Internet Key Exchange Security Protocol Commands on Cisco ASR 9000 Series Routers

This module describes the Cisco IOS XR software commands used to configure the Internet Key Exchange (IKE) security protocol on Cisco ASR 9000 Series Aggregation Services Routers.

For detailed information about IKE concepts, configuration tasks, and examples, see the *Implementing Internet Key Exchange Security Protocol on Cisco ASR 9000 Series Routers* module in the *Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.*

accounting (IKE)

To enable authentication, authorization, and accounting (AAA) services for all peers that connect through the ISAKMP profile, use the **accounting** command in ISAKMP profile configuration mode. To return to the default value, use the **no** form of this command.

accounting *list-name*

no accounting

Syntax Description

list-name	Name of a client accounting list. The maximum length of characters is 127.

Defaults

The default value is no accounting.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to create an accounting list:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# accounting aaalist
```

Related Commands

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

address

To specify the IP address for the Rivest, Shamir, and Adelman (RSA) public key of the remote peer you manually configure, use the **address** command in public key configuration mode. To remove the IP address of the remote peer, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	IP address of the remote RSA public key of the peer that you manually configure.

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **address** command to specify the RSA public key for the IP Security (IPSec) peer you manually configure next.

When you finish specifying the RSA key, you must return to global configuration mode by entering **quit** on a new line.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example manually specifies the RSA public keys of an IPSec peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey name host.vpn.com
RP/0/RSP0/CPU0:router(config-pubkey)# address 10.5.5.1
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
D58AD221 B583D7A4 71020301 0001
quit
```

Related Commands

Command	Description
key-string (IKE)	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during IKE authentication.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. To reset the authentication method to the default value, use the **no** form of this command.

authentication {**pre-share** | **rsa-sig** | **rsa-encr**}

no authentication {**pre-share** | **rsa-sig** | **rsa-encr**}

Syntax Description

pre-share	Specifies preshared keys as the authentication method.
rsa-sig	Specifies RSA signatures as the authentication method.
rsa-encr	Specifies Rivest, Shamir, and Adelman (RSA) encrypted nonces as the authentication method.

Defaults

RSA signatures

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IKE policies define a set of parameters during IKE negotiation. Use the **authentication** command to specify the authentication method in an IKE policy. If you specify preshared keys, you must also separately configure these preshared keys.

If you specify RSA encrypted nonces, you must ensure that each peer has the RSA public keys of the other peers. (See the **address**, **rsa-pubkey**, and **key-string** commands.)

If you specify RSA signatures, you must configure your peer routers to obtain certificates from a certification authority (CA).

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure an IKE policy with preshared keys as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication pre-share
```

The following example shows how to configure an IKE policy with RSA encrypted keys as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-encr
```

The following example configures an IKE policy with RSA signatures as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-sig
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you manually configure.
crypto isakmp policy	Defines an IKE policy.
crypto key generate rsa	Generates RSA key pairs.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
key-string (IKE)	Specifies the RSA public key of a remote peer.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
rsa-pubkey	Defines the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during IKE authentication.
show crypto isakmp policy	Displays the parameters for each IKE policy.

clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in EXEC mode.

clear crypto isakmp [*connection-id*]

Syntax Description

connection-id	(Optional) Name of connection to clear. If this argument is not used, all existing connections are cleared. The range is from 1 to 64000.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note If the *connection-id* argument is not used, all existing IKE connections are cleared when this command is issued.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
RP/0/RSP0/CPU0:router# show crypto isakmp sa

vrf             dst             src             state          conn-id    nodeid
----------      ------------    ------------    ---------      -------    ------
default         172.21.114.123  172.21.114.67   QM_IDLE        1          0
default         172.0.0.2       172.0.0.1       QM_IDLE        8          0

RP/0/RSP0/CPU0:router# configure
Enter configuration commands, one per line.  End with CNTL/Z.

RP/0/RSP0/CPU0:router# clear crypto isakmp 1
RP/0/RSP0/CPU0:router# show crypto isakmp sa
```

```
vrf             dst             src             state          conn-id    nodeid
----------      ------------    ------------    ---------      -------    ------
default         172.0.0.2       172.0.0.1       QM_IDLE        8          0
```

Related Commands

Command	Description
show crypto isakmp sa	Displays all current IKE SAs at a peer.

clear crypto isakmp call admission statistics

To clear ISAKMP call admission statistics, use the **clear crypto isakmp call admission statistics** command in EXEC mode.

clear crypto isakmp call isakmp call admission statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear call admission statistics:

```
RP/0/RSP0/CPU0:router# clear crypto isakmp call admission statistics
```

Related Commands

Command	Description
show crypto isakmp call admission statistics	Displays the configuration for Call Admission Control (CAC) to the IKE protocol.

clear crypto isakmp errors

To clear the statistics for Internet Security Association and Key Management Protocol (ISAKMP) errors, use the **clear crypto isakmp errors** command in EXEC mode.

clear crypto isakmp error

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear ISAKMP error statistics:

```
RP/0/RSP0/CPU0:router# show crypto isakmp errors

Control Plane Errors
--------------------
ERR NO MEMORY.....................................0
INVALID CERT......................................0
CRYPTO FAILURE....................................0
SA NOT AUTH.......................................0
AUTHENTICATION FAILED.............................0
GROUP AUTHOR FAILED...............................0
USER AUTHEN REJECTED..............................0
LOCAL ADDRESS FAILURE.............................0
FAILED TO CREATE SKEYID...........................0
RSA PUBLIC KEY NOT FOUND..........................0
RETRANSMITION LIMIT...............................0
MALFORMED MESSAGE.................................0
QUICK MODE TIMER EXPIRED..........................0
KEY NOT FOUND IN PROFILE..........................0
PROFILE NOT FOUND.................................0
PRESHARED KEY NOT FOUND...........................0
```

```
PHASE2 PROPOSAL NOT CHOSEN.....................0
POLICY MISMATCH................................0
NO POLICY FOUND................................0
PACKET PROCESS FAILURE.........................0

Warnings
---------
CERT DOESNT MATCH ID...........................0
CERT ISNT TRUSTED ROOT.........................0
PACKET NOT ENCRYPTED...........................0
UNRELIABLE INFO MSG............................0
NO SA..........................................0
BAD DOI SA.....................................0
UNKNOWN EXCHANGE TYPE..........................0
OUTGOING PKT TOO BIG...........................0
INCOMING PKT TOO BIG...........................0

Informational
--------------
CAC DROPS......................................0
DEFAULT POLICY ACCEPTED........................0

RP/0/RSP0/CPU0:router# clear crypto isakmp errors
```

Related Commands

Command	Description
show crypto isakmp errors	Displays the ISAKMP error that occurred during tunnel establishment.

clear crypto session

To delete crypto sessions (IP Security [IPSec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in EXEC mode.

clear crypto session [**user** *username* | **group** *group* | **interface** | **ivrf** *vrf-name* | **local** *ip-address* | **fvrf** *vrf-name* | **remote** *ip-address*]

Syntax Description

user *username*	(Optional) Specifies the name for the user.
group *group*	(Optional) Specifies the identity name for the group.
interface	(Optional) Specifies the name for the interface.
ivrf *vrf-name*	(Optional) Specifies the inside VRF (IVRF) session that is cleared.
local *ip-address*	(Optional) Clears crypto sessions for a local crypto endpoint. The *ip-address* argument is the IP address of the local crypto endpoint.
fvrf *vrf-name*	(Optional) Specifies the front door virtual routing and forwarding (FVRF) session that is cleared.
remote *ip-address*	(Optional) Clears crypto sessions for a remote IKE peer. The *ip-address* argument is the IP address of the remote IKE peer.

Defaults

If the **clear crypto session** command is entered without any keywords, all existing sessions are deleted. The IPSec SAs are deleted first. Then, the IKE SAs are deleted. The default value for the remote port is 500.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To clear a specific crypto session or a subset of all the sessions, you need to provide session specific parameters, such as local interface, local IP address, remote IP address (and port), FVRF name, or IVRF name.

If a local IP address is provided as a parameter, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) are deleted.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete all crypto sessions:

```
RP/0/RSP0/CPU0:router# clear crypto session
```

The following example shows that the crypto session of the FVRF named "blue" is deleted:

```
RP/0/RSP0/CPU0:router# clear crypto session fvrf blue
```

The following example shows that the crypto session of the local endpoint 10.1.1.1 is deleted:

```
RP/0/RSP0/CPU0:router# clear crypto session local 10.1.1.1
```

Related Commands

Command	Description
description (ISAKMP peer)	Adds the description of an Internet Key Exchange (IKE) peer.
show crypto session	Displays status information for active crypto sessions.

crypto isakmp

To globally enable Internet Key Exchange (IKE) at your peer router, use the **crypto isakmp** command in global configuration mode. To disable IKE at the peer, use the **no** form of this command.

crypto isakmp

no crypto isakmp

Syntax Description

This command has no arguments or keywords.

Defaults

IKE is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IKE need not be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to disable IKE at one peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp
RP/0/RSP0/CPU0:router(config)# no crypto isakmp
```

crypto isakmp call admission limit

To deny incoming or outgoing session requests based on several metrics, use the **crypto isakmp call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

crypto isakmp call admission limit {**cpu** {**total** *percent* | **ike** *percent*} | **in-negotiation-sa** *number* | **sa** *number*}

no crypto isakmp call admission limit {**cpu** {**total** *percent* | **ike** *percent*} | **in-negotiation-sa** *number* | **sa** *number*}

Syntax Description

cpu	Specifies the total resource limit for the CPU usage to accept new calls.
total *percent*	Specifies the maximum total CPU usage to accept new calls. The range for the *percent* argument is from 1 to 100.
ike *percent*	Specifies the maximum IKE CPU usage to accept new calls. The range for the *percent* argument is from 1 to 100.
in-negotiation-sa *number*	Specifies the maximum number of in-negotiation (embryonic) IKE security associations (SAs) that the router can establish before IKE begins rejecting new SA requests. The range for the number argument is from 1 to 100000.
sa *number*	Specifies that the maximum number of active IKE SAs that the router can establish before IKE begins rejecting new SA requests. You can configure a limit on the number of in-negotiation connects. This type of connect represents an aggressive mode IKE SA or main mode SA prior to the authentication and actual establishment. The range for the number argument is from 1 to 100000.

Defaults

The default value for the **in-negotiation-sa** keyword is set to 1000 SAs.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A request for an IKE SA is denied if insufficient system resources exist to handle the negotiation.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **crypto isakmp call admission limit** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp call admission limit cpu ike 30
```

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.

crypto isakmp identity

To specify the identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. To reset the Internet Security Association Key Management Protocol (ISAKMP) identity to the default value (address), use the **no** form of this command.

crypto isakmp identity {**address** | **hostname**}

no crypto isakmp identity

Syntax Description

address	Sets the ISAKMP identity to the IP address of the interface that communicates to the remote peer during IKE negotiations.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Defaults

The IP address is used for the ISAKMP identity.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **crypto isakmp identity** command to specify an ISAKMP identity either by IP address or by host name. As a general rule, you should set all identities for peers in the same way—either by IP address or by host name.

Set an ISAKMP identity whenever you specify preshared keys.

Use the **address** keyword when only one interface (and therefore only one IP address) is used by the peer for IKE negotiations, and the IP address is known.

Use the **hostname** keyword if more than one interface on the peer might be used for IKE negotiations, or if the IP address for the interface is unknown (such as with dynamically assigned IP addresses).

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use preshared keys at two peers and set both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1), the ISAKMP identity is set and the preshared key is specified.

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 192.168.1.33 key
presharedkey
```

At the remote peer (at 192.168.1.33), the ISAKMP identity is set and the same preshared key is specified.

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.0.0.1 key presharedkey
```

Note In the preceding example, if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would still have been set to the IP address, the default identity.

The following example shows how to use preshared keys at two peers and set both their ISAKMP identities to the host name.

At the local peer, the ISAKMP identity is set and the preshared key is specified.

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname remoterouter.example.com
key presharedkey
```

At the remote peer, the ISAKMP identity is set and the same preshared key is specified.

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname localrouter.example.com key
presharedkey
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto keyring	Defines a crypto keyring during IKE authentication.
local-address (keyring)	Limits the scope of an ISAKMP keyring configuration to a local termination address.
pre-shared-key	Defines a preshared key for IKE authentication.

crypto isakmp keepalive

To use the Internet Key Exchange (IKE) security association (SA) feature for providing a mechanism for detecting loss of connectivity between two IP Security (IPSec) peers, use the **crypto isakmp keepalive** command in global configuration mode. To disable this feature, use the **no** form of this command.

crypto isakmp keepalive *seconds retry-seconds*

no crypto isakmp keepalive

Syntax Description

seconds	Number of seconds between keepalive messages. The range is from 10 to 3600.
retry-seconds	Number of seconds between retries if keepalive fails. The range is from 2 to 60.

Defaults

IKE does not send keepalive messages until specified by this command.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If IKE does not receive the keepalive acknowledge message from the peer after four tries, IKE concludes that it has lost connectivity with its peer.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to set the number of seconds between keepalive messages to 20 seconds, and the number of seconds between retries to 20 seconds if keepalive fails:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp keepalive 20
```

Related Commands

Command	Description
crypto isakmp identity	Specifies the identity the router uses when participating in the IKE protocol.

crypto isakmp peer

To enable an IP Security (IPSec) peer for Internet Key Exchange (IKE), use the **crypto isakmp peer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

crypto isakmp peer {**address** *ip-address* | **hostname** *hostname*} [**description** *line* | **vrf** *fvrf-name*]

no crypto isakmp peer {**address** *ip-address* | **hostname** *hostname*} [**description** *line* | **vrf** *fvrf-name*]

Syntax Description

address *ip-address*	Specifies the IP address of the peer router.
hostname *hostname*	Specifies the hostname of the peer.
description *line*	(Optional) Specifies the IKE peer description. The maximum number of characters that you can use to describe the peer is 80.
vrf *fvrf-name*	(Optional) Specifies the VPN routing and forwarding (VRF) routing table through which the peer is reachable. The *fvrf-name* argument must match the FVRF name that was defined during VPN routing and forwarding (VRF) configuration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **crypto isakmp peer** command to enter ISAKMP peer configuration mode.

You can give a peer that is identified by an IP address a meaningful name or description.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the peer address is 40.40.40.2 and named citeA:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp peer address 40.40.40.2
RP/0/RSP0/CPU0:router(config-isakmp-peer)# description citeA
RP/0/RSP0/CPU0:router(config-isakmp-peer)# commit
```

```
RP/0/RSP0/CPU0:router# show crypto isakmp peers

Peer: 60.60.60.2   Port: 500   Local: 70.70.70.2   vrf: default
  UDP encapsulate: False
  SA information:
    Connection ID: 2
    State: QM_IDLE
    Phase 1 ID: IPV4_ADDR 60.60.60.2

Peer: 40.40.40.2   Port: 500   Local: 50.50.50.2   vrf: default
  Description: peerA
  UDP encapsulate: False
  SA information:
    Connection ID: 1
    State: QM_IDLE
    Phase 1 ID: IPV4_ADDR 40.40.40.2
```

Related Commands

Command	Description
description (ISAKMP peer)	Adds the description of an Internet Key Exchange (IKE) peer.
show crypto isakmp peers	Displays peer structures.

crypto isakmp policy

To define an Internet Key Exchange (IKE) policy, use the **crypto isakmp policy** command in global configuration mode. To delete an IKE policy, use the **no** form of this command.

crypto isakmp policy *priority*

no crypto isakmp policy *priority*

Syntax Description

priority	Value that uniquely identifies the IKE policy and assigns a priority to the protection policy. Use an integer from 1 to 10000, with 1 being the highest priority and 10000 the lowest.

Defaults

There is a default policy, which always has the lowest priority. The default policy contains default values for the encryption, hash, authentication, Diffie-Hellman group, and lifetime parameters. (The parameter defaults are listed in the "Usage Guidelines" section.) When you create an IKE policy, the default for a particular parameter is used if no value is specified.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **crypto isakmp policy** command to specify the parameters to use during an IKE negotiation. (These parameters create the IKE security association [SA].)

The **crypto isakmp policy** command enters ISAKMP policy configuration mode. The following commands are available in this mode to specify the parameters in the policy:

- **authentication (IKE policy)** command—Specifies that the default values are Rivest, Shamir, and Adelman (RSA) signatures.
- **description (IKE policy)** command—Creates a description of an IKE policy.
- **encryption (IKE policy)** command— Sets the encryption algorithm for protection suite according to one of the following standards.
- **group (IKE policy)** command—Specifies that the default value is 768-bit Diffie-Hellman.
- **hash (IKE policy)** command—Specifies that the default value is SHA-1.
- **lifetime (IKE policy)** command—Specifies that the default value is 86,400 seconds (1 day).

If you do not specify one of these commands for a policy, the default value is used for that parameter.

