sa ipsec through sessions maximum

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

sequence-number	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:

```
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
```

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.

sap mode-list (config-if-cts-dot1x)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

sap mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
no sap mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

Syntax Description

gcm-encrypt	Specifies GMAC authentication, GCM encryption.
gmac	Specifies GMAC authentication only, no encryption.
no-encap	Specifies no encapsulation.
null	Specifies encapsulation present, no authentication, no encryption.

Command Default

The default encryption is **sap mode-list gcm-encrypt null**. When the peer interface does not support dot1x, 802.1AE MACsec, or 802.REV layer-2 link encryption, the default encryption is **null**.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
IOS- XE 3.3.0 SG	This command was introduced on the Catalyst 4500 Series Switches.
15.0(1) SE	This command was introduced on the Catalyst 3000 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **sap mode-list** command to specify the authentication and encryption method to use during Dot1x authentication.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

Before the SAP exchange begins after a Dot1x authentication, both sides (supplicant and authenticator) have received the Pairwise Master Key (PMK) and the MAC address of the peer's port from the Cisco Secure Access Control Server (Cisco Secure ACS). If 802.1X authentication is not possible, SAP, and the PMK can be manually configured between two interfaces in CTS manual configuration mode.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

Use the **timer reauthentication** command to configure the reauthentication period to be applied to the CTS link in case the period is not available from the Cisco Secure ACS. The default reauthentication period is 86,400 seconds.

Note Because TrustSec NDAC and SAP are supported only on a switch-to-switch link, dot1x must be configured in multi-hosts mode. The authenticator PAE starts only when the **dot1x system-auth-control** command is enabled globally.

Examples

The following example specifies that SAP is to negotiate the use of CTS encapsulation with GCM cipher, or null-cipher as a second choice, but can accept no CTS encapsulation if the peer does not support CTS encapsulation in hardware.

```
Device(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
propagate sgt (config-if-cts-dot1x)	Enables Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface.
show cts interface	Displays CTS interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.
timer reauthentication (config-if-cts-dot1x)	Configures the reauthentication timer for a CTS device.

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.

Command Default

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.
standby-group-name	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.

Command Default

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.

search-filter

To configure a search request sent by the Lightweight Directory Access Protocol (LDAP) client to the server in order to find the user's node in the Directory Information Tree (DIT), use the **search-filter** command in LDAP server configuration mode. To delete the search request from the LDAP server group, use the **no** form of this command.

search-filter user-object-type *string*
no search-filter user-object-type *string*

Syntax Description

user-object-type	Adds a user attribute to the search filter.
string	Name of the object class attribute.

Command Default

No default search requests are configured.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can add multiple search filter attributes by using the **search-filter** command. The search filter is a mandatory configuration for an LDAP server, because it is used to filter the exact user from the search results. Without this configuration, a user cannot be authenticated. The **search-filter** command helps you to filter the search results based on the attributes mentioned in the search filter.

Examples

The following example shows how to filter the search results for an LDAP server. After you have specified the search criteria as shown below, the search filter string appears in the "(&(objectclass=person) (&(cn=$userid)(cid=$contextid)))" format.

```
Router(config)# ldap server server1
Router(config-ldap-server)# search-filter user-object-type cn
Router(config-ldap-server)# search-filter user-object-type cid
Router(config-ldap-server)# search-filter user-object-type objectclass
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

search-type nested

To configure nested-group search requests, use the **search-type nested** command in Lightweight Directory Access Protocol (LDAP) server configuration mode. To remove the configuration, use the **no** form of this command.

search-type nested
no search-type nested

Syntax Description

This command has no arguments or keywords.

Command Default

No nested-group search requests are configured.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **search-type nested** command to configure nested-group search requests. The nested-group search filter allows you to retrieve the complete nested-user-group chain information of a user in a particular Microsoft Active Directory domain. This customized filter is sent in an LDAP query to the server.

The **search-type nested** command overrides the **search-filter object-type** command, which is used to conduct a top-level search to obtain direct user groups from an LDAP server.

