IPSec Stateful Failover (VPN High Availability)

Feature History

Release	Modification
12.2(11)YX	This feature was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

This document describes IPSec Stateful Failover (VPN High Availability) in Cisco IOS Release 12.2(14)SU2, 12.2(14)SU1, 12.2(14)SU, 12.2(11)YX1, and 12.2(11)YX, and contains the following sections:

Feature Overview

IPSec Stateful Failover (VPN High Availability) is a feature that enables a router to continue processing and forwarding packets after a planned or unplanned outage. You can employ a backup (standby) router that automatically takes over the primary (active) router's tasks in the event of an active router failure. The process is transparent to users and to remote IPSec peers. The time that it takes for the standby router to take over depends on HSRP timers.

IPSec Stateful Failover (VPN High Availability) is designed to work in conjunction with Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP) with IPSec. When used together, RRI and HSRP provide a more reliable network design for VPNs and reduce configuration complexity on remote peers.

RRI and HSRP are supported together with the restriction that the HSRP configuration on the outside interface uses equal priorities on both routers. As an option, when not using RRI, you can use an HSRP configuration on the LAN side of the network (equal HSRP priority restriction still applies).

Reverse Route Injection (RRI)

RRI is a feature designed to simplify network design for VPNs which require redundancy and routing. RRI works with both dynamic and static crypto maps. When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This causes traffic flows requiring IPSec to be directed to the appropriate head-end VPN router for transport across the correct security associations (SAs) to avoid IPSec policy mismatches and possible packet loss.

Hot Standby Router Protocol (HSRP)

HSRP is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. By providing network redundancy for IP networks, user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

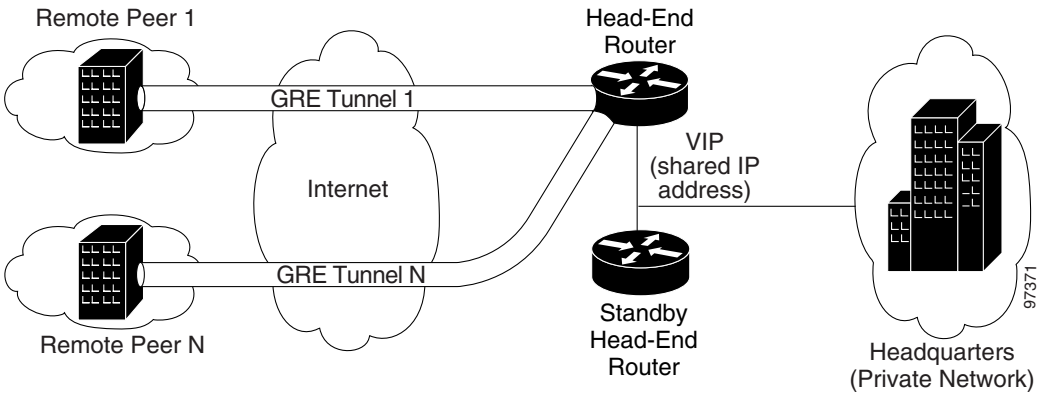
A network administrator enables HSRP, assigns a virtual IP address, and enables IPSec Stateful Failover (VPN High Availability). After enabling both HSRP and IPSec Stateful Failover, the network administrator uses the **show ssp**, **show crypto ipsec**, and **show crypto isakmp** commands to verify that all processes are running properly. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN peers.

The information that the active router transmits to the standby router includes:

- IKE cookies stamp
- Session keys
- Cisco Service Assurance (SA) Agent attributes
- Sequence number counter and window state
- Kilobyte (KB) lifetime expirations
- Dead peer detection (DPD) sequence number updates

Figure 1 shows a sample topology for site-to-site configuration of IPSec Stateful Failover with generic routing encapsulation (GRE), a tunnel interface not tied to specific "passenger" or "transport" protocols. GRE supports multicast traffic, critical for V3PN applications.

Figure 1 Site-to-Site VPN Configuration



There are four possible configurations for the Cisco 7200 series routers using Cisco IOS Release 12.2(14)SU, 12.2(14)SU1, or 12.2(14)SU2:

- non-GRE High Availability (HA) with a virtual IP (VIP), or redundancy groups, on the outside and a VIP on the inside (see Figure 2)
- non-GRE HA with only VIPs on the outside. The route to the outside is provided by Reverse Route Injection (RRI) (see Figure 3)
- GRE HA, with VIPs on the outside and tested inside faces (see Figure 4)
- GRE HA, with only a VIP on the outside, using RRI to inject routes (see Figure 5)

Figure 2 HSRP VIP on Inside and Outside

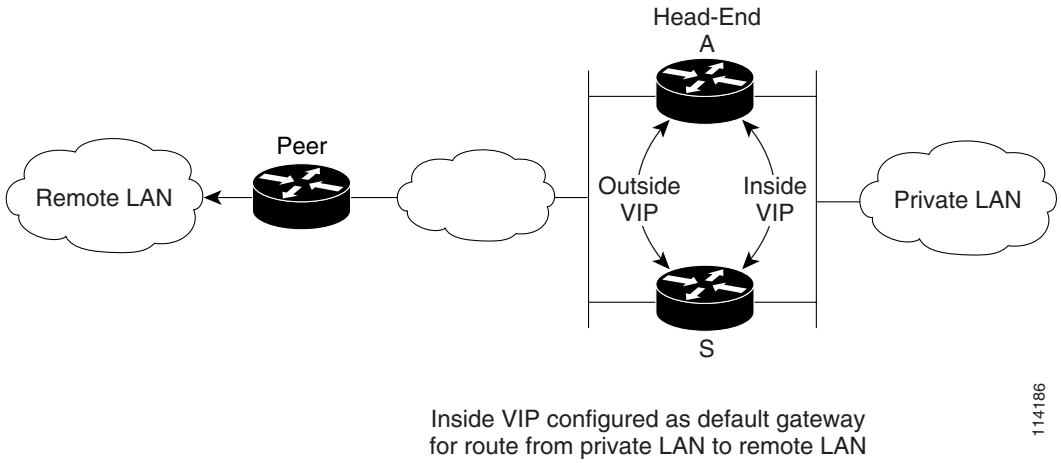
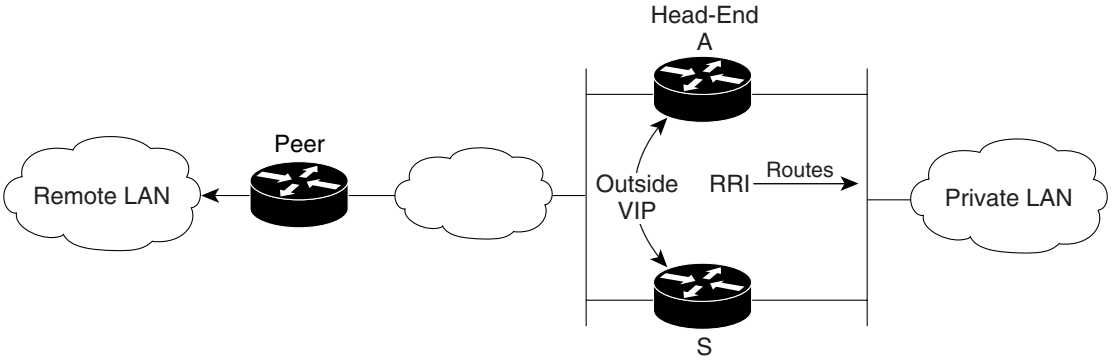
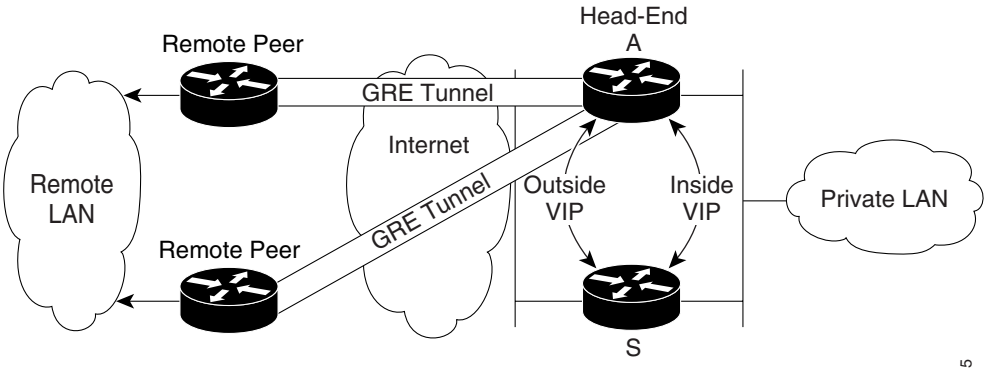