To exit ISAKMP policy configuration mode, use the **exit** command.

You can configure multiple IKE policies on each peer participating in IP Security (IPSec). When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure two policies for the peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# hash md5
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-sig
RP/0/RSP0/CPU0:router(config-isakmp)# group 2
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 5000
RP/0/RSP0/CPU0:router(config-isakmp)# exit

RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 20
RP/0/RSP0/CPU0:router(config-isakmp)# authentication pre-share
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 10000
RP/0/RSP0/CPU0:router(config-isakmp)# exit
```

The configuration results in the following policies:

```
Protection suite priority 15
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Message Digest 5
  authentication method: Rivest-Shamir-Adelman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman Group: #1 (768 bit)
  lifetime: 10000 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit
```

IKE policy 15 is the highest priority, and the default policy is the lowest priority.

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
description (IKE policy)	Specifies a description for an ISAKMP policy
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

crypto isakmp policy-set

To define a policy set for an ISAKMP protection suite, use the **crypto isakmp policy-set** command in global configuration mode. To cancel a previously configured policy set, use the no variant to the command.

crypto isakmp policy-set *policy-name*

no crypto isakmp policy-set *policy-name*

Syntax Description

policy-name	Name you want to give the policy set.

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use of this command takes you to ISAKMP policy set configuration mode.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to define an ISAKMP policy set, based on the local address, to restrict users with remote access from accessing certain ISAKMP policies:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy-set mypolicy
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)#
```

Related Commands

Command	Description
description (ISAKMP policy-set)	Description for the ISAKMP policy-set.

Command	Description
match identity (ISAKMP policy-set)	Creates an SVI tunnel source. When users connect to the IP identified in this step, a predefined encryption algorithm becomes operational.
policy (ISAKMP policy-set)	Specifies priority in which to use preconfigured policies.

crypto isakmp profile

To define an ISAKMP profile and audit IPSec user sessions, use the **crypto isakmp profile** command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

crypto isakmp profile local *profile-name*

no crypto isakmp profile local *profile-name*

Syntax Description

local	(Required) Specifies that the profile is used for locally sourced or terminated traffic. **Note** The **local** keyword is used for the ISAKMP profile to define locally sourced or destined traffic. This traffic is decrypted or encrypted by the route processor (RP).
profile-name	(Required) Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. At least one match identity command must also be defined in the ISAKMP profile for the profile to be complete.

Before you configure an ISAKMP profile, the key rings that are used for the profile should be configured.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to define an ISAKMP profile and match the peer identities:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local profile1
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity address 10.1.1.0/24
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-ipsec 1
```

Related Commands

Command	Description
keepalive (ISAKMP profile)	Specifies the authorization list that is used for authorization for Internet Key Exchange (IKE) interaction.
keepalive (ISAKMP profile)	Lets the gateway send dead peer detection (DPD) messages to the peer.
self-identity	Defines the identity that the local IKE uses to identify itself to the remote peer.
set interface tunnel-ipsec	Predefines the interface instance.
set ipsec-profile	Predefines the IPSec profile.
show crypto isakmp profile	Lists all the ISAKMP profiles that are defined on a router.

crypto keyring

To define a crypto keyring during IKE authentication, use the **crypto keyring** command in global configuration mode. To remove the keyring, use the **no** form of this command.

crypto keyring *keyring-name* [**vrf** *fvrf-name*]

no crypto keyring *keyring-name* [**vrf** *fvrf-name*]

Syntax Description

keyring-name	Name of the crypto keyring. The maximum length of the keyring name is 32 characters.
vrf *fvrf-name*	(Optional) Specifies that the front door virtual routing and forwarding (FVRF) name to which the keyring is referenced. The *fvrf-name* argument must match the FVRF name that was defined during virtual routing and forwarding (VRF) configuration.

Defaults

If the **vrf** keyword is not defined, the keyring is referenced to the global VRF.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A keyring is a repository of preshared and RSA public keys. The keyring is used in global configuration mode. The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile.

Use the **crypto keyring** command to enter keyring configuration mode.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **crypto keyring** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnsecret
```

Related Commands

Command	Description
crypto isakmp identity	Specifies the identity used by the router when participating in the Internet Key Exchange (IKE) protocol.
description (keyring)	Creates a description for a keyring.
local-address (keyring)	Limits the scope of an ISAKMP keyring configuration to a local termination address or interface.
pre-shared-key	Defines a preshared key for IKE authentication.
rsa-pubkey	Defines the Rivest, Shamir, and Adelman (RSA) public key by address or hostname.

crypto logging

To enable the appearance of the cyrpto tunnel up or down message, use the **crypto logging** command in global configuration mode. To disable this option, use the **no** form of this command.

crypto logging {**tunnel-status**}

no crypto logging {**tunnel-status**}

Syntax Description

tunnel-status	Enables the logging for the tunnel-status.

Defaults

The default is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **crypto logging** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto logging tunnel-status
```

description (IKE policy)

To create a description for an Internet Key Exchange (IKE) policy, use the **description** command in ISAKMP policy configuration mode. To delete an IKE policy description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Character string describing the IKE policy.

Defaults

The default description is blank.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **description** command inside the ISAKMP policy configuration submode to create a description for an IKE policy.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the creation of an IKE policy description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# description this is a sample IKE policy
```

description (ISAKMP policy-set)

To create a description for an ISAKMP policy set, use the **description** command in ISAKMP policy configuration mode. To delete an ISAKMP policy-set description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Character string describing the IKE policy set.

Defaults

The default description is blank

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **description** command inside the ISAKMP policy-set configuration submode to create a description for an IKE policy set.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the creation of an IKE policy description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy-set pol1
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)# description this is a sample IKE policy-set
```

Related Commands

Command	Description
crypto isakmp policy-set	Defines a policy set for an ISAKMP protection suite.
match identity (ISAKMP policy-set)	Creates an SVI tunnel source, based on an identity matching a preconfigured policy set.
policy (ISAKMP policy-set)	Specifies the routing priority of a preconfigured policy.

description (ISAKMP peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

description *string*

no description *string*

Syntax Description

string	Description given to an IKE peer. The maximum number of characters is 80.

Defaults

No default behavior or values

Command Modes

ISAKMP peer configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IKE peers that "sit" behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the description "connection from site A" is added for an IKE peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp peer address 10.2.2.9
RP/0/RSP0/CPU0:router(config-isakmp-peer)# description connection from site A
```

Related Commands

Command	Description
clear crypto isakmp	Deletes crypto sessions IPSec and IKE SAs for an ISAKMP group and user.
crypto isakmp peer	Enables an IP Security (IPSec) peer for Internet Key Exchange (IKE).
show crypto isakmp peers	Displays peer structures.

description (keyring)

To create a one-line description for a keyring, use the **description** command in keyring configuration mode. To delete a keyring description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Character string describing the keyring.

Defaults

The default description is blank.

Command Modes

Keyring configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **description** command inside the ISAKMP policy configuration submode to create a description for a keyring.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the creation of a keyring description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# description this is a sample keyring
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring during IKE authentication.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in ISAKMP policy configuration mode. To reset the encryption algorithm to the default value, use the **no** form of this command.

encryption {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

no encryption

Syntax Description

des	Specifies 56-bit DES-CBC as the encryption algorithm. This option is the default value.
3des	Specifies 168-bit Digital Encryption Standard (DES) as the encryption algorithm.
aes	Specifies 128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
aes 192	Specifies 192-bit AES as the encryption algorithm.
aes 256	Specifies 256-bit AES as the encryption algorithm.

Defaults

The 56-bit DES-CBC encryption algorithm (**des**).

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IKE policies define a set of parameters during IKE negotiation. Use the **encryption** command to specify the encryption algorithm in an IKE policy.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure an IKE policy with the 3DES encryption algorithm (and with all other parameters set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# encryption 3des
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

group (IKE policy)

To specify the Diffie-Hellman group identifier within an Internet Key Exchange (IKE) policy, use the **group** command in ISAKMP policy configuration mode. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

group {**1** | **2** | **5**}

no group

Syntax Description

1	Specifies the 768-bit Diffie-Hellman group. This option is the default.
2	Specifies the 1024-bit Diffie-Hellman group.
5	Specifies the 1536-bit Diffie-Hellman group.