Examples

The following example shows how to configure nested-group search requests.

```
ldap server ldap_dir_1
bind authenticate root-dn cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password
 example123
search-type nested
base-dn dc=sns,dc=example,dc=com
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
search-filter object-type	Configures a search request sent by an LDAP client to a server to find a user's node in the DIT.

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*
no sec-level minimum *value*

Syntax Description

value	Minimum security level, which is a value from 1 to 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and specifies 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

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

color	The value for the *color* 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): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default color is purple.

Command Default

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.

Command Default

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 CLI view or a superview with a password, use the **secret** command in view configuration mode. To remove the configured password, use the **no** form of this command.

secret {**0** *unencrypted-password* | **5** *encrypted-password* | *unencrypted-password*}
no secret {**0** *unencrypted-password* | **5** *encrypted-password* | *unencrypted-password*}

Syntax Description

0	Specifies that an unencrypted password follows.
unencrypted-password	Unencrypted password. A password that contains a combination of alphanumeric characters. The password is case sensitive. This password is encrypted by the message digest 5 (MD5) method.
5	Specifies that an encrypted password follows.
encrypted-password	Encrypted password that you enter or that is copied from another router configuration.

Command Default

A user cannot access a CLI view or superview.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

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

Before CSCts50236, the password could only be overwritten and not removed. With CSCts50236, the password can be removed or overwritten. Use the **no secret** command in the view configuration (config-view) mode to remove the configured password.

Examples

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

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# aaa new-model
Device(config)# enable secret cisco
Device(config)# exit
Device# enable view root
Password:
*Dec  9 00:50:51.283: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
Device# show parser view
Current view is 'root'
Device# configure terminal
Device(config)# parser view first
Device(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Device(config-view)# secret firstpassword
Device(config-view)# secret secondpassword
% Overwriting existing secret for the current view
Device(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Device(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
Device(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.
Device(config-view)# command exec include show version
Device(config-view)# command exec include configure terminal
Device(config-view)# command configure include all ip
Device(config-view)# exit


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

.
.
.
parser view second
 secret 5 $1$PWs8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
.
.
.
```

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

```
Device# show running-config | include parser view first

.
.
.
parser view first
 secret 5 $1$jj1e$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

key-name	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 secret-key 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.

Command Default

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.

Command Default

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.

secure cipher

To specify the ciphersuite in case of secure connection, use the **secure cipher**command in Lightweight Directory Access Protocol (LDAP) server configuration mode. To disable the secure connection, use the **no**form of this command.

secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha** | **null-md5**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]
no secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]

Syntax Description

3des-ede-cbc-sha	Specifies the encryption null MD5 ciphersuite.
des-cbc-sha	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-md5	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-sha	Specifies encryption ssl_rsa_with_rc4_128_sha ciphersuite.
null-md5	Encryption null MD5 ciphersuite.

Command Default

If no ciphersuite is specified, all ciphersuites are considered.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

A ciphersuite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During a Secure Socket Layer (SSL) handshake, for example, the two nodes negotiate to see which cipher uite they will use when transmitting messages back and forth.

The **secure cipher** command specifies the crypto methods supported by the Lightweight Directory Access Protocol (LDAP) client in Cisco IOS software. This command is applicable only when the **mode secure** command is enabled.

Examples

The following example shows how to configure the crypto methods that are supported by LDAP in Cisco IOS software:

```
Router(config)# ldap server server1
Router(config-ldap-server)# secure cipher des-cbc-sha
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
mode secure	Enables the security mode in LDAP server.

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

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

Command Default

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 *threshold-rate* 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 ISO 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.

Command Default

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

length	Minimum length of a configured password. The default is six characters.

Command Default

The command is not enabled.

Command Modes

Global configuration (config)

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 device 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 not work.

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 passwords 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.

security-group

To specify the membership of security group for an object group, use the **security-group** command in object-group identity configuration mode. To remove the security group identification number from the object group, use the **no** form of this command.

security-group tag-id *number*
no security-group tag-id *number*

Syntax Description

tag-id *number*	Specifies the Security Group Tag (SGT) identification number from 1 to 65535.

Command Default

No security group SGT identification number is defined.

Command Modes

Object-group identity configuration (config-object-group)

Command History

Release	Modification
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Usage Guidelines

A security group can be specified for the object group with an SGT ID. The SGT ID is used by a Security Group Access (SGA) Zone-Based Policy firewall (ZBPF) to apply an enforcement policy by filtering on this SGT ID. The **security-group** command is used in the class map configuration of the SGA ZBPF. Multiple security groups can be specified using this command.

