reauthentication time through rsa-pubkey

reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time**command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

seconds	Number of seconds after which reauthentication occurs. Range is from 1 to 4294967295. Default is 0.

Command Default

0 seconds, which means group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

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 that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
Router(config-radsrv-group)# reauthentication time 30
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.

Command	Description
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.
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.
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.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

reconnect

To enable Internet Key Exchange Version 2 (IKEv2) support for the Cisco AnyConnect Reconnect feature, use the **reconnect** command in IKEv2 profile configuration mode. To disable IKEv2 reconnect, use the **no** form of this command.

reconnect [**timeout** *seconds*]

no reconnect

Syntax Description

timeout *seconds*	(Optional) Interval, in seconds. The range is from 600 to 86400. The default is 1800.

Command Default

The IKEv2 reconnect is disabled.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The Auto Reconnect feature in the Cisco AnyConnect client helps the Cisco AnyConnect VPN client to remember the session for a period of time and to resume the connection when a network goes down or a client drops out of network after establishing the secure channel. As AnyConnect Client is extensively used with IKEv2, IKEv2 extends the Auto Reconnect feature support on IOS through the IOS IKEv2 support for Auto Reconnect feature of AnyConnect feature.

Examples

The following example shows how to configure an IKEv2 profile with a reconnect interval of 900 seconds:

```
Device(config)# crypto ikev2 profile profile2
Device(config-ikev2-profile)# reconnect 900
```

Related Commands

Command	Description
crypto ikev2 profile	Configures an IKEv2 profile.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect**command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url url

no redirect url url

Syntax Description

url	URL to which clients should be redirected.
url	Valid URL.

Command Default

No default behavior or values

Command Modes

Identity policy configuration (config-identity-policy)

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

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients are redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.example.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redirect gateway

To configure an Internet Key Exchange Version 2 (IKEv2) redirect mechanism on a gateway for specific profiles, use the **redirect gateway** command in IKEv2 profile configuration mode. To remove the redirects mechanism, use the **no** form of this command.

redirect gateway auth

no redirect gateway

Syntax Description

auth	Enables the redirects mechanism on the gateway upon security association (SA) authentication.

Command Default

The redirects mechanism is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(4)M	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to enable the redirect mechanism on the gateway when authenticating an SA for specific IKEv2 profiles.

A thorough security analysis shows that redirect during IKE_AUTH is neither more nor less secure than redirect during IKE_INIT. However, for performance and scalability reasons, we recommend redirect during IKE_INIT.

Examples

The following example shows how to enable the redirects mechanism:

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile prof1
Device(config-ikev2-profile)# redirect gateway auth
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

redundancy (cs-server)

To specify that the active certificate server (CS) is synchronized to the standby CS, use the **redundancy** command in certificate server configuration mode. To return to the default, use the **no** version of this command.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Redundancy is not configured for the certificate server.

Command Modes

Certificate server configuration (cs-server)

Command History

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

Usage Guidelines

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

Use the **redundancy** command only if the your router has redundant capabilities for an active and standby CS.

Examples

```
Router(config)#crypto pki server CA
Router(cs-server)#redundancy
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials

Command	Description
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.
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.

Command	Description
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
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.

redundancy (firewall)

To enable firewall high availability (HA), use the redundancy command in parameter-map type inspect configuration mode. To disable the firewall, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

The firewall is disabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Examples

```
Device>configure terminal
Device(config)#parameter-map type inspect global
Device(config-profile)# redundancy
```

Related Commands

Command	Description
parameter-map type inspect global	Configures a global parameter map.

redundancy (GDOI)

To enable Group Domain of Interpretation (GDOI) redundancy configuration mode and to allow for key server redundancy, use the **redundancy** command in GDOI local server configuration mode. To disable GDOI redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Key server redundancy is not supported for a key server.

Command Modes

GDOI local server configuration (config-local-server)

Command History

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

Usage Guidelines

This command must be configured before configuring related redundancy commands, such as for key server peers, local priority, and timer values. Use the **local priority** command to set the local key server priority. Use the **peer address ipv4**command to configure the peer address that belongs to the redundancy key server group.

Examples

The following example shows that key server redundancy has been configured:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.

Command	Description
peer address ipv4	Configures the peer key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

redundancy asymmetric-routing enable

To establish an asymmetric flow diversion tunnel for each redundancy group, use the **redundancy asymmetric-routing enable** command in interface configuration mode. To remove the established flow diversion tunnel, use the **no** form of this command.

redundancy asymmetric-routing enable

no redundancy asymmetric-routing enable

Syntax Description

This command has no arguments or keywords.

Command Default

An asymmetric routing traffic diversion tunnel is not configured for redundancy groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

You must configure this command on a traffic interface that sends or receives asymmetric routing traffic. A tunnel is established between the traffic interface and the asymmetric routing interface for each redundancy group.

Examples

The following example shows how to enable redundancy group asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# redundancy asymmetric-routing enable
```

Related Commands

Command	Description
asymmetric-routing	Sets up an asymmetric routing link interface and enables applications to divert packets received on the standby redundancy group to the active.
interface	Configures an interface and enters interface configuration mode.

redundancy group

To configure fault tolerance for the mobile router, use the **redundancy group** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

redundancy group *name*

no redundancy group *name*

Syntax Description

name	Name of the mobile router group.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **redundancy group** command provides f ault tolerance by selecting one mobile router in the redundancy group *name* argument to provide connectivity for the mobile networks. This mobile router is in the active state. The other mobile routers are passive and wait until the active mobile router fails before a new active mobile router is selected. Only the active mobile router registers and sets up proper routing for the mobile networks. The redundancy state is either active or passive.

