clear ip access-list counters through crl-cache none

clear ip access-template

To clear statistical information on the access template, use the **clear ip access-template** command in privileged EXEC mode.

clear ip access-template {*access-list-number*| *name*} *dynamic-name* {*source-address source-wildcard-bit*| **any**| **host** {*hostname*| *source-address*}} {*destination-address dest-wildcard-bit*| **any**| **host** {*hostname*| *destination-address*}}

Syntax Description

access-list-number	Access list number. Range is from 100 to 199 for an IP extended access list and from 2000 to 2699 for an expanded-range IP extended access list.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source host name.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added.

Examples

This example shows how to clear statistical information on the access list:

```
Router#
clear ip access-template 201 list1 any 172.0.2.1 172.0.2.2
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache**command in privileged EXEC mode.

clear ip admission cache {*****| **host ip address**}

Syntax Description

*	Clears all IP admission cache entries and associated dynamic access lists.
host ip address	Clears all IP admission cache entries and associated dynamic access lists for the specified host.

Command Modes

Privileged EXEC #

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to clear entries from the admission control cache before they time out.

Examples

The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

Related Commands

Command	Description
show ip admission cache	Displays the admission control entries or the running admission control configuration.

clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** command in EXEC mode.

clear ip audit configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
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 **clear ip audit configuration** EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.

Examples

The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** command in EXEC mode.

clear ip audit statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
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 **clear ip audit statistics** EXEC command to reset statistics on packets analyzed and alarms sent.

Examples

The following example clears all IP audit statistics:

```
clear ip audit statistics
```

clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

clear ip auth-proxy cache {*****| *host-ip-address*}

Syntax Description

*	Clears all authentication proxy entries, including user profiles and dynamic access lists.
host-ip-address	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

Command Modes

EXEC

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

Use this command to clear entries from the translation table before they time out.

Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

Related Commands

Command	Description
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries in Privileged EXEC configuration command mode, use the **clear ip auth-proxy watch-list** command.

clear ip auth-proxy watch-list {*ip-addr*| *****}

Syntax Description

ip-addr	IP address to be deleted from the watch list.
*	All watch-list entries from the watch list.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
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

This command is supported on the systems that are configured with a Supervisor Engine 2 Supervisor Engine 2 only.

If you see entries in the watch list that you suspect are not valid, you can enter the **clear ip auth-proxy watch-list** command to clear them manually instead of waiting for the watch list to expire.

Examples

This example shows how to delete a single watch-list entry:

```
Router# clear
 ip auth-proxy watch-list 10.0.0.2
Router#
```

This example shows how to delete all watch-list entries:

```
Router# clear
 ip auth-proxy watch-list *
Router#
```

Related Commands

Command	Description
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface and QoS filtering and enter the ARP ACL configuration submode.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

clear ip inspect ha

To delete the Firewall stateful failover sessions information from a router’s memory, use the **clear ip inspect ha**command in privileged EXEC mode.

clear ip inspect ha [**sessions all**| **statistics**]

Syntax Description

sessions all	(Optional) Clears all the firewall HA sessions.
statistics	(Optional) Clears the HA statistics on the device.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

If the **clear ip inspect ha sessions all**command is used on the standby device, the standby HA sessions are cleared. This initiates re-synchronization of all HA sessions from the active device to the standby device.

Examples

The following example shows all sessions being deleted:

```
Router# clear ip inspect ha sessions all
```

The following example shows statitics being deledted.

```
Router# clear ip inspect ha statistics
```

clear ip inspect session

To delete Context-Based Access Control (CBAC) configuration and session information from a router's memory, use the **clear ip inspect session**command in privileged EXEC mode.

clear ip inspect session *session-address*

Syntax Description

session-address	Deletes a specific session; the format is 0-FFFFFFFF.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Sessions consist of control channels and data channels.

Use the **clear ip inspect session** command to delete a control channel or a data channel. If you specify a control channel session, then data channel sessions may also be deleted, depending on the application protocols being used. If you specify a data channel session, then only that specific session is deleted.

If you attempt to delete a session and the **clear ip inspect session** command is not supported for the specified protocol, then an error message is generated.

If you want to delete a specific session, use the **show ip inspect session** command to display all session addresses.

Note

The **clear ip inspect session** command is recommended for advanced users only because it may disrupt network operations if traffic is still flowing through the session.

Examples

The following example displays the current session addresses:

```
Router# show ip inspect session
Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following example shows a specific session being deleted:

```
Router# clear ip inspect session 25A6E1C
```

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

clear ip ips configuration

To disable Cisco IOS Firewall Intrusion Prevention System (IPS), remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode.

clear ip ips configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit configuration** command to the **clear ip ips configuration** command.
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.

Examples

The following example clears the existing IPS configuration:

```
clear ip ips configuration
```

clear ip ips statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip ips statistics** command in privileged EXEC mode.

clear ip ips statistics [**vrf vrf-name**]

Syntax Description

vrf	(Optional) Resets statistics on packets analyzed and alarms sent per VRF.
vrf-name	User specific VRF.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit statistics** command to the **clear ip ips statistics** command.
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.
12.4(20)T	The **vrf** *keyword and argument were added.*

Examples

The following example clears all Intrusion Protection System (IPS) statistics:

```
clear ip ips statistics
```

Examples

The following example displays the output of the clear ip ips statistics vrf vrf-namecommand:

```
Router# clear ip ips statistics vrf VRF_600
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

clear ip sdee

To clear Security Device Event Exchange (SDEE) events or subscriptions, use the **clear ip sdee** command in privileged EXEC mode.

clear ip sdee {**events**| **subscriptions**}

Syntax Description

events	Clears SDEE events from the event buffer.
subscriptions	Clears SDEE subscriptions.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Because subscriptions are properly closed by the Cisco IOS Intrusion Prevention System (IPS) client, this command is typically used only to help with error recovery.

Examples

The following example shows how to clear all open SDEE subscriptions on the router:

```
Router# clear ip sdee subscriptions
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
ip sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

clear ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 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

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

Related Commands

Command	Description
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in user EXEC mode.

clear ip urlfilter cache {*ip-address*| **all**} [**vrf** *vrf-name*]

Syntax Description

ip-address	Clears the cache table of a specified server IP address.
all	Clears the cache table completely.
vrf *vrf-name*	(Optional) Clears the cache table only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

User EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair was added.
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

The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

Examples

The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

The following example shows how to clear the cache table of all IP addresses in the vrf named bank.

```
clear ip urlfilter cache all vrf bank
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

clear ipv6 access-list

To reset the IPv6 access list match counters, use the **clear ipv6 access-list**command in privileged EXEC mode.

clear ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

Usage Guidelines

The **clear ipv6 access-list**command is similar to the **clear ip access-list counters**command, except that it is IPv6-specific.

The **clear ipv6 access-list**command used without the *access-list-name*argument resets the match counters for all IPv6 access lists configured on the router.

This command resets the IPv6 global ACL hardware counters.

Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Router# clear ipv6 access-list marketing
```

Related Commands

Command	Description
hardware statistics	Enables the collection of hardware statistics.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

clear ipv6 inspect

To remove a specific IPv6 session or all IPv6 inspection sessions, use the **clear ipv6 inspect**command in privileged EXEC mode.

clear ipv6 inspect {**session** *session-number*| **all**}

Syntax Description

session *session-number*	Indicates the number of the session to clear.
all	Clears all inspection sessions.

Command Default

Inspection sessions previously configured are unaffected.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example clears all inspection sessions:

```
Router# clear ipv6 inspect all
```

Related Commands

Command	Description
ipv6 inspect name	Applies a set of inspection rules to an interface.

clear ipv6 snooping counters

To remove counter entries, use the **clear ipv6 snooping counters**command in privileged EXEC mode.

clear ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Clears the counter of entries that match the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **clear ipv6 snooping counters**command removes counters from all the configured interfaces. You can use the optional **interface** *type number* keyword and argument to remove counters from the specified interface.

Examples

The following example shows how to remove entries from the counter:

```
Router# clear
 ipv6 snooping counters
```

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

clear kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	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

Credentials are deleted when this command is issued.

Cisco supports Kerberos 5.

Examples

The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds

Default Principal: chet@cisco.com
Valid Starting          Expires                 Service Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/CISCO.COM@CISCO.COM
Router# clear kerberos creds
Router# show kerberos creds

No Kerberos credentials.
```

Related Commands

Command	Description
show kerberos creds	Displays the contents of your credentials cache.

clear ldap server

To clear the TCP connection with the Lightweight Directory Access Protocol (LDAP) server, use the **clear ldap server** command in privileged EXEC mode.

clear ldap server *server-name* **[statistics]**

Syntax Description

server-name	LDAP server name.
statistics	(Optional) Clears the statistical information.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Statistics details are not cleared when the server is cleared. To clear the statistics information, use the **statistics** keyword.

Examples

The following example shows how to clear the statistical information:

```
Router# clear ldap server server1 statistics
```

Related Commands

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

clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

clear logging ip access-list cache

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

Examples

This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router#
clear logging ip access-list cache
```

Related Commands

Command	Description
logging ip access-list cache (global configuration)	Configures the OAL parameters globally.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

clear parameter-map type protocol-info

To clear the Domain Name System (DNS) cache for name resolution of servers within a parameter map, use the **clear parameter-map type protocol-info** command in privileged EXEC mode.

clear parameter-map type protocol-info dns-cache *dns-name* [**ip-address** *ip-address*]

Syntax Description

dns-cache *dns-name*	Cache of the specified DNS server will be cleared.
ip-address *ip-address*	(Optional) Specified IP address is removed from the cache of the DNS server. If an IP address is not specified, all IP addresses from the specified DNS server are cleared from the cache.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to clear the cache of the DNS server “sdsc.msg.yahoo.com:

```
Router#
clear parameter-map type protocol-info dns-cache sdsc.msg.yahoo.com
```

Related Commands

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

clear policy-firewall

To reset the information collected by the firewall, use the **clear policy-firewall** command in user EXEC or privileged EXEC mode.

clear policy-firewall {**session** [*session address*| **class-map** *class-map-name*| **policy-map** *policy-map-name*]| **stats** [*drop-counters*]| **summary-log**| **zone-pair**}

Syntax Description

session *session address*	Clears the session.
class-map *class-map-name*	Clears the class map.
policy-map *policy-map-name*	Clears the policy map.
stats [*drop-counters*]	Clears the statistics and the drop-counters.
summary-log	Clears the summary log.
zone-pair	Clears the zone-pair.

Command Default

The firewall information is not cleared.

Command Modes

EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to clear the information that is collected by the firewall. The cleared counters include drop-counters, summary-log buffers, sessions and zone pairs.

Examples

The following example shows how to clear the zone pair:

```
Router(mode-prompt
)# clear policy-firewall zone-pair
```

Related Commands

Command	Description
show policy-firewall config	Displays the entire configuration of the firewall in the router.
show policy-firewall sessions	Displays the details of the firewall sessions.
show policy-firewall stats	Displays the statistics of all firewall activities in the router.
show policy-firewall summary-log	Displays the summary log of the firewall.

clear policy-firewall stats global

To reset the global statistics collected by the firewall, use the **clear policy-firewall stats global** command in user EXEC or privileged EXEC mode.

clear policy-firewall stats global

Syntax Description

This command has no arguments or keywords.

Command Default

The firewall global statistics are not cleared.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Use this command to clear the statistics collected by the firewall.

Examples

The following example shows how to clear the global firewall statistics:

```
Router# clear policy-firewall stats global
```

Related Commands

Command	Description
show policy-firewall stats global	Displays global firewall statistics.

clear policy-firewall stats vrf

To clear the policy firewall statistics at a VPN Routing and Forwarding (VRF) level, use the **clear policy-firewall stats vrf** command in privileged EXEC mode.

clear policy-firewall stats vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the configured policy firewall VRF statistics:

```
Router# clear policy-firewall stats vrf vrf1
```

Related Commands

Command	Description
show policy-firewall stats vrf	Displays VRF-level policy firewall statistics.

clear policy-firewall stats vrf global

To clear the global VPN Routing and Forwarding (VRF) policy firewall statistics, use the **clear policy-firewall stats vrf global** command in privileged EXEC mode.

clear policy-firewall stats vrf global

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the global policy firewall statistics:

```
Router# clear policy-firewall stats vrf global
```

Related Commands

Command	Description
show policy-firewall stats vrf global	Displays information about the global VRF firewall policies.