Note A policy map must also be configured for the SGA ZBPF.

Examples

The following example shows how the **security-group** command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# class-map type inspect match-any myclass1
Router(config-cmap)# match group-object security source myobject1
Router(config-cmap)# end
```

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
group-object	Specifies a nested reference to a type of user group.
match group-object security	Matches traffic from a user in the security group.

Command	Description
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
show object-group	Displays the content of all user groups.

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

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 FQDNthat 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 (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	The **address ipv6** keyword was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 (cs-server)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in certificate server 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 is not included in the certificate request.

Command Default

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

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

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.

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.

Command	Description
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
show (cs-server)	Displays the PKI CS configuration.

Command	Description
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

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.

Command Default

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

serial-number	Device serial number. The value is from 0 through infinity.

Command Default

No default behavior or values

Command Modes

Pubkey configuration (config-pubkey-key)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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.
ip-address	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-ymsgr configuration

cfg-appfw-policy-msnmsgr 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
!
```

```
 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 (CWS)

To configure the Cloud Web Security server for content scanning, use the **server** command in parameter-map type inspect configuration mode. To disable content scanning on the Cloud Web Security server, use the **no** form of this command.

server {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with Cloud Web Security server.
allow-all	Allows traffic to flow directly to the Cloud Web Security web server.
block-all	Blocks the traffic to the Cloud Web Security web server.
primary	Specifies the primary Cloud Web Security server.
secondary	Specifies the secondary Cloud Web Security server.
ipv4 *ip-address*	Specifies the IPv4 address of the Cloud Web Security server.
name *domain-name*	Specifies the domain name of the Cloud Web Security server.
port	Specifies the listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **server scansafe** command.

Usage Guidelines

Use the **server** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary Cloud Web Security servers are unreachable, the traffic is dropped if you have configured the **server on-failure block-all** command or, if you have configured the **server on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type cws global
Device(config-profile)# server primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

server_(Diameter)

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

name	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 (ldap)

To associate a particular Lightweight Directory Access Protocol (LDAP) server with a AAA server group, use the **server** command in LDAP server group configuration mode. To delete a server name from the LDAP server, use the **no** form of this command.

server *name*
no server *name*

Syntax Description

name	LDAP server name.

Command Default

No server name is configured in the LDAP server.

Command Modes

LDAP server group configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to associate an LDAP server named server1 with a AAA server group:

```
Router(config)# aaa group server ldap name1
Router(config-ldap-sg)# server server1
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

server (parameter-map)

To configure a set of Domain Name System (DNS) servers with which a given instant messenger application interacts, use the **server** command in parameter-map configuration mode. To disable the configuration, 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 *string*	Specifies the name of the 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.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied. **Note** You cannot configure network addresses that are reserved for special purposes as the server IP address. For example, IP addresses such as 0.0.0.0, 127.0.0.0, and 127.0.0.1 cannot be configured as the server IP address.
range *ip-address-start ip-address-end*	Specifies the range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

At least one server instance should be configured for the configured instant messenger policy to be enforced; otherwise, the parameter map will not have any definitions to enforce.

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. 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 traffic from an instant messenger 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, you must also enable the **ip domain name** and **ip name-server** commands.

To configure more than one set of servers, you can configure 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 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" the DNS responses that are going through the router. The firewall can obtain the necessary addresses from the DNS responses because the DNS inspection engine decodes the DNS response packets and returns a list of addresses to the address database.

When using DNS snooping, network administrators no longer have to give a complete address, such as abcd.example1.example.com; instead, they can specify a partial address with a "wildcard character," such as *.example1.example.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 addressess 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

! 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 hostname-to-address translation.
ip domain name	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
ip name-server	Specifies the address of one or more name servers to be used 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

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

Command Default

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: • **auth-port** *port-number* • **acct-port** *port-number*
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.

Command	Description
aaa new-mode l	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

ip-address	IP address of the selected server.