Examples

The following example selects the mobile router in the sanjose group, to provide fault tolerance:

```
ip mobile router
 redundancy group sanjose
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
standby name	Configures the name of the standby group, which is associated with the mobile router.

redundancy group (interface)

To enable the redundancy group (RG) traffic interface configuration, use the **redundancy group** command in interface configuration mode. To remove the redundancy group traffic interface configuration, use the **no** form of this command.

redundancy group *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}| **autoconfig**} [**exclusive**] [**decrement** *value*]

no redundancy group *id* {**ip**| **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}}

Syntax Description

id	Redundancy group ID. Valid values are from 1 and 2.
ip *virtual-ip*	Enables IPv4 RGs and sets a virtual IPv4 address.
ipv6	Enables IPv6 RGs.
link-local-address	Link local address.
ipv6-address/*prefix-length*	IPv6 address and the length of the IPv6 prefix. IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
autoconfig	Obtains IP addresses through autoconfiguration.
exclusive	(Optional) Specifies whether the interface is exclusive to an RG.
decrement *number*	(Optional) Specifies the number that is decremented from the priority when the state of an interface goes down. The configured decrement value overrides the default number that is configured for an RG. Valid values are from 1 to 255.

Command Default

Redundancy group traffic interface configuration is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. The *virtual-ip*, *link-local-address*, *ipv6-address*/*prefix-length* arguments and **ip**, **ipv6**, and **autoconfig** keywords were added.

Usage Guidelines

Use this command to configure a redundancy group for stateful switchover.

The virtual IP address and the physical address must be in the same subnet.

When autoconfiguration is enabled, the interface obtains an IP address automatically.

Examples

The following example shows how to enable the IPv6 redundancy group traffic interface configuration:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# redundancy group 2 ipv6 FE80::260:3EFF:FE11:6770 exclusive
```

Related Commands

Command	Description
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
interface	Configures an interface and enters interface configuration mode.
name	Configures the name of a redundancy group.
preempt	Enables preemption on a redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures an RII for a redundancy group.

redundancy inter-device

To enter inter-device configuration mode, use the **redundancy inter-device** command in global configuration mode. To exit inter-device configuration mode, use the **exit** command. To remove all inter-device configuration, use the no form of this command.

redundancy inter-device

no redundancy inter-device

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, you cannot configure stateful failover for IPSec.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Use the **redundancy inter-device** command to enter inter-device configuration mode, which allows you to enable and protect Stateful Switchover (SSO) traffic.

Examples

The following example shows how to issue the **redundancy inter-device** command when enabling SSO:

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

The following example shows how to issue the **redundancy inter-device** command when configuring SSO traffic protection:

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

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the redundant peer.
local-port	Defines the local SCTP that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.
scheme	Defines that redundancy scheme that is used between two devices.

redundancy rii

To configure the redundancy interface identifier (RII) for redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode. To remove the redundant interface from the redundancy group, use the **no** form of this command.

redundancy rii *id* [**decrement** *number*]

no redundancy rii

Syntax Description

id	Redundancy interface identifier. The range is from 1 to 65535.
decrement *number*	(Optional) Specifies the decrement value. When the redundant interface is down, the run-time priority of all redundancy groups configured on the router will be decremented. Valid values are from 1 to 255.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T. The **decrement** *number* keyword-argument pair was added.

Usage Guidelin

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.

Every interface associated with one or more redundancy groups must have a unique RII assigned to it. The RII allows interfaces to have a one-to-one mapping between peers.

Examples

The following example shows how to configure the RII for Gigabit Ethernet interface 0/0/0:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

Related Commands

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

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful**command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Command Default

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

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

Usage Guidelines

The **redundancy stateful**command uses an existing IPSec profile (which is specified via the **crypto ipsec profile**command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
```

```
ip address 209.165.201.1 255.255.255.224
standby 1 ip 209.165.201.3
standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Command Default

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”.

```
crypto ca trustpoint trustme2
 enrollment url
http://
trustme2
```

```
.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

regexp (profile map configuration)

To create an entry in a cache profile group that allows authentication and authorization matches based on a regular expression, use the **regexp** command in profile map configuration mode. To disable a regular expression entry, use the **no** form of this command.

regexp *matchexpression* {**any**| **only**} **[no-auth]**

no regexp *matchexpression* {**any**| **only**}

Syntax Description

matchexpression	String representing a regular expression on which to match.
any	Specifies that any unique instance of a AAA server response that matches the regular expression is saved in the cache.
only	Specifies that only one instance of a AAA server response that matches the regular expression is saved in the cache.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No regular expression entries are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to create an entry in a cache profile group that matches based on a regular expression, such as .*@example.com or .*@xyz.com.

Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

Examples

The following example creates an entry in the cache profile group networkusers that authorizes network access to any example company user. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa cache profile networkusers
Router(config-profile-map)# regexp .*@example.com any no-auth
```

Related Commands

Command	Description
profile	Creates an individual authentication and authorization cache profile based on an exact username match.

registration interface

To specify the interface to be used for a Group Domain of Interpretation (GDOI) registration, use the **registration interface** command in GDOI local server configuration mode. To disable an interface, use the **no** form of this command.

registration interface *type slot/port*

noregistration interface *type slot/port*

Syntax Description

type	Type of interface (see the table below).
slot /port	Slot and port number of the interface.

