CHAPTER 28

Configuring Duplicate Hardware and IPsec Failover Using the IPsec VPN SPA

This chapter provides information about configuring duplicate hardware and IPsec failover using the IPsec VPN SPA on the Catalyst 6500 Series switch. It includes the following sections:

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* and *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* publications.

For detailed information on Cisco IOS IPsec cryptographic operations and policies, refer to the *Cisco IOS Security Configuration Guide, Release 12.2* and *Cisco IOS Security Command Reference, Release 12.2*.

For more information about the commands used in this chapter, see the *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX* publication. Also refer to the related Cisco IOS Release 12.2 software command reference and master index publications. For more information about accessing these publications, see the "Related Documentation" section on page xlv.

Tip To ensure a successful configuration of your VPN using the IPsec VPN SPA, read all of the configuration summaries and guidelines before you perform any configuration tasks.

Overview of Duplicate Hardware Configurations and IPsec Failover

For critical VPN communications, you can deploy redundant VPN hardware and configure your system for failover in case of hardware failure. The following topics provide information about configuring for IPsec failover using the IPsec VPN SPA:

Configuring Multiple IPsec VPN SPAs in a Chassis

You can deploy up to ten IPsec VPN SPAs in a single chassis, with the restriction that no more than one IPsec VPN SPA can be used to perform IPsec services for any given interface VLAN.

Multiple IPsec VPN SPAs in a Chassis Configuration Guidelines

When configuring multiple IPsec VPN SPAs in a chassis, follow these guidelines:

- If you enter the **no switchport** command followed by the **switchport** command, all VLANs are readded to a trunk port (this situation occurs when you are first switching to a routed port and then back to a switch port). For detailed information on configuring trunk ports, see the "Configuring a Trunk Port" section on page 21-15 of Chapter 21, "Configuring VPNs in Crypto-Connect Mode."
- As with single IPsec VPN SPA deployments, you must properly configure each IPsec VPN SPA's inside and outside port. You can add an interface VLAN only to the inside port of one IPsec VPN SPA. Do not add the same interface VLAN to the inside port of more than one IPsec VPN SPA.

  Assigning interface VLANs to the inside ports of the IPsec VPN SPAs allows you to decide which IPsec VPN SPA can be used to provide IPsec services for a particular interface VLAN.

  Note You do not need to explicitly add interface VLANs to the inside trunk ports of the IPsec VPN SPAs. Entering the **crypto engine slot** command achieves the same results.

  Note There is no support for using more than one IPsec VPN SPA to do IPsec processing for a single interface VLAN.

- SA-based load balancing is not supported.
- If you assign the same crypto map to multiple interfaces, then you must use the **crypto map local address** command, and all interfaces must be assigned to the same crypto engine.

For a configuration example of multiple IPsec VPN SPAs in a chassis, see the "Multiple IPsec VPN SPAs in a Chassis Configuration Example" section on page 28-24.

Understanding Stateless Failover Using HSRP

The IPsec failover (VPN high availability) feature allows you to employ a secondary (standby) switch that automatically takes over the primary (active) switch's tasks in the event of an active switch failure. IPsec failover, stateless or stateful, is designed to work in conjunction with the Hot Standby Routing Protocol (HSRP) and Reverse Route Injection (RRI).

HSRP is used between the active and standby switch in either stateless or stateful mode, tracking the state of switch interfaces and providing a failover mechanism between primary and secondary devices. An HSRP group shares a single virtual IP address as its crypto peer address so that the remote crypto peer requires no reconfiguration after a failover. The configured HSRP timers determine the time that it takes for the standby switch to take over.

RRI uses information derived from the negotiated IPsec SAs to create static routes to the networks identified in those SAs. During an HSRP and IPsec failover, RRI allows dynamic routing information updates.

In an IPsec stateless failover, the HSRP group's virtual IP address transfers over to the standby switch, but no IPsec or ISAKMP SA state information is transferred to the standby switch. The remote crypto peer detects the failure using Dead Peer Detection (DPD) or a keepalive mechanism. The remote crypto peer then communicates with the standby switch at the HSRP group address to renegotiate the dropped ISAKMP SAs and IPsec SAs before traffic transmission can resume.

When used together, HSRP and RRI provide a reliable network design for VPNs and reduce configuration complexity on remote peers.

For HSRP configuration information, refer to this URL:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800942f7.shtml

Understanding Stateful Failover Using HSRP and SSP

Note Support for IPsec stateful failover using HSRP and SSP is removed in Cisco IOS Release 12.2(33)SXH and later releases. The feature is supported in Release 12.2SXF.

IPsec stateful failover enables a switch to continue processing and forwarding IPsec packets after a planned or unplanned outage. The failover process is transparent to users and to remote IPsec peers.

As with IPsec stateless failover, IPsec stateful failover is designed to work with HSRP and RRI, but IPsec stateful failover also uses the State Synchronization Protocol (SSP). During an HSRP and IPsec failover, SSP transfers IPsec and ISAKMP SA state information between the active and standby switches, allowing existing VPN connections to be maintained after a switch failover.

IPsec Stateful Failover Configuration Guidelines and Restrictions

When configuring IPsec stateful failover, follow these guidelines and restrictions:

- When configuring IPsec stateful failover with the IPsec VPN SPA, all IPsec VPN SPA configuration rules apply. You must apply crypto maps to interface VLANs.
- When configuring IPsec stateful failover with an IPsec VPN SPA in two chassis, the hardware configurations of both chassis must be exactly the same. For example, in one chassis if the IPsec VPN SPA that is in slot 2 is used to protect interface VLAN 100 and the IPsec VPN SPA that is in

slot 3 is used to protect interface VLAN 101, the exact same configuration must be reflected in the second chassis. An example of a misconfiguration would be if the IPsec VPN SPA in slot 3 of the second chassis is used to protect interface VLAN 100.

