CHAPTER 21

Configuring VPNs in Crypto-Connect Mode

This chapter provides information about configuring IPsec VPNs in crypto-connect mode, one of the two VPN configuration modes supported by the IPsec VPN SPA. For information on the other VPN mode, Virtual Routing and Forwarding (VRF) mode, see Chapter 22, "Configuring VPNs in VRF Mode."

This chapter includes the following topics:

For general information on configuring IPsec VPNs with the IPsec VPN SPA, see the "Overview of Basic IPsec and IKE Configuration Concepts" section on page 20-3.

Note The procedures in this chapter assume you have familiarity with security configuration concepts, such as VLANs, ISAKMP policies, preshared keys, transform sets, access control lists, and crypto maps. For detailed information on configuring these features, refer to the following Cisco IOS documentation:

Cisco IOS Security Configuration Guide, *Release 12.2*, at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

Cisco IOS Security Command Reference, *Release 12.2*, at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

For additional information about the commands used in this chapter, see the *Catalyst 6500 Series Cisco IOS Command Reference, Release 12.2SX* and the related Cisco IOS Release 12.2 software configuration guide 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.

Configuring Ports in Crypto-Connect Mode

Before beginning your crypto-connect mode port configurations, you should read the following subsections:

- Crypto-Connect Mode Configuration Guidelines and Restrictions, page 21-4

Then perform the procedures in the following subsections:

- Configuring the IPsec VPN SPA Inside Port and Outside Port, page 21-7
- Configuring an Access Port, page 21-8
- Configuring a Routed Port, page 21-11
- Configuring a Trunk Port, page 21-15
- Configuring IPsec VPN SPA Connections to WAN Interfaces, page 21-20
- Displaying the VPN Running State, page 21-21

Note The configuration procedures in this section do not provide GRE tunneling support. For information on how to configure GRE tunneling support in crypto-connect mode, see the "Configuring GRE Tunneling in Crypto-Connect Mode" section on page 21-22.

Note The procedures in this section do not provide detailed information on configuring the following Cisco IOS features: IKE policies, preshared key entries, Cisco IOS ACLs, and crypto maps. For detailed information on configuring these features, refer to the following Cisco IOS documentation:

Cisco IOS Security Configuration Guide, *Release 12.2*, at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

Cisco IOS Security Command Reference, *Release 12.2*, at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

Understanding Port Types in Crypto-Connect Mode

To configure IPsec VPNs in crypto-connect mode, you should understand the following concepts:

- Switch Outside Ports and Inside Ports, page 21-2
- IPsec VPN SPA Outside Port and Inside Port, page 21-3
- Port VLAN and Interface VLAN, page 21-3
- Access Ports, Trunk Ports, and Routed Ports, page 21-4

Switch Outside Ports and Inside Ports

The Fast Ethernet or Gigabit Ethernet ports on the Catalyst 6500 Series switch that connect to the WAN routers are referred to as switch outside ports. These ports connect the LAN to the Internet or to remote sites. Cryptographic policies are applied to the switch outside ports.

The Fast Ethernet or Gigabit Ethernet ports on the Catalyst 6500 Series switch that connect to the LAN are referred to as switch inside ports.

The IPsec VPN SPA sends encrypted packets to the switch outside ports and decrypted packets to the Policy Feature Card (PFC) for Layer 3 forwarding to the switch inside ports.

IPsec VPN SPA Outside Port and Inside Port

The IPsec VPN SPA appears to the CLI as a SPA with two Gigabit Ethernet ports. The IPsec VPN SPA has no external connectors; the Gigabit Ethernet ports connect the IPsec VPN SPA to the switch backplane and Switch Fabric Module (SFM) (if installed).

One Gigabit Ethernet port handles all the traffic going to and coming from the switch outside ports. This port is referred to as the IPsec VPN SPA outside port. The other Gigabit Ethernet port handles all traffic going to and coming from the LAN or switch inside ports. This port is referred to as the IPsec VPN SPA inside port.

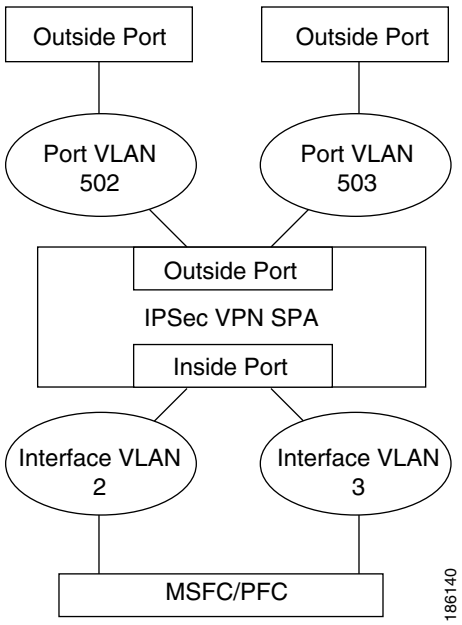
Port VLAN and Interface VLAN

Your VPN configuration can have one or more switch outside ports. To handle the packets from multiple switch outside ports, you must direct the packets from multiple switch outside ports to the IPsec VPN SPA outside port by placing the switch outside ports in a VLAN with the outside port of the IPsec VPN SPA. This VLAN is referred to as the port VLAN. The port VLAN is a Layer 2-only VLAN. You do not configure Layer 3 addresses or features on this VLAN; the packets within the port VLAN are bridged by the PFC.