Figure 3 HSRP VIP on Outside, RRI Injected Routes on Inside



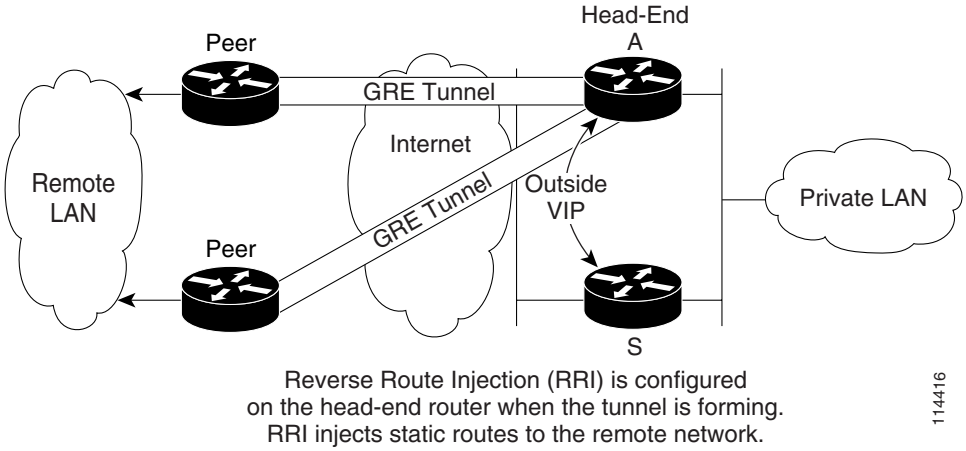
Reverse Route Injection (RRI) is configured on the head-end router when the tunnel is forming. RRI injects static routes to the remote network.

Figure 4 GRE HA with VIPs on the Outside and Inside Faces



Inside VIP configured as default gateway for route from private LAN to remote LAN

Figure 5 GRE HA with Only a VIP on the Outside, Using RRI to Inject Routes



Feature Summary

Table 1 provides a summary of features, by Cisco IOS software release.

Table 1 Feature List Comparison

Feature	12.2(11)YX	12.2(11)YX1	12.2(14)SU	12.2(14)SU1	12.2(14)SU2
GRE + IPSec Stateful Failover	No	Yes	Yes	Yes	Yes
Encrypted Pre-Shared Keys	No	No	Yes	Yes	Yes
AES support	No	No	Only for pre-shared keys	Only for pre-shared keys	Only for pre-shared keys
G1 processor	No	No	Yes	Yes	Yes
VAM	Yes	Yes	Yes	Yes	Yes
VAM2	No	No	Yes	Yes	Yes

Benefits

- IPSec VPN tunnels assigned to an active router will automatically be transitioned to a standby router upon any active router failure. Any transition from an active router to a standby router is transparent to peers, and requires no remote peer adjustment or reconfiguration.
- Businesses employing IPSec Stateful Failover (VPN High Availability) are 100% redundant with regard to IPSec VPN traffic.
- Utilizing IPSec Stateful Failover (VPN High Availability) does not appreciably affect overall router performance.
- Generic routing encapsulation (GRE) supports multicast traffic, critical for V3PN applications.

Restrictions

- Does not support failover of IKECFG attributes.
- Does not support IKE XAUTH states.
- Supports just a single VAM/VAM2 card in each active/standby router.
- Requires identical security policy configurations on both active and standby routers.
- Requires that IKE keepalives must not be used; enabling this feature will cause the connection to be torn down after the standby router assumes ownership control.
- Supports keepalives only with dead peer detection (DPD).
- Requires that priority values are equal on both active and standby routers for IP redundancy.
- IPSec MIB statistics could be erroneous on the standby router after a failover.
- Requires that active and standby routers be connected to an Ethernet interface.
- Does not support Cisco VPN Client 3.X client.
- Does not support PKI certificates.

Related Features and Technologies

- Internet Key Exchange (IKE)
- IP Security (IPSec)
- Reverse Route Injection (RRI)
- Hot Standby Router Protocol (HSRP)
- State Synchronization Protocol (SSP)

Related Documents

- HSRP Features and Functions

Supported Platforms

- Cisco 7200 series

Supported Standards, MIBs, and RFCs

Standards

- None

MIBs

- None

  To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

- None

Prerequisites

You must configure IPSec and IKE on the router and a crypto map to all interfaces that require encryption service. See the "Configuration Tasks" section on page 7 for configuration procedures.

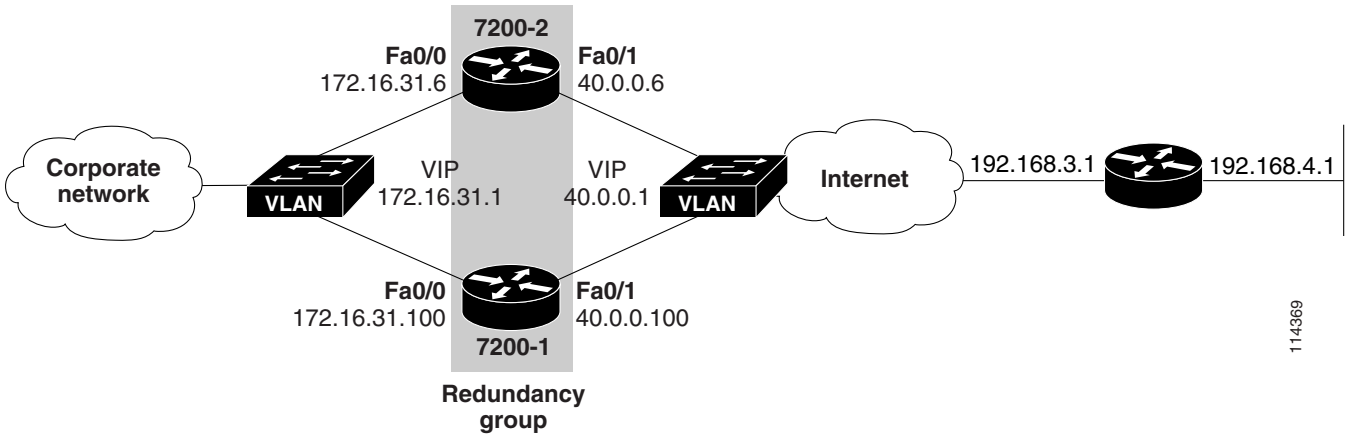
- Cisco IOS Release 12.2(14)SU2, 12.2(14)SU1, 12.2(14)SU, 12.2(11)YX1, or Cisco IOS Release 12.2(11)YX
- Two Cisco 72xx routers configured with the same Cisco IOS release
- HSRP running

Configuration Tasks

See Figure 6 and use the following commands to implement, maintain, and debug IPSec Stateful Failover (VPN High Availability).

