the IP DNS-based host name-to-address translation. |
| ip name-server | Specifies the address of one or more name servers to use for name and address resolution. |
| parameter-map type | Creates or modifies a parameter map. |

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

```
server ip-address [auth-port port-number] [acct-port port-number]
```

```
no server ip-address [auth-port port-number] [acct-port port-number]
```

Syntax Description

| | |
|-------------------------------------|---|
| <i>ip-address</i> | IP address of the RADIUS server host. |
| auth-port <i>port-number</i> | (Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The <i>port-number</i> argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. |
| acct-port <i>port-number</i> | (Optional) Specifies the UDP destination port for accounting requests. The <i>port-number</i> argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0. |

Defaults

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

| Release | Modification |
|-------------|---|
| 12.0(5)T | This command was introduced. |
| 12.0(7)T | The following new keywords/arguments were added: <ul style="list-style-type: none"> • auth-port <i>port-number</i> • acct-port <i>port-number</i> |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
    server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
    server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

Related Commands

| Command | Description |
|---------------------------|---|
| aaa group server | Groups different server hosts into distinct lists and distinct methods. |
| aaa new-model | Enables the AAA access control model. |
| radius-server host | Specifies a RADIUS server host. |

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

```
server ip-address
```

```
no server ip-address
```

Syntax Description

| | |
|-------------------|------------------------------------|
| <i>ip-address</i> | IP address of the selected server. |
|-------------------|------------------------------------|

Defaults

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

| Release | Modification |
|-------------|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
  server 10.0.0.1
  server 10.2.0.1
tacacs-server host 10.0.0.1
tacacs-server host 10.2.0.1
```

Related Commands

| Command | Description |
|----------------------|---------------------------------------|
| aaa new-model | Enables the AAA access control model. |

| Command | Description |
|---------------------------|---|
| aaa server group | Groups different server hosts into distinct lists and distinct methods. |
| tacacs-server host | Specifies a RADIUS server host. |

server address ipv4

To specify the address of the server that a Group Domain of Interpretation (GDOI) group is trying to reach, use the **server address ipv4** command in GDOI group configuration mode. To disable the address, use the **no** form of this command.

```
server address ipv4 {address | hostname}
```

```
no server address ipv4 {address | hostname}
```

Syntax Description

| | |
|-----------------|---------------------------|
| <i>address</i> | IP address of the server. |
| <i>hostname</i> | Hostname of the server. |

Command Default

None

Command Modes

GDOI group configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.4(6)T | This command was introduced. |

Usage Guidelines

The **server address ipv4** command can be used only on a group member. This command must be specified or the group configuration on the group member is not complete.

Examples

The following example shows that the GDOI group is trying to reach the server with the IP address “10.34.255.57”:

```
server address ipv4 10.34.255.57
```

Related Commands

| Command | Description |
|--------------------------|---|
| crypto gdoi group | Identifies a GDOI group and enters GDOI group configuration mode. |
| server local | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

server local

To designate a device as a Group Domain of Interpretation (GDOI) key server and enter GDOI local server configuration mode, use the **server local** command in GDOI group configuration mode. To remove a device as a key server, use the **no** form of this command.

server local

no server local

Syntax Description This command has no arguments or keywords.

Command Default A device is not designated as a GDOI key server.

Command Modes GDOI group configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(6)T | This command was introduced. |

Usage Guidelines This command is used on the key server to specify the key server policy that will be downloaded to the group members that are registered with the key server.

Examples The following example shows that the device has been designated as a GDOI key server:

```
server local
```

| Related Commands | Command | Description |
|------------------|--------------------------|---|
| | crypto gdoi group | Identifies a GDOI group and enters GDOI group configuration mode. |

server vendor

To specify the URL filtering server, use the **server vendor** command in URL parameter-map configuration mode. To remove a server from your configuration, use the **no** form of this command.