Before the switch can forward the packets using the correct routing table entries, the switch needs to know which interface a packet was received on. For each port VLAN, you must create another VLAN so that the packets from every switch outside port are presented to the switch with the corresponding VLAN ID. This VLAN contains only the IPsec VPN SPA inside port and is referred to as the interface VLAN. The interface VLAN is a Layer 3-only VLAN. You configure the Layer 3 address and Layer 3 features, such as ACLs and the crypto map, to the interface VLAN.

You associate the port VLAN and the interface VLAN together using the **crypto engine** *slot* command on the interface VLAN followed by the **crypto connect vlan** command on the port VLAN. Figure 21-1 shows an example of the port VLAN and interface VLAN configurations.

Figure 21-1 Port VLAN and Interface VLAN Configuration Example



Port VLAN 502 and port VLAN 503 are the port VLANs that are associated with two switch outside ports.

Interface VLAN 2 and interface VLAN 3 are the interface VLANs that correspond to port VLAN 502 and port VLAN 503, respectively.

You configure the IP address, ACLs, and crypto map that apply to one switch outside port on interface VLAN 2. You configure the features that apply to another switch outside port on interface VLAN 3.

Packets coming from the WAN through the switch outside port belonging to VLAN 502 are directed by the PFC to the IPsec VPN SPA outside port. The IPsec VPN SPA decrypts the packets and changes the VLAN to interface VLAN 2 and then presents the packet to the switch through the IPsec VPN SPA inside port. The PFC then routes the packet to the proper destination.

Packets going from the LAN to the outside ports are first routed by the PFC. Based on the route, the PFC routes the packets to one of the interface VLANs and directs the packet to the IPsec VPN SPA inside port. The IPsec VPN SPA applies the cryptographic policies that are configured on the corresponding interface VLAN, encrypts the packet, changes the VLAN ID to the corresponding port VLAN, and sends the packet to the switch outside port through the IPsec VPN SPA outside port.

Access Ports, Trunk Ports, and Routed Ports

When you configure VPNs on the IPsec VPN SPA using crypto-connect mode, you attach crypto maps to interface VLANs. Using the **crypto connect vlan** command, you then attach an interface VLAN either to a Layer 2 port VLAN associated with one or more physical ports, or directly to a physical port. The physical ports can be ATM, POS, serial, or Ethernet ports.

When you crypto-connect an interface VLAN to a port VLAN that is attached to one or more Ethernet ports configured in switchport mode, the Ethernet ports can be configured as either access ports or trunk ports:

- Access ports—Access ports are switch ports that have an external or VLAN Trunk Protocol (VTP) VLAN associated with them. You can associate more than one port to a defined VLAN.
- Trunk ports—Trunk ports are switch ports that carry many external or VTP VLANs, on which all packets are encapsulated with an 802.1Q header.

When you crypto-connect an interface VLAN to a physical Ethernet port without defining a port VLAN, a hidden port VLAN is automatically created and associated with the port. In this configuration, the Ethernet port is a routed port:

- Routed ports—By default, every Ethernet port is a routed port until it is configured as a switch port. A routed port may or may not have an IP address assigned to it, but its configuration does not include the **switchport** command.

Crypto-Connect Mode Configuration Guidelines and Restrictions

Follow these guidelines and restrictions to prevent IPsec VPN SPA misconfigurations when configuring VPN ports in crypto-connect mode:

- Ethernet ports installed in a Cisco 7600 SIP-400 in the chassis cannot be configured as switch ports.
- When attaching a crypto VLAN to an outside port VLAN or to a physical interface with the **crypto connect vlan** command, do not apply Layer 3 configurations to that physical interface or port VLAN. Layer 3 configurations (for example, IP address, PIM, et alia), are supported only on the crypto VLAN interface.

Note For Dialer and serial interfaces such as WAN PPP and MLPPP, the **ip unnumbered Null0** command is added automatically to the outside interface configuration for internal Cisco purposes. The **ip unumbered Null0** command is not automatically added, and should not be manually added to outside interface configurations for legacy LAN or WAN interfaces or their subinterfaces (for example, Gigabit or FastEthernet).

Note For routed ports, use the **no ip address** command on the physical interface or port VLAN to remove Layer 3 configurations.

- Removing a line in a crypto ACL causes all crypto maps using that ACL to be removed and reattached to the IPsec VPN SPA. This action causes intermittent connectivity problems for all the security associations (SAs) derived from the crypto maps that reference that ACL.
- A loopback interface can be used as tunnel source address.
- Do not attach a crypto map set to a loopback interface. However, you can maintain an IPsec security association database independent of physical ingress and egress interfaces with the IPsec VPN SPA by entering the **crypto map local-address** command.