Defaults

768-bit Diffie-Hellman (group 1)

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IKE policies define a set of parameters during IKE negotiation. Use this command to specify the Diffie-Hellman group in an IKE policy.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure an IKE policy with the 1024-bit Diffie-Hellman group (all other parameters are set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# group 2
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange (IKE) policy, use the **hash** command in ISAKMP policy configuration mode. To reset the hash algorithm to the default SHA-1 hash algorithm, use the **no** form of this command.

hash {**sha** | **md5**}

no hash

Syntax Description

sha	Specifies SHA-1 (Hashed Message Authentication Code [HMAC]) as the hash algorithm. This option is the default.
md5	Specifies Message Digest 5 (MD5) (HMAC variant) as the hash algorithm.

Defaults

SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **hash** command to specify the hash algorithm in an IKE policy. IKE policies define a set of parameters during IKE negotiation.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# hash md5
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

keepalive (ISAKMP profile)

To let the gateway send dead peer detection (DPD) messages to the Cisco IOS XR peer, use the **keepalive** command in ISAKMP profile configuration mode. To return to the default, use the **no** form of this command.

keepalive disable

no keepalive

Syntax Description

disable	Disables keepalive global declarations.

Defaults

Keepalive is enabled.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **keepalive** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# keepalive disable
```

Related Commands

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

keyring

To configure a keyring with an ISAKMP profile, use the **keyring** command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *kr-name1* [*kr-name2* [*kr-name3* [*kr-name4* [*kr-name5* [*kr-name6*]]]]]

no keyring *kr-name1* [*kr-name2* [*kr-name3* [*kr-name4* [*kr-name5* [*kr-name6*]]]]]

Syntax Description

kr-name1	Name for keyring 1 that must match the keyring name that was defined in the global configuration.
kr-name2	Name for keyring 2 that must match the keyring name that was defined in the global configuration.
kr-name3	Name for keyring 3 that must match the keyring name that was defined in the global configuration.
kr-name4	Name for keyring 4 that must match the keyring name that was defined in the global configuration.
kr-name5	Name for keyring 5 that must match the keyring name that was defined in the global configuration.
kr-name6	Name for keyring 6 that must match the keyring name that was defined in the global configuration.

Defaults

No default behavior or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. You must define at least one keyring.

An ISAKMP profile can define one or more keyrings. For example, multiple keyrings can be used when few IKE peer endpoints are in the public address space; whereas, others are in the front door virtual routing and forwarding (FVRF) space as the IKE local endpoints.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure vpnkeyring as the keyring name:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# keyring vpnkeyring
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
crypto keyring	Defines a crypto keyring during IKE authentication.
show crypto isakmp profile	Lists all the ISAKMP profiles that are defined on a router.

key-string (IKE)

To manually specify the Rivest, Shamir, and Adelman (RSA) public key of a remote peer, use the **key-string** command in public key configuration mode.

key-string *key-string*

Syntax Description

key-string	Public key for a remote peer. Enter the key in hexadecimal format.

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **key-string** command to manually specify the RSA public key of an IP Security (IPSec) peer. Before using this command, you must identify the remote peer.

To avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

When you finish specifying the RSA key, you must return to global configuration mode by entering **quit** on a new line.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually specify the RSA public keys of an IPSec peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey address 10.5.5.1
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
```

Related Commands

Command	Description
rsa-pubkey	Defines the Rivest, Shamir, and Adelman (RSA) public key by address or hostname.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime** command in ISAKMP policy configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	Length of time (in seconds) that each SA should exist before expiring. Use an integer from 60 to 86400 seconds.

Defaults

seconds: 86400 seconds (1 day)

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **lifetime** command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, it first agrees upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the lifetime of the SA expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when new IP Security (IPSec) SAs are set up.

To save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note When your local peer initiates an IKE negotiation between itself and a remote peer, if the lifetimes are not equal, an IKE policy with the shorter lifetime is selected.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure an IKE policy with an SA lifetime of 600 seconds (all other parameters are set to the defaults):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 600
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

local-address (keyring)

To limit the scope of an ISAKMP keyring configuration to a local termination address, use the **local-address** command in keyring configuration mode. To disable the feature, use the **no** form of this command.

local-address *ip-address*

no local-address *ip-address*

Syntax Description

ip-address	IP address to which to bind.

Defaults

If the **local-address** command is not configured, the ISAKMP keyring is available to all local addresses.

Command Modes

Keyring configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 130.40.1.1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# local-address 130.40.1.1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 0.0.0.0 0.0.0.0 key mykey
```

Related Commands

Command	Description
crypto isakmp identity	Specifies the identity used by the router when participating in the Internet Key Exchange (IKE) protocol.
crypto keyring	Defines a crypto keyring during IKE authentication.

match identity (ISAKMP profile)

To match the identity of a peer in an ISAKMP profile, use the **match identity** command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name* | **address** *address* [*mask*] **vrf** [*fvrf*] | **host** *hostname* | **host domain** *domain-name* | **user** *username* | **user domain** *domain-name*}

no match identity {**group** *group-name* | **address** *address* [*mask*] **vrf** [*fvrf*] | **host** *hostname* | **host domain** *domain-name* | **user** *username* | **user domain** *domain-name*}

Syntax Description

group *group-name*	Specifies a Unity group that matches identification (ID) type ID_KEY_ID. If RSA signatures are used, the *group-name* argument matches the organizational unit (OU) field of the distinguished name (DN).
address *address*	Matches the *address* argument with the ID type ID_IPV4_ADDR.
mask	The *mask* argument is used to specify a range of addresses.
vrf	Specifies the front door VPN routing and forwarding (FVRF) of the peer.
fvrf	The *fvrf* argument matches the address in the front door VPN routing and forwarding (FVRF) Virtual Private Network (VPN) space.
host *hostname*	Specifies an identity that matches the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
host domain *domain-name*	Specifies an identity that matches type ID_FQDN. The domain name is the same as the *domain-name* argument.
user *username*	Specifies an identity that matches the FQDN.
user domain *domain-name*	Specifies an identity that matches the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with *domain-name* are matched.

Defaults

No default behavior or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An ISAKMP profile configuration must have at least one **match identity** command. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the IKE exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure the group as vpngroup for the **match identity** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local tunnel_ipsec
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity address 10.1.1.6/32 vrf default
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-ipsec 3001
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
self-identity	Defines the identity that the local IKE uses to identify itself to the remote peer.
set interface tunnel-ipsec	Predefines the interface instance.
set ipsec-profile	Predefines the IPSec profile instance.

match identity (ISAKMP policy-set)

To create an SVI tunnel source, use the **match identity** command in ISAKMP policy-set configuration mode. To remove the identity, use the **no** form of this command.

match identity {**local-address** *IP-address }*

no match identity {**local-address** *IP-address}*

Syntax Description

local-address	This creates the SVI tunnel source for a remote peer.
IP-address	IP prefix for the SVI tunnel source.

Defaults

No default behavior or values

Command Modes

ISAKMP policy-set configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An ISAKMP profile configuration must have at least one **match identity** command. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the IKE exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

The IP address identified in this command requires a particular preconfigured encryption algorithm and it should be the only one operational.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure the **match identity (ISAKMP policy-set)** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy-set p1
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)# policy pol2
```

Related Commands

Command	Description
crypto isakmp policy-set	Defines a policy set for an ISAKMP protection suite.
description (ISAKMP policy-set)	Creates a description for an ISAKMP policy set.
match identity (ISAKMP policy-set)	Specifies the routing priority of a preconfigured policy.

policy (ISAKMP policy-set)

To specify the routing priority of a preconfigured policy, use the **policy** command within the ISAKMP policy-set submode. To cancel the priority, use the no variant of this command.

policy *policy-number*

no policy

Syntax Description

policy-number	From 1 to 10000, with the low end of the range signifying the highest priority.