```
server vendor {n2h2 | websense} {ip-address | hostname [port port-number]} [outside] [log]
[retrans retransmission-count] [timeout seconds]
```

```
no server vendor {n2h2 | websense} {ip-address | hostname [port port-number]} [outside] [log]
[retrans retransmission-count] [timeout seconds]
```

| Syntax Description | | |
|---|--|--|
| n2h2 | | N2H2 server will be used. |
| websense | | Websense server will be used. |
| <i>ip-address</i> | | IP address of the URL filtering server that you want to configure. |
| <i>hostname</i> | | Host name of the URL filtering server that you want to configure. |
| port <i>port-number</i> | | (Optional) Port number on which the vendor server listens. The default is 15868. |
| outside | | (Optional) Vendor server will be deployed on the outside network. |
| log | | (Optional) |
| retrans <i>retransmission-count</i> | | (Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is 2. |
| timeout <i>seconds</i> | | (Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default is 5. |

Command Default None

Command Modes URL parameter-map configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(6)T | This command was introduced. |

Usage Guidelines

Use this command to specify the URL filtering server. If there is no server, there can be no url filtering.

When you are creating a URL filter parameter map, you can use the **server vendor** subcommand after entering the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Use the **server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS Firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout seconds** keyword and argument, the firewall checks the **retrans retransmission-count** keyword and argument configured for the vendor server. If the firewall has not exceeded the maximum retransmit tries allowed, it resends the HTTP lookup request. If the firewall has exceeded the maximum retransmit tries allowed, it deletes the outstanding request from the queue and checks the value specified in the **allow-mode** command. The firewall forwards the request if the allow-mode is on; otherwise, it drops the request.

By default, URL lookup requests that are made to the vendor server contain non-natted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network. Cisco IOS software sends, in the URL lookup request, the client's IP address that has undergone network address translation (NAT).

Primary and Secondary Servers

When you configure multiple vendor servers, the Cisco IOS firewall uses only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system goes to the beginning of the configured servers list and tries to activate the first server on the list. If the first server on the list is unavailable, it tries the second server on the list; the system keeps trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it sets a flag indicating that all of the servers are down, and it enters allow-mode. When allow-mode is on, HTTP traffic is permitted.

Examples

The following example specifies the n2h2 vendor server for URL filtering:

```
parameter-map type urlfilter ul
  server vendor n2h2 10.193.64.22 port 3128 outside
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| ip urlfilter server vendor | Configures a vendor server for URL filtering. |
| max-request | Specifies the maximum number of outstanding requests that can exist at any given time. |
| parameter-map type url | Creates a parameter map that will hold parameters pertaining to the URL filter. |

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

```
server-private ip-address [auth-port port-number | acct-port port-number] [non-standard]
[timeout seconds] [retransmit retries] [key string]
```

```
no server-private ip-address [auth-port port-number | acct-port port-number] [non-standard]
[timeout seconds] [retransmit retries] [key string]
```

Syntax Description

| | |
|-------------------------------------|--|
| <i>ip-address</i> | IP address of the private RADIUS server host. |
| auth-port <i>port-number</i> | (Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645. |
| acct-port <i>port-number</i> | (Optional) UDP destination port for accounting requests. The default value is 1646. |
| non-standard | (Optional) RADIUS server is using vendor-proprietary RADIUS attributes. |
| timeout <i>seconds</i> | (Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. |
| retransmit <i>retries</i> | (Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command. |
| key <i>string</i> | (Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. |

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

| Release | Modification |
|------------|---|
| 12.2(1)DX | This command was introduced on the Cisco 7200 series and Cisco 7401ASR. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

| Release | Modification |
|-------------|---|
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default “radius” server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.



Note

If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private (RADIUS)** command.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
  server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
  server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

| Command | Description |
|---------------------------------------|---|
| aaa group server | Groups different server hosts into distinct lists and distinct methods. |
| aaa new-model | Enables the AAA access control model. |
| radius-server host | Specifies a RADIUS server host. |
| radius-server directed-request | Allows users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication. |

server-private (TACACS+)