clear policy-firewall stats zone

To clear the policy firewall statistics at a zone level, use the **clear policy-firewall stats zone** command in privileged EXEC mode.

clear policy-firewall stats zone *zone-name*

Syntax Description

zone-name	Name of the zone.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the configured policy firewall zone statistics:

```
Router# clear policy-firewall stats zone zone1
```

Related Commands

Command	Description
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.

clear port-security

To delete configured secure MAC addresses and sticky MAC addresses from the MAC address table in the Priveleged EXEC configuration command mode, use the **clear port-security**command.

clear port-security dynamic [**address mac-addr**| **interface interface-id**] [**vlan vlan-id**]

Syntax Description

address *mac-addr*	(Optional) Deletes the specified secure MAC address or sticky MAC address.
interface *interface-id*	(Optional) Deletes all secure MAC addresses and sticky MAC addresses on the specified physical port or port channel.
vlan *vlan-id*	(Optional) Deletes the specified secure MAC address or sticky MAC address from the specified VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The output of this command was changed to support sticky MAC addresses on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on negotiated trunks only.

If you enter the **clear port-security**command without adding any keywords or arguments, the switch removes all the secure MAC addresses and sticky MAC addresses from the MAC address table.

If you enter the **clear port-security dynamic interface***interface-id* command, all the secure MAC addresses and sticky MAC addresses on an interface are removed from the MAC address table.

You can verify that the information was deleted by entering the **show port-security** command.

Examples

This example shows how to remove a specific secure address from the MAC address table:

```
Router# clear port-security dynamic address 0008.0070.0007
Router#
```

This example shows how to remove all the secure MAC addresses and sticky MAC addresses learned on a specific interface:

```
Router# clear port-security dynamic interface gigabitethernet0/1
Router#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
switchport port-security mac-address	Adds a MAC address to the list of secure MAC addresses.

clear radius

To clear the RADIUS server information, use the **clear radius**command in privileged EXEC mode.

clear radius {**sg-stats**| **statistics**}

Syntax Description

sg-stats	Clears the RADIUS server group statistics.
statistics	Clears the RADIUS statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to clear the RADIUS statistics information:

```
Router# clear radius statistics
```

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.

clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server**command in privileged EXEC mode.

clear radius local-server {**statistics**| **user** *username*}

Syntax Description

statistics	Clears the display of statistical information.
user	Unblocks the locked username specified.
username	Locked username.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows how to unblock the locked username “smith”:

```
Router# clear radius local-server user smith
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.

clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a SSL VPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

clear webvpn nbns [**context** {*name*| **all**}]

Syntax Description

context	(Optional) Clears NBNS statistics for a specific context or all contexts.
name	Clears NBNS statistics for a specific context.
all	Clears NBNS statistics for all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Entering this command without any keywords or arguments clears all NBNS counters on the network device.

Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

Related Commands

Command	Description
clear webvpn session	Clears remote users sessions on a SSL VPN gateway.
clear webvpn stats	Clears application and access counters on a SSL VPN gateway.

clear webvpn session

To clear SSL VPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

clear webvpn session [**user** *name*] **context** {*name*| **all**}

Syntax Description

user *name*	(Optional) Clears session information for a specific user.
context *name* | **all**	Clears session information for a specific context or all contexts.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a SSL VPN gateway.
clear webvpn stats	Clears application and access counters on a SSL VPN gateway.

clear webvpn stats

To clear (or reset) SSL VPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

clear webvpn stats [[**cifs**| **citrix**| **mangle**| **port-forward**| **sso**| **tunnel**] [**context** {*name*| **all**}]]

Syntax Description

cifs	(Optional) Clears Windows file share (CIFS) statistics.
citrix	(Optional) Clears Citrix application statistics.
mangle	(Optional) Clears URL mangling statistics.
port-forward	(Optional) Clears port forwarding statistics.
sso	(Optional) Clears statistics for Single SignOn (SSO) activities.
tunnel	(Optional) Clears Cisco AnyConnect VPN Client tunnel statistics.
context *name* | **all**	(Optional) Clears information for either a specific context or all contexts.

Command Default

If no keywords are entered, all SSL VPN application and access counters are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **sso** keyword was added.

Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, SSO, and Cisco AnyConnect VPN Client tunnels. The counters are cleared for either the specified context or all contexts on the SSL VPN gateway.

Examples

The following example clears all statistics counters for all SSL VPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a SSL VPN gateway.
clear webvpn session	Clears remote users sessions on a SSL VPN gateway.

clear xsm

To clear XML Subscription Manager (XSM) client sessions, use the **clear xsm** command in privileged EXEC mode.

clear xsm [**session** *number*]

Syntax Description

session	(Optional) Specifies an XSM client session to clear.
number	(Optional) ID number of the specific XSM client session to be cleared.

Command Default

No XSM client sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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

This command disconnects all active client sessions (such as with a VPN Device Manager [VDM]) on the XSM server, unless you state a specific session number. This command allows troubleshooting of the XSM server and its active clients by allowing individual clients to be disconnected. Use the **show xsm status** command to obtain specific session numbers.

When the optional **session** *number* keyword and argument are not used, the **clear xsm** command clears all XSM client sessions.

Examples

The following example shows how to clear all XSM client sessions:

```
Router# clear xsm
```

The following example shows how to clear XSM client session 10:

```
Router# clear xsm session 10
```

Related Commands

Command	Description
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

clear zone-pair

To clear the policy map counters, inspect sessions, or the URL filter cache on a zone-pair, use the **clear zone-pair** command in privileged EXEC mode.

clear zone-pair [*zone-pair-name*] {**counter**| **inspect session**| **urlfilter cache**}

Syntax Description

zone-pair-name	(Optional) Name of the zone-pair on which counters, inspect sessions, or the uRL filter cache are cleared.
counter	Clears the policy-map counters. Resets the statistics of the inspect type policy map on the specified zone-pair.
inspect session	Deletes the inspect sessions on the specified zone-pair.
urlfilter cache	Clears the URL filter cache on the specified zone-pair.

Command Default

Disabled (it is not necessary to enter this command).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888.

Usage Guidelines

If you do not specify a zone-pair name, the policy map counters, sessions, or the URL filter cache are cleared for all the configured zone-pairs.