- Do not add nonexistent or inadequately configured HSRP standby groups to the State Synchronization Protocol (SSP) configuration because this action disables high-availability features until the configuration is corrected.
- The recommended HSRP timer values are one second for hello timers and three seconds for hold timers. These values should prevent an undesirable failover that is caused by temporary network congestion or transient, high CPU loads.

  These timer values can be adjusted upward if you are running high loads or have a large number of HSRP groups. Temporary failures and load-related system stability can be positively affected by raising the timer values as needed. The hello timer value should be approximately a third of the hold timer value.
- Use the HSRP delay timers to allow a device to finish booting, initializing, and synchronizing before participating as a high-availability pair. Set the minimum delay at 30 seconds or more to help prevent active/standby flapping and set the reload delay at some value greater than the minimum. You can use the delay timers to reflect the complexity and size of a particular configuration on various hardware. The delay timers tend to vary from platform to platform.
- Sequence number updates from active to standby have a 20-second minimum interval per SA.
- The **standby preempt** command is required, and should be configured with no **priority** or **delay** options.
- To allow dynamic routing information updates during the HSRP and IPsec failover, enable the Reverse Route Injection (RRI) feature using the **reverse-route** command.
- To verify that all processes are running properly after enabling both HSRP and IPsec stateful failover, use the **show ssp**, **show standby**, **show crypto ipsec**, and **show crypto isakmp** commands.
- The following features are not supported with IPsec stateful failover:
  - The **standby use-bia** command—Always use a virtual HSRP MAC address for the switch's MAC address.
  - Easy VPN clients or IKE keepalives— IPsec stateful failover can be used with peers when DPD is used.
  - DMVPN or tunnel protection.
  - Secured WAN ports (for example, IPsec over FlexWAN or SIP module port adapters)— This restriction is due to limitations of HSRP.

Configuring IPsec Failover

The following sections describe how to configure IPsec stateless and stateful failover in crypto-connect and VRF modes:

- Configuring IPsec Stateless Failover Using HSRP with Crypto-Connect Mode, page 28-5
- Configuring IPsec Stateful Failover Using HSRP and SSP with Crypto-Connect Mode, page 28-11
- Configuring IPsec Stateless and Stateful Failover with VRF Mode, page 28-17

Configuring IPsec Stateless Failover Using HSRP with Crypto-Connect Mode

To configure IP stateful failover using HSRP and SSP, perform this task beginning in global configuration mode:

	Command	Purpose

Step 1	`Router(config)# crypto isakmp policy priority`
	`...`
	`Router(config-isakmp) # exit`
		Defines an ISAKMP policy and enters ISAKMP policy configuration mode.
		• *priority*—Identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10000, with 1 being the highest priority and 10000 the lowest.
		For details on configuring an ISAKMP policy, see the *Cisco IOS Security Configuration Guide*.

Step 2	`Router(config)# crypto isakmp key keystring address peer_address [mask]`	Configures a preshared authentication key. • *keystring*—Preshared key. • *peer_address*—IP address of the remote peer. • *mask*—(Optional) The subnet mask of the remote peer. For details on configuring a preshared key, see the *Cisco IOS Security Configuration Guide*.

Step 3	`Router(config)# crypto ipsec transform-set transform_set_name transform1[transform2[transform3]]`
	`...`
	`Router(config-crypto-tran)# exit`
		Defines a transform set (an acceptable combination of security protocols and algorithms) and enters crypto transform configuration mode.
		• *transform_set_name*—Name of the transform set.
		• *transform1*[*transform2*[*transform3*]]—Defines IPsec security protocols and algorithms.
		For accepted *transformx* values, and more details on configuring transform sets, see the *Cisco IOS Security Command Reference*.

Step 4	`Router(config)# crypto dynamic-map dynamic_map_name seq_number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		Creates or modifies a dynamic crypto map template and enters the crypto map configuration mode.
		• *dynamic_map_name*—Name that identifies the dynamic crypto map template.
		• *seq_number*—Sequence number you assign to the crypto map entry. Lower values have higher priority.
		• **ipsec-isakmp**—Indicates that IKE will be used to establish the IPsec security associations.
		For details on configuring a crypto map, see the *Cisco IOS Security Configuration Guide*.

	Command	Purpose

Step 5	`Router(config)# crypto map map_name seq_number [ipsec-isakmp] [dynamic dynamic_map_name]`
	`...`
	`Router(config-crypto-map)# exit`
		Creates a crypto map entry and binds it to the dynamic crypto map template.
		• *map_name*—Name that identifies the crypto map set.
		• *seq_number*—Sequence number you assign to the crypto map entry. Lower values have higher priority.
		• **ipsec-isakmp**—(Optional) Specifies that IKE will be used to establish the IPsec security associations.
		• **dynamic**—(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map.
		• *dynamic_map_name*—Name that identifies the dynamic crypto map template.

Step 6	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the LAN-side Gigabit Ethernet interface.
Step 7	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 8	`Router(config-if)# standby [group_number] ip ip_address`	Enables the HSRP. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. • *ip_address*— IP address of the standby switch interface.