Command Default

None

Command Modes

GDOI local server configuration

Command History

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

Usage Guidelines

The table below lists the types of interface that may be used for the *type* argument.

Table 1: Type of Interface

Interface	Description
Async	Async interface
BVI	Bridge-Group Virtual Interface
CDMA-1x	Code division multiple access 1x interface
CTunnel	CTunnel interface
Dialer	Dialer interface
Ethernet	Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3

Interface	Description
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink group interface
Null	Null interface
Serial	Serial
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example shows that the interface is Ethernet 0/0:

```
registration interface Ethernet 0/0
```

Related Commands

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

registration periodic crl trustpoint

To enable periodic registrations for the Group Domain of Interpretation (GDOI) key server (KS) when new certificate revocation lists (CRLs) become available for the configured public key infrastructure (PKI) trustpoint certificate authority (CA), use the **registration periodic crl trustpoint** command in GDOI local server configuration mode. To disable the registration, use the **no** form of this command.

registration periodic crl trustpoint *trustpoint-name*

no registration periodic crl trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of the PKI trustpoint CA.

Command Default

Periodic registrations are not enabled.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

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

Examples

The following example enables the GET VPN CRL Checking feature on KSs:

```
crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
server local	Designates a device as a GDOI key server.

registration retry count

To configure the number of times that a Transitory Messaging Services (TMS) registration message is sent to a controller, use the **registration retry count** command in parameter-map configuration mode. To configure the consumer to use the default registration retry count value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry count** command is not available in Cisco IOS software.

registration retry count *number*

no registration retry count *number*

Syntax Description

number	Number of times that a registration message is retransmitted. A number from 1 through 5 is entered.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered: 3

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **registration retry count** command is entered on a consumer to configure the number of times that an implicit registration request message is transmitted.

The consumer must register with the controller before the controller can send Control Information Messages (CIMs). Implicit registration requests are automatically sent to the controller when a TMS type service policy is activated on the consumer.

By default, a consumer sends a registration request message to the controller once every 3 minutes for up to three times or until successfully registered. If the consumer is a member of multiple groups, it sends a separate registration request messages to the controller of each group.

Note Explicit registration is configured by entering the **tms consumer registration** command on a consumer in privileged EXEC mode. This command is unaffected by registration timer configuration and can be used to register the consumer if the count has been exceeded for implicit registration.

Examples

The following example configures a consumer to send up to five registration messages to a controller:

```
Router(config)# parameter-map type tms PARAMAP_1
Router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# logging tms events
Router(config-profile)# registration retry interval 60
Router(config-profile)# registration retry count 5
Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.
registration retry interval	Configures the length of time between consumer registration attempts.

registration retry interval

To configure the length of time between consumer registration attempts, use the **registration retry interval** command in parameter-map configuration mode. To configure the consumer to use the default registration timer interval, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry interval** command is not available in Cisco IOS software.

registration retry interval *time*

no registration retry interval *time*

Syntax Description

time	Time, in seconds, between registration attempts. A number from 30 through 3000 can be entered for the *seconds* argument.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered:

180

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **registration retry interval** command is entered on a consumer to configure the time interval between the transmission of implicit registration request messages.

The consumer must register with the controller before the controller can send Control Information Messages (CIMs). Implicit registration requests are automatically sent to the controller when a Transitory Messaging Services (TMS) type service policy is activated on the consumer.

By default, a consumer sends a registration request message to the controller once every 3 minutes for up to three times or until successfully registered. If the consumer is a member of multiple groups, it sends a separate registration request messages to the controller of each group.

Note Explicit registration is configured by entering the **tms consumer registration** command on a consumer in privileged EXEC mode. This command is unaffected by registration timer configuration and can be used to register the consumer if the count has been exceeded for implicit registration.