- Configuring HSRP, page 8 (required)
- Configuring an IKE Policy, page 10 (required)
- Configuring IKE Pre-Shared Key, page 11 (required)
- Configuring an IPSec Transform Set, page 12 (required)
- Configuring Crypto Access Lists for IPSec Traffic, page 15 (required)
- Configuring Crypto Maps, page 17 (required)
- Configuring SSP Communications, page 20 (required)
- Applying Crypto Map Sets to Interfaces and Enabling Transferring IPSec State, page 21 (required)

Figure 6 Sample Configuration for IPSec Stateful Failover (VPN High Availability



Configuring HSRP

This section describes the Hot Standby Router Protocol (HSRP) Support for Virtual Private Networks (VPNs) and includes the following sections:

- Enabling HSRP, page 9
- Configuring HSRP Group Attributes, page 9
- Configuring HSRP Examples, page 9

The HSRP Support for VPNs feature ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table.

Keep in mind the following when configuring HSRP:

- Both the inside (private) and outside (public) interfaces must belong to separate HSRP groups. The interfaces then must track each other.
- The HSRP state of the inside and outside interface of each must be the same, that is, both must be active or both must be standby, otherwise there will be a black hole - packets won't have a route out of the private network. To avoid having one interface on standby while another is on active, confirm the conditions below:
  - Standby priorities should be equal on active and standby routers. If they are not, IPSec Stateful failover may or may not occur automatically when the active router fails.
  - The IP addresses on the HSRP-tracked interfaces on the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state based on IP address. If an addressing scheme exists so that the public IP address of router A is lower than the public IP address of router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could happen, which will break IPSec connectivity.

Enabling HSRP

To enable the HSRP on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# standby [hsrp-group-number] ip ip-address`	Enables the HSRP.
Repeat this command to enable HSRP on each router.	

Configuring HSRP Group Attributes

To configure other HSRP group attributes that affect how the local router participates in HSRP, use one or more of the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime`	Configures the time between hello packets and the hold time before other routers declare the active router to be down.
`Router(config-if)# standby [group-number] [priority priority] preempt [delay [minimum | sync] delay]`	Sets the Hot Standby priority used in choosing the active router. The priority value range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. Specify that, if the local router has priority over the current active router, the local router should attempt to take its place as the active router. Configure a preemption delay, after which the Hot Standby router preempts and becomes the active router.
`Router(config-if)# standby [group-number] track type number [interface-priority]`	Configures the interface to track other interfaces, so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered.
`Router(config-if)# standby [group-number] name`	Configures the standby group name for the interface.
Repeat this command to enable HSRP on each router.	

Configuring HSRP Examples

The following example shows how to configure the outside interface:

```
Router(config-if)# interface fastEthernet 0/1
Router(config-if)# standby 1 ip 40.0.0.1
Router(config-if)# standby 1 name isp
Router(config-if)# standby 1 timers msec 500 3
Router(config-if)# standby delay minimum 30 reload 60
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 track fastEthernet 0/0
```

Note The **standby delay** command is not essential, but recommended. All other commands are required.

The following commands shows how to configure the HSRP inside interface:

```
Router(config-if)# interface fastEthernet 0/0
Router(config-if)# standby 2 ip 172.16.31.1
Router(config-if)# standby 2 name lan
```

```
Router(config-if)# standby 2 timers msec 500 3
Router(config-if)# standby delay minimum 30 reload 60
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 track fastEthernet 0/1
```

Note Configure the same commands on Router 2, including the same HSRP priority values (the default is 100) as on Router 1.

Configuring an IKE Policy

If you do not specify a value for a parameter, the default value is assigned. For information on default values, refer to the "IP Security and Encryption" chapter of the *Security Command Reference* publication.

To configure an IKE policy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto isakmp policy` *priority*	Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode.
Step 2	`Router(config-isakmp)# encryption {des | 3des | aes | aes 192 | aes 256}`	Specifies the encryption algorithm within an IKE policy. • **des**—Specifies 56-bit DES as the encryption algorithm. • **3des**—Specifies 168-bit DES as the encryption algorithm. • **aes**—(Not applicable) • **aes 192**—(Not applicable) • **aes 256**—(Not applicable)
Step 3	`Router(config-isakmp)# authentication {rsa-sig | rsa-encr | pre-share}`	(Optional) Specifies the authentication method within an IKE policy. • **rsa-sig**—Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method. • **rsa-encr**—The VPN Acceleration Module (VAM) or VPN Acceleration Module 2 (VAM2) does not support this authentication method. **Note** Use RSA signature-based authentication without certificate authority. To do this, apply the same configuration used for **rsa-encr**, but change the isakmp authentication method to **rsa-sig**. • **pre-share**—Specifies preshared keys as the authentication method. **Note** If this command is not enabled, the default value (**rsa-sig**) will be used.

	Command	Purpose
Step 4	`Router(config-isakmp)# lifetime seconds`	(Optional) Specifies the lifetime of an IKE security association (SA). *seconds*—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds. **Note** If this command is not enabled, the default value (86,400 seconds [one day]) will be used.
Step 5	`Router(config-isakmp)# hash {sha | md5}`	(Optional) Specifies the hash algorithm within an IKE policy. • **sha**—Specifies SHA-1 (HMAC variant) as the hash algorithm. • **md5**—Specifies MD5 (HMAC variant) as the hash algorithm. **Note** If this command is not enabled, the default value (**sha**) will be used.
Step 6	`Router(config-isakmp)# group {1 | 2 | 5}`	(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy. **1**—Specifies the 768-bit DH group. **2**—Specifies the 1024-bit DH group. **5**—Specifies the 1536-bit DH group. **Note** If this command is not enabled, the default value (768-bit) will be used.
Step 7	Repeat these steps to configure an IKE policy on each router.	

For detailed information on creating IKE policies, refer to the "Configuring Internet Key Exchange Security Protocol" chapter in the *Security Configuration Guide* publication.

Configuring IKE Pre-Shared Key

To specify pre-shared keys with a peer, use the following commands in global configuration mode:

	Command	Purpose

Step 1	`Router (config)# crypto isakmp key keystring address peer-address`
	or
	`Router (config)# crypto isakmp key keystring hostname peer-hostname`
		At the local peer:
		Specify the shared key to be used with a particular remote peer.
		If the remote peer specified their ISAKMP identity with an address, use the **address** keyword in this step; otherwise use the **hostname** keyword in this step.

Step 2	`Router (config)# crypto isakmp key_keystring address peer-address`
	or
	`Router (config)# crypto isakmp key_keystring hostname peer-hostname`
		At the remote peer:
		Specify the shared key to be used with the local peer. This is the same key you just specified at the local peer.
		If the local peer specified their ISAKMP identity with an address, use the **address** keyword in this step; otherwise use the **hostname** keyword in this step.

Step 3	Repeat the previous two steps for each remote peer.	

Remember to repeat these tasks at each peer that uses pre-shared in an IKE policy.

Configuring an IPSec Transform Set

This section includes the following topics:

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Defining an IPSec Transform Set

A transform set is a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a specific transform set to protect a particular data flow.