	Command	Purpose
Step 9	`Router(config-if)# standby [group_number] timers [msec] hellotime [msec] holdtime`	Configures the time between hello packets and the hold time before other switches declare the active switch to be down. • *group_number*—(Optional) Group number to which the timers apply. • **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover. • *hellotime*—Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, *hellotime* is in milliseconds. This is an integer from 15 to 999. • *holdtime*—Time (in seconds) before the active or standby switch is declared to be down. This is an integer from x to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from y to 3000.
Step 10	`Router(config-if)# standby [group_number] priority priority`	(Optional) Sets the standby priority used in choosing the active switch. • *group_number*—(Optional) Group number to which this command applies. • *priority*—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 switch has priority over the current active switch, the local switch should attempt to take its place as the active switch.
Step 11	`Router(config-if)# standby [group_number] preempt`	Configure HSRP preemption. • *group_number*—(Optional) Group number to which this command applies. **Note** In software releases earlier than Cisco IOS Release 12.2(33)SXH, **preempt** is a keyword of the **standby priority** command. In Cisco IOS Release 12.2(33)SXH and later releases, **standby preempt** and **standby priority** are separate commands.

	Command	Purpose
Step 12	`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. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. • *type*—Interface type (combined with interface number) that will be tracked. • *number*—Interface number (combined with interface type) that will be tracked. • *interface_priority*—(Optional) Amount by which the Hot Standby priority for the switch is decremented (or incremented) when the interface goes down (or comes back up). Range is from 0 to 255. Default is 10.
Step 13	`Router(config-if)# standby [group_number] name`	Configures the standby group name for the interface. • *group_number*—(Optional) Group number to which the name is being applied. • *name*—Name of the HSRP standby group.
Step 14	`Router(config-if)# interface vlan vlan_ID`	Enters interface configuration mode for the specified crypto interface VLAN.
Step 15	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 16	`Router(config-if)# standby [group_number] ip ip_address`	Enables the HSRP. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. • *ip_address*—Virtual IP address of the HSRP standby group.

	Command	Purpose
Step 17	`Router(config-if)# standby [group_number] timers [msec] hellotime [msec] holdtime`	Configures the time between hello packets and the hold time before other switches declare the active switch to be down. • *group_number*—(Optional) Group number to which the timers apply. • **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover. • *hellotime*—Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, *hellotime* is in milliseconds. This is an integer from 15 to 999. • *holdtime*—Time (in seconds) before the active or standby switch is declared to be down. This is an integer from x to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from y to 3000.
Step 18	`Router(config-if)# standby [group_number] priority priority`	(Optional) Sets the standby priority used in choosing the active switch. • *group_number*—(Optional) Group number to which this command applies. • *priority*—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 switch has priority over the current active switch, the local switch should attempt to take its place as the active switch.
Step 19	`Router(config-if)# standby [group_number] preempt`	Configure HSRP preemption. • *group_number*—(Optional) Group number to which this command applies. **Note** In software releases earlier than Cisco IOS Release 12.2(33)SXH, **preempt** is a keyword of the **standby priority** command. In Cisco IOS Release 12.2(33)SXH and later releases, **standby preempt** and **standby priority** are separate commands.

	Command	Purpose
Step 20	`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. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. • *type*—Interface type (combined with interface number) that will be tracked. • *number*—Interface number (combined with interface type) that will be tracked. • *interface_priority*—(Optional) Amount by which the Hot Standby priority for the switch is decremented (or incremented) when the interface goes down (or comes back up). Range is from 0 to 255. Default is 10.
Step 21	`Router(config-if)# standby [group_number] name`	Configures the standby group name for the interface. • *group_number*—(Optional) Group number to which the name is being applied. • *name*—Name of the standby switch.
Step 22	`Router(config-if)# crypto map map_name redundancy name`	Defines a backup IPsec peer. Both routers in the standby group are defined by the redundancy standby name and share the same virtual IP address. • *map_name*—Name of the crypto map set. • *name*—Name of the HSRP standby group.
Step 23	`Router(config-if)# crypto engine slot slot/subslot`	Assigns the crypto engine to the inside interface VLAN. • *slot/subslot*—The slot and subslot where the IPsec VPN SPA is located.
Step 24	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the outside Gigabit Ethernet interface.
Step 25	`Router(config-if)# crypto connect vlan vlan_ID`	Connects the outside access port to the inside interface VLAN and enters crypto-connect mode. • *vlan_ID*—Interface VLAN identifier.

For examples of IPsec stateless failover configurations using HSRP, see the "IPsec Stateless Failover Using HSRP with Crypto-Connect Mode Configuration Examples" section on page 28-26.

Configuring IPsec Stateful Failover Using HSRP and SSP with Crypto-Connect Mode

The configuration of IPsec stateful failover using HSRP is very similar to the configuration of IPsec stateless failover using HSRP with the addition of the SSP-related commands.

Note Support for IPsec stateful failover using HSRP and SSP is removed in Cisco IOS Release 12.2(33)SXH and later releases. The feature is supported in Release 12.2SXF.

To configure IP stateful failover using HSRP and SSP, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ssp group group`	Indicates channel used to communicate high availability (HA) information and enters SSP configuration mode. • *group*—Integer between 1 and 100.
Step 2	`Router(config-ssp)# redundancy name`	Identifies the HSRP group. • *name*—Valid IP redundancy group name.
Step 3	`Router(config-ssp)# remote ipaddr`	Identifies peer that will receive high availability (HA) transmissions. • *ipaddr*—IP address of the standby switch.

Step 4	`Router(config)# crypto isakmp policy priority`
	`...`
	`Router(config-isakmp) # exit`
		Defines an ISAKMP policy and enters ISAKMP policy configuration mode.
		• *priority*—Identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10000, with 1 being the highest priority and 10000 the lowest.
		For details on configuring an ISAKMP policy, see the *Cisco IOS Security Configuration Guide*.

Step 5	`Router(config)# crypto isakmp key keystring address peer_address`	Configures a preshared authentication key. • *keystring*—Preshared key. • *peer_address*—IP address of the remote peer. For details on configuring a preshared key, see the *Cisco IOS Security Configuration Guide*.
Step 6	`Router(config)# 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 switch will be removed and any new state entries will not be added. • *id*—Channel used to transfer SA entries.