Examples

The following example configures a consumer to send registration messages at 60-second intervals:

```
Router(config)# parameter-map type tms PARAMAP_1
Router(config-profile)# controller ipv4 10.1.1.1

Router(config-profile)# logging tms events
Router(config-profile)# registration retry interval 60

Router(config-profile)# registration retry count 5

Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.
registration retry count	Configures the number of times that a registration message is sent to a controller.

registration retry-interval (TIDP)

To configure the length of time and number of attempts for TIDP group registration, use the **registration retry-interval** command in TIDP group configuration mode. To configure TIDP to use default registration timer values, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry-interval** command is not available in Cisco IOS software.

registration retry-interval min *interval* **max** *interval*

no registration retry-interval

Syntax Description

min*interval*	Time interval, in seconds, at which TIDP attempts to register a group member. This argument is entered as a number from 0 through 65000.
max*interval*	Total time, in seconds, TIDP attempts to register a TIDP group member. The value for this argument can be a number from 0 through 65000.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

min 60 **max** 3600

Command Modes

TIDP group configuration (config-tidp-grp)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The controller registers consumers. By default, the controller sends a registration request message once every 60 seconds for up to 1 hour until the consumer is successfully registered. The value entered for the **max** keyword must be equal to or greater than the value entered for the **min** keyword. Entering a value of zero after both the **min** and **max** keywords configures the controller not to retry registration if the initial registration message receives no response.

Examples

The following example configures TIDP to attempt to register group members at 30-second intervals for up to 10 minutes or until consumers are registered:

```
Router(config)# tidp group 10

Router(config-tidp-grp)# key-set KEY_1

Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.1

Router(config-tidp-grp)# peer 10.1.1.2

Router(config-tidp-grp)# peer 10.1.1.3

Router(config-tidp-grp)# active
```

Related Commands

Command	Description
active	Activates a TIDP group.
key-set	Configures a key set for a TIDP group.
peer	Configures a consumer as a member of a TIDP group.
tidp group	Configures a TIDP group.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number*| *access-list-name*}

no rekey address ipv4 {*access-list-number*| *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

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

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys (for example, access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848).

Examples

The following example shows that the rekey address is access list “101”:

```
rekey address ipv4 101
```

The following example shows that a rekey message is to be sent to access control list (ACL) address 239.10.10.10:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
```

access-list 120 permit udp host 10.5.90.1 eq 848 host 239.10.10.10 eq 848

Related Commands

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

rekey algorithm

To define the type of encryption algorithm used for a Group Domain of Interpretation (GDOI) group, use the **rekey algorithm** command in GDOI local server configuration mode. To disable an algorithm that was defined, use the **no** form of this command.

rekey algorithm *type-of-encryption-algorithm*

no rekey algorithm *type-of-encryption-algorithm*

Syntax Description

type-of-encryption-algorithm	Type of encryption algorithm used (see the table below). The default algorithm is 3des-cbc. • The rekey algorithm is used to encrypt the rekey message that is sent from the key server to the multicast group.

Command Default

If this command is not configured, the default value of 3des-cbc takes effect. However, the default is used only if the commands required for a rekey to occur are specified (see the Note below in "Usage Guidelines").

Command Modes

GDOI local server configuration

Command History

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

Usage Guidelin

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.

The table below lists the types of encryption algorithms that may be used.

Table 2: Types of Encryption

Encryption Type	Description
3des-cbc	Cipher Block Chaining mode of the Triple Data Encryption Standard (3des).

Encryption Type	Description
aes 128	128-bit Advanced Encrytion Standard (AES).
aes 192	192-bit AES.
aes 256	256-bit AES.
des-cbc	Cipher Block Chaining mode of the Data Encryption Standard (des).

At a minimum, the following commands are required for a rekey to occur:

rekey address ipv4 {*access-list-number*| *access-list-name*}

rekey authentication {**mypubkey** | **pubkey**} {*rsa key-name*}

If the **rekey algorithm** command is not configured, the default of 3des-cbc is used if the above minimum rekey configuration is met.

Examples

The following example shows that the 3des-cbc encryption standard is used:

```
rekey algorithm 3des-cbc
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
rekey address ipv4	Specifies the source or destination information of the rekey message.
rekey authentication	Specifies the keys to be used to a rekey to GDOI group members.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey authentication

To specify the keys to be used for a rekey to Group Domain of Interpretation (GDOI) group members, use the **rekey authentication**command in GDOI local server configuration mode. To disable the keys, use the **no** form of this command.

rekey authentication {**mypubkey**| **pubkey**} **rsa** *key-name*

no rekey authentication {**mypubkey**| **pubkey**} **rsa** *key-name*

Syntax Description

mypubkey	Keypair associated with this device.
pubkey	Public key associated with a different device.
rsa	Identifies an Rivest, Shamir, and Adelman (RSA) keypair.
key-name	Key to be used for rekey.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(24)T	This command was modified. The **pubkey** keyword was removed.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

For this command to work, Rivest, Shamir, and Adelman (RSA) keys must be generated first on the router using the following command:

crypto key generate rsa {**general keys**} [**label** *key-label*]

For example:

```
crypto key generate rsa general keys label group_1234_key_name
```

Examples

The following example shows that the keypair to be used for a rekey is RSA “group_1234_key_name”:

```
rekey authentication mypubkey rsa group_1234_key_name
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto key generate rsa	Generates RSA key pairs.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey lifetime

To limit the number of days or seconds for which any one key encryption key (KEK) should be used, use the **rekey lifetime** command in GDOI local server configuration mode. To disable the number of days or seconds that were set, use the **no** form of this command.

rekey lifetime {**days** *number-of-days*| **seconds** *number-of-seconds*}

no rekey lifetime {**days**| **seconds**}

Syntax Description

number-of-days	Lifetime in days. The range is 1 to 30.
number-of-seconds	Lifetime in seconds. The range is 300 to 2592000.

Command Default

1 day (86400 seconds).