  If you apply the same crypto map set to each secure interface and enter the **crypto map local-address** command with the interface as a loopback interface, you will have a single security association database for the set of secure interfaces. If you do not enter the **crypto map local-address** command, the number of IKE security associations is equal to the number of interfaces attached.
- You can attach a crypto map to an interface VLAN that is associated with a GRE/IPsec tunnel, but do not attach a crypto map to an interface VLAN that is associated with a DMVPN tunnel.
- A crypto map local address (for example, the interface VLAN address if the crypto map is applied to the interface VLAN) can share the same address as the GRE/IPsec tunnel source address, but it cannot share the same address as a DMVPN tunnel source address.
- You can attach the same crypto map to multiple interfaces only if the interfaces are all bound to the same crypto engine.
- If you configure a crypto map with an empty ACL (an ACL that is defined but has no lines) and attach the crypto map to an interface, all traffic goes out of the interface in the clear (unencrypted) state.
- Do not convert existing crypto-connected port characteristics. When the characteristics of a crypto-connected access port or a routed port change (switch port to routed port or vice versa), the associated crypto connection is deleted.
- Do not remove the interface VLAN or port VLAN from the VLAN database. All interface VLANs and port VLANs must be in the VLAN database. When you remove these VLANs from the VLAN database, the running traffic stops.

  When you enter the **crypto connect vlan** command and the interface VLAN or port VLAN is not in the VLAN database, this warning message is displayed:

  ```
  VLAN id 2 not found in current VLAN database. It may not function correctly unless
  VLAN 2 is added to VLAN database.
  ```

- When replacing a crypto map on an interface, always enter the **no crypto map** command before reapplying a crypto map on the interface.

- Inbound and outbound traffic for the same tunnel must use the same outside interface. Asymmetric routing, in which encrypted traffic uses a different outside interface than decrypted traffic for the same tunnel, is not supported.
- After a supervisor engine switchover, the installed SPAs reboot and come back online. During this period, the IPsec VPN SPA's established security associations (SAs) are temporarily lost and are reconstructed after the SPA comes back online. The reconstruction is through IKE (it is not instantaneous).
- Crypto ACLs support only the EQ operator. Other operators, such as GT, LT, and NEQ, are not supported.

Note When configuring a permit policy for multiple ports with the EQ operator, you must use multiple lines as in this example:

```
permit ip any any port eq 300
permit ip any any port eq 400
permit ip any any port eq 600
```

In Cisco IOS Release 12.2(33)SXH1 and later releases, when configuring a deny policy for multiple ports with the EQ operator, you can use commas to declare the ports as in this example:

```
deny ip any any port eq 300,400,600
```

- Noncontiguous subnets in a crypto ACL, as in the following example, are not supported:

```
deny ip   10.0.5.0   0.255.0.255   10.0.175.0   0.255.0.255
deny ip   10.0.5.0   0.255.0.255   10.0.176.0   0.255.0.255
```

- ACL counters are not supported for crypto ACLs.
- An egress ACL is not applied to packets generated by the route processor. An ingress ACL is not applied to packets destined for the route processor.
- Do not apply an IP ACL to the crypto-connect interface or port VLAN. Instead, you can apply IP ACLs to the interface VLAN, as in the following example:

```
interface GigabitEthernet1/2
 ! switch outside port
 switchport
 switchport access vlan 502
 switchport mode access
 ip access-group TEST_INBOUND in  <--- do not apply IP ACL here
!
interface Vlan2
 ! interface VLAN
 ip address 11.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0
 ip access-group TEST_INBOUND in  <--- apply IP ACL here
!
interface Vlan502
 ! port VLAN
 no ip address
 crypto connect vlan 2
 ip access-group TEST_INBOUND in  <--- do not apply IP ACL here
!
```

Note An IP ACL on the interface VLAN will not block inbound encrypted traffic from reaching the VSPA, but can prevent traffic from being routed further after decryption.

- In Cisco IOS Release 12.2(33)SXF and earlier releases, IPsec can be configured with manual keying instead of IKE. If you configure manual keying, you must configure SPI to be greater than 4096.

Supported and Unsupported Features in Crypto-Connect Mode

A list of the supported and unsupported features in crypto-connect mode can be found in the "IPsec Feature Support" section on page 20-6.

Configuring the IPsec VPN SPA Inside Port and Outside Port

In most cases, you do not explicitly configure the IPsec VPN SPA inside and outside ports. Cisco IOS software configures these ports automatically.

IPsec VPN SPA Inside and Outside Port Configuration Guidelines and Restrictions

When configuring the IPsec VPN SPA inside and outside ports, follow these guidelines:

- Do not change the port characteristics of the IPsec VPN SPA inside or outside port unless it is necessary to set the trusted state. Cisco IOS software configures the ports automatically.

  Note Although the default trust state of the inside port is trusted, certain global settings may cause the state to change. To preserve the ToS bytes for VPN traffic in both directions, configure the **mls qos trust** command on both the inside and outside ports to set the interface to the trusted state. For information on the **mls qos trust** command, see the "Module QoS Configuration Guidelines and Restrictions" section on page 25-17.