	Command	Purpose

Step 7	`Router(config)# crypto ipsec transform-set transform_set_name transform1[transform2[transform3]]`
	`...`
	`Router(config-crypto-tran)# exit`
		Defines a transform set (an acceptable combination of security protocols and algorithms) and enters crypto transform configuration mode.
		• *transform_set_name*—Name of the transform set.
		• *transform1*[*transform2*[*transform3*]]—Defines IPsec security protocols and algorithms.
		For accepted *transformx* values, and more details on configuring transform sets, see the *Cisco IOS Security Command Reference*.

Step 8	`Router(config)# crypto map name ha replay-interval inbound inbound-interval outbound outbound-interval`	(Optional) Specifies the intervals at which the active switch should update the standby switch with anti-replay sequence numbers. • *name*—Tag name of the crypto map described in the configuration. • *inbound-interval*—The interval at which the active switch sends packet sequence updates for incoming packets. The range is 0 to 10000 (packets); the default is 1000. • *outbound-interval*—The interval at which the active switch sends packet sequence updates for outgoing packets. The range is 1 to 10 (in millions of packets); the default is 1.
Step 9	`Router(config)# access-list access_list_number {deny | permit} ip source source_wildcard destination destination_wildcard`	Defines an extended IP access list. • *access_list_number*—Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699. • {**deny** | **permit**}—Denies or permits access if the conditions are met. • *source*—Address of the host from which the packet is being sent. • *source_wildcard*—Wildcard bits to be applied to the source address. • *destination*—Address of the host to which the packet is being sent. • *destination_wildcard*—Wildcard bits to be applied to the destination address. For details on configuring an access list, see the *Cisco IOS Security Configuration Guide*.

	Command	Purpose

Step 10	`Router(config)# crypto dynamic-map dynamic_map_name seq_number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		Creates or modifies a dynamic crypto map template and enters the crypto map configuration mode.
		• *dynamic_map_name*—Name that identifies the dynamic crypto map template.
		• *seq_number*—Sequence number you assign to the crypto map entry. Lower values have higher priority.
		• **ipsec-isakmp**—Indicates that IKE will be used to establish the IPsec security associations.
		For details on configuring a crypto map, see the *Cisco IOS Security Configuration Guide*.

Step 11	`Router(config)# crypto map map_name seq_number ipsec-isakmp dynamic dynamic_map_name`	Creates a crypto map entry and binds it to the dynamic crypto map template. • *map_name*—Name that identifies the crypto map set. • *seq_number*—Sequence number you assign to the crypto map entry. Lower values have higher priority. • **ipsec-isakmp**—Indicates that IKE will be used to establish the IPsec security associations. • *dynamic_map_name*—Name that identifies the dynamic crypto map template.
Step 12	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the LAN-side Gigabit Ethernet interface.
Step 13	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 14	`Router(config-if)# standby delay minimum min-seconds reload reload-seconds`	Specifies the delay period before the initialization of HSRP groups. • *min-seconds*—Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events. The valid range is 0 to 300 seconds. The default is 1 second. The recommended value is 30 seconds. • *reload-seconds*—Time (in seconds) to delay after the switch has reloaded. This delay period applies only to the first interface-up event after the switch has reloaded. The valid range is 0 to 300 seconds. The default is 5 seconds. The recommended value is 60 seconds.

	Command	Purpose
Step 15	`Router(config-if)# standby [group_number] ip ip_address`	Enables the HSRP. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. • *ip_address*—Virtual IP address of the HSRP standby group.
Step 16	`Router(config-if)# standby [group_number] timers [msec] hellotime [msec] holdtime`	(Optional) Configures the time between hello packets and the hold time before other switches declare the active switch to be down. • *group_number*—(Optional) Group number to which the timers apply. • **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover. • *hellotime*—Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, *hellotime* is in milliseconds. This is an integer from 15 to 999. • *holdtime*—Time (in seconds) before the active or standby switch is declared to be down. This is an integer from x to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from y to 3000.
Step 17	`Router(config-if)# standby [group_number] preempt`	Configure HSRP preemption. • *group_number*—(Optional) Group number to which this command applies. **Note** In software releases earlier than Cisco IOS Release 12.2(33)SXH, **preempt** is a keyword of the **standby priority** command. In Cisco IOS Release 12.2(33)SXH and later releases, **standby preempt** and **standby priority** are separate commands.

	Command	Purpose
Step 18	`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. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. • *type*—Interface type (combined with interface number) that will be tracked. • *number*—Interface number (combined with interface type) that will be tracked. • *interface_priority*—(Optional) Amount by which the Hot Standby priority for the switch is decremented (or incremented) when the interface goes down (or comes back up). Range is from 0 to 255. Default is 10.
Step 19	`Router(config-if)# standby [group_number] name`	Configures the standby group name for the interface. • *group_number*—(Optional) Group number to which the name is being applied. • *name*—Name of the HSRP standby group.
Step 20	`Router(config-if)# interface vlan vlan_ID`	Enters interface configuration mode for the specified crypto interface VLAN.
Step 21	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 22	`Router(config-if)# standby delay minimum min-seconds reload reload-seconds`	Specifies the delay period before the initialization of HSRP groups. • *min-seconds*—Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events. The valid range is 0 to 300 seconds. The default is 1 second. The recommended value is 30 seconds. • *reload-seconds*—Time (in seconds) to delay after the switch has reloaded. This delay period applies only to the first interface-up event after the switch has reloaded. The valid range is 0 to 300 seconds. The default is 5 seconds. The recommended value is 60 seconds.