Defaults

No default behavior or values

Command Modes

ISAKMP policy-set configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure a routing policy priority:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy-set p1
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)# policy pol2
```

Related Commands

Command	Description
description (ISAKMP policy-set)	Defines an ISAKMP policy set.
crypto isakmp policy-set	Defines a policy set for an ISAKMP protection suite.
match identity (ISAKMP policy-set)	Creates an SVI tunnel source.

pre-shared-key

To define a preshared key for IKE authentication, use the **pre-shared-key** command in keyring configuration mode. To disable, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*

no pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*

Syntax Description

address *address*	Specifies the IP address of the remote peer or a subnet and mask.
mask	(Optional) The *mask* argument matches the range of the address. The default value is 255.255.255.255.
hostname *hostname*	Specifies the fully qualified domain name (FQDN) of the peer.
key *key*	Specifies the preshared key.

Defaults

No default behaviors or values

Command Modes

Keyring configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure a preshared key using an IP address and hostname:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

Related Commands

Command	Description
crypto isakmp identity	Specifies the identity used by the router when participating in the Internet Key Exchange (IKE) protocol.
crypto keyring	Defines a crypto keyring during IKE authentication.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during IKE authentication, use the **rsa-pubkey** command in keyring configuration mode. To disable the feature, 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*	Specifies the IP address of the RSA public key of the remote peer. The *address* argument is the IP address of the remote RSA public key of the remote peer that you manually configure.
name *fqdn*	Specifies the fully qualified domain name (FQDN) of the peer.
encryption	(Optional) Specifies that the manual key is used for encryption.
signature	(Optional) Specifies that the manual key is used for a signature. The **signature** keyword is the default.

Defaults

The key is used for the signature.

Command Modes

Keyring configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **rsa-pubkey** command to enter public key 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.

When you finish specifying the RSA key, you must return to global configuration mode by entering **quit** on a new line.

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey name host.vpn.com
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
```

Related Commands

Command	Description
address	Specifies the IP address for the Rivest, Shamir, and Adelman (RSA) public key of the remote peer you manually configure.
crypto keyring	Defines a crypto keyring during IKE authentication.
key-string (IKE)	Specifies the Rivest, Shamir, and Adelman (RSA) public key of a remote peer manually.

self-identity

To define the identity that the local IKE uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the ISAKMP identity that was defined for the IKE, use the **no** form of this command.

self-identity {**address** | **fqdn** | **user-fqdn** *user-fqdn*}

no self-identity {**address** | **fqdn** | **user-fqdn** *user-fqdn*}

Syntax Description

address	Specifies the IP address of the local endpoint.
fqdn	Specifies the fully qualified domain name (FQDN) of the host.
user-fqdn *user-fqdn*	Specifies the user FQDN that is sent to the remote endpoint.

Defaults

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

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the **self-identity** command is not defined, IKE uses the globally configured value.

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RR/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# self-identity user-fqdn user@vpn.com
```

Related Commands

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

set interface tunnel-ipsec

To predefine the interface instance when IKE negotiates for tunnel mode IPSec service associations (SAs) for the traffic that is locally sourced or terminated, use the **set interface tunnel-ipsec** command in ISAKMP profile match configuration mode. To disable the feature, use the **no** form of this command.

set interface tunnel-ipsec *intf-index*

no set interface tunnel-ipsec *intf-index*

Syntax Description

intf-index	The range is from 0 to 4294967295.

Defaults

No default behavior or values

Command Modes

ISAKMP profile match configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The interface must be predefined by using the **set interface** command. Otherwise, the IKE SA cannot be established.

When the local endpoint is the IKE responder, the predefined interface is found according to the peers identity. When the local endpoint is the IKE initiator, the predefined interface is used to find the appropriate ISAKMP profile to be used. Thus, a virtual interface cannot be predefined in more than one ISAKMP profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to predefine the interface instance:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity group vpngroup
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-ipsec 50
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
set ipsec-profile	Predefines an IPSec profile instance.

set ipsec-profile

To predefine the IPSec profile instance when IKE negotiates for transport mode IPSec service associations (SAs) for the traffic that is locally sourced or terminated, use the **set ipsec-profile** command in ISAKMP profile match configuration mode. To disable the feature, use the **no** form of this command.

set ipsec-profile *profile-name*

no set ipsec-profile *profile-name*

Syntax Description

profile-name	Name of the IPsec profile.

Defaults

No default behavior or values

Command Modes

ISAKMP profile match configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The IPSec profile must be predefined by using the **set ipsec-profile** or the **set interface tunnel-ipsec** command when transport mode IPSec SAs are negotiated. Otherwise, the IKE SA cannot be established.

When the local endpoint is the IKE responder, the predefined interface is found according to the peer's identity. When the local endpoint is the IKE initiator, the predefined interface is used to find the appropriate ISAKMP profile to be used. Therefore, a virtual interface cannot be predefined in more than one ISAKMP profile.

The profile for the identity is determined based on the selected virtual interface, which can only be tunnel-ipsec.

When the local endpoint is the IKE initiator, the profile or interface configured is used to select the correct ISAKMP profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to predefine the IPSec profile instance:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local vpnprofile
```

```
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity group vpngroup
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set ipsec-profile myprofile
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
set interface tunnel-ipsec	Predefines the interface instance.

show crypto isakmp call admission statistics

To monitor the Call Admission Control (CAC) statistics of the IKE protocol, use the **show cyrpto isakmp call admission statistics** command in EXEC mode.

show cyrpto isakmp call admission statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following example shows how to display the configuration for the **show crypto isakmp call admission statistics** command:

```
RP/0/RSP0/CPU0:router# show crypto isakmp call admission statistics

------------------------------------------------------------------
               Crypto Call Admission Control Statistics
------------------------------------------------------------------
IKE Active SA Limit: 1, IKE In-Negotiation SA limit: 2
Total CPU usage limit: 100, IKE CPU usage limit: 100
Total IKE SA Count: 0, active: 0, negotiating: 0
Incoming IKE Calls: 24      , accepted 24      , rejected 0
Outgoing IKE Calls: 16      , accepted 6       , rejected 10
Total Calls: 40
Rejected IKE Calls: 10, resources low 0, limit exceeded 10
```

Table 9 describes the significant fields shown in the display.

Table 9 show crypto isakmp call admission statistics Field Descriptions

Field	Description
IKE Active SA Limit	Default value of 0 has no limitations.
In-Negotiation SA limit	Default value is 1000.
Total IKE SA Count	Number of IKE SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Calls	Number of incoming IKE SA requests. The number of incoming IKE calls equals to the total of accepted plus rejected requests.
accepted	Number of accepted incoming or outgoing IKE SA requests.
rejected	Number of rejected incoming or outgoing IKE SA requests.
Outgoing IKE Calls	Number of outgoing IKE SA requests. The number of outgoing IKE calls equals to the total of accepted plus rejected requests.
Total Calls	Total calls equals to the number of incoming IKE calls plus outgoing IKE calls.
Rejected IKE Calls	Number of IKE requests that were rejected. The number of rejected IKE calls equals to the total number of resources low plus limit exceeded.
resources low	Number of IKE requests that were rejected because system resources were low or because the preconfigured system resource limit was exceeded.
limit exceeded	Number of IKE SA requests that were rejected because the SA limit has been reached.

Related Commands

Command	Description
clear crypto isakmp call admission statistics	Clears ISAKMP call admission statistics.

show crypto isakmp errors

To display the Internet Security Association and Key Management Protocol (ISAKMP) error that occurred during tunnel establishment, use the **show crypto isakmp errors** command in EXEC mode.

show crypto isakmp errors

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto isakmp errors** command:

```
RP/0/RSP0/CPU0:router# show crypto isakmp errors

Control Plane Errors
--------------------
ERR NO MEMORY.....................................0
INVALID CERT......................................0
CRYPTO FAILURE....................................0
SA NOT AUTH.......................................0
AUTHENTICATION FAILED.............................0
GROUP AUTHOR FAILED...............................0
USER AUTHEN REJECTED..............................0
LOCAL ADDRESS FAILURE.............................0
FAILED TO CREATE SKEYID...........................0
RSA PUBLIC KEY NOT FOUND..........................0
RETRANSMITION LIMIT...............................0
MALFORMED MESSAGE.................................0
QUICK MODE TIMER EXPIRED..........................0
KEY NOT FOUND IN PROFILE..........................0
PROFILE NOT FOUND.................................0
PRESHARED KEY NOT FOUND...........................0
```

```
PHASE2 PROPOSAL NOT CHOSEN.....................0
POLICY MISMATCH................................0
NO POLICY FOUND................................0
PACKET PROCESS FAILURE.........................0

Warnings
---------
CERT DOESNT MATCH ID...........................0
CERT ISNT TRUSTED ROOT.........................0
PACKET NOT ENCRYPTED...........................0
UNRELIABLE INFO MSG............................0
NO SA..........................................0
BAD DOI SA.....................................0
UNKNOWN EXCHANGE TYPE..........................0
OUTGOING PKT TOO BIG...........................0
INCOMING PKT TOO BIG...........................0