To configure the IP address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

```
server-private {ip-address | name} [nat] [single-connection] [port port-number] [timeout
seconds] [key [0 | 7] string]
```

```
no server-private
```

| Syntax Description | |
|------------------------------------|--|
| <i>ip-address</i> | IP address of the private RADIUS or TACACS+ server host. |
| <i>name</i> | Name of the private RADIUS or TACACS+ server host. |
| nat | (Optional) Port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server. |
| single-connection | (Optional) Maintains a single open connection between the router and the TACACS+ server. |
| port <i>port-number</i> | (Optional) Specifies a server port number. This option overrides the default, which is port 49. |
| timeout <i>seconds</i> | (Optional) Specifies a timeout value. This value overrides the global timeout value set with the tacacs-server timeout command for this server only. |
| key [0 7] | (Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global tacacs-server key command for this server only. <ul style="list-style-type: none"> If no number or 0 is entered, the string that is entered is considered to be plain text. If 7 is entered, the string that is entered is considered to be encrypted text. |
| <i>string</i> | (Optional) Character string specifying the authentication and encryption key. |

Command Default If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes Server-group configuration (server-group)

| Command History | Release | Modification |
|-----------------|--------------|--|
| | 12.3(7)T | This command was introduced. |
| | 12.2(33)SRA1 | This command was integrated into Cisco IOS Release 12.2(33)SRA1. |
| | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default “TACACS+” server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
aaa group server tacacs+ tacacs1
  server-private 10.1.1.1 port 19 key cisco

ip vrf cisco
  rd 100:1

interface Loopback0
  ip address 10.0.0.2 255.0.0.0
  ip vrf forwarding cisco
```

Related Commands

| Command | Description |
|---|--|
| aaa group server | Groups different server hosts into distinct lists and distinct methods. |
| aaa new-model | Enables the AAA access control model. |
| ip tacacs source-interface | Uses the IP address of a specified interface for all outgoing TACACS+ packets. |
| ip vrf forwarding (server-group) | Configures the VRF reference of an AAA RADIUS or TACACS+ server group. |
| tacacs-server host | Specifies a TACACS+ server host. |

service action

To specify an action when a specific service is detected in the instant messenger traffic, use the **service action** command in the appropriate configuration mode. To disable or change a specified action, use the **no** form of this command.

```
service { default | text-chat } action { allow [alarm] | reset [alarm] | alarm }
```

```
no service { default | text-chat } action { allow [alarm] | reset [alarm] | alarm }
```

Syntax Description

| | |
|------------------|--|
| default | Matches all services that are not explicitly configured under the application. Note It is recommended that when an IM application is allowed, always specify the default option for an IM application. |
| text-chat | Controls the text-based chat service that is provided by instant messenger applications. |
| action | Indicates that a specific action is to follow. |
| allow | Allows a specific service. |
| reset | Blocks the service specified in the configuration. If the default option is being used, only services for which a specific action has been identified are allowed; all other services are denied. |
| alarm | Generates an alarm message when the specified service is encountered over the connection. |

Command Default

If the command is not configured, the default is **service default action reset**.

Command Modes

cfg-appfw-policy-aim configuration
 cfg-appfw-policy-ymsggr configuration
 cfg-appfw-policy-msnmsggr configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.4(4)T | This command was introduced. |

Usage Guidelines

When the **reset** keyword is used, the connection is reset if TCP is used, and the packet is dropped if UDP is used. When dropping a packet from a UDP connection, the session will not be immediately deleted; instead, the session will time out to prevent additional sessions from being immediately created.

The **alarm** keyword can be specified alone or with the **allow** or **reset** keywords; however, the **allow** or **reset** keywords are mutually exclusive.

Examples

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
  application http
  port-misuse im reset
!
  application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
  application im aol
  server deny name login.user1.aol.com
!
  application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
  description Inside interface
  ip inspect test in
```

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description This command has no arguments or keywords.

Command Default No passwords are encrypted.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 10.0 | This command was introduced. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| | 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| | 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

Usage Guidelines The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.



Caution

This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.