	Command	Purpose
Step 23	`Router(config-if)# standby [group_number] ip ip_address`	Enables the HSRP. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. • *ip_address*—(Optional) Virtual IP address of the HSRP standby group.
Step 24	`Router(config-if)# standby [group_number] timers [msec] hellotime [msec] holdtime`	(Optional) Configures the time between hello packets and the hold time before other switches declare the active switch to be down. • *group_number*—(Optional) Group number to which the timers apply. • **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover. • *hellotime*—Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, *hellotime* is in milliseconds. This is an integer from 15 to 999. • *holdtime*—Time (in seconds) before the active or standby switch is declared to be down. This is an integer from x to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from y to 3000.
Step 25	`Router(config-if)# standby [group_number] preempt`	Configure HSRP preemption. • *group_number*—(Optional) Group number to which this command applies. **Note** In software releases earlier than Cisco IOS Release 12.2(33)SXH, **preempt** is a keyword of the **standby priority** command. In Cisco IOS Release 12.2(33)SXH and later releases, **standby preempt** and **standby priority** are separate commands.

	Command	Purpose
Step 26	`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. • *group_number*—(Optional) Group number on the interface for which HSRP is being activated. • *type*—Interface type (combined with interface number) that will be tracked. • *number*—Interface number (combined with interface type) that will be tracked. • *interface_priority*—(Optional) Amount by which the Hot Standby priority for the switch is decremented (or incremented) when the interface goes down (or comes back up). Range is from 0 to 255. Default is 10.
Step 27	`Router(config-if)# standby [group_number] name`	Configures the standby group name for the interface. • *group_number*—(Optional) Group number to which the name is being applied. • *name*—Name of the HSRP standby group.
Step 28	`Router(config-if)# crypto map map_name ssp id`	Enables IPsec state information 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.
Step 29	`Router(config-if)# crypto engine slot slot`	Assigns the crypto engine to the inside interface VLAN. • *slot*—The slot where the IPsec VPN SPA is located.
Step 30	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the outside Gigabit Ethernet interface.
Step 31	`Router(config-if)# crypto connect vlan vlan_ID`	Connects the outside access port to the inside interface VLAN and enters crypto-connect mode. • *vlan_ID*—interface VLAN identifier.

For an example of IPsec stateful failover configuration using HSRP and SSP, see the "IPsec Stateful Failover Using HSRP and SSP with Crypto-Connect Mode Configuration Example" section on page 28-29.

Configuring IPsec Stateless and Stateful Failover with VRF Mode

Note Support for IPsec stateful failover is removed in Cisco IOS Release 12.2(33)SXH. The feature is supported in Release 12.2SXF.

Chassis-to- chassis failover with VRF mode is configured differently than in non-VRF (crypto-connect) mode. In VRF mode, the HSRP configuration goes on the physical interface, but the crypto map is added to the interface VLAN. In non-VRF mode, both the HSRP configuration and the crypto map are on the same interface. RRI dynamically inserts and removes routes from the active and standby switch VRF routing tables.

For a configuration example of VRF mode with stateless failover, see the "IPsec Stateless Failover Using HSRP with VRF Mode Configuration Example" section on page 28-32.

For a configuration example of VRF mode with stateful failover, see the "IPsec Stateful Failover Using HSRP with VRF Mode Configuration Example" section on page 28-33

Verifying HSRP Configurations

To verify the IPsec stateful failover HSRP configuration, use the **show crypto isakmp ha standby**, **show crypto ipsec ha**, **show crypto ipsec sa**, and **show crypto ipsec sa standby** commands.

To view your ISAKMP standby or active SAs, enter 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
```

To view your IPsec HA Manager state, enter the **show crypto ipsec ha** command:

```
Router# show crypto ipsec ha

Interface              VIP              SAs     IPSec Ha State

GigabitEthernet5/0/1   172.16.31.100    1800    Active since 13:00:16 EDT Tue Oct 1 2002
```

To view HA status of the IPsec SA (standby or active), enter the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa

interface: GigabitEthernet5/0/1
   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
    ssa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

  outbound pcp sas:
```

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

```
Router# show crypto ipsec sa standby

interface: GigabitEthernet5/0/1
    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:
```

Displaying SSP Information

To verify the IPsec stateful failover SSP configuration, use the **show ssp client**, **show ssp packet**, **show ssp peers**, and **show ssp redundancy** commands.

To view SSP client information, enter 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
```

To view SSP packet information, enter 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
```

To view SSP peer information, enter 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
```

To view redundancy information, enter 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                 GigabitEthernet5/0/1GigabitEthernet0/0
```

For complete configuration information for Cisco IOS IPsec stateful failover support, refer to this URL:

http://www.cisco.com/en/US/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html

For IPsec stateful failover configuration examples, see the "IPsec Stateful Failover Using HSRP and SSP with Crypto-Connect Mode Configuration Example" section on page 28-29.

Configuring Intrachassis IPsec Stateful Failover Using a Blade Failure Group

This section describes how to configure IPsec stateful failover within a chassis using a blade failure group (BFG).

When one or more pairs of IPsec VPN SPAs are installed in a chassis, each pair can be configured as a blade failure group (BFG). The two modules do not need to reside within the same SSC. Within the BFG, each IPsec VPN SPA serves as a backup for the other IPsec VPN SPA. A BFG may be in either an active/active or an active/standby configuration.

Each IPsec tunnel is associated with only one active IPsec VPN SPA. In a BFG, the other IPsec VPN SPA will act as a backup for that IPsec tunnel. For each IKE SA or IPsec tunnel, there is an active IPsec VPN SPA and its backup. For example, in a system that supports 1000 tunnels with two IPsec VPN SPAs, 500 of the tunnels may be active on one SPA and the remaining 500 may be active on the second SPA. Both SPAs then replicate data to each other so that either one can take over in the event of a failure.