Examples

The following example deletes the inspect sessions on the zp zone-pair:

```
Router# clear zone-pair zp inspect session
```

The following example clears the URL filter cache on the zp zone-pair.

```
Router# clear zone-pair zp urlfilter cache
```

clid

To preauthenticate calls on the basis of the Calling Line IDentification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

clid [**if-avail**| **required**] **[accept-stop]** [**password** *password*]

no clid [**if-avail**| **required**] **[accept-stop]** [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as ctype or dnis from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element. The default password string is cisco.

Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
 group radius
 clid required
```

Related Commands

Command	Description
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

client

To specify a RADIUS client from which a device can accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*hostname* | *ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string* | *string*} | **vrf** *vrf-id*]

no client {*hostname* | *ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string* | *string*} | **vrf** *vrf-id*]

Syntax Description

hostname	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
server-key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (clear text) shared key.
vrf *vrf-id*	(Optional) Virtual routing and forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

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

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added.

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 **client** command to specify the RADIUS clients for which the router can act as server.

Examples

The following example shows how to configure the router to accept requests from the RADIUS client at IP address 10.0.0.1:

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

Related Commands

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

client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list**command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

client authentication list *list-name*

no client authentication list *list-name*

Syntax Description

list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.

Command Default

No default behaviors or values

Command Modes

ISAKMP profile configuration (config-isakmp-profile)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11.5)	Xauth no longer has to be disabled globally for it to be enabled on a profile basis.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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.

Before configuring Xauth, you must set up an authentication list using AAA commands.

Xauth can be enabled on a profile basis if it has been disabled globally.

Effective with Cisco IOS Release 12.4(11.5), Xauth on either a server or client does not need to be disabled globally to enable it on profile basis.

Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
 client authentication list xauthlist
```

The following example shows that Xauth has been disabled globally and enabled for the profile “nocerts”:

```
no crypto xauth FastEthernet0/0
!
crypto isakmp policy 1
 encr aes
 group 14
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 14
crypto isakmp client configuration group HRZ
crypto isakmp client configuration group vpngroup
 key cisco123
 pool vpnpool
crypto isakmp profile cert_sig
   match identity group HRZ
   isakmp authorization list isakmpauth
   client configuration address respond
   client configuration group HRZ
crypto isakmp profile nocerts
   match identity group vpngroup
   client authentication list vpn-login
   isakmp authorization list isakmpauth
   client configuration address respond
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address**command in ISAKMP profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

client configuration address {**initiate**| **respond**}

no client configuration address {**initiate**| **respond**}

Syntax Description

initiate	Router will attempt to set IP addresses for each peer.
respond	Router will accept requests for IP addresses from any requesting peer.

Command Default

IKE configuration is not enabled.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples

The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called “vpnprofile”:

```
crypto isakmp profile vpnprofile
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

client configuration group

To associate a group with the peer that has been assigned an Internet Security Association Key Management Protocol (ISAKMP) profile, use the client configuration group command in crypto ISAKMP profile configuration mode. To disable this option, use the no form of this command.

client configuration group *group-name*

no client configuration group *group-name*

Syntax Description

group-name	Name of the group to be associated with the peer.

Command Default

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **client configuration group** command is used after the crypto map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following example shows that the group “some_group” is to be associated with the peer:

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

Related Commands

Command	Description
match certificate (ISAKMP)	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

client inside

To specify the inside interface for the FlexVPN client, use the **client inside** command in IKEv2 FlexVPN client profile configuration mode. To disable the inside interface, use the **no** form of this command.

client inside *interface-type number*

no client inside *interface type number*

Syntax Description

interface-type number	Interface type and number.

Command Default

The inside interface is not specified.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

You can specify more than one inside interface in a FlexVPN client profile. The inside interfaces can be shared across FlexVPN client profiles.

Note Enabling this command is optional. Any changes to this command terminates the active session.

Examples

The following example shows how to specify the inside interface:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# peer 1 10.0.0.1
Router(config-ikev2-flexvpn)# client inside Ethernet 1
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

client pki authorization list

To specify the authorization list of AAA servers that will be used to obtain per-user AAA attributes on the basis of the username that is constructed from the certificate, use the **client pki authorization list** command in crypto ISAKMP profile configuration mode. To disable the list name, use the **no** form of this command.

client pki authorization list *listname*

no client pki authorization list *listname*

Syntax Description

listname	Definition of the argument needed, including syntax-level defaults, if any.

Command Default

User attributes are not pushed to the remote device.

Command Modes

Crypto ISAKMP profile configuration (config-isakmp-profile)

Command History

Release	Modification
12.4(4)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

This command is used inside the crypto Internet Security Association and Key Management Protocol (ISAKMP) profile.

Examples

The following example shows that user attributes are to be obtained from the AAA server (list name “usrgrp”) and pushed to the remote device:

```
crypto isakmp profile ISA-PROF
   match certificate CERT-MAP
   isakmp authorization list usrgrp
   client pki authorization list usrgrp
   client configuration address respond
   client configuration group pkiuser
   virtual-template 2
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPsec user sessions.

client recovery-check interval

To set the interval of time for the client group member (GM) to monitor for control-plane errors, use the **client recovery-check interval** command in GDOI group configuration mode. To remove the control-plane error monitoring, use the **no** form of this command.

client recovery-check interval *interval*

no client recovery-check interval *interval*

Syntax Description

interval	Specifies the waiting period in seconds between consecutive recovery registrations. The range is from 100 to 1000 seconds.

Command Default

Control-plane error monitoring is disabled.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **client recovery-check interval** command to ensure GMs reactively try to recover from data plane errors, such as invalid stateful packet inspection (SPI) and Time-Based Anti-Replay (TBAR) errors, by registering to the configured key servers (KSs) to obtain the latest policies.

Examples

The following example shows how to enable the GM to monitor for control-plane errors every 300 seconds:

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# client recovery-check interval 300
```

Related Commands

Command	Description
crypto gdoi group	Creates a GDOI group and enters GDOI group configuration mode.

client connect

To assign a tunnel interface to the FlexVPN client, use the **client connect** command in IKEv2 FlexVPN client profile configuration mode. To remove the tunnel interface, use the **no** form of this command.

client connect tunnel *number*

no client connect tunnel *number*

Syntax Description

tunnel	Tunnel interface.
number	Tunnel interface number.