  If you accidentally change the inside port characteristics, enter the following commands to return the port characteristics to the defaults:

```
Router(config-if)# switchport
Router(config-if)# no switchport access vlan
Router(config-if)# switchport trunk allowed vlan 1,1002-1005
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# mtu 9216
Router(config-if)# flow control receive on
Router(config-if)# flow control send off
Router(config-if)# span portfast trunk
```

- Do not configure allowed VLANs on the inside trunk port. Cisco IOS software configures the VLAN list on the inside port automatically based on the **crypto engine slot** command. These VLANs are visible in the port configuration using the **show run** command.
- Do not configure allowed VLANs on the outside trunk port. Cisco IOS software configures these VLANs automatically as hidden VLANs. These VLANs are not visible in the port configuration using the **show run** command.
- Do not remove a VLAN from the IPsec VPN SPA inside port. The running traffic stops when you remove an interface VLAN from the IPsec VPN SPA inside port while the crypto connection to the interface VLAN exists. The crypto connection is not removed and the **crypto connect vlan** command still shows up in the **show running-config** command display. If you enter the **write memory** command with this running configuration, your startup-configuration file would be misconfigured.

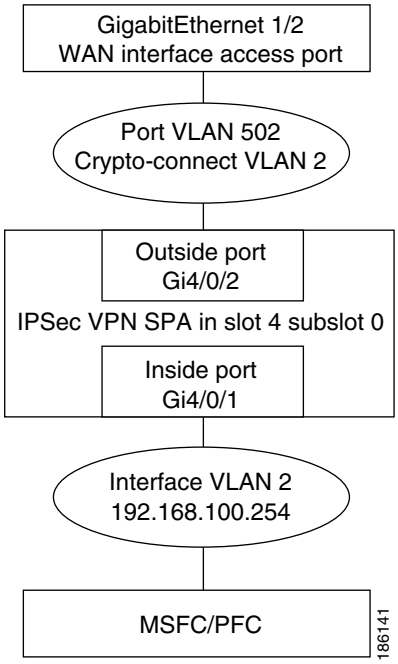
Note It is not possible to remove an interface VLAN from the IPsec VPN SPA inside port while the crypto connection to the interface VLAN exists. You must first remove the crypto connection.

- Do not remove a VLAN from the IPsec VPN SPA outside port. The running traffic stops when you remove a port VLAN from the IPsec VPN SPA outside port while the crypto connection to the interface VLAN exists. The crypto connection is not removed and the **crypto connect vlan** command still shows up in the **show running-config** command display. Removing a VLAN from the IPsec VPN SPA outside port does not affect anything in the startup-configuration file because the port VLAN is automatically added to the IPsec VPN SPA outside port when the **crypto connect vlan** command is entered.

Configuring an Access Port

This section describes how to configure the IPsec VPN SPA with an access port connection to the WAN router (see Figure 21-2).

Figure 21-2 Access Port Configuration Example



Note Ethernet ports installed in a Cisco 7600 SIP-400 in the chassis cannot be configured as switch ports.

To configure an access port connection to the WAN router, perform the following 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`	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 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)# 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 5	`Router(config)# crypto map map-name seq-number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		Creates or modifies a crypto map entry and enters the crypto map configuration mode.
		• *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.
		For details on configuring a crypto map, see the *Cisco IOS Security Configuration Guide*.

Step 6	`Router(config)# vlan inside-vlan-id`	Adds the VLAN ID into the VLAN database. • *inside-vlan-id*—VLAN identifier.
Step 7	`Router(config)# vlan outside-vlan-id`	Adds the VLAN ID into the VLAN database. • *outside-vlan-id*—VLAN identifier.
Step 8	`Router(config)# interface vlan inside-vlan-id`	Enters interface configuration mode for the specified VLAN interface. • *inside-vlan-id*—VLAN identifier.
Step 9	`Router(config-if)# description inside_interface_vlan_for_crypto_map`	(Optional) Adds a comment to help identify the interface.
Step 10	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 11	`Router(config-if)# crypto map map-name`	Applies a previously defined crypto map set to the interface. • *map-name*—Name that identifies the crypto map set. Enter the *map-name* value you created in Step 5.
Step 12	`Router(config-if)# no shutdown`	Enables the interface as a Layer 3 inside interface VLAN.
Step 13	`Router(config-if)# crypto engine slot slot/subslot`	Assigns the crypto engine to the crypto interface VLAN. • *slot/subslot*—Enter the slot and subslot where the IPsec VPN SPA is located.
Step 14	`Router(config)# interface vlan outside-vlan-id`	Enters interface configuration mode for the specified VLAN interface. • *outside-vlan-id*—VLAN identifier.
Step 15	`Router(config-if)# description outside_access_vlan`	(Optional) Adds a comment to help identify the interface.
Step 16	`Router(config-if)# no shutdown`	Enables the interface as an outside access port VLAN.

	Command	Purpose
Step 17	`Router(config-if)# crypto connect vlan inside-vlan-id`	Connects the outside access port VLAN to the inside interface VLAN and enters crypto-connect mode. • *inside-vlan-id*—VLAN identifier.
Step 18	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the secure port.
Step 19	`Router(config-if)# description outside_secure_port`	(Optional) Adds a comment to help identify the interface.
Step 20	`Router(config-if)# switchport`	Configures the interface for Layer 2 switching.
Step 21	`Router(config-if)# switchport access vlan outside-vlan-id`	Specifies the default VLAN for the interface. • *outside-vlan-id*—VLAN identifier.
Step 22	`Router(config-if)# exit`	Exits interface configuration mode.