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.3(2)T	This command was modified. The **days** *number-of-days* keyword and argument pair was added, and the maximum value for the **seconds** *number-of-seconds* keyword and argument pair was extended from 86400 seconds to 2592000 seconds.
Cisco IOS XE Release 3.9S	This command was modified. The **days** *number-of-days* keyword and argument pair was added, and the maximum value for the **seconds** *number-of-seconds* keyword and argument pair was extended from 86400 seconds to 2592000 seconds.

Usage Guidelines

When the rekey lifetime is reached, a new KEK is sent to the group members so that the next rekey is encrypted with the new KEK.

Examples

The following example shows how to set the rekey lifetime to 600 seconds:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
```

```
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime seconds 600
Device(gdoi-local-server)# end
```

Related Commands

Command	Description
crypto gdoi group	Creates or identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey retransmit

To specify the duration of a rekey message retransmission and the number of retransmissions, use the **rekey retransmit** command in GDOI local server configuration mode. To disable the duration and number that were specified, use the **no** form of this command.

rekey retransmit *number-of-seconds* {**number** *number-of-retransmissions*| **periodic**}

no rekey retransmit

Syntax Description

number-of-seconds	Number of seconds that the rekey message is retransmitted. The range is 10 to 60.
periodic	Periodically sends retransmit rekeys.
periodic	Periodically sends retransmit rekeys.

Command Default

10 seconds and 2 transmissions.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.3(2)T	This command was modified. The **periodic** keyword was added.
Cisco IOS XE Release 3.9S	This command was modified. The **periodic** keyword was added.

Usage Guidelines

Use this command if you are concerned about network loss.

The **periodic** keyword sends periodic reminder rekeys to group members (GMs) that did not respond with an acknowledgment in the last scheduled rekey. Combining this keyword with the long SA lifetime feature makes a KS effectively synchronize GMs in case they miss a scheduled rekey before the keys roll over.

Each periodic rekey increments the sequence number, just as for rekey retransmissions. Also, the GM is removed from the GM database on the key server (KS) after three scheduled rekeys (not retransmissions) for which the GM does not send an acknowledgment.

Examples

The following example shows how to specify that the rekey message is retransmitted three times for 15 seconds each time:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 15 number 3
Device(gdoi-local-server)# end
```

Examples

The following example shows how to specify that the rekey message is retransmitted periodically for 30 seconds each time:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GROUP-GDOI
Device(config-gdoi-group)# identity number 4444
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 30 periodic
Device(gdoi-local-server)# end
```

Related Commands

Command	Description
crypto gdoi group	Creates or identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey sig-hash algorithm

To configure the signature hash algorithm for a key encryption key (KEK), use the **rekey sig-hash algorithm** command in GDOI local server configuration mode. To return a signature hash algorithm to the default (SHA-1), use the **no** form of this command.

rekey sig-hash algorithm *algorithm*

no rekey sig-hash algorithm

Syntax Description

algorithm	Signature hash algorithm. You can specify **sha** (for SHA-1), **sha256**, **sha384**, or **sha512**.

Command Default

SHA-1

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Using SHA-1 guarantees interoperability with group members (GMs) that are running earlier versions of Cisco IOS software. Suite B requires SHA-256, SHA-384, or SHA-512.

Examples

The following example shows how to configure the signature hash algorithm to use SHA-512:

```
Device# crypto gdoi group GETVPN
Device(config-gdoi-group) server local
Device(gdoi-local-server) rekey sig-hash algorithm sha512
```

Related Commands

Command	Description
rekey algorithm	Defines the type of encryption algorithm used for a GDOI group.

rekey transport unicast

To configure unicast delivery of rekey messages to group members, use the **rekey transport unicast**command in global configuration mode. To remove unicast delivery of rekey messages and enable the default to multicast rekeying, use the **no** form of this command.

rekey transport unicast

no rekey transport unicast

Syntax Description

This command has no arguments or keywords.

Command Default

If **rekey transport unicast** is not specified or **no rekey transport unicast** is specified, multicast rekeying is the default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command is configured on the key server under the **server local** command, along with other rekey configurations.

Examples

The following example shows that unicast delivery of rekey messages to group members has been configured:

```
crypto gdoi group diffint
 identity number 3333
 server local
  rekey lifetime seconds 300
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa mykeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 64
   address ipv4 10.0.5.2
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the remark command in access list configuration mode. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access-list entry, up to 100 characters long.

Command Default

The access-list entries have no remarks.

Command Modes

Standard named or extended named access list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 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 remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the host1 subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark**command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*

no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

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.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IP) command, except that it is IPv6-specific.

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

Command	Description
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.

replay counter window-size

To turn on counter-based anti-replay protection for traffic defined inside an access list using Group Domain of Interpretation (GDOI) if there are only two group members in a group, use the **replay counter window-size**command in GDOI SA IPsec configuration mode. To disable counter-based anti-replay protection, use the **no** form of this command.

replay counter window-size [*number*]

no replay counter window-size

Syntax Description

number	Size of the Sychronous Anti-Replay (SAR) clock window expressed in bytes. Values are equal to 64, 128, 256, 512, and 1024 bytes. Default window size is 64 bytes.