Command Default

A tunnel interface is not assigned to the FlexVPN client.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** and the **interface** command with the **tunnel** keyword.

You can configure only one tunnel interface for a FlexVPN client profile.

Note Any changes to this command terminates the active session.

Examples

The following example shows how to assign the tunnel interface 1 to the FlexVPN client profile "client1":

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# client inside Ethernet 1
Router(config-ikev2-flexvpn)# client connect tunnel 1
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

Command	Description
interface	Specifies an interface.

client rekey encryption

To set the client acceptable rekey ciphers for the key-encryption-key (KEK), use the **client rekey encryption** command in GDOI group configuration mode. To remove the client acceptable rekey ciphers, use the **no** form of this command.

client rekey encryption *cipher* [... [*cipher*]]

no client rekey encryption

Syntax Description

cipher	Any of the following ciphers: • **3des-cbc** —Specifies triple Data Encryption Standard (3DES) in Cipher-block chaining (CBC) mode (no longer recommended). • **aes 128** —Specifies 128-bit Advanced Encryption Standard (AES). • **aes 192** —Specifies 192-bit AES. • **aes 256** —Specifies 256-bit AES. • **des-cbc** —Specifies DES in CBC mode (no longer recommended).

Command Default

Any cipher assigned by the key server is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
Cisco IOS Release 15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

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.

Use the **client rekey encryption** command to specify the acceptable ciphers for KEK. Multiple ciphers can be specified. If a cipher is not set using this command, the cipher assigned by the key server is accepted.

Examples

The following example shows how to set the acceptable ciphers for KEK:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey encryption aes 128 aes 192 aes 256
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

client rekey hash

To set acceptable hash algorithms for rekey message signing, use the **client rekey hash** command in GDOI group configuration mode. To remove acceptable hash algorithms, use the **no** form of this command.

client rekey hash *hash1* [...[*hash4*]]

no client rekey hash *hash1* [...[*hash4*]]

Syntax Description

hash	Hash for rekey message signing. You can use any combination of the following values: **sha**, **sha256**, **sha384**, and **sha512**.

Command Default

Any hash selected by the key server (KS) is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.2(4)M	This command was modified. The **sha256**, **sha384**, and **sha512** keywords were added.

Usage Guidelines

Use the **client rekey hash** command to select the acceptable hash for the rekey message signing. If a hash is not set using this command, the hash selected by the KS is accepted.

Suite B requires SHA-256, SHA-384, or SHA-512. Suite B is a set of cryptographic algorithms that includes Galois Counter Mode Advanced Encryption Standard (GCM-AES) as well as algorithms for hashing, digital signatures, and key exchange.

Examples

The following example shows how to set the acceptable hash for rekey message signing:

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server address ipv4 192.10.2.10
Device(config-gdoi-group)# client rekey hash sha512
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

client transform-sets

To specify up to 6 acceptable transform-set tags used by the traffic-encryption-key (TEK) for data encryption or authentication, use the **client transform-sets**command in GDOI group configuration mode. To remove the acceptable transform-set tags, use the **no** form of this command.

client transform-sets *transform-set-name1* [... [*transform-set-name6*]]

no client transform-sets

Syntax Description

transform-set-name	Transform-tags used by the TEK for data encryption or authentication.

Command Default

The transform-set selected by the key server is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
Cisco IOS Release 15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **client transform-sets** command to specify up to 6 transform-set tags used by the TEK for data encryption or authentication. If this command is not issued, the transform-set selected by the key server is accepted. The security protocol configured in the transform set must be Encapsulating Security Payload (ESP), which is the only protocol supported by GETVPN in Cisco IOS XE Release 2.4.1.

Examples

The following example shows how to set the transform-set tags used by TEK for data encryption or authentication:

```
Router# configure terminal
Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac
Router(cfg-crypto-trans)# exit
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# client transform-sets g1
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto ipsec transform-set	Defines a transform set--an acceptable combination of security protocols and algorithms.

commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands**command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

Syntax for Adding and Deleting Commands to a View

commands *parser-mode* {**include**| **include-exclusive**| **exclude**} **[all]** [*command*]

no commands *parser-mode* {**include**| **include-exclusive**| **exclude**} **[all]** [*command*]

Syntax for Adding and Deleting Interfaces to a View

commands *parser-mode* {**include**| **include-exclusive**} **[all]** [**interface** *name*] [*command*]

no commands *parser-mode* {**include**| **include-exclusive**} **[all]** [**interface** *name*] [*command*]

Syntax Description

parser-mode	Mode in which the specified command exists. See the table in the “Usage Guidelines” section for a list of available options for this argument.
include	Adds a specified command or a specified interface to the view and allows the same command or interface to be added to a view.
include-exclusive	Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views.
exclude	Denies access to commands in the specified parser mode. **Note** This keyword is available only for command-based views.
all	(Optional) A “wildcard” that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view.
command	(Optional) Command that is added to the view. **Note** If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate.
interface *name*	(Optional) Interface that is added to the view.

Command Default

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The **exclude** keyword and the **interface** *interface-name* option were added.
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

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keyword) or denied access (via the **exclude** keyword) to all commands within the specified parser mode.

parser-mode Options

The table below shows some of the keyword options for the *parser-mode*argument in the **commands**command. The available mode keywords vary depending on your hardware and software version. To display a list of available mode options on your system, use the **commands ?**command.

Table 1: parser-mode Argument Options

Command	Description
accept-dialin	VPDN accept-dialin group configuration mode
accept-dialout	VPDN accept-dialout group configuration mode
address-family	Address family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode

Command	Description
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signaling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request configuration mode
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map configuration mode
crypto-transform	Crypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	EXEC mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map-class configuration mode
map-list	Map-list configuration mode
mpoa-client	MPOA client
mpoa-server	MPOA server
null-interface	Null interface configuration mode

Command	Description
preaut	AAA Preauth definitions
request-dialin	VPDN accept-dialin group configuration mode
request-dialout	VPDN accept-dialout group configuration mode
route-map	Route-map configuration mode
router	Router configuration mode
rsvp_policy_local	RSVP local policy configuration mode
rtr	RTR entry configuration mode
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to add the privileged EXEC command **show version** to both CLI views “first” and “second.” Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include show version
```

```
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view “first” to execute all commands that start with the word “show” except the **show interfaces** command, which is excluded by the view “second”:

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

configuration url

To specify on a server the URL that an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange, use the **configuration url** command in global configuration or IKEv2 authorization policy configuration mode. To delete the URL, use the **no** form of this command.

configuration url *url*

no configuration url *url*

Syntax Description

url	Specifies the URL the Easy VPN remote device must use to get the configuration from the server. • The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.

Command Default

An Easy VPN remote device cannot request a configuration from a server in a Mode Configuration Exchange.

Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.4(4)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

After the server "pushes" the URL to a Cisco Easy VPN remote device, the remote device can download the content located at the URL site and apply the configuration content to its running configuration.

Before this command can be configured, the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command must already have been configured.

Examples

The file served by the configuration URL should have a Cisco IOS command-line interface(CLI) listing. The listing can have an optional "transient" section. The keyword to begin the transient section is "!%transient," and the keyword should be on a single line. A persistent section can be optionally identified by the keyword “!%persistent,” also shown on a single line. An example of a CLI listing follows:

```
ip cef
cdp advertise-v2
!%transient
ip domain-name example.com
ntp server 10.2.3.4
ntp update-calendar
```

In the above example, the first two lines stay in the configuration even after the tunnel is disconnected (but they are not written into the nonvolatile configuration). The last three lines are effective only as long as the tunnel is “up.”

The following example shows that a server has specified the URL the Easy VPN remote device must use to download the URL:

```
crypto isakmp client configuration group group1
 configuration url http://10.10.8.8/easy.cfg
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

configuration version

To specify on a server the version that a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange, use the **configuration version** command in global configuration or IKEv2 authorization policy configuration mode. To delete the version number, use the **no** form of this command.

configuration version *version-number*

no configuration version *version-number*

Syntax Description

version-number	Specifies the version of the configuration. • The version number will be an unsigned integer in the range 1 through 32767.

Command Default

A version number is not sent.

Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.4(4)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

Before this command can be configured, the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command must already have been configured.

Examples

The following example shows that a server has specified the version number a Cisco Easy VPN remote device must use to obtain that particular configuration version:

```
crypto isakmp client configuration group group1
 configuration version 10
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

config-exchange

To enable the configuration exchange options, use the **config-echange** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

config-exchange{**request**| **set**{**accept**| **send**}}

no config-exchange{**request**| **set**{**accept**| **send**}}

Syntax Description

request	Enables configuration exchange request.
set	Enables configuration exchange request set options.
accept	Accepts configuration exchange request set.
send	Enables sending of configuration exchange set.

Command Default

The configuration exchange options is enabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced. This command replaces the **config-mode set** command.

Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 profile** command. Use this command to enable the exchange of configuration options. The acceptance of configuration exchange options is enabled by default.

Examples

The following example show how to set the acceptance of configuration exchange request for the IKEv2 profile “profile2”:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# config-exchange set accept
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

config-mode set

Note Effective with Cisco IOS Release 15.2(2)T, the **config-mode set** command is replaced by the **config-exchange** command. See the **config-exchange** command for more information.

To enable sending the configuration mode set, use the **config-mode set** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

config-mode set

no config-mode set

Syntax Description

This command has no keywords or arguments.

Command Default

The configuration mode set is enabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.2(2)T	This command was replaced by the **config-exchange** command.

Usage Guidelines

Before using this command, you must first configure the crypto ikev2 profile command. Use this command to enable sending of configuration mode set. The acceptance of configuration mode set is enabled by default.

Examples

The following example show how to configure the configuration mode set for the IKEv2 profile “profile1”:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# config-mode set
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

connect

To connect the FlexVPN client to the tunnel, use the **connect** command in IKEv2 FlexVPN client profile configuration mode. To disable the connection, use the **no** form of this command.

connect {**manual**| **auto**| **track** *track-number* [**up**| **down**]}

no connect {**manual**| **auto**| **track**}

Syntax Description

manual	Manually establishes connection with the tunnel.
auto	Automatic connection. This is the default mode.
track *track-number*	Estalishes a connection based on state of the track object.
up	Establishes a connection when the state of the track object is up.
down	Establishes a connection when the state of the track object is down.

Command Default

The default connect mode is auto.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

Note Any changes to this command terminates the active session.

Examples

The following examples shows how to set the tunnel connection to auto.

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# peer 1 10.0.0.1
Router(config-ikev2-flexvpn)# connect track 10 up
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

content-length

To permit or deny HTTP traffic through the firewall on the basis of message size, use the **content-length** command in appfw-policy-http configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

content-length {**min** *bytes* **max** *bytes*| **min** *bytes*| **max** *bytes*} **action** {**reset**| **allow**} **[alarm]**

no content-length {**min** *bytes* **max** *bytes*| **min** *bytes*| **max** *bytes*} **action** {**reset**| **allow**} **[alarm]**

Syntax Description

min *bytes*	Minimum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
max *bytes*	Maximum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
action	Messages whose size do not meet the minimum or exceed the maximum number of bytes are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not enabled, message size is not considered when permitting or denying HTTP messages.

Command Modes

appfw-policy-http configuration

Command History

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

Usage Guidelines

All messages exceeding the specified content-length range, will be subjected to the configured action (**reset** or **allow**).

Examples

The following example, which shows how to define the HTTP application firewall policy "mypolicy," will not permit HTTP messages longer than 1 byte. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

content-scan out

To enable content scanning on an egress interface, use the **content-scan out** command in interface configuration mode. To disable content scanning, use the **no** form of this command.

content-scan out

no content-scan out

Syntax Description

This command has no arguments or keywords.

Command Default

Content scanning is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The content scanning process redirects client web traffic to ScanSafe. Content scanning is enabled on an Internet-facing WAN interface to protect the web traffic going out.

In case you enable content scanning on a interface that has Wide Area Application Services (WAAS) configured, you must not apply both the WAAS and the content scanning feature on the same TCP session.

Examples

The following example shows how to enable content scanning on a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0
Router(config-if)# content-scan out
```

Related Commands

Command	Description
content-scan whitelisting	Enables content scan whitelisting and enters content-scan whitelisting configuration mode.
interface	Configures an interface and enters interface configuration mode.

content-scan whitelisting

To enable whitelisting of incoming traffic and to enter content-scan whitelisting configuration mode, use the **content-scan whitelisting** command in global configuration mode. To disable the whitelisting of traffic, use the **no** form of this command.

content-scan whitelisting

no content-scan whitelisting

Syntax Description

This command has no arguments or keywords.