For access port configuration examples, see the "Access Port in Crypto-Connect Mode Configuration Example" section on page 21-30.

Verifying the Access Port Configuration

To verify an access port configuration, enter the **show crypto vlan** command.

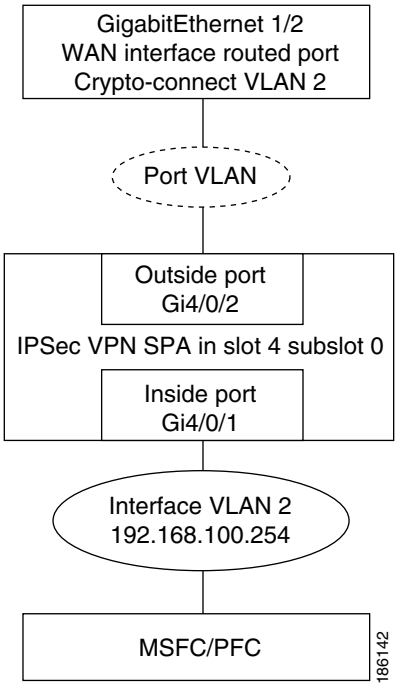
```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port Gi4/0/1 connected to VLAN 502 with crypto
map set MyMap
```

Configuring a Routed Port

This section describes how to configure the IPsec VPN SPA with a routed port connection to the WAN router (see Figure 21-3).

Note When a routed port without an IP address is crypto-connected to an interface VLAN, a hidden port VLAN is created automatically. This port VLAN is not explicitly configured by the user and does not appear in the running configuration.

Figure 21-3 Routed Port Configuration Example



Routed Port Configuration Guidelines

When configuring a routed port using the IPsec VPN SPA, follow these configuration guidelines:

- When a routed port has a crypto connection, IP ACLs cannot be attached to the routed port. Instead, you can apply IP ACLs to the attached interface VLAN.
- Unlike an access port or trunk port, the routed port does not use the **switchport** command in its configuration.
- The **ip unumbered Null0** command is not automatically added, and should not be manually added to outside interface configurations for legacy LAN or WAN interfaces or their subinterfaces (for example, Gigabit or FastEthernet).

To configure a routed port connection to the WAN router, 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`	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 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)# 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 5	`Router(config)# crypto map map-name seq-number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		Creates or modifies a crypto map entry and enters the crypto map configuration mode.
		• *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.
		For details on configuring a crypto map, see the *Cisco IOS Security Configuration Guide*.

Step 6	`Router(config)# vlan inside-vlan-id`	Adds the VLAN ID into the VLAN database. • *inside-vlan-id*—VLAN identifier.
Step 7	`Router(config)# interface vlan inside-vlan-id`	Enters interface configuration mode for the specified VLAN interface. • *inside-vlan-id*—VLAN identifier.
Step 8	`Router(config-if)# description inside_interface_vlan_for_crypto_map`	(Optional) Adds a comment to help identify the interface.
Step 9	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 10	`Router(config-if)# crypto map map-name`	Applies a previously defined crypto map set to the interface. • *map-name*—Name that identifies the crypto map set. Enter the *map-name* value you created in Step 5.
Step 11	`Router(config-if)# no shutdown`	Enables the interface as a Layer 3 crypto interface VLAN.
Step 12	`Router(config-if)# crypto engine slot slot/subslot`	Assigns the crypto engine to the crypto interface VLAN. • *slot/subslot*—Enter the slot and subslot where the IPsec VPN SPA is located.
Step 13	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the secure port.
Step 14	`Router(config-if)# description outside_secure_port`	(Optional) Adds a comment to help identify the interface.
Step 15	`Router(config-if)# no ip address`	Ensures that any Layer 3 configurations on the outside interface are ignored.

	Command	Purpose
Step 16	`Router(config-if)# crypto connect vlan` *inside-vlan-id*	Connects the routed port to the crypto interface VLAN and enters crypto-connect mode. • *inside-vlan-id*—VLAN identifier.
Step 17	`Router(config-if)# exit`	Exits interface configuration mode.

For routed port configuration examples, see the "Routed Port in Crypto-Connect Mode Configuration Example" section on page 21-32.

Verifying a Routed Port Configuration

To verify a route port configuration, enter the **show crypto vlan** command. In the following example, Gi 1/2 is the crypto-connected port:

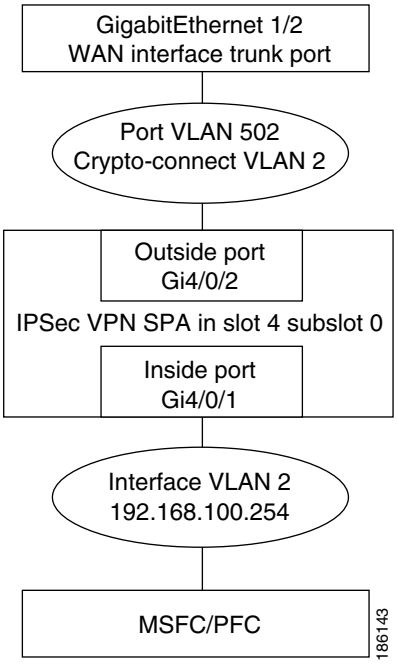
```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port Gi4/0/1 connected to Gi1/2 with crypto map
set MyMap
```

Configuring a Trunk Port

Caution When you configure an Ethernet port as a trunk port, all the VLANs are allowed on the trunk port by default. This default configuration does not work well with the IPsec VPN SPA and causes network loops. To avoid this problem, you must explicitly specify only the desirable VLANs.