IPsec Stateful Failover Using a BFG Configuration Guidelines

When configuring IPsec stateful failover using a BFG, follow these guidelines:

- You can install or remove one of the IPsec VPN SPAs comprising a BFG without disrupting any of the tunnels on the other IPsec VPN SPA.
- We recommend deploying a BFG in an active/standby configuration to avoid oversubscription in the case of a failover.
- When deploying a BFG in an active/active configuration, we recommend that you limit each IPsec VPN SPA to no more than 50% utilization to avoid oversubscription in the case of a failover.

Configuring a BFG for IPsec Stateful Failover

To configure IPsec stateful failover using a BFG, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Router(config-red)# linecard-group` *group_number* `feature-card`	Identifies the line card group ID for a Blade Failure Group and enters redundancy line card configuration mode. • *group_number*—Specifies a group ID for the BFG.
Step 3	`Router(config-r-lc)# subslot` *slot/subslot*	Adds the first SPA to the group. • *slot*—Specifies the chassis slot number where the SSC is installed. • *subslot*—Specifies the secondary slot number on an SSC where a SPA is installed.
Step 4	`Router(config-r-lc)# subslot` *slot/subslot*	Adds the second SPA to the group.

For an IPsec stateful failover using a BFG configuration example, see the "IPsec Stateful Failover Using a Blade Failure Group Configuration Example" section on page 28-37.

Verifying the IPsec Stateful Failover Using a BFG Configuration

To verify the IPsec stateful failover using a BFG configuration, use the **show redundancy linecard group** and **show crypto ace redundancy** commands.

To display the components of a Blade Failure Group, enter the **show redundancy linecard group** command:

```
Router# show redundancy linecard-group 1

Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Sublot:0
Slot:5 Sublot:0
```

To display information about a Blade Failure Group, enter the **show crypto ace redundancy** command:

```
Router# show crypto ace redundancy

--------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
--------------------------------------
Slot:3 subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running
```

Configuration Examples

This section provides examples of the following configurations:

Note The following examples use commands at the level of Cisco IOS Release 12.2(33)SXH.

As of Cisco IOS Release 12.2(33)SXH, the **crypto engine subslot** command used in previous releases has been replaced with the **crypto engine slot** command (of the form **crypto engine slot** *slot* {**inside** | **outside**}). The **crypto engine subslot** command is no longer supported. When upgrading, ensure that this command has been modified in your startup configuration to avoid extended maintenance time.

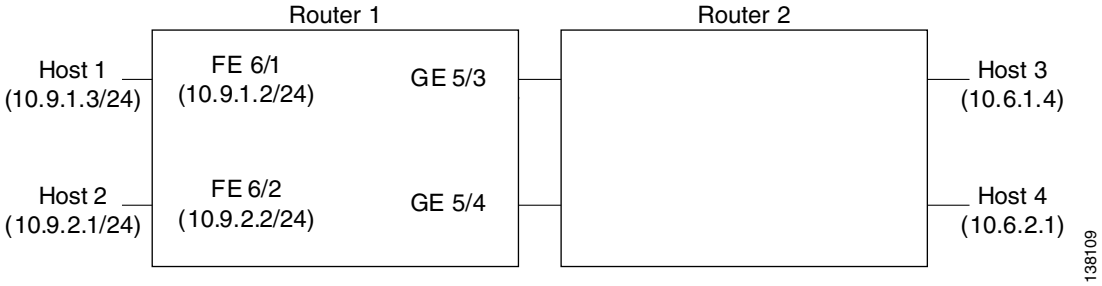
Multiple IPsec VPN SPAs in a Chassis Configuration Example

This section provides an example of a configuration using multiple IPsec VPN SPAs in a chassis as shown in Figure 28-1. Note the following in these examples:

- An IPsec VPN SPA is in slot 2, subslot 0 and slot 3, subslot 0 of router 1.
- In the configuration example, three exclamation points (!!!) precede descriptive comments.

Note In the following figure, the router with the IPsec VPN SPA could be a Cisco 7600 series router or a Catalyst 6500 series switch.

Figure 28-1 Multiple IPsec VPN SPAs in a Chassis Configuration Example




```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key mykey address 10.8.1.1
crypto isakmp key mykey address 10.13.1.1
!
crypto ipsec transform-set xform1 ah-md5-hmac esp-des esp-sha-hmac
crypto ipsec transform-set xform2 esp-3des esp-sha-hmac
!
!!! crypto map applied to VLAN 12, which is
!!! assigned to "inside" port of IPsec VPN SPA in slot 3
crypto map cmap2 10 ipsec-isakmp
 set peer 10.8.1.1
 set transform-set xform1
 match address 102
!
!!! crypto map applied to VLAN 20, which is
!!! assigned to "inside" port of IPsec VPN SPA in slot 2/0
crypto map cmap3 10 ipsec-isakmp
 set peer 10.13.1.1
 set transform-set xform2
 match address 103
!
!!! "port" VLAN, crypto connected to VLAN 12 by IPsec VPN SPA on slot 3/0
interface Vlan11
 no ip address
 crypto connect vlan 12
!
!!! "interface" VLAN, assigned to IPsec VPN SPA on slot 3/0
interface Vlan12
 ip address 10.8.1.2 255.255.0.0
```

```
 crypto map cmap2
 crypto engine slot 3/0
!
!!! "port" VLAN, crypto connected to VLAN 20 by IPsec VPN SPA on slot 2/0
interface Vlan19
 no ip address
 crypto connect vlan 20
!
!!! "interface" VLAN, assigned to IPsec VPN SPA on slot 2/0
interface Vlan20
 ip address 10.13.1.2 255.255.0.0
 crypto map cmap3
 crypto engine slot 2/0
!
!!! connected to Host 1
interface FastEthernet6/1
 ip address 10.9.1.2 255.255.255.0
!
!!! connected to Host 2
interface FastEthernet6/2
 ip address 10.9.2.2 255.255.255.0
!
!!! connected to Router 2
interface GigabitEthernet5/3
 switchport
 switchport mode access
 switchport access vlan 11
!
!!! connected to Router 2
interface GigabitEthernet5/4
 switchport
 switchport mode access
 switchport access vlan 19
!
interface GigabitEthernet2/0/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 12,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet2/0/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/0/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/0/2
 no ip address
 flowcontrol receive on
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 19,1002-1005
 switchport mode trunk
 cdp enable
!
ip classless
!
!!! packets from Host 1 to Host 3 are routed from FastEthernet6/1
!!! to VLAN 12, encrypted with crypto map cmap2
!!! using IPsec VPN SPA in slot 3/0, and forwarded to peer 10.8.1.1
!!! through GigabitEthernet5/3
ip route 10.6.1.4 255.255.255.255 10.8.1.1
!
!!! packets from Host 2 to Host 4 are routed from FastEthernet6/2
!!! to VLAN 20, encrypted with crypto map cmap3
!!! using IPsec VPN SPA in slot 2/0, and forwarded to peer 10.13.1.1
!!! through GigabitEthernet5/4
ip route 10.6.2.1 255.255.255.255 10.13.1.1
!
!!! ACL matching traffic between Host 1 and Host 3
access-list 102 permit ip host 10.9.1.3 host 10.6.1.4
!
!!! ACL matching traffic between Host 2 and Host 4
access-list 103 permit ip host 10.9.2.1 host 10.6.2.1
```