Command Default

Whitelisting of traffic is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

A whitelist is an approved list that contains entities that are provided a particular privilege, service, mobility, access, or recognition. Whitelisting means to grant access.

The web traffic that you have configured for whitelisting will bypass the content scanning by ScanSafe.

Examples

The following example shows how to enable content scan whitelisting and enter content-scan whitelisting configuration mode:

```
Router(config)# content-scan whitelisting
Router(config-cont-scan-wl)#
```

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.

content-type-verification

To permit or deny HTTP traffic through the firewall on the basis of content message type, use the **content-type-verification** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

content-type-verification [match-req-resp] action {**reset**| **allow**} **[alarm]**

no content-type-verification [match-req-resp] action {**reset**| **allow**} **[alarm]**

Syntax Description

match-req-resp	(Optional) Verifies the content type of the HTTP response against the accept field of the HTTP request.
action	Messages that match the specified content type are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not issued, all traffic will be allowed.

Command Modes

appfw-policy-http configuration

Command History

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

Usage Guidelines

After the **content-type-verification** command is issued, all HTTP messages are subjected to the following inspections:

- Verify that the content type of the message header is listed as a supported content type. (See the table below.)
- Verify that the content type of the header matches the content of the message data or entity body portion of the message.

The table below contains a list of supported content types.

Table 2: HTTP Header Supported Content Types

Supported Content Types
audio/*
audio/basic
audio/midi
audio/mpeg
audio/x-adpcm
audio/x-aiff
audio/x-ogg
audio/x-wav
application/msword
application/octet-stream
application/pdf
application/postscript
application/vnd.ms-excel
application/vnd.ms-powerpoint
application/x-gzip
application/x-java-arching
application/x-java-xm
application/zip
image/*
image/cgf
image/gif
image/jpeg
image/png
image/tiff

Supported Content Types
image/x-3ds
image/x-bitmap
image/x-niff
image/x-portable-bitmap
image/x-portable-greymap
image/x-xpm
text/*
text/css
text/html
text/plain
text/richtext
text/sgml
text/xmcd
text/xml
video/*
video/-flc
video/mpeg
video/quicktime
video/sgi
video/x-avi
video/x-fli
video/x-mng
video/x-msvideo

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

control

To configure the control interface type and number for a redundancy group, use the **control**command in redundancy application group configuration mode. To remove the control interface for the redundancy group, use the **no** form of this command.

control *interface-type interface-number* **protocol** *id*

no control

Syntax Description

interface-type	Interface type.
interface-number	Interface number.
protocol	Specifies redundancy group protocol media.
id	Redundancy group protocol instance. The range is from 1 to 8.

Command Default

The control interface is not configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group protocol media and instance for the control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol
 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

copy (consent-parameter-map)

To configure a consent page to be downloaded from a file server, use the **copy** command in parameter-map type consent configuration mode.

copy *src-file-name dst-file-name*

Syntax Description

src-file-name	Source file location in which the specified file will be retrieved. The source file location must b e TFTP; for example, tftp://10.1.1.1/username/myfile.
dst-file-name	Destination location in which a copy of the file will be stored. The destination file should be copied to Flash; for example, flash. username .html.

Command Default

The consent page that is specified via the default parameter-map will be used.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **copy** command to transfer a file (consent web page) from an external server to a local file system on a device. Thus, the file name specified via the **copy** command is retrieved from the destination file location and displayed to the end user as the consent page.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used .

Examples

In the following example, both parameter maps are to use the consent file "tftp://192.168.104.136/consent_page.html" and store it in "flash:consent_page.html":

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

Related Commands

Command	Description
file (consent-parameter-map)	Specifies a local filename that is to be used as the consent webpage.

copy idconf

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

copy *url* **idconf**

Syntax Description

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

Command Default

None

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
 engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms - packets
 for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for this
 engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this signature
 is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
```

*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms

Related Commands

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

copy ips-sdf

Note In Cisco IOS Release 12.4(11)T, the **copy ips-sdf** command was replaced with the **copy idconf** command. For more information, see the **copy idconf** command.

To load or save the signature definition file (SDF) in the router, use the **copy ips-sdf**command in EXEC mode.

Syntax for Loading the SDF

copy [**/erase**]*url* **ips-sdf**

Syntax for Saving the SDF

copy ips-sdf *url*

Syntax Description

/erase	(Optional) Erases the current SDF in the router before loading the new SDF. **Note** This option is typically available only on platforms with limited memory.
url	Description for the *url* argument is one of the following options: • If you want to load the SDF in the router, the *url* argument specifies the location in which to search for the SDF. • If you are saving the SDF, the *url* argument represents the location in which the SDF is saved after it has been generated. Regardless of what option the URL is used for, available URL locations are as follows: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Command Modes

EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was replaced with the **copy idconf** command.

Usage Guidelines

Loading Signatures From the SDF

Issue the **copy** *url* **ips-sdf** command to load the SDF in the router from the location specified via the *url* argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the **/erase** keyword is issued, which overwrites the current SDF with the new SDF.

Cisco IOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.

If the **no ip ips sdf built-in** command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the **ip ips fail**command to either fail open or fail closed.

Note For Cisco IOS Release 12.3(8)T, the SDF should be loaded directly from Flash.

After the signatures are loaded in the router, the signature engines are built. Only after the signature engines are built can Cisco IOS IPS beginning scanning traffic.

Note Whenever signatures are replaced or merged, the router is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built. Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

The **ip sdf ips location** command can also be used to load the SDF. However, unlike the **copy ips-sdf**command, this command does not force and immediately load the signatures. Signatures are not loaded until the router reboots or IPS is initially applied to an interface (via the **ip ips**command).

Saving a Generated or Merges SDF

Issue the **copy ips-sdf** *url* command to save a newly created SDF file to a specified location. The next time the router is reloaded, IPS can refer to the SDF from the saved location by including the **ip ips sdf location** command in the configuration.

Tip It is recommended that you save the SDF back out to Flash. Also, you should save the file to a different name than the original attack-drop.sdf file; otherwise, you risk loosing the original file.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the reload command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
exit
```

Related Commands

Command	Description
ip ips sdf location	Specifies the location in which the router should load the SDF.

crl

To specify the certificate revocation list (CRL) query and CRL cache options for the public key infrastructure (PKI) trustpool, use the **crl** command in ca-trustpool configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

no crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

Syntax Description

cache	Specifies CRL cache options.
delete-after	Removes the CRL from cache after a timeout.
minutes	The number of minutes from 1 to 43200 to wait before deleting CRL from cache.
none	Specifies that CRLs are not cached.
query *url*	Specifies the URL published by the certification authority (CA) server to query the CRL.