This section describes how to configure the IPsec VPN SPA with a trunk port connection to the WAN router (see Figure 21-4).

Figure 21-4 Trunk Port Configuration Example



Note Ethernet ports installed in a Cisco 7600 SIP-400 in the chassis cannot be configured as switch ports.

Trunk Port Configuration Guidelines

When configuring a trunk port using the IPsec VPN SPA, follow these configuration guidelines:

- When you configure a trunk port for cryptographic connection, do not use the "all VLANs allowed" default. You must explicitly specify all the desirable VLANs using the **switchport trunk allowed vlan** command.
- Due to an incorrect startup configuration or through the default trunk port configuration, an interface VLAN might be associated with a trunk port. When you try to remove the interface VLAN from the VLAN list, you might receive an error message similar to the following:

  ```
  Command rejected:VLAN 2 is crypto connected to V502.
  ```

  To remove the interface VLAN from the VLAN list, enter the following commands:

  ```
  Router# configure terminal
  Router(config)# interface g1gabitethernet1/2
  Router(config-if)# no switchport mode trunk
  Router(config-if)# switchport trunk allowed vlan 1
  Router(config-if)# switchport mode trunk
  Router(config-if)# switchport trunk allowed vlan 1,502,1002-1005
  ```

Note VLANs in the VLAN list must not include any interface VLANs.

- To ensure that no interface VLANs are associated when you put an Ethernet port into the trunk mode, enter the following commands in the exact order given:

  ```
  Router# configure terminal
  Router(config)# interface g1gabitethernet1/2
  ```

```
Router(config)# no shut
Router(config-if)# switchport
Router(config-if)# switchport trunk allowed vlan 1
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1,502,1002-1005
```

Note VLANs in the VLAN list must not include any interface VLANs.

- A common mistake when configuring a trunk port occurs when you use the **add** option as follows:

  ```
  Router(config-if)# switchport trunk allowed vlan add 502
  ```

  If the **switchport trunk allowed vlan** command has not already been used, the **add** option does not make VLAN 502 the only allowed VLAN on the trunk port; all VLANs are still allowed after entering the command because all the VLANs are allowed by default. After you use the **switchport trunk allowed vlan** command to add a VLAN, you can then use the **switchport trunk allowed vlan add** command to add additional VLANs.
- To remove unwanted VLANs from a trunk port, use the **switchport trunk allowed vlan remove** command.

Caution Do not enter the **switchport trunk allowed vlan all** command on a secured trunk port. In addition, do not set the IPsec VPN SPA inside and outside ports to "all VLANs allowed."

To configure a trunk port connection to the WAN switch, 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*	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*.

	Command	Purpose

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)# 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*.

Step 5	`Router(config)# crypto map` *map-name seq-number* **ipsec-isakmp**
	`...`
	`Router(config-crypto-map)# exit`
		Creates or modifies a crypto map entry and enters the crypto map configuration mode.
		• *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.
		For details on configuring a crypto map, see the *Cisco IOS Security Configuration Guide*.

Step 6	`Router(config)# vlan` *inside-vlan-id*	Adds the VLAN ID into the VLAN database. • *inside-vlan-id*—VLAN identifier.
Step 7	`Router(config)# vlan` *outside-vlan-id*	Adds the VLAN ID into the VLAN database. • *outside-vlan-id*—VLAN identifier.

	Command	Purpose
Step 8	`Router(config)# interface vlan inside-vlan-id`	Enters interface configuration mode for the specified VLAN interface. • *inside-vlan-id*—VLAN identifier.
Step 9	`Router(config-if)# description inside_interface_vlan_for_crypto_map`	(Optional) Adds a comment to help identify the interface.
Step 10	`Router(config-if)# ip address address mask`	Specifies the IP address and subnet mask for the interface. • *address*—IP address. • *mask*—Subnet mask.
Step 11	`Router(config-if)# crypto map map-name`	Applies a previously defined crypto map set to the interface. • *map-name*—Name that identifies the crypto map set. Enter the *map-name* value you created in Step 5.
Step 12	`Router(config-if)# no shutdown`	Enables the interface as a Layer 3 crypto interface VLAN.
Step 13	`Router(config-if)# crypto engine slot slot/subslot`	Assigns the crypto engine to the crypto interface VLAN. • *slot/subslot*—Enter the slot and subslot where the IPsec VPN SPA is located.
Step 14	`Router(config)# interface vlan outside-vlan-id`	Adds the specified VLAN interface as an outside trunk port VLAN and enters interface configuration mode for the specified VLAN interface. • *outside-vlan-id*—VLAN identifier.
Step 15	`Router(config-if)# description outside_trunk_port_vlan`	(Optional) Adds a comment to help identify the interface.
Step 16	`Router(config-if)# crypto connect vlan inside-vlan-id`	Connects the outside trunk port VLAN to the inside (crypto) interface VLAN and enters crypto-connect mode. • *inside-vlan-id*—VLAN identifier.
Step 17	`Router(config-if)# no shutdown`	Enables the interface as a Layer 3 crypto interface VLAN.
Step 18	`Router(config-if)# interface gigabitethernet slot/subslot/port`	Enters interface configuration mode for the secure port.
Step 19	`Router(config-if)# description outside_secure_port`	(Optional) Adds a comment to help identify the interface.
Step 20	`Router(config-if)# switchport`	Configures the interface for Layer 2 switching.
Step 21	`Router(config-if)# no switchport access vlan`	Resets the access VLAN to the appropriate default VLAN for the device.
Step 22	`Router(config-if)# switchport trunk encapsulation dot1q`	Sets the trunk encapsulation to 802.1Q.
Step 23	`Router(config-if)# switchport mode trunk`	Specifies a trunk VLAN Layer 2 interface.