IPsec Stateless Failover Using HSRP with Crypto-Connect Mode Configuration Examples

This section provides the following configuration examples of IPsec stateless failover using HSRP:

- IPsec Stateless Failover for the Active Chassis Configuration Example, page 28-26
- IPsec Stateless Failover for the Remote Switch Configuration Example, page 28-27

IPsec Stateless Failover for the Active Chassis Configuration Example

The following example shows the configuration for an active chassis that is configured for IPsec stateless failover using HSRP:

```
hostname router-1
!
vlan 2-1001
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set PYTHON esp-3des
!
crypto dynamic-map dynamap_1 20
 set transform-set PYTHON
 reverse-route
!
!
crypto map MONTY 1 ipsec-isakmp dynamic dynamap_1
```

```
!
interface GigabitEthernet1/3
 switchport
 switchport access vlan 502
 switchport mode access
!
interface GigabitEthernet1/4
 ip address 50.0.0.3 255.0.0.0
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 502
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 172.1.1.3 255.255.255.0
 standby ip 172.1.1.100
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/3
 standby track GigabitEthernet1/4
 no mop enabled
 crypto map MONTY redundancy KNIGHTSOFNI
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route 50.0.0.0 255.0.0.0 50.0.0.13
ip route 50.0.1.1 255.255.255.255 50.0.0.13
ip route 50.0.2.1 255.255.255.255 50.0.0.13
ip route 50.0.3.1 255.255.255.255 50.0.0.13
ip route 50.0.4.1 255.255.255.255 50.0.0.13
ip route 50.0.5.1 255.255.255.255 50.0.0.13
```

IPsec Stateless Failover for the Remote Switch Configuration Example

The following example shows the configuration for a remote switch that is configured for IPsec stateless failover using HSRP.

```
hostname router-remote
!
crypto isakmp policy 1
```

```
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_1
!
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-2,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
ip access-list extended test_1
 permit ip host 10.0.1.1 host 50.0.1.1
```

IPsec Stateful Failover Using HSRP and SSP with Crypto-Connect Mode Configuration Example

Note Support for IPsec stateful failover using HSRP and SSP is removed in Cisco IOS Release 12.2(33)SXH and later releases. The feature is supported in Release 12.2SXF.

Note This configuration example does not protect the SSP traffic. To protect the SSP traffic, you will need to define a new crypto map and attach it to the SSP interface without the ssp tag. The ACL for this crypto map can be derived from the remote IP address and the TCP port that are defined in the SSP group.

The following example shows the configuration for an IPsec stateful failover using HSRP and SSP:

```
hostname router-1
!
ssp group 100
 remote 50.0.0.6
 redundancy PUBLIC
 redundancy PRIVATE
!
vlan 502
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 0.0.0.0 0.0.0.0
crypto isakmp ssp 100
!
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto dynamic-map ha_dynamic 10
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
!
!
crypto map ha_dynamic 10 ipsec-isakmp dynamic ha_dynamic
!
!
!
interface GigabitEthernet1/1
 no ip address
 crypto connect vlan 502
!
interface GigabitEthernet1/2
 ip address 50.0.0.5 255.255.255.0
 load-interval 30
 no keepalive
 standby delay minimum 30 reload 60
 standby 2 ip 50.0.0.100
 standby 2 preempt
 standby 2 name PRIVATE
 standby 2 track GigabitEthernet1/1
```

```
 standby 2 track Vlan502
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan502
 ip address 172.1.1.5 255.255.255.0
 no mop enabled
 standby delay minimum 30 reload 60
 standby 1 ip 172.1.1.100
 standby 1 preempt
 standby 1 name PUBLIC
 standby 1 track GigabitEthernet1/1
 standby 1 track GigabitEthernet1/2
 crypto map ha_dynamic ssp 100
 crypto engine slot 4/0
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route 50.0.0.0 255.0.0.0 50.0.0.13
```

The following example shows the configuration for a remote peer switch that is configured for IPsec stateful failover using HSRP and SSP:

```
hostname router-remote
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_1
!
```

```
crypto map test_2 local-address Vlan3
crypto map test_2 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_2
!
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 no ip address
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan3
 ip address 20.0.2.1 255.255.255.0
 crypto map test_2
 crypto engine slot 4/0

interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Vlan503
 no ip address
 crypto connect vlan 3
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 50.0.2.0 255.255.255.0 20.0.2.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
ip access-list extended test_1
```

```
 permit ip host 10.0.1.1 host 50.0.1.1
ip access-list extended test_2
 permit ip host 10.0.2.1 host 50.0.2.1
```