Command Default

Counter-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

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

Usage Guidelines

This command is configured on the key server.

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size in bytes, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Note GDOI anti-replay can be either counter based or time based. Use this command for counter-based anti-replay protection. For time-based anti-replay protection, use the **replay time window-size** command.

Examples

The following example shows that the anti-replay window size for unicast traffic has been set to 512:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
 sa ipsec 10
   profile group1111
   match address ipv4 101
   replay counter window-size 512
```

Related Commands

Command	Description
replay time window-size	Sets the the window size for anti-replay protection using GDOI if there are more than two group members in a group.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

replay time window-size

To set the window size for anti-replay protection using Group Domain of Interpretation (GDOI) if there are more than two group members in a group, use the **replay time window-size**command in GDOI SA IPsec configuration mode. To disable time-based anti-replay, use the **no** form of this command.

replay time window-size seconds

no replay time window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. The value range is 1 through 100. The default value is 100.

Command Default

Time-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

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

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. This command turns on time-based anti-replay. For counter-based anti-replay protection, use the **replay counter window-size** command.

Examples

The following example shows that the number of seconds of the interval duration of the SAR clock has been set to 1:

```
sa ipsec 10
 profile group1111
 match address ipv4 101
 replay time window-size 1
```

Related Commands

Command	Description
replay counter window-size	Sets the window size for counter-based anti-replay protection for unicast traffic defined inside an access list.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

request-method

To permit or deny HTTP traffic according to either the request methods or the extension methods, use the **request-method**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

request-method {**rfc** *rfc-method*| **extension** *extension-method*} **action** {**reset**| **allow**} **[alarm]**

no request-method {**rfc** *rfc-method*| **extension** *extension-method*} **action** {**reset**| **allow**} **[alarm]**

Syntax Description

rfc	Specifies that the supported methods of RFC 2616, *Hypertext Transfer Protocol--HTTP/1.1* , are to be used for traffic inspection.
rfc-method	Any one of the following RFC 2616 methods can be specified: **connect**, **default, delete**, **get**, **head**, **options**, **post**, **put**, **trace**.
extension	Specifies that the extension methods are to be used for traffic inspection.
extension-method	Any one of the following extension methods can be specified: **copy**, **default, edit**, **getattribute**, **getproperties**, **index**, **lock**, **mkdir**, **move**, **revadd**, **revlabel**, **revlog**, **save**, **setattribute**, **startrev**, **stoprev**, **unedit, unlock**.
action	Methods and extension methods outside of the specified method 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 a given method is not specified, all methods and extension methods are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

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

Usage Guidelines

Only methods configured by the **request-method** command are allowed thorough the firewall; all other HTTP traffic is subjected to the specified action (**reset** or **allow**).

Examples

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 maximum 1 action allow alarm
  content-type-verification match-req-rsp 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
!
!
```

request-queue (GTP)

To specify the number of General Packet Radio Service (GPRS) Tunneling Protocol (GTP) requests that can be queued to wait for a response, use the **request-queue** command in parameter-map type inspect configuration mode. To remove the specified number of GTP requests queued, use the **no** form of this command.

request-queue *max-requests*

no request-queue

Syntax Description

max-requests	Maximum number of GTP requests that are queued to wait for a response. Valid values are from 1 to 4294967295. The default is 200.

Command Default

By default, 200 GTP requests are queued to wait for a response.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

The **request-queue** command specifies the maximum number of GTP requests that can be queued to wait for a response. When the specified maximum limit is reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, Version Not Supported, and Serving GPRS Support Node (SGSN) Context Acknowledge messages are considered as requests and these messages will not be part of the request queue.

Examples

The following example shows how to configure the GTP request queue size as 2345:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# request-queue 2345
Device(config-profile)#
```

Related Commands

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

request-timeout

To set the number of seconds before an authentication request times out, use the **request-timeout**command in webvpn sso server configuration mode.

request-timeout *number-of-seconds*

no request-timeout *number-of-seconds*

Syntax Description

number-of-seconds	Number of seconds. Value = 10 through 30. Default = 15.

Command Default

None

Command Modes

Webvpn sso server configuration

Command History

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

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the number of seconds before an authentication request times out is 25:

```
webvpn context context1
 sso-server test-sso-server
  request-timeout 25
```

Related Commands

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

reset (policy-map)

To reset an SMTP connection with an SMTP sender (client) if it violates the specified policy, use the **reset** command in policy-map configuration mode. This action sends an error code to the sender and closes the connection gracefully.

reset

Command Default No default behavior or values.

Command Modes Policy-map configuration

Command History

12.4(20)T	This command was introduced in Cisco IOS Release 12.4(20)T.

Examples The following example displays the reset command configuration for DSP 1:

```
Router(config)# policy-map type inspect smtp p1
Router(config-pmap)# class type inspect smtp c1
Router(config-pmap)# reset
```

reset (zone-based policy)

To reset a TCP connection if the data length of the Simple Mail Transfer Protocol (SMTP) body exceeds the value that you configured in the **class-map type inspect smtp**command, use the **reset** command in policy-map configuration mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP connection is not reset.

Command Modes

Policy-map configuration

Command History

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

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

You can enter **reset** only for TCP traffic.

Examples

The following example creates a Layer 7 SMTP policy map named mysmtp-policy and applies the reset action to each of the match criteria:

```
policy-map type inspect smtp mysmtp-policy
 class-map type inspect smtp huge-mails
  reset
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

responder-only

To configure a device as responder-only, use the **responder-only**command in IPsec profile configuration mode. To remove the responder-only setting, use the no form of this command.

responder-only

no responder-only

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not configured as responder-only.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

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

This command is relevant only for a virtual interface scenario and is configurable only under an IPsec profile. Neither static nor crypto maps are supported.