	Command	Purpose
Step 24	`Router(config-if)# switchport trunk allowed vlan remove vlan-list`	Removes the specified list of VLANs from those currently set to transmit from this interface. *vlan-list*—List of VLANs that transmit the interface in tagged format when in trunking mode. Valid values are from 1 to 4094.
Step 25	`Router(config-if)# switchport trunk allowed vlan add outside-vlan-id`	Adds the specified VLAN to the list of VLANs currently set to transmit from this interface. *outside-vlan-id*—VLAN identifier from Step 14.
Step 26	`Router(config-if)# exit`	Exits interface configuration mode.

For trunk port configuration examples, see the "Trunk Port in Crypto-Connect Mode Configuration Example" section on page 21-34.

Verifying the Trunk Port Configuration

To verify the VLANs allowed by a trunk port, enter the **show interfaces trunk** command. The following display shows that all VLANs are allowed:

```
Router# show interfaces GigabitEthernet 1/2 trunk

Port      Mode         Encapsulation  Status        Native vlan
Gi1/2     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Gi1/2     1-4094

Port      Vlans allowed and active in management domain
Gi1/2     1-4,7-8,513,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/2     1-4,7-8,513,1002-1005
```

Configuring IPsec VPN SPA Connections to WAN Interfaces

The configuration of IPsec VPN SPA connections to WAN interfaces is similar to the configuration of Ethernet-routed interfaces.

IPsec VPN SPA Connections to WAN Interfaces Configuration Guidelines and Restrictions

When configuring a connection to a WAN interface using an IPsec VPN SPA, follow these guidelines and note these restrictions:

- To configure an IPsec VPN SPA connection to a WAN interface, make a crypto connection from the WAN subinterface to the interface VLAN as follows:

```
Router(config)# interface Vlan101
Router(config-if)# ip address 192.168.101.1 255.255.255.0
Router(config-if)# no mop enabled
Router(config-if)# crypto map cwan
Router(config-if)# crypto engine slot 4/0

Router(config)# interface ATM6/0/0.101 point-to-point
```

```
Router(config-subif)# pvc 0/101
Router(config-subif)# crypto connect vlan 101
```

- You must configure a crypto connection on subinterfaces for ATM and Frame Relay.
- For ATM, there is no SVC support, no RFC-1483 bridging, and no point-to-multipoint support.
- For Frame Relay, there is no SVC support, no RFC-1490 bridging, and no point-to-multipoint support.
- For Point-to-Point Protocol (PPP) and Multilink PPP (MLPPP), you must make the physical interface passive for routing protocols, as follows:

```
Router(config)# router ospf 10
Router(config-router)# passive-interface multilink1
```

- For PPP and MLPPP, when the **crypto connect vlan** command is configured on an interface, an **ip unnumbered Null0** command is automatically added to the port configuration to support IPCP negotiation. If you configure a **no ip address** command on the WAN port in the startup configuration, the **no ip address** command will be automatically removed in the running configuration so that it does not conflict with the automatic configuration.
- For PPP and MLPPP, there is no Bridging Control Protocol (BCP) support.
- When enabled on an inside VLAN, OSPF will be configured in broadcast network mode by default, even when a point-to-point interface (such as T1, POS, serial, or ATM) is crypto-connected to the inside VLAN. In addition, if OSPF is configured in point-to-point network mode on the peer router (for example, a transit router with no crypto card), OSPF will not establish full adjacency. In this case, you can manually configure OSPF network point-to-point mode in the inside VLAN:

```
Router(config)# interface vlan inside-vlan
Router(config-if)# ip ospf network point-to-point
```

For IPsec VPN SPA connections to WAN interfaces configuration examples, see the "IPsec VPN SPA Connections to WAN Interfaces Configuration Examples" section on page 21-37

Displaying the VPN Running State

Use the **show crypto vlan** command to display the VPN running state. The following examples show the **show crypto vlan** command output for a variety of IPsec VPN SPA configurations.