Command Default

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.
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 {*addresshostname*}
no server address ipv4 {*addresshostname*}

Syntax Description

address	IP address of the server.
hostname	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 ip

To add a server to an Intelligent Services Gateway (ISG) Layer 4 redirect server group, use the **server ip** command in Layer 4 redirect server group configuration mode. To remove a server from a redirect server group, use the **no** form of this command.

server ip *ip-address* [**port** *port*]
no server ip *ip-address* [**port** *port*]

Syntax Description

ip *ip-address*	IP address of the server to be added to the redirect server group.
port *port*	(Optional) TCP port of the server to be added to the redirect server group.

Command Default

A server is not added to the redirect server group.

Command Modes

Layer 4 redirect server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was modified. The *ip-address* argument accepts IPv6 addresses.

Usage Guidelines

Use the **server ip** command in Layer 4 redirect server group configuration mode to add a server, defined by its IP address and TCP port, to a redirect server group. The **server ip** command can be entered more than once to add multiple servers to the server group.

ISG Layer 4 redirection provides nonauthorized users with access to controlled services. Packets sent upstream from an unauthenticated user are forwarded to the server group, which deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services to which they are not logged in.

Examples

The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a redirect server group named “ADVT-SERVER”:

```
redirect server-group ADVT-SERVER
 server ip 10.0.0.0 port 8080
 server ip 10.1.2.3 port 8081
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
show redirect group	Displays information about ISG Layer 4 redirect server groups.

Command	Description
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

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 name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name**command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*
no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

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

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

server scansafe

Note Effective with Cisco IOS Release 15.4(2)T, the **server scansafe** command is replaced by the **server (CWS)** command. See the **server (CWS)** command for more information.

To configure the Cloud Web Security server for content scanning, use the **server scansafe** command in parameter-map type inspect configuration mode. To disable the Cloud Web Security server for content scanning, use the **no** form of this command.

server scansafe {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server scansafe {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with ScanSafe.
allow-all	Allows traffic to flow directly to the web server.
block-all	Blocks the traffic to the web server.
primary	Specifies the primary security as a service (SaaS) server.
secondary	Specifies the secondary SaaS server.
ipv4 *ip-address*	Specifies the IPv4 address of the server.
name *domain-name*	Specifies the domain name of the server.
port	Specifies the SaaS listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was replaced by the **server (CWS)** command.

Usage Guidelines

Use the **server scansafe** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name

or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary towers are unreachable, the traffic is dropped if you have configured the **server scansafe on-failure block-all** command or, if you have configured the **server scansafe on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# server scan-safe primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type content-scan global	Configures a global content-scan parameter map and enters parameter-map type inspect 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 the configuration, use the **no** form of this command.

server vendor {**n2h2** | **websense**} {*ip-addresshostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]
no server vendor {**n2h2** | **websense**} {*ip-addresshostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]

Syntax Description

n2h2	Specifies the N2H2 server.
websense	Specifies the Websense server.
ip-address	IP address of the URL filtering server that you want to configure.
hostname	Hostname of the URL filtering server that you want to configure.
outside	(Optional) Specifies that the vendor server is on the outside network.
port *port-number*	(Optional) Specifies the port number on which the vendor server listens. The range is from 1 to 65535. The default port for the Websense vendor is 15868 and the N2H2 vendor is 4005.
retrans *retransmission-count*	(Optional) Specifies the number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The range is from 1 to 10. The default value is 2.
timeout *seconds*	(Optional) Specifies the length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The range is from 1 to 300. The default value is 6.

Command Default

No URL filtering is performed.

Command Modes

URL parameter-map configuration (config-profile)

Command History

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

Usage Guidelines

Use the **server vendor** 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** command 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 nonnatted 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 shows how to specify the N2H2 vendor server for URL filtering:

```
parameter-map type urlfilter u1
 server vendor n2h2 10.193.64.22 port 3128 outside
```

Related Commands

Command	Description
allow-mode	Turns the default mode of the filtering algorithm on or off.
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 urlfilter	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 RADIUS 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

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(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 *retries*	(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 *string*	(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. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server 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

RADIUS server-group configuration (config-sg-radius)

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.

Release	Modification
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.
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.
15.4(1)T	This command was modified. The **6** keyword was added.

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 forwarding (VRF) instances, 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.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

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

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# 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.
password encryption aes	Enables a type 6 encrypted preshared key.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users to log in to a Cisco NAS and select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ 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 ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [{**0** | **6** | **7**}] *string*]
no server-private

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
name	Name of the private RADIUS or TACACS+ server host.
ipv6-address	IPv6 address of the private RADIUS or TACACS+ server host.
nat	(Optional) Specifies the 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 *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout *seconds*	(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** | **6** | **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. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 6 is entered, the string that is entered is considered to be an advanced encryption scheme [AES] encrypted text. If 7 is entered, the string that is entered is considered to be hidden text.
string	(Optional) Character string specifying the authentication and encryption key.

Command Default

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

Command Modes

TACACS+ server-group configuration (config-sg-tacacs+)

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.

Release	Modification
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.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.2S	This command was modified. The *ipv6-address* argument was added.
15.4(1)T	This command was modified. The **6** keyword was added.

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.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

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

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)# ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ip vrf forwarding cisco
Device(config-if)# exit
```