To define a transform set, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto ipsec transform-set` *transform-set-name transform1* `[`*transform2* `[`*transform3*`]]`	*transform-set-name* Specify the name of the transform set to create (or modify). *transform1* *transform2* *transform3* Specify up to three transforms (one is required) that define the IPSec security protocol(s) and algorithm(s). Accepted transform values are described in Table 2.
Step 2	`Router(cfg-crypto-tran)# mode [tunnel | transport]`	(Optional) Changes the mode associated with the transform set. The mode setting is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 3	**end**	Exits the crypto transform configuration mode to enabled mode.
Step 4	**clear crypto sa** or **clear crypto sa peer** {*ip-address* | *peer-name*} or **clear crypto sa map** *map-name* or **clear crypto sa spi** *destination-address protocol spi*	Clears existing IPSec security associations so that any changes to a transform set take effect on subsequently established security associations (SAs). (Manually established SAs are reestablished immediately.) Using the **clear crypto sa** command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database.
Step 5	Repeat these steps to configure IPSec transform sets on each router.	

Table 2 shows allowed transform combinations for the AH and ESP protocols.

Table 2 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform (Pick up to one.)	**ah-md5-hmac**	AH with the MD5 (Message Digest 5) (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (HMAC variant) authentication algorithm
ESP Encryption Transform (Note: If an **ESP Authentication Transform** is used, you must pick one.)	**esp-aes**	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm (Note: AES is not available with Cisco IOS Release 12.2(14)SU2, 12.2(14)SU1, 12.2(14)SU)
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
ESP Authentication Transform (Pick up to one.)	**esp-md5-hmac**	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform (Pick up to one.)	**comp-lzs**	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Note AES is not available with Cisco IOS Release 12.2(14)SU2, 12.2(14)SU1 or 12.2(14)SU.

Examples of acceptable transform combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**
- **comp-lzs**

The parser will prevent you from entering invalid combinations; for example, once you specify an AH transform it will not allow you to specify another AH transform for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates/protects the payload of an IP datagram. For more information about modes, refer to the **mode (IPSec)** command description.

Selecting Appropriate Transforms

The following tips may help you select transforms that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform, also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH) you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slightly slower.
- Note that some transforms might not be supported by the IPSec peer.

Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform combinations follow:

- **esp-aes** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-aes** and **esp-sha-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, refer to the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transforms

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms will replace the existing transforms for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Transform Example

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that only supports the older transforms.

```
crypto ipsec transform-set SDM_TRASFORMSET_1 esp-3des esp-sha-hmac
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform that the hardware does not support:

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

Configuring Crypto Access Lists for IPSec Traffic

This section includes the following topics:

Creating Crypto Access Lists for IPSec Traffic

Crypto access lists define which IP traffic will be protected by encryption. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or Telnet traffic between Host A and Host B.

To create crypto access lists, use the following command in global configuration mode:

Step	Command	Purpose

Step 1	`Router(config)# access-list access-list-number {permit | deny} protocol source source-wildcard destination destination-wildcard [log]`
	
	or
	
	`Router(config)# ip access-list extended name`
		access-list-number
		Specify an integer from 100 to 199 that you select for the list.
		
		permit
		Permits the frame.
		
		deny
		Denies the frame.
		
		Specifies conditions to determine which IP packets will be protected.[1] (Enable or disable crypto for traffic that matches these conditions.)
		
		We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

Step 2	Add **permit** and **deny** statements as appropriate.	Adds permit or deny statements to access lists.
Step 3	**End**	Exits the configuration command mode.
Step 4	Repeat these steps to create access lists on each router.	

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

Creating Crypto Access List Example

The following example shows a typical example for creating an access list for IPSec traffic on both routers:

```
access-list 100 permit ip any 192.168.4.0.0.0.0.255
```

Ensuring That Access Lists Are Compatible with IPSec

IKE uses UDP port 500. The IPSec Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your interface access lists are configured so that protocol numbers 50, 51, and UDP port 500 traffic are not blocked at interfaces used by IPSec. In some cases, you might need to add a statement to your access lists to explicitly permit this traffic.

Setting Global Lifetimes for IPSec Security Associations

You can change the global lifetime values which are used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire.

To change a global lifetime for IPSec security associations, use one or more of the following commands in global configuration mode:

Step	Command	Purpose
Step 1	`Router(config)# crypto ipsec security-association lifetime seconds seconds`	Changes the global "timed" lifetime for IPSec SAs. This command causes the security association to time out after the specified number of seconds have passed.
Step 2	`Router(config)# crypto ipsec security-association lifetime kilobytes kilobytes`	Changes the global "traffic-volume" lifetime for IPSec SAs. This command causes the security association to time out after the specified amount of traffic (in kilobytes) have passed through the IPSec "tunnel" using the security association.

Step 3	`Router(config)# clear crypto sa`
	or
	`Router(config)# clear crypto sa peer {ip-address | peer-name}`
	or
	`Router(config)# clear crypto sa map map-name`
	or
	`Router (config)# clear crypto sa entry destination-address protocol spi`
		(Optional) Clears existing security associations. This causes any existing security associations to expire immediately; future security associations will use the new lifetimes. Otherwise, any existing security associations will expire according to the previously configured lifetimes.
		Note Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command.

Step 4	Repeat these steps to set global lifetimes for IPSec security associations on each router.	

Configuring Crypto Maps

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE and IPSec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

This section includes the following topics:

Creating Crypto Map Entries

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	`Router (config)# crypto map map-name seq-num ipsec-isakmp`	Create the crypto map and enter crypto map configuration mode.
Step 2	`Router (config)# set peer {hostname | ip-address}`	Specify a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded. Repeat for multiple remote peers.
Step 3	`Router (config)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 4	`Router (config)# match address access-list-id`	Specify an extended access list. This access list determines which traffic is protected by IPSec and which is not.
Step 5	Repeat these steps to create additional crypto maps on each router.	

Configuring Crypto Map Example

The following example shows an example of configuring a crypto map:

```
crypto map SDM_CMAP_1 1 ipsec-isakmp
    description Tunnel to 192.168.3.1
    set peer 192.168.3.1
    set transform-set SDM_TRASNFORMSET_1
    match address 100
```

Creating Dynamic Crypto Maps

A dynamic crypto map entry is a crypto map entry with some parameters not configured.The missing parameters are later dynamically configured (as the result of an IPSec negotiation). Dynamic crypto maps are only available for use with ISAKMP.

Dynamic crypto map entries are grouped into sets. A set is a group of dynamic crypto map entries all with the same *dynamic-map-name*, each with a different *dynamic-seq-num*.

To create a dynamic crypto map entry, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto dynamic-map dynamic-map-name dynamic-seq-num`	Creates a dynamic crypto map entry.
Step 2	`Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.

	Command	Purpose
Step 3	`Router(config-crypto-m)# match address` *access-list-id*	(Optional) Access list number or name of an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. **Note** Although access lists are optional for dynamic crypto maps, they are highly recommended. If this is configured, the data flow identity proposed by the IPSec peer must fall within a **permit** statement for this crypto access list. If this is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets. This is similar to static crypto maps because they also require that an access list be specified. Care must be taken if the **any** keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.
Step 4	`Router(config-crypto-m)# set peer {`*hostname* | *ip-address*`}`	(Optional) Specifies a remote IPSec peer. Repeat for multiple remote peers. This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.
Step 5	`Router(config-crypto-m)# set security-association lifetime seconds` *seconds* and `Router (config-crypto-m)# set security-association lifetime kilobytes` *kilobytes*	(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec security association lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry.
Step 6	`Router(config-crypto-m)# set pfs [group1 | group2]`	(Optional) Specifies that IPSec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry or should demand perfect forward secrecy in requests received from the IPSec peer.
Step 7	`Router(config-crypto-m)# exit`	Exits crypto-map configuration mode and return to global configuration mode.
Step 8	Repeat these steps to create dynamic crypto maps on each router, as required.	

To add a dynamic crypto map set into a crypto map set, use the following command in global configuration mode:

Command	Purpose
`Router(config)# crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`	Adds a dynamic crypto map set to a static crypto map set.

Configuring SSP Communications

Perform the following commands to enable and debug SSP:

Command	
`Router(config)# ssp group group`	Indicates channel used to communicate HA information.
`Router(config-ssp-group)# redundancy name`	Identifies the HSRP group.
`Router(config-ssp-group)# remote ipaddr`	Identifies peer that will receive HA transmissions.
`Router(config-ssp-group)# port tcp-port`	Identifies the TCP port for SSP communications.
`Router# show ssp [packet | peers | redundancy | clients]`	Displays SSP related information.
`Router# debug ssp [fsm | socket | packet | peers | redundancy | config]`	Enables SSP debugging.

Configuring SSP Communications Example

The following example shows an SSP communications configuration on each HA router:

Router 1:

```
ssp group 1
    remote 172.16.31.6
    redundancy ISP
    redundancy LAN
```

Router 2:

```
ssp group 1
    remote 172.16.31.100
    redundancy ISP
    redundancy LAN
```

Transferring ISAKMP State

Perform the following commands, starting in configuration mode to enable SSP communication state transfers for ISAKMP:

	Command	Purpose
Step 1	`Router# crypto isakmp ssp id`	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID on the standby router will be removed and any new state entries will not be added.
Step 2	`Router# show crypto isakmp ha [standby | active]`	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those not used, but could be used if the router goes active. active ISAKMP SAs are those currently in use.
Step 3	Repeat the previous two steps for each remote peer.	

Transferring IPSec State

Perform the following command in global mode to transfer IPSec state from the active router to the standby router:

Global Mode

Command	Purpose
`Router(config)# crypto map name ha replay-interval inbound inbound interval outbound outbound-interval`	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.

Applying Crypto Map Sets to Interfaces and Enabling Transferring IPSec State

Apply a crypto map set to each interface through which IPSec traffic will flow. Crypto maps instruct the router to evaluate the interface traffic against the crypto map set and use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

To apply a crypto map set to an interface, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	`Router (config)# interface type number`	Specify an interface on which to apply the crypto map and enter interface configuration mode.
Step 2	`Router(config-if)# crypto map name ssp id`	Enables IPSec state to be transferred by the SSP channel described by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.

	Command	Purpose
Step 3	`Router (config)# end`	Exit interface configuration mode.
Step 4	Repeat these steps to apply crypto maps on each router.	

Applying Crypto Map Sets to Interfaces Example

The following example shows the application of a crypto map:

```
interface FastEthernet0/1
    crypto map SDM_CMAP_1 ssp 1
```

Configuration Examples

The following examples show sample output for IPSec HA configurations:

Example 1

```
hostname 7200-1
!
ssp group 1
 remote 172.16.31.6
 redundancy ISP
 redundancy LAN

!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.3.1
crypto isakmp ssp 1
!
!
!
crypto ipsec transform-set TRANSFORMSET_1 esp-3des esp-sha-hmac
!
crypto map CMAP_1 1 ipsec-isakmp
 description Tunnel to 192.168.3.1
 set peer 192.168.3.1
 set transform-set TRANSFORMSET_1
 match address 100
!
interface FastEthernet0/0
 description INSIDE_INTERFACE
 ip address 172.16.31.100 255.255.255.0
 standby delay minimum 30 reload 60
 standby 1 ip 172.16.31.1
 standby 1 timers msec 500 3
 standby 1 preempt
 standby 1 name LAN
 standby 1 track FastEthernet0/1
!
interface FastEthernet0/1
 description OUTSIDE_INTERFACE
```

```
 ip address 40.0.0.100 255.255.255.0
 standby delay minimum 30 reload 60
 standby 2 ip 40.0.0.1
 standby 2 timers msec 500 3
 standby 2 preempt
 standby 2 name ISP
 standby 2 track FastEthernet0/0
 crypto map CMAP_1 ssp 1
!
access-list 100 remark IPSec Rule
access-list 100 permit ip any 192.168.4.0 0.0.0.255
!
end
```

Example 2

```
hostname 7200-2
!
ssp group 1
 remote 172.16.31.100
 redundancy ISP
 redundancy LAN
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.3.1
crypto isakmp ssp 1
!
!
!
crypto ipsec transform-set TRANSFORMSET_1 esp-3des esp-sha-hmac
!
crypto map CMAP_1 1 ipsec-isakmp
 description Tunnel to 192.168.3.1
 set peer 192.168.3.1
 set transform-set TRANSFORMSET_1
 match address 100
!
interface FastEthernet0/0
 description INSIDE_INTERFACE
 ip address 172.16.31.6 255.255.255.0
 standby delay minimum 30 reload 60
 standby 1 ip 172.16.31.1
 standby 1 timers msec 500 3
 standby 1 preempt
 standby 1 name LAN
 standby 1 track FastEthernet0/1
!
interface FastEthernet0/1
 description OUTSIDE_INTERFACE
 ip address 40.0.0.6 255.255.255.0
 standby delay minimum 30 reload 60
 standby 2 ip 40.0.0.1
 standby 2 timers msec 500 3
 standby 2 preempt
 standby 2 name ISP
 standby 2 track FastEthernet0/0
 crypto map CMAP_1 ssp 1
!
```

```
access-list 100 remark IPSec Rule
access-list 100 permit ip any 192.168.4.0 0.0.0.255
!
end
```

Show Configuration Tasks and Examples

This section provides the following configuration tasks and examples:

Verifying IKE Configurations

To view information about your IKE configurations, use **show crypto isakmp policy** EXEC command. The following is sample output from that command:

```
Router# show crypto isakmp policy 1
           encr 3des
           authentication pre-share
           group 2
       crypto isakmp key cisco address 192.168.3.1
```

Note If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed in the **show crypto isakmp policy** output.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

Verifying IPSec Configurations

Some configuration changes take effect only after subsequent security associations are negotiated. For the new settings to take effect immediately, clear the existing security associations.

To clear (and reinitialize) IPSec security associations, use one of the commands in Table 3 in global configuration mode:

Table 3 Commands to Clear IP Sec Security Associations

Command	Purpose
clear crypto sa or **clear crypto sa peer** {*ip-address* | *peer-name*} or **clear crypto sa map** *map-name* or **clear crypto sa spi** *destination-address protocol spi*	Clear IPSec security associations (SAs). Using the **clear crypto sa** command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the **peer**, **map**, or **spi** keywords to clear out only a subset of the SA database.

The following steps provide information on verifying your configurations:

Step 1 Enter the **show crypto ipsec transform-set** command to view your transform set configuration:

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   {esp-des}
   will negotiate = {Tunnel,},
```

Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed in the **show crypto ipsec transform-set** command output.