Note

You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples The following example causes password encryption to take place:

```
service password-encryption
```

| Related Commands | Command | Description |
|------------------|--|---|
| | enable password | Sets a local password to control access to various privilege levels. |
| | key-string (authentication) | Specifies the authentication string for a key. |
| | neighbor password | Enables MD5 authentication on a TCP connection between two BGP peers. |

service password-recovery

To enable password recovery capability, use the **service password-recovery** command in global configuration mode. To disable password recovery capability, use the **no service password-recovery** command.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

Password recovery capability is enabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(8)YA | This command was introduced. |
| 12.3(14)T | This command was integrated into Cisco IOS Release 12.3(14)T. |

Usage Guidelines



Note

This command is not available on all platforms. Use Feature Navigator to ensure that it is available on your platform.

If you plan to disable the password recovery capability with the the **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the switch or router. If you are using a switch that is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.



Caution

Entering the **no service password-recovery** command at the command line disables password recovery. Always disable this command before downgrading to an image that does not support password recovery capability, because you cannot recover the password after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration, and bit 8, which enables a break should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

It may be necessary to use the **config-register** global configuration command to set the configuration register to autoboot before entering the **no service password-recovery** command. The last line of the **show version EXEC** command displays the configuration register setting. Use the **show version EXEC** command to obtain the current configuration register value, configure the router to autoboot with the **config-register** command if necessary, then enter the **no service password-recovery** command.

Once disabled, the following configuration register values are invalid for the **no service password-recovery** command:

- 0x0
- 0x2002 (bit 8 restriction)
- 0x0040 (bit 6)
- 0x8000 (bit 15)

Catalyst Switch Operation

Use the **service password-recovery** command to reenble the password-recovery mechanism (the default). This mechanism allows a user with physical access to the switch to hold down the Mode button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable the password-recovery capability.

When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration. Use the **show version EXEC** command to verify if password recovery is enabled or disabled on a switch.

The **service password-recovery** command is valid only on Catalyst 3550 Fast Ethernet switches; it is not available for Gigabit Ethernet switches.

Examples

Router Configuration Examples

The following example shows how to obtain the configuration register setting (which in this example is set to autoboot), disable the password-recovery capability, and then verify that the configuration persists through a system reload. The **noconfirm** keyword prevents a confirmation prompt from interrupting the booting process.

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000

ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)

Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012

Router# configure terminal

Router(config)# no service password-recovery noconfirm
```

```

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload

Proceed with reload? [confirm] yes

00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.

```

The following example shows what happens when a break is confirmed and when a break is not confirmed.

Confirmed Break

```

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :

#####
##### [OK] !The 5-second window starts.

telnet> send break

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514

PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.

Reset router configuration to factory default.

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use

```

encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
 Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
 3 Ethernet interfaces
 4 FastEthernet interfaces
 128K bytes of NVRAM
 24576K bytes of processor board System flash (Read/Write)
 2048K bytes of processor board Web flash (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
 !Start up config is erased.

SETUP: new interface FastEthernet1 placed in "up" state
 SETUP: new interface FastEthernet2 placed in "up" state
 SETUP: new interface FastEthernet3 placed in "up" state
 SETUP: new interface FastEthernet4 placed in "up" state

Press RETURN to get started!

Router> **enable**
 Router# **show startup configuration**

startup-config is not present

Router# **show running-config | incl service**

no service pad
 service timestamps debug datetime msec
 service timestamps log datetime msec
 no service password-encryption !The "no service password-recovery" is disabled.

=====

Unconfirmed Break

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

telnet> **send break**

program load complete, entry point: 0x80013000, size: 0x8396a8
 Self decompressing the image :

 ##### [OK]

telnet> **send break**

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)

Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.

Router> **enable**

Router# **show startup configuration**

```
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
```

```
no ip address
shutdown
!
interface Ethernet1
no ip address
shutdown
duplex auto
!
interface Ethernet2
no ip address
shutdown
!
interface FastEthernet1
no ip address
duplex auto
speed auto
!
interface FastEthernet2
no ip address
duplex auto
speed auto
!
interface FastEthernet3
no ip address
duplex auto
speed auto
!
interface FastEthernet4
no ip address
duplex auto
speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
no modem enable
transport preferred all
transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

```
Router# show running-configuration | incl service
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
```

Configuration Register Messages Example

The **no service password-recovery** command expects the router configuration register to be configured to autoboot. If the configuration register is set to something other than to autoboot before the **no service password-recovery** command is entered, you will see a prompt like the one shown in the following example asking you to use the **config-register** global configuration command to change the setting.

```
Router(config)# no service password-recovery
```

```
Please setup auto boot using config-register first.
```



Note

To avoid any unintended result due to the behavior of this command, use the **show version EXEC** command to obtain the current configuration register value. If not set to autoboot, you will need to configure the router to autoboot with the **config-register** command before entering the **no service password-recovery** command.