Informational
--------------
CAC DROPS......................................0
DEFAULT POLICY ACCEPTED........................0
```

Table 10 describes the significant fields shown in the display.

Table 10 show crypto isakmp errors Field Descriptions

Field	Description
ERR NO MEMORY	A memory allocation failure has occurred in which the process cannot automatically recover. The process must be restarted to ensure correct operation. If memory is repeatedly exhausted, you can upgrade to a larger memory configuration.
INVALID CERT	The certificate, which is given by the remote peer, has either been revoked or expired (certificate invalid) or the signature check on the certificate failed (bad signature). We recommend to contact the CA of the remote peer to report a possible bad CA certificate.
CRYPTO FAILURE	IKE found a failure that is returned from encryption or decryption service. We recommend to contact the remote peer's administrator.
SA NOT AUTH	The IKE security association with the remote peer was not authenticated; however, the peer attempted to begin a Quick Mode exchange. The exchange must be done only with an authenticated security association. We recommend to contact the peer's administrator.
AUTHENTICATION FAILED	The IKE process was unable to authenticate the security association with the remote peer. We recommend to contact the peer's administrator.

Table 10 show crypto isakmp errors Field Descriptions (continued)

Field	Description
GROUP AUTHOR FAILED	Group authorization failed. We recommend to check the connectivity for AAA.
USER AUTHEN REJECTED	Phase 1.5 (Xauth) processing failed with the peer. You must ensure that the password, which was delivered, matches the client. Otherwise, contact Cisco Technical Support with the exact log message that was received.
LOCAL ADDRESS FAILURE	Failed to allocate IP address for the client. You must ensure that the IP local pool is defined and contains at least one free address. In addition, ensure that the specific pool is assigned to the proper ISAKMP profile from the **show crypto isakmp profile** command. Otherwise, contact Cisco Technical Support with the exact log message that was received.
FAILED TO CREATE SKEYID	Failed to generate SKEYID. We recommend to contact Cisco Technical Support.
RSA PUBLIC KEY NOT FOUND	Failed to query the RSA key. You can check the subject name in the certificate.
RETRANSMITION LIMIT	Retransmission limit exceeded. We recommend to contact your administrator.
MALFORMED MESSAGE	A quick sanity check is done on all received ISAKMP messages to verify that all component payload types are valid, and that the sum of their individual lengths equals to the total length of the received message. This message failed the sanity check. The continuous bad messages can imply the denial of a service attack. We recommend to contact the peer's administrator.
QUICK MODE TIMER EXPIRED	We cannot always wait before we start Quick Mode and initiate Phase 2. Most likely, the reason for failing to start Phase 2 is that the process failed to complete Phase I. If so, it should have also logged another message that should appear immediately before this one.

Table 10 show crypto isakmp errors Field Descriptions (continued)

Field	Description
KEY NOT FOUND IN PROFILE	In Main Mode, the ID payloads are exchanged only in MM5 and MM6. Since keyring material is needed in earlier stages of the negotiation, it is looked up based on peer address. The error is seen when the selected keyring appears to not match the keyring configured under the ISAKMP profile for that peer. You must ensure that the keyring in which the key exist is attached to the ISAKMP profile.
PROFILE NOT FOUND	The following explanations are listed: • No ISAKMP profile is found that matches the peer identity. This is applicable only to RESPONDER mode. • No ISAKMP profile is found that matches the interface name. This is applicable only to INITIATOR mode. • Peer identity does not match the ISAKMP profile that is associated with the interface. This is applicable only to INITIATOR mode. The following recommendations are listed: • You must ensure an ISAKMP profile exists for the peer match-id. • You must ensure that the ISAKMP profile is attached to the proper interface. • You must ensure that the ISAKMP profile, which is attached to the interface, matches the peers identity.
PRESHARED KEY NOT FOUND	Failed to find preshared key. We recommend to contact the administrator.
PHASE2 PROPOSAL NOT CHOSEN	Phase 2 parameters negotiation failed with the peer. We recommend to contact the peer's administrator.
POLICY MISMATCH	Phase 1policy parameters negotiation failed with peer. We recommend to contact the peer's administrator.

Table 10 show crypto isakmp errors Field Descriptions (continued)

Field	Description
NO POLICY FOUND	The peer key failed to derive through either of the following ways: • Preshared keys • RSA keys • Certificates We recommend to contact the administrator.
PACKET PROCESS FAILURE	The error message implies a severe error condition, which likely resulted from an internal error. We recommend to contact Cisco Technical Support.
CERT DOESNT MATCH ID	The peers claimed that the identity does not match what we can gather from the certificate. If the session does not come up, you can contact the remote peer or the administrator.
CERT ISNT TRUSTED ROOT	During IKE Phase I signature verification, the initiator sends a list of the CA certificates. This warning is printed by the responder if none of the CAs in the list is a trusted root. **Note** This is not necessarily an error, as there can be multiple cert-req payloads. If the session does not come up, you can contact the remote peer or the administrator.
PACKET NOT ENCRYPTED	The received packet should have been encrypted by the peer but it was not. We recommend to contact the remote peer's administrator.
UNRELIABLE INFO MSG	The received INFO message before the peer is authenticated, which is why it called unreliable. We recommend to contact the remote peer's administrator.
NO SA	No security association exists for this packet and it is not an initial offer from the peer to establish one. These errors can imply the denial of a service attack. We recommend to contact the remote peer or the administrator.

Table 10 show crypto isakmp errors Field Descriptions (continued)

Field	Description
BAD DOI SA	The DOI field in a SA offer is needed for message parsing. SA offer with unknown DOI can't be parsed. If the situation persists, you can contact the remote peer's administrator.
UNKNOWN EXCHANGE TYPE	IKE performs actions on messages that are based on defined exchanges. A message is received with an unknown exchange. If the problem appears to be more than a transient one, you can contact the peer's administrator.
OUTGOING PKT TOO BIG	Trying to send an ISAKMP packet that is above the maximum UDP packet size allowed, which can happen if an extremely large number of IKE policies were being proposed by the initiator. You can try to reduce the number of ISAKMP policies configured.
INCOMING PKT TOO BIG	The packet size is limited to 3K, which the peer sends out long length info that forces a large buffer allocation, for example, Denial-of-Service (DoS). We recommend that you contact the remote peer or the administrator.
CAC DROPS	The Call Admission Control (CAC) policy is configured on the device. Consequently, an IKE SA request was denied due to the reason described in the error message. Depending on the reason that the request was denied, you can either reduce the load on the system so that it can handle new IKE SA requests, or increase the maximum allowed IKE sessions if more are needed.
DEFAULT POLICY ACCEPTED	The default policy is being used because the local configured policies did not match with the peer's policies. You can check if this is indeed the desired ISAKMP policy to use. To avoid using the default policy, you can reconfigure the local policy to match with the peer's policy.

Related Commands

Command	Description
clear crypto isakmp errors	Clears the statistics for the ISAKMP errors.

show crypto isakmp key

To display the Internet Security Association and Key Management Protocol (ISAKMP) preshared keys for a router, use the **show crypto isakmp key** command in EXEC mode.

show crypto isakmp key

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following example shows how to display the IP hostname and address preshared keys:

```
RP/0/RSP0/CPU0:router# show crypto isakmp key

Keyring         Hostname/Address      Preshared Key
K1              3.3.3.1               rd26
K2              5.5.5.5               ex22
K2              tzvi.cisco.com        ppp
```

Table 11 describes the significant fields shown in the display.

Table 11 show crypto isakmp key Field Descriptions

Field	Description
Hostname/Address	IP hostname or address of the router.
Preshared Key	ISAKMP preshared key for the router.

show crypto isakmp peers

To display peer structures, use the **show crypto isakmp peers** command in EXEC mode.

show crypto isakmp peers [*ip-address* | **vrf** *vrf-name*]

Syntax Description

ip-address	(Optional) IP address of the peer.
vrf *vrf-name*	(Optional) Specifies the front door VRF of the peer. The *vrf-name* argument is the name assigned to a VRF.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following example shows sample output from the **show crypto isakmp peers** command:

```
RP/0/RSP0/CPU0:router# show crypto isakmp peers

Peer: 10.0.83.1   Port: 4500   Local: 30.0.0.4   vrf: default
  UDP encapsulate: True
  SA information:
    Connection ID: 1
    State: QM_IDLE
    Phase 1 ID: DER_ASN1_DN srbu
```

Table 12 describes the significant fields shown in the display.

Table 12 show crypto isakmp peers Field Descriptions

Field	Description
Connection ID	Internet Key Exchange (IKE) ID.
State	Output display for the various states. For a detailed description of each state, see Table 16 on page 202.
Phase1 ID	Internet Key Exchange (IKE) ID.

Related Commands

Command	Description
crypto isakmp peer	Enables an IP Security (IPSec) peer for Internet Key Exchange (IKE).
description (ISAKMP peer)	Adds the description of an Internet Key Exchange (IKE) peer.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in EXEC mode.

show crypto isakmp policy

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto isakmp policy** command after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
RP/0/RSP0/CPU0:router# show crypto isakmp policy

Protection suite priority 15
    encryption algorithm: DES - Data Encryption Standard (56 bit keys)
    hash algorithm: Message Digest 5
    authentication method:  Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group: #2 (1024 bit)
    lifetime: 5000 seconds, no volume limit
Protection suite priority 20
    encryption algorithm: DES - Data Encryption Standard (56 bit keys)
    hash algorithm: Secure Hash Standard
    authentication method: preshared Key
    Diffie-Hellman Group: #1 (768 bit)
    lifetime: 10000 seconds, no volume limit
Default protection suite
    encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
    hash algorithm: Secure Hash Standard
    authentication method: Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group: #1 (768 bit)
```

```
lifetime: 86400 seconds, no volume limit
```

Note Although the output shows "no volume limit" for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

Table 13 describes the significant fields shown in the display.