The following sample output from the **show crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPSec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set
Transform set transform-1:{esp-256-aes esp-md5-hmac}
   will negotiate = {Tunnel, },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

Step 2 Enter the **show crypto map** [**interface** *interface* **| tag** *map-name]* **command** to view your crypto map configuration:

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
        Peer = 172.21.114.67
        Extended IP access list 141
            access-list 141 permit ip
                source: addr = 172.21.114.123/0.0.0.0
                dest:   addr = 172.21.114.67/0.0.0.0
        Current peer: 172.21.114.67
        Security-association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={t1,}
```

Step 3 Enter the **show crypto ipsec sa** [**map** map-name **| address | identity | detail | interface**] command to view information about IPSec security associations:

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
interface: Tunnel0
   Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
   current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
```

```
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
  inbound ah sas:
  outbound esp sas:
   spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
  outbound ah sas:
```

For a detailed description of the information displayed by the **show** commands, refer to the "IP Security and Encryption" chapter of the *Security Command Reference* publication.

Verifying IPSec High Availability

Perform the following commands to verify and display IPSec High Availability information:

Step 1 Enter the **show crypto isakmp ha standby** command to view your ISAKMP standby or active SAs.

```
dst             src             state       I-Cookie           R-Cookie
172.16.31.100   20.3.113.1      QM_IDLE     796885F3 62C3295E  FFAFBACD
EED41AFF

172.16.31.100   20.2.148.1      QM_IDLE     5B78D70F 3D80ED01  FFA03C6D
09FC50BE

172.16.31.100   20.4.124.1      QM_IDLE     B077D0A1 0C8EB3A0  FF5B152C
D233A1E0

172.16.31.100   20.3.88.1       QM_IDLE     55A9F85E 48CC14DE  FF20F9AE
DE37B913

172.16.31.100   20.1.95.1       QM_IDLE     3881DE75 3CF384AE  FF192CAB
```

Step 2 Enter the **show crypto ipsec ha** command to view your IPSec High Availability HA Manager state.

```
Router# show crypto ipsec ha
Interface           VIP               SAs   IPSec HA State
FastEthernet0/0     172.16.31.100     1800   Active since 13:00:16 EDT Tue Oct 1 2002
```

Step 3 Enter the **show crypto ipsec sa** command to view HA status of the IPSec SA (standby or active).

```
Router# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
   current_peer: 172.168.3.1
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

 local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
 path mtu 1500, media mtu 1500
 current outbound spi: 132ED6AB

 inbound esp sas:
  spi: 0xD8C8635F(3637011295)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

 inbound ah sas:
  spi: 0xAAF10A60(2867923552)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

 inbound pcp sas:

 outbound esp sas:
  spi: 0x132ED6AB(321836715)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

 outbound ah sas:
  spi: 0x1951D78(26549624)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

 outbound pcp sas:
```

Step 4 Enter the **show crypto ipsec sa standby** command to view your standby SAs:

```
Router# show crypto ipsec sa standby
interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
   current_peer: 172.168.3.1
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
path mtu 1500, media mtu 1500
current outbound spi: 132ED6AB

inbound esp sas:
 spi: 0xD8C8635F(3637011295)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
   sa timing: remaining key lifetime (k/sec): (4499/59957)
   IV size: 8 bytes
   replay detection support: Y
   HA Status: STANDBY

inbound ah sas:
 spi: 0xAAF10A60(2867923552)
   transform: ah-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
   sa timing: remaining key lifetime (k/sec): (4499/59957)
   replay detection support: Y
   HA Status: STANDBY

inbound pcp sas:

outbound esp sas:
 spi: 0x132ED6AB(321836715)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
   sa timing: remaining key lifetime (k/sec): (4499/59957)
   IV size: 8 bytes
   replay detection support: Y
   HA Status: STANDBY

outbound ah sas:
 spi: 0x1951D78(26549624)
   transform: ah-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
   sa timing: remaining key lifetime (k/sec): (4499/59957)
   replay detection support: Y
   HA Status: STANDBY

outbound pcp sas:
```

Step 5 This example is baselined on a previous synchronization command. Every time a **clear crypto isakmp ha standby resync** command on the standby router is run, the delete and add metrics will return to zero. This example assumes some number of SAs have been created.

```
Router# show crypto isakmp ssp
VIP             ADDS         DELETES      REQUESTS     REPLIES
172.16.31.100   538          33           0            0


After a clear cryp isa ha standby resync:

Router# show crypto isakmp ssp
VIP             ADDS         DELETES      REQUESTS     REPLIES
172.16.31.100   0            0            514          514
```

Monitoring and Maintaining IPSec Stateful Failover (VPN High Availability)

Perform the following commands in EXEC mode to monitor and maintain IPSec Stateful Failover (VPN High Availability) information:

Command	Purpose
`Router# show crypto ipsec ha`	Displays HA Manager state for each interface that has HA enabled.
`Router# show crypto ipsec sa`	A modification of the existing command. It now displays the HA status of the IPSec SA (standby or active).
`Router# show crypto ipsec sa addr`	A modification of the existing command, show crypto ipsec sa addr. Displays the HA status of the IPSec SA (standby or active).
`Router# show crypto ipsec sa standby`	Displays the standby SAs.

Displaying SSP Information

The following example uses the **show ssp client** command:

```
router# show ssp client

SSP Client Information
    DOI   Client Name                       Version   Running Ver
      1   IPSec HA Manager                   1.0       1.0
      2   IKE HA Manager                     1.0       1.0
```

The following example uses the **show ssp packet** command:

```
router# show ssp packet

SSP packet Information
    Socket creation time: 01:01:06
    Local port: 3249      Server port: 3249
    Packets Sent = 38559, Bytes Sent = 2285020
    Packets Received = 910, Bytes Received = 61472
```

The following example uses the **show ssp peers** command:

```
router# show ssp peers

SSP Peer Information
    IP Address      Connection State   Local Interface
    40.0.0.1        Connected          FastEthernet0/1
```

The following example uses the **show ssp redundancy** command:

```
router# show ssp redundancy

SSP Redundancy Information
  Device has been ACTIVE for 02:55:34
    Virtual IP      Redundancy Name             Interface
    172.16.31.100   KNIGHTSOFNI                 FastEthernet0/0
```

Debug Configuration Tasks and Examples

This section provides the following debug configuration tasks and examples:

Clearing Dormant SAs on Standby Routers

Perform the following commands in EXEC mode to clear associated SA entries:

Command	Purpose
`Router# clear crypto isakmp ha [standby][resync]`	Clears all dormant (standby) entries from the device. If the **resync** keyword is used, all standby IKE SAs will be removed, and a resynchronization of state will occur.
`Router# clear crypto sa ha standby [peer ip address | resync]`	Clears all standby SAs for the device if peer is specified.

Debugging

Perform the following commands in EXEC mode to enable debugging:

Command	Purpose
`Router# debug crypto isakmp ha [detail | fsm | update]`	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
`Router# debug crypto ipsec ha [detail | fsm | update]`	Enables IPSec HA debugging.
`Router# debug ssp [fsm | socket | packet | peers | redundancy | config]`	Enables SSP debugging.

To prevent debug messages from flooding the console, disable the console log and enable the buffer log as follows:

```
Router# configure terminal
Router(config)# logging buffered
Router(config)# no logging console
```

Troubleshooting Tips

Enabling IPSec Stateful Failover (VPN High Availability) is dependent on the proper operation of HSRP, and includes the virtual IP address that is specified during HSRP setup.

To enable IPSec Stateful Failover (VPN High Availability), a network administrator should perform the following procedures:

- Enable HSRP.
- Enable IPSec Stateful Failover (VPN High Availability).
- Verify processes are working properly.