IPsec Stateless Failover Using HSRP with VRF Mode Configuration Example

The following example shows a VRF mode configuration with HSRP chassis-to-chassis stateless failover with crypto maps:

```
hostname router-1
!
ip vrf ivrf
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto engine mode vrf
!
vlan 2,3
!
crypto keyring key1
  pre-shared-key address 14.0.1.1 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp keepalive 10
crypto isakmp profile ivrf
   vrf ivrf
   keyring key1
   match identity address 14.0.1.1 255.255.255.255
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto map map_vrf_1 local-address Vlan3
crypto map map_vrf_1 10 ipsec-isakmp
 set peer 14.0.1.1
 set transform-set ts
 set isakmp-profile ivrf
 match address acl_1
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 13.254.254.1 255.255.255.0
!
interface GigabitEthernet1/1.1
 encapsulation dot1Q 2000
 ip vrf forwarding ivrf
 ip address 13.254.254.1 255.0.0.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 3
 switchport mode access
!

interface GigabitEthernet4/0/1
 !IPsec VPN SPA inside port
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 !IPsec VPN SPA outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan3
 ip address 15.0.0.2 255.255.255.0
 standby delay minimum 0 reload 0
 standby 1 ip 15.0.0.100
 standby 1 timers msec 100 1
 standby 1 priority 105
 standby 1 preempt
 standby 1 name std-hsrp
 standby 1 track GigabitEthernet1/2
 crypto engine slot 4/0 outside
!
interface Vlan2
 ip vrf forwarding ivrf
 ip address 15.0.0.252 255.255.255.0
 crypto map map_vrf_1 redundancy std-hsrp
 crypto engine slot 4/0 inside

!
ip classless
ip route 12.0.0.0 255.0.0.0 15.0.0.1
ip route 13.0.0.0 255.0.0.0 13.254.254.2
ip route 14.0.0.0 255.0.0.0 15.0.0.1
ip route 223.255.254.0 255.255.255.0 17.1.0.1
ip route vrf ivrf 12.0.0.1 255.255.255.255 15.0.0.1
!
ip access-list extended acl_1
 permit ip host 13.0.0.1 host 12.0.0.1
!
!
arp vrf ivrf 13.0.0.1 0000.0000.2222 ARPA
```

IPsec Stateful Failover Using HSRP with VRF Mode Configuration Example

Note Support for IPsec stateful failover with HSRP is removed in Cisco IOS Release 12.2(33)SXH and later releases. The feature is supported in Release 12.2SXF.

The following example shows a VRF mode configuration with HSRP chassis-to-chassis stateful failover with crypto maps:

```
hostname router-1
!
ip vrf vrf1
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ssp group 100
 remote 172.1.1.60
 redundancy PUBLIC
 redundancy PRIVATE
!
crypto engine mode vrf
!
vlan 2-1001
!
crypto keyring key1
  pre-shared-key address 0.0.0.0 0.0.0.0 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp ssp 100
!
crypto isakmp profile prof1
   vrf vrf1
   keyring key1
   match identity address 0.0.0.0
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto dynamic-map ha_dynamic 10
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set isakmp-profile prof1
 reverse-route
!
!
crypto map ha_dynamic local-address GigabitEthernet1/3
crypto map ha_dynamic 10 ipsec-isakmp dynamic ha_dynamic
!
!
!
interface GigabitEthernet1/2
 no ip address
!
interface GigabitEthernet1/2.1
 encapsulation dot1Q 2500
 ip vrf forwarding vrf1
 ip address 50.0.0.5 255.0.0.0
 standby delay minimum 30 reload 90
 standby 2 ip 50.0.0.100
 standby 2 preempt
 standby 2 name PRIVATE
 standby 2 track GigabitEthernet1/3
 standby 2 track Vlan100
!
interface GigabitEthernet1/3
```

```
 ip address 172.1.1.50 255.255.255.0
 standby delay minimum 30 reload 90
 standby 1 ip 172.1.1.100
 standby 1 preempt
 standby 1 name PUBLIC
 standby 1 track GigabitEthernet1/2
 standby 1 track Vlan100
 crypto engine slot 2/0
!
interface GigabitEthernet2/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan100
 ip vrf forwarding vrf1
 ip address 172.1.1.6 255.255.255.0
 crypto map ha_dynamic ssp 100
 crypto engine slot 2/0
!
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route vrf vrf1 50.0.1.1 255.255.255.255 50.0.0.13
!
```

The following example shows the configuration for a remote peer switch that is configured for IPsec stateful failover in VRF mode:

```
hostname router-remote
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 match address test_1
```

```
!
crypto map test_2 local-address Vlan3
crypto map test_2 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 match address test_2
!
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 no ip address
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!

interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan3
 ip address 20.0.2.1 255.255.255.0
 crypto map test_2
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Vlan503
 no ip address
 crypto connect vlan 3
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 50.0.2.0 255.255.255.0 20.0.2.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
```

```
ip access-list extended test_1
 permit ip host 10.0.1.1 host 50.0.1.1
ip access-list extended test_2
 permit ip host 10.0.2.1 host 50.0.2.1
```

IPsec Stateful Failover Using a Blade Failure Group Configuration Example

The following example shows how to configure IPsec stateful failover using a Blade Failure Group (BFG):

```
Router(config)# redundancy
Router(config-red)# line-card-group 1 feature-card
Router(config-r-lc)# subslot 3/1
Router(config-r-lc)# subslot 5/1
```