Table 13 show crypto isakmp policy Field Descriptions

Field	Description
encryption algorithm	Encryption algorithm within the IKE policy.
hash algorithm	Hash algorithm within the IKE policy.
authentication method	Authentication method used in the IKE policy.
Diffie-Hellman group	Diffie-Hellman group identifier in the IKE policy.
lifetime	Length of time (in seconds) the security association (SA) exists before expiring.

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto isakmp profile

To list all the ISAKMP profiles that are defined on a router, use the **show crypto isakmp profile** command in EXEC mode.

show crypto isakmp profile [**interface** *intf-name* | **ipsec-profile** *ipsec-prof-name* | **tag** *isakmp-prof-name*]

Syntax Description

interface *intf-name*	(Optional) Displays the ISAKMP profile by the interface for the IPSec match ID.
ipsec-profile *ipsec-prof-name*	(Optional) Displays the ISAKMP profile by the IPSec profile for the IPSec match ID.
tag *isakmp-prof-name*	(Optional) Displays the ISAKMP profile by name.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto isakmp profile** command:

```
RP/0/RSP0/CPU0:router# show crypto isakmp profile

ISAKMP Profile: isakmp-prof2
   Keyring(s): kr2
   Identities matched are:
      Address: 10.0.2.1 255.255.255.255 fvrf: green
         Interface: service-ipsec2

ISAKMP Profile: isakmp-prof1
   Keyring(s): kr1
   Identities matched are:
      Group: srbu
         Interface: service-gre1
```

Table 14 describes the fields for the **show crypto isakmp profile** command.

Table 14 show crypto isakmp profile Field Descriptions

Field	Description
ISAKMP Profile	Name of the ISAKMP profile.
Keyring(s)	Name for keyring that must match the keyring name that was defined in the global configuration.
Identities matched are	All identities that the ISAKMP profile can match.

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
keyring	Configures a keyring with an ISAKMP profile.

show crypto isakmp sa

To display all current Internet Key Exchange (IKE) security associations (SAs) at a peer, use the **show crypto isakmp sa** command in EXEC mode.

show crypto isakmp sa [*connection ID*]

Syntax Description		
	connection ID	(Optional) IKE SA identifier. The range is from 1 to 65535.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the *connection ID* argument to display the list of identifiers.'

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto isakmp sa** command, after IKE negotiations have been successfully completed between two peers:

```
RP/0/RSP0/CPU0:router# show crypto isakmp sa

vrf            dst            src            state          conn-id    nodeid
----------     ------------   ------------   ---------      -------    ------
default        30.0.0.4       10.0.83.1      QM_IDLE        1          0
```

Table 15 describes the fields shown in the display. Table 16 shows the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it is most likely in its quiescent state (QM_IDLE). For long exchanges, some MM_*xxx* states may be observed.

Table 15 show crypto isakmp sa Field Descriptions

Field	Description
vrf	Virtual route forwarding (VRF) for the ISAKMP SA details per VRF.
dst	Destination IP address.
src	Source IP address.
state	Table 16 shows the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it is most likely in its quiescent state (QM_IDLE). For long exchanges, some MM_*xxx* states may be observed.
conn-id	Connection ID.
nodeid	Node ID.

Table 16 Mode States

State: Main Mode Exchange	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state makes the transition immediately to QM_IDLE, and a quick mode exchange begins.
State: Aggressive Mode Exchange	**Explanation**
AG_NO_STATE	The ISAKMP SA has been created but nothing else has happened yet. It is “larval” at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state makes the transition immediately to QM_IDLE, and a quick mode exchange begins.
State: Quick Mode Exchange	**Explanation**
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

Command	Description
show crypto isakmp stats	Displays the number of ISAKMP security associations (SAs).
show crypto isakmp stats	Displays the ISAKMP security association (SA) details.

show crypto isakmp stats

To display the information for ISAKMP global statistics, use the **show crypto isakmp stats** command in EXEC mode.

show cryto isakmp stats [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the ISAKMP statistics per VPN routing and forwarding (VRF) instance. The *vrf-name* argument is the name assigned to a VRF.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show crypto isakmp stats** command to display the ISAKMP statistics per VRF instance. If the VRF instance is not specified, the default for the statistics of the VRF instance is shown.

The following global statistics are printed from the **show crypto isakmp stats** command:

- Active ISAKMP SAs
- ISAKMPs that are currently being negotiated
- Maximum number of concurrent ISAKMP SAs
- Maximum number of concurrent established SAs
- Number of expired SAs

Task ID

Task ID	Operations
crypto	read

Examples

The following example displays sample output from the **show crypto isakmp stats** command:

```
RP/0/RSP0/CPU0:router# show crypto isakmp stats

VRF ISAKMP statistics:
```

```
Active Tunnels:                 0
Previous Tunnels:               0

In Octets:                      0
In Packets:                     0
In Drop Packets:                0
In Notifys Messages:            0
In Phase2 Exchanges:            0
In Phase2 Exchange Invalids:    0
In Phase2 Exchange Rejects:     0
In Phase2 SA Delete Requests:   0

Out Octets:                     0
Out Packets:                    0
Out Drop Packets:               0
Out Notifys Messages:           0
Out Phase2 Exchanges:           0
Out Phase2 Exchange Invalids:   0
Out Phase2 Exchange Rejects:    0
Out Phase2 SA Delete Requests:  0

Initiator Tunnels:              0
Initiator Tunnel Setup Fails:   0
Responder Tunnel Setup Fails:   0
Sys Cap Fails:                  0
Auth Failures:                  0
Decryption Fails:               0
Hash Valid Fails:               0
No SA Fails:                    0
```

Table 17 describes the significant fields shown in the display.

Table 17 show crypto isakmp stats Field Descriptions

Field	Description
Active Tunnels	The number of currently active IPSec Phase-1 IKE Tunnels.
Previous Tunnels	The total number of previously active IPSec Phase-1 IKE Tunnels.
In Octets	The total number of octets received by all currently and previously active IPSec Phase-1 IKE Tunnels.
In Packets	The total number of packets received by all currently and previously active IPSec Phase-1 IKE Tunnels.
In Drop Packets	The total number of packets that were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels.
In Notifys Messages	The total number of notifications that are received by all currently and previously active IPSec Phase-1 IKE Tunnels.
In Phase2 Exchanges	The total number of IPSec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels.

Table 17 show crypto isakmp stats Field Descriptions (continued)

Field	Description
In Phase2 Exchange Invalids	The total number of IPSec Phase-2 exchanges that were received and found to be invalid by all currently and previously active IPSec Phase-1 IKE Tunnels.
In Phase2 Exchange Rejects	The total number of IPSec Phase-2 exchanges that were received and rejected by all currently and previously active IPSec Phase-1 IKE Tunnels.
In Phase2 SA Delete Requests	The total number of IPSec Phase-2 security association delete requests received by all currently and previously active and IPSec Phase-1 IKE Tunnels.
Out Octets	The total number of octets sent by all currently and previously active and IPSec Phase-1 IKE Tunnels.
Out Packets	The total number of packets sent by all currently and previously active and IPSec Phase-1 Tunnels.
Out Drop Packets	The total number of packets that were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels.
Out Notifys Messages	The total number of notifications that are sent by all currently and previously active IPSec Phase-1 IKE Tunnels.
Out Phase2 Exchanges	The total number of IPSec Phase-2 exchanges which were sent by all currently and previously active IPSec Phase-1 IKE Tunnels.
Out Phase2 Exchange Invalids	The total number of IPSec Phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPSec Phase-1 Tunnels.
Out Phase2 Exchange Rejects	The total number of IPSec Phase-2 exchanges that were sent and rejected by all currently and previously active IPSec Phase-1 IKE Tunnels.
Out Phase2 SA Delete Requests	The total number of IPSec Phase-2 SA delete requests that are sent by all currently and previously active IPSec Phase-1 IKE Tunnels.
Initiator Tunnels	The total number of IPSec Phase-1 IKE Tunnels that were locally initiated.
Initiator Tunnel Setup Fails	The total number of IPSec Phase-1 IKE Tunnels that were locally initiated and failed to activate.
Responder Tunnel Setup Fails	The total number of IPSec Phase-1 IKE Tunnels that were remotely initiated and failed to activate.
Sys Cap Fails	The total number of system capacity failures that occurred during processing of all current and previously active IPSec Phase-1 IKE Tunnels.