Examples

The following example shows that the device has been configured as a responder-only:

```
crypto ipsec profile vti
 set transform-set 3dessha
 set isakmp-profile clients
 responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.

retired (IPS)

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

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

no retired

Syntax Description

true	Retires all signatures within a given category.
false	“Unretires” all signatures within a given category.

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
```

```
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
```

Related Commands

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

retransmit (config-radius-server)

To specify the number of times a RADIUS request is re-sent to a server when that server is not responding or responding slowly, use the **retransmit** command in RADIUS server configuration mode. To restore the default value, use the **no** form of this command.

retransmit *retries*

no retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is from 0 to 100. The default is 3.

Command Default

The default number of retransmission attempts is 3.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the router, it is recommended that you configure the RADIUS server retransmit rate to 5.

Examples

The following example shows how to specify a retransmit counter value of five times:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

Effective with Cisco IOS Release 12.4(15)T

reverse-route [**static**| **remote-peer** *ip-address* **[gateway] [static]**]

no reverse-route [**static**| **remote-peer** *ip-address* **[gateway] [static]**]

Before Cisco IOS Release 12.4(15)T

reverse-route [**static**| **tag** *tag-id* **[static]**| **remote-peer [static]**| **remote-peer** *ip-address* **[static]**]

no reverse-route [**static**| **tag** *tag-id* **[static]**| **remote-peer [static]**| **remote-peer** *ip-address* **[static]**]

Syntax Description

tag *tag-id*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. **Note** Effective with Cisco IOS Release 12.4(15)T, the **tag** keyword and *tag-id* argument were removed.
remote-peer	(Optional) Indicates two routes: one for the tunnel endpoint, with the next hop being the interface to which the crypto map is bound. **Note** The **remote-peer** keyword and its variants (*ip-address* argument and **gateway** keyword) are applicable only to crypto maps.
ip-address	(Optional) If this argument is used without the optional **gateway** keyword, there is only one route: the protected subnet. The next hop is determined by the user-added value for the *ip-address* argument.
gateway	(Optional) Used with the *ip-address* argument. If the **gateway** keyword is used, there are two routes: one to the protected subnet through the remote-tunnel endpoint and the other to the remote-tunnel endpoint that is determined by the user-added value for the *ip-address* argument. **Note** The optional **gateway** keyword enables the behavior of the **reverse-route remote-peer** *ip-address* command syntax used for software releases before Cisco IOS Release 12.3(14)T.

static	(Optional) Creates routes on the basis of crypto ACLs, regardless of whether flows have been created for these ACLs.

Command Default

No default behavior or values.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The **remote-peer** keyword and *ip-address* argument were added.
12.3(14)T	The **static** and **tag** keywords and *tag-id* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **tag** keyword and *tag-id* argument were deleted. The **gateway** keyword was added.
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 Guidelin

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.

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

The **remote-peer** keyword is required when RRI is performed in a VRF-Aware IPsec scenario.

Examples

Examples

The following example shows how to configure RRI when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102
Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Note In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be necessary, that is, **reverse-route static.**

The **reverse-route** command in this situation creates routes that are analogous to the following static route CLI (**ip route**):

- Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

- VPN Services Module (VPNSM)

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

Examples

The following configuration example shows how to configure RRI for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
```

```
   match address 101
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Device# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The previous example yields the following before Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
 table)
```

Examples

In the following example, routes are created from the destination information in the access control list (ACL). One route will list 10.2.2.2 as the next-hop route to the ACL information, and one will indicate that to get to 10.2.2.2, the route will have to go via 10.1.1.1. All routes will have a metric of 10. Routes are created only at the time the map and specific ACL rule are created.

```
crypto map map1 1 ipsec-isakmp
 set peer 10.2.2.2
 reverse-route remote-peer 10.1.1.1 gateway
 set reverse-route distance 10
 match address 101
Configuring RRI with Route Tags 12.4(15)T or later: Example
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Device# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check**command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2* [*method3*]]

no revocation-check *method1* [*method2* [*method3*]]

Syntax Description

method1 [*method2 method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: • **crl** --Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none** --Certificate checking is not required. • **ocsp** --Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Command Default

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the **crl best-effort** and **crl optional**commands.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate--unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki crl request**command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional**command, it will be written back as the **revocation-check none**command. However, there is a difference between the **crl optional** command and the **revocation-check none**command. The **crl optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid. Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort**command, it will be written back as the **revocation-check crl none**command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

revocation-check (ca-trustpool)

To disable a revocation checking method when the public key infrastructure (PKI) trustpool policy is being used, use the **revocation-check** command in ca-trustpool configuration mode. To return to the default, use the **no** form of this command.

revocation-check *method1* [*method2* [*method3*]]

no revocation-check *method1* [*method2* [*method3*]]

Syntax Description

method1 [*method2 method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are identified by the following keywords: • **crl**--Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none** --Certificate checking is not required. • **ocsp**--Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.