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.
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs-server host	Specifies a TACACS+ server host.

server-key

To configure the RADIUS key to be shared between a device and RADIUS clients, use the **server-key** command in dynamic authorization local server configuration mode. To remove this configuration, use the **no** form of this command.

server-key [{**0** | **7**}] *word*
no server-key [{**0** | **7**}] *word*

Syntax Description

0	(Optional) An unencrypted key will follow.
7	(Optional) A hidden key will follow.
word	Unencrypted server key.

Command Default

A server key is not configured.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **server-key** command to configure the key to be shared between the Intelligent Services Gateway (ISG) and RADIUS clients.

Examples

The following example configures “cisco” as the shared server key:

```
aaa server radius dynamic-author
 client 10.0.0.1
 server-key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

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-ymsgr configuration

cfg-appfw-policy-msnmsgr 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 automatically convert unencrypted passwords to encrypted 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 [strict]** command.

service password-recovery
no service password-recovery[strict]

Syntax Description

[strict]	(Optional) Restricts device recovery.

Command Default

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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S. The **strict** keyword was added to the **no** form of this command.

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 **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the device. If you are using a device 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 device.

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)

The **no service password-recoverystrict** command does not allow device recovery and prevents the **send break** command, which is used to recover a device from the no service password-recovery feature, from having any effect during bootup.

The **strict** keyword is supported on the Cisco ASR 1000 Series platform, effective from Cisco IOS XE Release 3.10.

Note Since the **strict** keyword makes the router unrecoverable, before you use the keyword, ensure that you configure the password and configuration register, set up the autoboot image, save the configuration and reboot the router. Only if the correct image is autobooted and the enable password works, should you add the **no service password-recovery strict** command to the configuration. If the enable password is lost, the router should be shipped back to the Cisco support center to fix it.

Catalyst Switch Operation

Use the **service password-recovery** command to reenable 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.

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, 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** command to obtain the current configuration register value. If not set to autoboot, then the router needs to be configured to autoboot with the **config-register** command before entering the **no service password-recovery** command.

Once password recovery is disabled, you cannot set the bit pattern value to 0x40, 0x8000, or 0x0 (disables 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 resets the invalid bit pattern and continue to allow modification of nonrelated bit patterns. The configuration register value resets 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** command on a device 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
```

Disabling Password Recovery Example

The following example shows how to disable password recovery capability using the **no service password-recovery strict** command:

```
Router# configure terminal
Router(config)# no service password-recovery strict
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]: yes
.
.
```

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 *slot* argument and the *port*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.

Command Default

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 failsafe 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

slot **/**	Number of the router chassis slot for the network module. The slash mark (/) is required between the *slot* argument and the *port*argument.
port	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.

Command Default

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 *protocol-name policy-map*
no service-policy *protocol-name policy-map*

Syntax Description

protocol-name	Layer 7 application-specific service policy. The supported protocols are as follows: • **h323** —Associates the class with an H.323 protocol Deep Packet Inspection (DPI). • **gtpv0**—General Packet Radio Service (GPRS) Tunnel Protocol version 0 (GTPv0). • **gtpv1**—GTP version 1 (GTPv1). • **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**.
policy-name	Name of the Layer 7 policy map.

Command Default

Attachments are 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.
Cisco IOS XE Release 3.4S	This command was modified. Support for General Packet Radio Service (GPRS) Tunneling Protocol (GTP) was added.