Table 17 show crypto isakmp stats Field Descriptions (continued)

Field	Description
Auth Failures	The total number of authentications that ended in failure by all current and previous IPSec Phase-1 IKE Tunnels.
Decryption Fails	The total number of decryptions that ended in failure by all current and previous IPSec Phase-1 IKE Tunnels.
Hash Valid Fails	The total number of hash validations that ended in failure by all current and previous IPSec Phase-1 IKE Tunnels.
No SA Fails	The total number of nonexistent Security Association in failures that occurred during processing of all current and previous IPSec Phase-1 IKE Tunnels.

show crypto key pubkey-chain rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys stored on your router for the peer, use the **show crypto key pubkey-chain rsa** command in EXEC mode.

show crypto key pubkey-chain rsa [**name** *key-name* | **address** *key-address*]

Syntax Description

name *key-name*	(Optional) Displays the name of a particular public key.
address *key-address*	(Optional) Displays the address of a particular public key.

Defaults

All RSA public keys stored on your router is displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display RSA public keys stored on your router. The display includes the RSA public keys for the peer that were manually configured at your router and keys received by your router through other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any public key derived by certificates are lost because the router asks for certificates again, at which time the public key is derived again.

Use the **name** or **address** keyword to display details about a particular RSA public key stored on your router.

If no keyword is used, this command displays a list of all RSA public keys stored on your router.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto key pubkey-chain rsa** command:

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code Usage      IP-Address        VRF             Keyring      Name
M    Encrypt                                      K1           example.cisco.com
M    Signing    5.5.5.5           green           K2
```

The following example shows manually configured special-usage RSA public keys for the peer named somerouter. This example also shows three keys obtained from peer certificates: two special-usage keys for peer routerA and a general-purpose key for peer routerB.

Certificate support is used in the example; if certificate support were not in use, none of the peer keys would show "C" in the Code column, and would all need to be manually configured.

Table 18 describes the significant fields shown in the display.

Table 18 show crypto key pubkey-chain rsa Field Descriptions

Field	Description
Code	RSA public keys that were manually configured on your router (M) and keys received by your router through other means, such as by a certificate (C).
Usage	Type of RSA keys generated.
IP-address	IP address of the local or remote peer for which RSA keys are being configured.
VRF	The virtual route forwarding (VRF) of the keyring.
Keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
Name	Name of the local or remote peer.

The following sample output is from the **show crypto key pubkey-chain rsa** command for the **name** keyword that names the public key as somerouter.example.com:

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa name somerouter.example.com

Key name: somerouter.example.com
Key address: 10.0.0.1
 Usage: Signature Key
 Source: Manual
 Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 10.0.0.1
 Usage: Encryption Key
 Source: Manual
 Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

Note The Source field in the example indicates "Manual," meaning that the keys were manually configured on the router, not received in the certificate from the peer.

The following sample output is from the **show crypto key pubkey-chain rsa** command for address 192.168.10.3:

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa address 192.168.10.3

Key name: routerB.example.com
Key address: 192.168.10.3
 Usage: General Purpose Key
```

```
Source: Certificate
Data:
 0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
 58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
 0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

The Source field in the example indicates “Certificate,” meaning that the keys were received by the router by way of the certificate from the other router.

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in EXEC mode.

show crypto session [**detail** | **fvrf** *fvrf-name* [**detail**] | **group** *group-name* | **groups** | **interface** *interface-name* | **ivrf** *ivrf-name* | **local** *IP-address* [**fvrf** *fvrf-name* | **detail**] | **profile** *profile-name* [**detail**] | **remote** *IP-address* [**detail** | **port** *remote-port* | **fvrf** *fvrf-name*] | **user** *username* [**detail**] | **users**]

Syntax Description

detail	(Optional) Provides more detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP Security (IPSec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPSec SA.
fvrf *vrf-name*	(Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session. The *fvrf-name* argument is the name assigned to a FVRF.
group *group-name*	(Optional) Displays the usage for the group identity name that is currently active on the Virtual Private Network (VPN) device. The *group name* argument is the identity name for the group.
groups	(Optional) Displays the usage for all the connected groups that are currently active on the Virtual Private Network (VPN) device.
interface *interface-name*	Non-operational on Cisco ASR 9000 Series Routers; the default interface is *tunnel-ipsec,* or IPSec tunnel interfaces.
ivrf *ivrf-name*	(Optional) Displays status information about the inside VRF (IVRF) session. The *ivrf-name* argument is the name of the inside VRF.
local *IP-address*	(Optional) Displays status information about crypto sessions of a local crypto endpoint. The *IP address* argument is the IP address of the local crypto endpoint.
profile *profile-name*	(Optional) Displays Internet Security Association and Key Management Protocol (ISAKMP) profiles that are defined on a router. The *profile name* argument is the name of the ISAKMP profile.
remote *IP-address*	(Optional) Displays status information about crypto sessions of a remote session.The *IP address* argument is the IP address of the remote crypto endpoint.
port *remote-port*	(Optional) Displays status information about crypto sessions of a remote crypto endpoint. The *remote-port* argument is from 1 to 65535. The default value is 500.
user *username*	(Optional) Displays the usage for the connected user. The *user name* argument is the name of the user.
users	(Optional) Displays the usage for all the connected users.

Defaults

If the **show crypto session** command is entered without any keywords, all existing sessions are displayed. Port default values are 500.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Routers.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can get a list of all the active ISAKMP sessions and of the IKE and IPSec SAs for each session by using the **show crypto session** command. The following list is included:

- Interface
- IKE SAs that are associated with the peer by whom the IPSec SAs are created
- IPSec SAs serving the flows of a session

Multiple IKE or IPSec SAs are established for the same peer (for the same session), in which case, IKE peer descriptions are repeated with different values for the IKE SAs that are associated with the peer and for the IPSec SAs that are serving the flows of the session.

Task ID

Task ID	Operations
crypto	read

Examples

The following example shows the list of fields from the **show crypto session** command:

```
RP/0/RSP0/CPU0:router# show crypto session

Interface:      tunnel-ipsec3001
Profile:        TUNNEL_IPSEC
ISAKMP policy:  10
Fvrf:           default
Ivrf:           default
Peer:           10.1.1.5/500
Ike SAs:        1
IPsec Flows:      1
  IKE SA : conn-id 1 local 10.1.1.6/500 remote 10.1.1.5/500  QM_IDLE
  IPSEC FLOW 1: permit ipv4 10.7.208.2/255.255.255.255 10.7.208.2/255.255.255.255
        Active SAs 2
```

The following example shows the detailed information of the session:

```
RP/0/RSP0/CPU0:router# show crypto session detail

Interface:      tunnel-ipsec3001
Profile:        TUNNEL_IPSEC
ISAKMP policy:  10
Fvrf:           default
Ivrf:           default
Peer:           10.1.1.6/500
Ike SAs:        1
IPsec Flows:      1
  IKE SA : conn-id 2 local 10.1.1.5/500 remote 10.1.1.6/500  QM_IDLE
```

```
IPSEC FLOW 2: permit ipv4 10.7.208.2/255.255.255.255 10.7.208.2/255.255.255.255
      Active SAs 2
      Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 100000000/3249
      Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 100000000/3249
```

Table 19 describes the significant fields shown in the display.

Table 19 show crypto session Field Descriptions

Field	Description
Interface	Interface to which the crypto session is related.
IKE SA	Information is provided about the IKE SA, such as local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPSec-protected traffic flow, such as what the flow is; how many IPSec SAs there are; the origin of the SA; the number of encrypted or decrypted packets or dropped packets; and the IPSec SA remaining lifetime in kilobytes per second.

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IP Security [IPSec] and Internet Key Exchange [IKE] security associations [SAs]).
description (ISAKMP peer)	Adds the description of an Internet Key Exchange (IKE) peer.
show crypto isakmp peers	Displays peer structures.