Command Default

The CRL is not queried and no CRL cache parameters are configured.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

The **crl query** command is used if the CDP is in Lightweight Directory Access Protocol (LDAP) form, which means that the CDP location in the certificate indicates only where the CRL distribution point (CDP) is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

The Cisco IOS software queries the CRL to ensure that the certificate has not been revoked in order to verify a peer certificate (for example, during Internet Key Exchange (IKE) or Secure Sockets Layer (SSL) handshake). The query looks for the CDP extension in the certificate, which is used to download the CRL. If this query is unsuccessful, then the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl
- LDAP URL with a hostname. For example: ldap://CN=myca, O=cisco
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco
- LDAP/X.500 DN. For example: CN=myca, O=cisco

The Cisco IOS needs a complete URL in order to locate the CDP.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.

Command	Description
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

crl (cs-server)

To specify the certificate revocation list (CRL) public key infrastructure (PKI) certificate server (CS), use the **crl** command in certificate server configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

crl {*CRL-serial-number*}

no crl

Syntax Description

CRL-serial-number	Specifies CRL serial number of the PKI CS.

Command Default

The CRL is not queried and no CRL cache parameters are configured.

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.

The **crl** command is used with the *CRL-serial-number* argument to identify the serial number of the PKI CS. If the **crl** command is entered without this argument, then PKI hexmode is entered. In this mode, the hexidecimal data can be specified for the CS so that it can be appended to the parse buffer.

Note To exit this mode and return to global configuration mode, use the **quit** command.

Examples

```
Router(config)# crypto pki server CA
Router(ca-server)# crl 0x0-0xFFFFFFFF
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
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.
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.

Command	Description
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.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

crl query

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl query** command in ca-trustpoint configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

crl query ldap://*url:[port]*

no crl query

Syntax Description

ldap://*url:[port]*	The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server to query the CRL; for example, ldap://another_server. **Note** If a port number is not specified, then the default LDAP server port 389 is used. The URL can be the LDAP server hostname, IPv4 address.

Command Default

The CRL is not queried.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(1)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **crl query** command is disabled, the router checks the CRL distribution point (CDP) that is embedded in the certificate. The **crl query** command does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, **http://***url* or **ldap://***url*, including the fully qualified domain name (FQDN) of the host where the CRL is held.

The **crl query** command is used if the CDP is in LDAP form, which means that the CDP location in the certificate indicates only where the CDP is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl)
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl
- LDAP URL with a hostname. For example: ldap:///CN=myca, O=cisco)
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco
- LDAP/X.500 DN. For example: CN=myca, O=cisco

To locate the CRL, a complete URL needs to be formed. The **ldap://** *hostname***:**[*port*] keywords and arguments are used to provide this information.

Note The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root command, the configuration mode and command is written back as ca-trustpoint.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all ca-identity and trusted-root configuration mode commands).

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 crl query ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment url (ca-trustpoint)	Specifies the enrollment parameters of a CA.
ocsp url	Specifies the URL of an OCSP server to override the OCSP server URL (if one exists) in the AIA extension of the certificate.
revocation-check	Checks the revocation status of a certificate.

crl best-effort

Note Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort**command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

Command Modes

Ca-identity configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	This command was replaced by the **revocation-check** command.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the appropriate CRL is in the router memory, the CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer--unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

Examples

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl optional

Note Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

crl optional

no crl optional

Syntax Description

This command has no arguments or keywords.

Command Default

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(2)T	This command was replaced by the **revocation-check** command.
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

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.

Note: If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
 enrollment url http://ca_server
 enrollment retry-period 20
 enrollment retry-count 100
 crl optional
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl-cache delete-after

To configure the maximum time a router will cache a certificate revocation list (CRL), use the **crl-cache delete-after** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

crl-cache delete-after *time*

no crl-cache delete-after *time*

Syntax Description

time	The maximum lifetime of a CRL in minutes.

Command Default

A CRL is deleted from the cache when the CRL default lifetime expires.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Use this command to limit the amount of time a router will cache a CRL. You may use the **crl-cache delete-after** command to force a router to download a CRL before the existing CRL expires by configuring a value shorter than the default lifetime of the CRL.

By default, a new CRL will be downloaded after the currently cached CRL expires. The **crl-cache delete-after** command does not effect any currently cached CRLs. The configured lifetime will only effect CRLs downloaded after this command is configured.

When the maximum CRL time expires, the cached CRL will be deleted from the router cache. A new copy of the CRL will be downloaded from the issuing certificate authority (CA) the next time the router has to validate a certificate.

Note Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed to the user.

Examples

The following example shows how to configure a maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration shown above:

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate
 time and the crl-cache delete-after
command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after
a maximum lifetime of 2 minutes.
You can verify that the CRL will be cached for 2 minutes by executing the show crypto pki
crls
 command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.
```

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 22:57:42 GMT Nov 26 2005
    NextUpdate: 22:59:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

Related Commands

Command	Description
crl-cache none	Disables CRL caching.

crl-cache none

To disable certificate revocation list (CRL) caching, use the **crl-cache none** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

crl-cache none

no crl-cache none

Syntax Description

This command has no arguments or keywords.

Command Default

CRL caching is enabled.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Use this command to disable CRL caching for all CRLs associated with a trustpoint. By default, a new CRL is issued when the currently cached CRL expires.

The **crl-cache none** command does not effect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.

This functionality is useful is when a certification authority (CA) issues CRLs with no expiration date or with expiration dates far into the future-days or weeks.

Note Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Examples

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time. The **crl-cache none**command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

Related Commands

Command	Description
crl-cache delete-after	Configures the maximum lifetime of a CRL.