Once password recovery is disabled, you will not be able set bit pattern 0x40, 0x8000 or set the value to 0x0 to disable autoboot. The following example shows the messages displayed when invalid configuration register settings are attempted on a router with password recovery disabled.

```
Router(config)# config-register 0x2143
```

```
Password recovery is disabled, cannot enable diag or ignore configuration.
```

The command will reset the invalid bit pattern and continue to allow modification of nonrelated bit patterns. The configuration register value will be reset to 0x3 at the next system reload, which can be verified by checking the last line of the **show version** command output:

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

Catalyst Switch Example

The following example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration:

```
Switch(config)# no service-password recovery  
Switch(config)# exit
```

To use the password-recovery procedure, a user with physical access to the switch holds down the Mode button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, the following message is displayed:

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to  
the boot loader prompt through the password-recovery mechanism is disallowed at this  
point. However, if you agree to let the system be reset back to the default system  
configuration, access to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

If you choose not to reset the system back to the default configuration, the normal boot process continues, as if the Mode button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted and the VLAN database file, flash:vlan.dat (if present), is deleted.

The following is sample output from the **show version** privileged EXEC command on a switch when password recovery is disabled:

```
Switch# show version

Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864

ROM: Bootstrap program is C3550 boot loader

flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on

Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

Related Commands

| Command | Description |
|------------------------|---|
| config-register | Changes the configuration register settings. |
| show version | Displays version information for the hardware and firmware. |

service-module ids bootmode

To enter failsafe or normal boot mode for a Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), use the **service-module ids bootmode** command in privileged EXEC mode.

```
service-module ids slot/port bootmode { failsafe | normal }
```

| Syntax Description | slot | Number of the router chassis slot for the network module. The slash mark (/) is required between the <i>slot</i> argument and the <i>port</i> argument. |
|--------------------|----------|---|
| | port | Port number of the network module. For Cisco IPS network modules, always use 0. |
| | failsafe | Enters IDS failsafe boot mode on a Cisco IPS network module. |
| | normal | Enters IDS normal boot mode on a Cisco IPS network module. |

Defaults None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.4(15)XY | This command was introduced. |
| | 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines If a confirmation prompt is displayed, press **Enter** to confirm the action, or press **n** to cancel.

Examples The following example enters the IDS failsafe boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode failsafe
```

The following example enters the IDS normal boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode normal
```

| Related Commands | Command | Description |
|------------------|--------------------------------------|--|
| | ids-service-module monitoring | Enables IDS monitoring on a specified interface. |

service-module ids heartbeat-reset

To prevent the Cisco IOS software from rebooting the Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), when the heartbeat is lost, use the **service-module ids heartbeat-reset** command in privileged EXEC mode.

```
service-module ids slot/port heartbeat-reset {enable | disable}
```

| Syntax Description | | |
|--------------------|----------------|---|
| | <i>slot/</i> | Number of the router chassis slot for the network module. The slash mark (/) is required between the <i>slot</i> argument and the <i>port</i> argument. |
| | <i>port</i> | Port number of the network module. For Cisco IPS network modules, always use 0. |
| | enable | Enables IDS heartbeat on a Cisco IPS network module. |
| | disable | Disables IDS heartbeat on a Cisco IPS network module. |

Defaults None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.4(15)XY | This command was introduced. |
| | 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

When the Cisco IPS network module, or NME-IPS, is booted in failsafe mode or is undergoing an upgrade, the **service-module ids heartbeat-reset** command does not permit a reboot during the process.

When the NME-IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the NME-IPS and stops sending traffic to the NME-IPS, and sets the NME-IPS to error state. The router performs a hardware reset on the NME-IPS and monitors the NME-IPS until the heartbeat is reestablished.

Examples The following example disables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset disable
```