Command Default

CRL checking is mandatory for current trustpoint policy usage.

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.

If a revocation policy needs to be altered for specific certificate authority (CA) certificates in the PKI trustpool, use certificate maps instead.

Examples

The **revocation-check** command in following example disables both CRL and OCSP revocation checks:

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# revocation-check ocsp crl none
```

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.
crl	Specifes the CRL query and cache options for 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 subcommand to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.

Command	Description
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.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

root tftp *server-hostname filename*

no root tftp *server-hostname filename*

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
server-hostname filename	Specifies a name for the server and a name for the file that will store the trustpoint CA.

Command Default

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)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.(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 allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint**command , which puts you in ca-trustpoint configuration mode.

Note The **crypto ca trustpoint**commanddeprecates the **crypto ca identity**and **crypto ca trusted-root**commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
 root tftp xxx fff
 crl optional
```

Related Commands

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

root CEP

The **crypto ca trustpoint**commanddeprecates the **crypto ca trusted-root**command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY**command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy**command for more information.

root TFTP

The **root TFTP**command is replaced by the **root** command. See the **root**command for more information.

route accept

To filter the routes received from the peer and save the routes on the router based on the specified values, use the **route accept** command in IKEv2 authorization policy configuration mode. To reject the routes , use the **no** form of this command.

route accept any [**tag** *tag-id*] [**distance** *value*]

no route accept

Syntax Description

any	Accepts all routes received from the peer.
tag *tag-id*	(Optional) Tags the route with the specified ID. The default value is 1.
distance *value*	(Optional) Sets the metric of the route with the specified value. The default value is 2.

Command Default

The routes received from the peer are not filtered.

Command Modes

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

Command History

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

Usage Guidelines

Before using the **route accept** command, you must first configure the **crypto ikev2 authorization policy** command.

Examples

The following example show how to filter the routes received from the peer and save the routes on the router based on the specified values:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route accept any tag 1
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

route set

To specify the route set parameters to the peer via configuration mode, use the **route set** command in IKEv2 authorization policy configuration mode. To disable, use the **no** form of this command.

route set {**interface** *interface*| **access-list** {*access-list-name*| *access-list-number*| *expanded-access-list-number*| **ipv6** *access-list-name*}}

no route set {**interface**| **access-list** {*access-list-name*| *access-list-number*| *expanded-access-list-number*| **ipv6** *access-list-name*}}

Syntax Description

interface *interface*	Specifies the route interface.
access-list	Specifies the route access list.
access-list-name	Specifies the access list name.
access-list-number	Specifies the standard access list number. The range is from 1 to 99.
expanded-access-list-number	Specifies the expanded access list number. The range is from 1300 to 1999.
ipv6	Specifies an IPv6 access list.

Command Default

Route set parameters are not set.

Command Modes

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

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.3(3)M	This command was modified. The *interface* argument was added.

Usage Guidelines

Before using the **route set** command, you must first configure the **crypto ikev2 authorization policy** command. This command allows running routing protocols such as BGP over VPN.

Examples

The following example show how to send the IP address of the VPN interface to the peer via configuration mode:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route set interface Ethernet
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

route set remote

To push route set parameters to be pushed to the remote peer via configuration mode, use the **route set remote** command in IKEv2 authorization policy configuration mode. To disable, use the **no** form of this command.

route set remote{**ipv4***ip-address mask*| **ipv6***ip-address*/*mask*}

no route set remote{**ipv4***ip-address mask*| **ipv6***ip-address*/*mask*}

Syntax Description

ipv4	Specifies an IPv4 route.
ipv6	Specifies an IPv6 route.
ip-address mask	The IP address and network mask for the route.

Command Default

Route set parameters are not set.

Command Modes

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

Command History

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

Usage Guidelines

Before using the **route set remote** command, you must first configure the **crypto ikev2 authorization policy** command.

Examples

The following example show how to push an IPv4 address to the remote peer via configuration mode:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route set ipv4 10.0.0.1 255.255.255.0
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in RA guard policy configuration mode.

router-preference maximum {**high**| **low**| **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default routers advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised default router preference is set to **high** in the received packet, then the packet is dropped. If the command option is set to **medium** or **low** in the received packet, then the packet is not dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

Related Commands

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

rsakeypair

To specify which Rivest, Shamir, and Adelman (RSA) key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key pair. If the size is not specified, the existing key size is used.
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Command Default

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)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.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was added.

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.

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair “exampleCAkeys”:

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

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

rsa-pubkey {**address** *address*| **name** *fqdn*} [**encryption**| **signature**]

no rsa-pubkey {**address** *address*| **name** *fqdn*} [**encryption**| **signature**]

Syntax Description

address *address*	IP address of the remote peer.
name *fqdn*	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Command Default

No default behavior or values

Command Modes

Keyring configuration

Command History

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

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
```

```
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```