If you follow the above procedures, but find that either the active or standby IPSec Stateful Failover (VPN High Availability) processes are dysfunctional, you can perform the following checks:

- Use the **show ssp** command to verify the SSP process is running.
- Make sure that both routers share identical IPSec configurations. This is critical. If routers are configured differently, IPSec Stateful Failover (VPN High Availability) will not work.
- Verify that an IPSec connection can be formed with existing maps, transforms, and access lists.
- Configure HSRP on the inside and outside interfaces and make the HSRP groups track one another. Verify this works properly by performing a **shut** command on either of the interfaces, then observe that the HSRP standby router takes active control from the active router.
- Verify that SSP peers can see each other by performing a **show ssp peer** command on both the active and standby router.
- Bind the IKE and IPSec to SSP and send traffic over the tunnels. A user can view HA messages on the standby router as both the active and standby routers synchronize.

HSRP settings may require adjustments depending on the interface employed, such as Fast Ethernet or Gigabit Ethernet. To tune HSRP settings, perform the following steps:

Step 1 Ensure that the interfaces are synchronized by using the **show standby brief** command.

```
Router# show standby brief
Interface group priority p state active address standby address group address
FA 0/0     1       100     Active  local       172.16.31.6     172.16.31.100
FA 0/1     2       100     Active local        40.0.0.6        40.0.0.0.100
```

Step 2 Leave the delay timers at their default settings by using the **no standby delay timer** command.

```
Router# no standby delay timer
```

Step 3 When the other router comes online, issue the **show standby brief** command once again. If you see the following output, you must set the standby router's delay timer.

```
Router# show standby brief
interface group priority p state active address standby address group address
FA 0/0     1   100         Standby 172.16.31.6 local         172.16.31.100
FA 0/1     2   100         Active  local       40.0.0.6        40.0.0.100
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release12.2(2) command reference publications.

clear crypto isakmp ha standby

To clear dormant entries from the router, use the **clear crypto isakmp ha standby** command.

clear crypto isakmp ha standby [**resync**]

Syntax Description

resync	All dormant SA entries will be removed, and a resynchronization will take place.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for SSP channel.

Command	Description
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP channel.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI SSP sub-mode.
show ssp	Displays SSP information.

clear crypto sa ha standby

To clear SAs, use the **clear crypto sa ha standby** command.

clear crypto sa ha standby [**peer** *ip address* | **resync**]

Syntax Description

peer	Clears SAs associated with peer.
ip address	Specifies peer IP address.
resync	Resynchronizes SA state entries between active and standby routers.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
redundancy	Identifies the HSRP group.

Command	Description
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

crypto isakmp ssp

To enable ISAKMP state to be transferred by the SSP channel identified by the ID, use the **crypto isakmp ssp** command. To disable this feature, use the **no** form of this command.

crypto isakmp ssp *id*

[no] crypto isakmp ssp *id*

Syntax Description

id	Designates the SSP channel for IKE SA communications.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Usage Guidelines

If this feature is disabled, all dormant SA entries bound to that ID will be removed.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.

Command	Description
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

crypto map

To enable IPSec state information to be transferred by the SSP channel identified, use the **crypto map** command. To disable this feature, use the **no** form of this command.

crypto map *name* **ssp** *id*

[no] crypto map *name* **ssp** *id*

Syntax Description

name	This identifies the crypto map.
id	This is the channel used to transfer SA entries.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.

Command	Description
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

crypto map ha

To specify the intervals that the active router should update the standby router with anti-replay sequence numbers, use the **crypto map ha** command. To disable this feature, use the **no** form of this command.

crypto map *name* **ha replay-interval inbound** *inbound interval* **outbound** *outbound interval*

[no] crypto map *name* **ha replay-interval inbound** *inbound interval* **outbound** *outbound interval*

Syntax Description

name	Tag name of the crypto map described in the configuration.
inbound interval	The interval at which the active router sends packet sequence updates for incoming packets. Integer between 0 and 10000.
outbound interval	The interval at which the active router sends packet sequence updates for outgoing packets. Integer between 1 and 10 (in millions of packets).

Defaults

The default for inbound is 1000. The default for outbound is one (indicating 1,000,000).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Usage Guidelines

This feature protects against anti-replay attacks. Suppose an errant user was planning an anti-replay attack. If the active router goes down, the standby will assume control and ownership. If the standby router does not have a current anti-replay counter, it cannot know what packets have already be sent to the active router because it will not have a current updated anti-replay window. So in theory, the errant user would be able to send packets that have already be sent. If the network administer employs the **crypto map ha** command, this will force the active router to update at constant intervals the anti-replay counter to the standby router. If the active would fail, the standby would assume control, and also be in possession of an updated anti-replay window, so anti-replay attacks would be difficult to undertake.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

debug crypto isakmp ha

To enable IKE HA Manager debugging, use the **debug crypto isakmp ha** command. To disable debugging, use the **no** form of this command.

debug crypto isakmp ha ?

[no] debug crypto isakmp ha [**detail | fsm | update**]

Syntax Description

detail	Enables detailed IKE HA Manager debugging.
fsm	Enables finite state machine debugging.
update	Enables updates for IKE HA Manager debugging.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto ipsec ha	Enables HA debugging.

Command	Description
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

debug crypto ipsec ha

To enable IPSec HA debugging, use the **debug crypto ipsec ha** command. To disable debugging, use the **no** form of this command.

debug crypto ipsec ha [**detail | fsm | update**]

[no] debug crypto ipsec ha [**detail | fsm | update**]

Syntax Description

detail	Enables detailed IPSec HA debugging.
fsm	Enables finite state machine debugging.
update	Enables debugging for SSP updates.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
port	Identifies the TCP port for ssp communications.

Command	Description
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

debug ssp

To enable ssp debugging, use the **debug ssp** command. To disable ssp debugging, use the **no** form of this command.

debug ssp [**fsm** | **socket** | **packet** | **peers** | **redundancy** | **config**]

[no] debug ssp [**fsm** | **socket** | **packet** | **peers** | **redundancy** | **config**]

Syntax Description

fsm	Enables finite state machine debugging.
socket	Enables socket debugging.
packet	Enables packet debugging.
peers	Enables peer debugging.
redundancy	Enables redundancy debugging.
config	Enables config debugging.

Defaults

No default behavior or values.

Command Modes

SSP configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.

Command	Description
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

port

To define the TCP port that SSP will use for communications, use the **port** command. To disable this feature, use the **no** form of this command.

port *tcp-port*

[no] port *tcp-port*

Syntax Description

tcp-port	Specifies the port that SSP will use for communications. Integer between 1024 and 49150.

Defaults

Default tcp-port is 3249

Command Modes

SSP configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.

Command	Description
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

remote

To define the channel that the active router communicates SA states to the standby router, use the **remote** command. To disable this feature, use the **no** form of this command.

remote *ipaddr*

[no] remote *ipaddr*

Syntax Description

ipaddr	Specifies IP address of the standby router.

Defaults

None

Command Modes

SSP configuration

Command History

Release	Modification
12.2(2)E	New command
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
redundancy	Identifies the HSRP group.

Command	Description
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

redundancy

To define the HSRP group, use the **redundancy** command. To disable this feature, use the **no** form of this command.

redundancy *name*

[no] redundancy *name*

Syntax Description

name	Valid IP redundancy group name.

Defaults

None

Command Modes

SSP configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
remote	Defines the channel for SSP communications.

Command	Description
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

show crypto ipsec ha

To display IPSec HA information, use the **show crypto ipsec ha** command.

show crypto ipsec

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

The following example is output from the **show crypto ipsec ha** command:

```
router# show crypto ipsec ha
Interface           VIP                SAs   IPSec HA State
FastEthernet0/0     172.16.31.100     1800   Active since 13:00:16 EDT Tue Oct 1 2002
```

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
redundancy	Identifies the HSRP group.

Command	Description
remote	Defines the channel for SSP communications.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

show crypto isakmp ha

To show the ISAKMP standby or active SAs, use the **show crypto isakmp ha** command.

show crypto isakmp ha [**standby** | **active**]

Syntax Description

standby	Displays standby SAs.
active	Displays active SAs.

Defaults

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

The following example is output from the **show crypto isakmp ha standby** command:

```
router# show crypto isakmp ha standby
dst             src             state       I-Cookie           R-Cookie
172.16.31.100   20.3.113.1      QM_IDLE     796885F3 62C3295E  FFAFBACD
EED41AFF

172.16.31.100   20.2.148.1      QM_IDLE     5B78D70F 3D80ED01  FFA03C6D
09FC50BE

172.16.31.100   20.4.124.1      QM_IDLE     B077D0A1 0C8EB3A0  FF5B152C
D233A1E0

172.16.31.100   20.3.88.1       QM_IDLE     55A9F85E 48CC14DE  FF20F9AE
DE37B913

172.16.31.100   20.1.95.1       QM_IDLE     3881DE75 3CF384AE  FF192CAB
795019AB
```

The following example is output from the **show crypto isakmp ha** command:

```
router# show crypto isakmp ha

VIP             SAs    Stamp     HA State
172.16.31.100   902    72C28872  Active since 13:03:21 EDT Tue Oct 1 2002dst
```

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

show crypto ipsec sa

To display IPSec HA status, use the **show crypto ipsec sa** command.

show crypto ipsec sa [**addr** | **standby**]

Syntax Description

addr	Displays HA status of the IPSec SA.
standby	Displays standby SAs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

The following example is output from the **show crypto ipsec sa** command:

```
router# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
   current_peer: 172.168.3.1
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
     path mtu 1500, media mtu 1500
     current outbound spi: 132ED6AB

     inbound esp sas:
      spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
```

```
        HA Status: STANDBY

      inbound ah sas:
       spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

      inbound pcp sas:

      outbound esp sas:
       spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

      outbound ah sas:
       spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

      outbound pcp sas:
-------------------------------------------------------------------------------
```

The following example is output from the **show crypto ipsec sa addr** command:

```
router# show crypto ipsec sa addr
dest address: 172.168.3.100
   protocol: AH
      spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

   protocol: ESP
      spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

dest address: 172.168.3.1
   protocol: AH
      spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
```

```
        replay detection support: Y
        HA Status: STANDBY

    protocol: ESP
       spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY
------------------------------------------------------------------------------
```

The following example is output from the **show crypto ipsec sa standby** command:

```
router# show crypto ipsec sa standby
interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
   current_peer: 172.168.3.1
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
     path mtu 1500, media mtu 1500
     current outbound spi: 132ED6AB

     inbound esp sas:
      spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

     inbound ah sas:
      spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

     inbound pcp sas:

     outbound esp sas:
      spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY
```

```
outbound ah sas:
 spi: 0x1951D78(26549624)
   transform: ah-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
   sa timing: remaining key lifetime (k/sec): (4499/59957)
   replay detection support: Y
   HA Status: STANDBY

outbound pcp sas:
```

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
ssp group	Enter into the CLI ssp sub-mode.
show ssp	Displays SSP information.

show ssp

To show the SSP state information, use the **show ssp** command.

show ssp [**packet** | **peers** | **redundancy** | **clients**]

Syntax Description

packet	Displays byte count and packet count for the current socket, the creation time of the socket, the server port number, and the port number used for SSP communication.
peers	Displays the IP address of the remote peer, the interface used, and the connection state.
redundancy	Displays the current SSP state, the HSRP group name, interface used, elapsed time since last state change.
clients	Displays the DOI, name, running version and available version of each client that is registered with SSP.

Defaults

No default behavior or values.

Command Modes

SSP configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

The following example is output from the **show ssp** command:

```
router# show ssp client

SSP Client Information
    DOI   Client Name                       Version   Running Ver
      1   IPSec HA Manager                   1.0       1.0
      2   IKE HA Manager                     1.0       1.0

router# show ssp packet

SSP packet Information
    Socket creation time: 01:01:06
    Local port: 3249      Server port: 3249
    Packets Sent = 38559, Bytes Sent = 2285020
```

```
    Packets Received = 910, Bytes Received = 61472


router# show ssp peers

SSP Peer Information
    IP Address      Connection State   Local Interface
    40.0.0.1        Connected          FastEthernet0/1

router# show ssp redundancy

SSP Redundancy Information
  Device has been ACTIVE for 02:55:34
    Virtual IP      Redundancy Name             Interface
    172.16.31.100   KNIGHTSOFNI                 FastEthernet0/0
```

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the ID. If this feature is disabled, all dormant SA entries bound to that ID will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the ID. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
debug crypto ipsec ha	Enables HA debugging.
debug ssp	Enables SSP debugging.
port	Identifies the TCP port for ssp communications.
redundancy	Identifies the HSRP group.
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
ssp group	Enter into the CLI ssp sub-mode.

ssp group

To enter into the CLI ssp sub-mode, use the **ssp group** command. To disable this feature, use the **no** form of this command.

ssp group *group*

[no] ssp group *group*

Syntax Description

group	Integer identifier between 1 and 100.

Defaults

No default behavior or values.

Command Modes

SSP configuration

Command History

Release	Modification
12.2(11)YX	This command was introduced.
12.2(11)YX1	This feature was integrated into Cisco IOS Release 12.2(11)YX1.
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU.
12.2(14)SU1	This feature was integrated into Cisco IOS Release 12.2(14)SU1.
12.2(14)SU2	This feature was integrated into Cisco IOS Release 12.2(14)SU2.

Examples

None

Related Commands

Command	Description
clear crypto isakmp ha standby	Clears all dormant entries from the router.
clear crypto sa ha standby	Clears all standby SAs.
crypto isakmp ssp	Enables ISAKMP state to be transferred by the SSP channel described by the id. If this feature is disabled, all dormant SA entries bound to that id will be removed and any new state conditions will not be added.
crypto map	Enables IPSec state to be transferred by the SSP channel identified by the id. If this feature is disabled, all standby entries bound to that interface will be removed.
crypto map ha	Specifies the intervals at which the active router should update the standby router with anti-replay sequence numbers.
debug crypto isakmp ha	Enables basic debug messages related to the IKE HA Manager itself, as well as its interactions with the ISADB.
redundancy	Identifies the HSRP group.

Command	Description
remote	Defines the channel for SSP communications.
show crypto isakmp ha	Displays the ISAKMP standby or active SAs. Standby ISAKMP SAs are those SAs not used, but could be used if the standby router goes active.
show crypto ipsec ha	Displays HA Manager state for each interface that has HA enabled.
show crypto ipsec sa	Displays IPSec SAs.
show ssp	Displays SSP information.

Glossary

Active—Active IPSec High Availability router.

DPD—Dead peer detection. DPD allows two IPSec peers to determine if the other is still "alive" during the lifetime of a VPN connection.

GRE—Generic Routing Encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

HSRP—Hot Standby Routing Protocol. HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

IPSec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

SA—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and they are unique in each security protocol.

SSP—State Synchronization Protocol (SSP) is a protocol developed to transfer state information between the active and standby routers.

Standby—Standby IPSec High Availability router.

Stateful Failover—Feature that enables a backup (standby) router to automatically take over the primary (active) router's tasks in the event of a active router failure with minimal or no loss of traffic. The remote peer sees no difference between the two routers since it is connected to a virtual end point (VEP), owned by either headend router that shares the same IPSec information.