The following example enables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset enable
```

The status of the heartbeat-reset is displayed by using the **service-module ids slot/port status** command:

```
Router# service-module ids 0/0 status
Service Module is Cisco IDS-Sensor 0/0
Service Module supports session via TTY line 194
```

```
Service Module heartbeat-reset is enabled <=====
```

Related Commands

| Command | Description |
|--------------------------------------|--|
| ids-service-module monitoring | Enables IDS monitoring on a specified interface. |

service-policy (policy-map)



Note

Effective with Cisco IOS Release 12.4(20)T, the **service-policy (policy-map)** command replaces the **service-policy inspect** command.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy** command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

```
service-policy {h323 | http | im | imap | p2p | pop3 | sip | smtp | sunrpc | urlfilter} policy-map
```

```
no service-policy {h323 | http | im | imap | p2p | pop3 | sip | smtp | sunrpc | urlfilter} policy-map
```

Syntax Description

| | |
|-------------------|---|
| h323 | Associates the class with an H.323 protocol Deep Packet Inspection (DPI). |
| http | Associates the class with an HTTP DPI. |
| im | Associates the class with an Instant Messenger (IM) protocol DPI. |
| imap | Associates the class with an Internet Message Access Protocol (IMAP) DPI. |
| p2p | Associates the class with a P2P protocol DPI. |
| pop3 | Associates the class with a Post Office Protocol, Version 3 (POP3) DPI. |
| sip | Associates the class with a Session Initiation Protocol (SIP) DPI. |
| smtp | Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI. |
| sunrpc | Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI. |
| urlfilter | Associates the class with a URL filter DPI. |
| <i>policy-map</i> | Name of the Layer 7 policy map. |

Command Default

Disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

| Release | Modification |
|-----------|---|
| 12.4(20)T | This command was introduced. This command replaces the service policy-inspect command. |

Usage Guidelines

The **service-policy (policy-map)** command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example creates a Layer 3 or Layer 4 policy called test, attaches a Layer 7 policy called p11 to that policy, and inspects H.323 traffic.

```
!  
class-map type inspect match-all test  
  match protocol h323  
class-map type inspect h323 match-any c1  
  match message setup  
!  
policy-map type inspect h323 p11  
  class type inspect h323 c1  
  log  
  rate-limit 15  
policy-map type inspect test  
  class type inspect test  
  inspect  
  service-policy h323 p11  
  class class-default  
  drop  
!
```

Related Commands

| Command | Description |
|--------------------------------|---|
| policy-map type inspect | Creates a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map. |

service-policy (zones)

To attach a Layer 7 policy map to a top-level policy map, use the **service-policy** command in zone-pair configuration mode. To delete a Layer 7 policy map from a top-level policy map, use the **no** form of this command.

service-policy *policy-map-name*

no service-policy *policy-map-name*

| | | |
|---------------------------|------------------------|--|
| Syntax Description | <i>policy-map-name</i> | Name of the Layer 7 policy map to be attached to a top-level policy map. |
|---------------------------|------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| | |
|----------------------|-------------------------|
| Command Modes | Zone-pair configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.4(6)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | You can enter the service-policy (zones) command after entering the zone-pair command. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following example attaches a Layer 7 policy map to a top-level policy map: |
|-----------------|--|

```
policy-map type inspect p1
  class type inspect c1
    inspect
  service-policy http myhttppolicy
```

| | | |
|-------------------------|------------------|----------------------|
| Related Commands | Command | Description |
| | zone-pair | Creates a zone-pair. |

service-policy inspect



Note

Effective with Cisco IOS Release 12.4(20)T, the **service-policy inspect** command is replaced by the **service-policy (policy-map)** command. See the **service-policy (policy-map)** command for more information.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy inspect** command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