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
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
class type inspect	Specifies the traffic (class) on which an action is to be performed.
inspect	Enables Cisco IOS stateful packet inspection.
log (policy-map)	Generates a log of messages.
match message	Configures the match criterion for a class map on the basis of H.323 protocol messages.
match protocol (zone)	Configures the match criterion for a class map on the basis of the specified protocol.
policy-map type inspect	Creates a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map.
rate-limit	Limits the number of Layer 7 Session Initiation Protocol (SIP) or H.323 protocol messages that strike the Cisco IOS firewall every second.

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

policy-map-name	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** 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.
policy-map	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

policy-map-name	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.
15.1(2)T	Support for IPv6 was added.

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.

session packet

To configure the number of simultaneous traffic packets that can be configured per session, use the **session packet** command in parameter-map type inspect configuration mode. To remove the configured limit, use the **no** form of this command

session packet *number-of-simultaneous-packets*
no session packet *number-of-simultaneous-packets*

Syntax Description

number-of-simultaneous-packets	Number of simultaneous packets per session. The range is from 25 to 100. The default is 25.

Command Default

25 simultaneous packets can be configured per session.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

All packets that exceed the configured limit are dropped by the zone-based policy firewall.

You must configure either the **parameter-map type inspect** or the **parameter-map type inspect global** command before configuring the **session packet** command.

The session packet limit configured under the **parameter-map type inspect** command has precedence over the limit configured under the **parameter-map type inspect global** command.

Examples

The following example shows how to configure the number of simultaneous packets per flow under the **parameter-map type inspect** command:

```
Device(config)# parameter-map type inspect inspect-pmap
Device(config-profile)# session packet 35
```

The following example shows how to configure the number of simultaneous packets per flow under the **parameter-map type inspect global** command:

```
Device(config)# parameter-map type inspect inspect global
Device(config-profile)# session packet 55
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type inspect global	Defines a global inspect parameter map and enter parameter-map type inspect configuration mode.
show parameter-map type inspect	Displays user-configured or default inspect-type parameter maps.

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

Default value is unlimited.

Command Modes

Parameter-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **sessions maximum** command to limit the number of inspect sessions that match a certain class. Session limiting is activated when this parameter is configured.

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 abc
 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.

sessions rate

To specify a time duration for defining the session quota, use the **sessions rate** command in parameter-map type inspect configuration mode. To disable the specified time duration, use the **no** form of this command.

sessions rate {**high** *number-of-connections* | **low** *number-of-connections*} **time** *duration*
no sessions rate {**high** | **low**}

Syntax Description

high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.
low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
time	Specifies the time for which the session rate limit is applied.
duration	Time duration, in seconds, for which the session rate is limited. Range is from 1 to 2147483.

Command Default

The system does not start or stop deleting half-open sessions.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

You can use the **one-minute** command to define session quota within one minute. You can use the **sessions rate** command to specify the time duration in which session quota can be defined. The **sessions rate** command and the **one-minute** command are mutually exclusive. If the **one-minute** command is configured in an inspect parameter map, the **sessions rate** command is rejected, and vice versa.

Examples

The following example shows how to configure a session rate of 25 seconds:

```
Router> enable
Router# configure terminal
Router(config)# parameter-type inspect type par1
Router(config-profile)# sessions-rate high 250 time 25
```

Related Commands

Command	Description
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

server scansafe

Note Effective with Cisco IOS Release 15.4(2)T, the **server scansafe** command is replaced by the **server (CWS)** command. See the **server (CWS)** command for more information.

To configure the Cloud Web Security server for content scanning, use the **server scansafe** command in parameter-map type inspect configuration mode. To disable the Cloud Web Security server for content scanning, use the **no** form of this command.

server scansafe {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server scansafe {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with ScanSafe.
allow-all	Allows traffic to flow directly to the web server.
block-all	Blocks the traffic to the web server.
primary	Specifies the primary security as a service (SaaS) server.
secondary	Specifies the secondary SaaS server.
ipv4 *ip-address*	Specifies the IPv4 address of the server.
name *domain-name*	Specifies the domain name of the server.
port	Specifies the SaaS listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was replaced by the **server (CWS)** command.

Usage Guidelines

Use the **server scansafe** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name

or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary towers are unreachable, the traffic is dropped if you have configured the **server scansafe on-failure block-all** command or, if you have configured the **server scansafe on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# server scan-safe primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type content-scan global	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.