```
service-policy inspect {http | imap | pop3 | smtp | sunrpc} policy-map
```

```
no service-policy inspect {http | imap | pop3 | smtp | sunrpc} policy-map
```

Syntax Description

| | |
|-------------------|---|
| http | Associates the class with an HTTP deep inspection policy (DPI). |
| imap | Associates the class with an Internet Message Access Protocol (IMAP) DPI. |
| pop3 | Associates the class with a Post Office Protocol, Version 3 (POP3) DPI. |
| smtp | Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI. |
| sunrpc | Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI. |
| <i>policy-map</i> | Name of the Layer 7 policy map. |

Command Default

Disabled.

Command Modes

Policy-map-class configuration

Command History

| Release | Modification |
|-----------|--|
| 12.4(6)T | This command was introduced. |
| 12.4(20)T | This command was replaced by the service-policy (policy-map) command. |

Usage Guidelines

The **service-policy inspect** command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example creates a Layer 3 or Layer 4 policy map p1, attaches a Layer 7 policy called p11 to that policy, and inspects HTTP traffic.

```
policy-map type inspect p1
  class type inspect c1
    service-policy inspect http p11
```


service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*

no service-policy type inspect *policy-map-name*

| Syntax Description | <i>policy-map-name</i> | Name of the policy map. The name can be a maximum of 40 alphanumeric characters. |
|--------------------|------------------------|--|
|--------------------|------------------------|--|

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command Modes | Zone-pair configuration (config-sec-zone-pair) |
|---------------|--|
|---------------|--|

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(6)T | This command was introduced. |

Usage Guidelines Use the **service-policy type inspect** command to attach a policy-map and its associated actions to a zone-pair.

Enter the command after entering the **zone-pair security** command.

Examples The following example defines zone-pair z1-z2 and attaches the service policy p1 to the zone-pair:

```
!
zone security z1
zone security z2
!
class-map type inspect match-all c1
  match protocol tcp
policy-map type inspect p1
  class type inspect c1
    inspect
!
zone-pair security zp source z1 destination z2
  service-policy type inspect p1
!
```

| Related Commands | Command | Description |
|------------------|---------------------------|----------------------|
| | zone-pair security | Creates a zone-pair. |

sessions maximum

To set the maximum number of allowed sessions that can exist on a zone pair, use the **sessions maximum** command in parameter-map configuration mode. To change the number of allowed sessions, use the **no** form of this command.

sessions maximum *sessions*

no sessions maximum

Syntax Description

sessions Maximum number of allowed sessions. Range: 1 to 2147483647.

Command Default

Maximum number of sessions: 200

Command Modes

Parameter-map configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.4(9)T | This command was introduced. |

Usage Guidelines

Use the **sessions maximum** command to limit the number of inspect sessions that match a certain class. This command is available only within an inspect type parameter map and takes effect only when the parameter map is associated with an inspect action in a policy.

If the **sessions maximum** command is configured, the number of established sessions on the router can be shown via the **show policy-map type inspect zone-pair** command.

Examples

The following example shows how to limit the maximum number of allowed sessions to 200 and how verify the number of established sessions:

```
parameter map type inspect foo
  sessions maximum 200

Router# show policy-map type inspect zone-pair

Zone-pair: zp

Service-policy inspect : test-udp

Class-map: check-udp (match-all)
  Match: protocol udp
  Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]

Session creations since subsystem startup or last reset 92
Current session counts (estab/half-open/terminating) [5:33:0]<---
Maxever session counts (estab/half-open/terminating) [5:59:0]
```

```

Last session created 00:00:06
Last statistic reset never
Last session creation rate 61
Last half-open session total 33
Police
rate 8000 bps,1000 limit
conformed 2327 packets, 139620 bytes; actions: transmit
exceeded 36601 packets, 2196060 bytes; actions: drop
conformed 6000 bps, exceed 61000 bps

Class-map: class-default (match-any)
Match: any
Drop (default action)
  0 packets, 0 bytes

```

Related Commands

| Command | Description |
|---------------------------|--------------------------------------|
| parameter map type | Creates or modifies a parameter map. |