In the following example, the interface VLAN belongs to the IPsec VPN SPA inside port:

```
Router# show crypto vlan

  Interface VLAN 2 on IPSec Service Module port Gi4/0/1 connected to Fa8/3
```

In the following example, VLAN 2 is the interface VLAN and VLAN 2022 is the hidden VLAN:

```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port Gi4/0/1 connected to VLAN 2022 with crypto
map set coral2
```

In the following example, the interface VLAN is missing on the IPsec VPN SPA inside port, the IPsec VPN SPA is removed from the chassis, or the IPsec VPN SPA was moved to a different subslot:

```
Router# show crypto vlan

  Interface VLAN 2 connected to VLAN 502 (no IPSec Service Module attached)
```

Configuring GRE Tunneling in Crypto-Connect Mode

This section contains the following GRE configuration topics:

Understanding GRE Tunneling in Crypto-Connect Mode

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to switches at remote points over an IP network.

Note The IPsec VPN SPA is able to accelerate packet processing for up to 2048 GRE tunnels per chassis. Any tunnels not taken over by the IPsec VPN SPA, or any tunnels in excess of 2048, are handled in platform hardware or by the route processor. The switch supports any number of GRE tunnels, but adding more IPsec VPN SPAs does not increase the 2048 tunnels per-chassis maximum that will be handled by IPsec VPN SPAs. If you configure more than 2048 tunnels per chassis, you could overload the route processor. Monitor the route processor CPU utilization when configuring more than 2048 tunnels per chassis.

Note Beginning with Cisco IOS Release 12.2(18)SXF, the GRE fragmentation behavior of the VPN module is changed to be consistent with the fragmentation behavior of the route processor. If GRE encapsulation is performed by the VPN module, prefragmentation of outbound packets will be based on the IP MTU of the tunnel interface. After GRE encapsulation is performed by the VPN module, depending on the IPsec prefragmentation settings, further fragmentation may occur. The IPsec fragmentation behavior is unchanged in this release, and is based on the IPsec MTU configuration of the egress interface.

GRE Tunneling Configuration Guidelines and Restrictions

When configuring point-to-point GRE tunneling in crypto-connect mode using the IPsec VPN SPA, follow these guidelines:

- In a Catalyst 6500 Series switch, GRE encapsulation and decapsulation is traditionally performed by the route processor or the supervisor engine hardware. When routing indicates that encapsulated packets for a GRE tunnel will egress through an interface VLAN that is attached to an IPsec VPN SPA inside port, the IPsec VPN SPA attempts to take over the GRE tunnel interface only if the supervisor engine is unable to process the GRE tunnel interface in hardware. If the supervisor engine cannot process the GRE tunnel interface in hardware, the IPsec VPN SPA will determine if it can take over the interface. By seizing the tunnel, the IPsec VPN SPA takes the GRE encapsulation and decapsulation duty from the route processor. No explicit configuration changes are required to use this feature; configure GRE as you normally would. As long as routing sends the GRE-encapsulated packets over an interface VLAN, the IPsec VPN SPA will seize the GRE tunnel.
- If the same source address is used for more than one GRE tunnel, the supervisor engine hardware will not take over the tunnel. The IPsec VPN SPA will take over the tunnel if it meets the criteria discussed in the previous bullet item.

- Point-to-point GRE with tunnel protection is not supported in crypto-connect mode, but DMVPN is supported.
- If routing information changes and the GRE-encapsulated packets no longer egress through an interface VLAN, the IPsec VPN SPA yields the GRE tunnel. After the IPsec VPN SPA yields the tunnel, the route processor resumes encapsulation and decapsulation, which increases CPU utilization on the route processor.

Caution Ensure that your GRE tunnel configuration does not overload the route processor.

- A delay of up to 10 seconds occurs between routing changes and the IPsec VPN SPA seizing the GRE tunnel.
- The crypto map must only be applied to the interface VLAN and not to the tunnel interface.
- The following options are supported on the tunnel interface: ACLs, service policy, TTL, and ToS.
- The following options are not supported on the tunnel interface: checksum enabled, sequence check enabled, tunnel key, IP security options, policy-based routing (PBR), traffic shaping (can be applied to the crypto engine configuration within the tunnel interface configuration), QoS preclassification, and NAT.
- When the GRE tunnel is taken over in crypto-connect mode, any ACL configured on the interface VLAN will not be applied to packets routed to the GRE interface. The ACL will be applied to packets that do not have GRE processing.
- GRE tunneling of all non-IPv4 packets is done by the route processor even if the tunnel is seized by the IPsec VPN SPA.
- In crypto-connect mode, to avoid fragmentation after encryption, set the tunnel IP MTU to be equal to or less than the egress interface MTU minus the GRE and IPsec overheads.
- When applied to the GRE tunnel interface, the **ip tcp adjust-mss** command is ignored. Apply the command to the ingress LAN interface instead.

To configure a GRE tunnel, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface tunnel` *number*	Creates the tunnel interface if it does not exist and enters interface configuration mode. • *number*—Number of the tunnel interface to be configured.
Step 2	`Router(config-if)# ip address` *address*	Sets the IP address of the tunnel interface. • *address*—IP address.
Step 3	`Router(config-if)# tunnel source {`*ip-address* | *type number*`}`	Configures the tunnel source. The source is the switch where traffic is received from the customer network. • *ip-address*—IP address to use as the source address for packets in the tunnel. • *type number*—Interface type and number; for example, VLAN1.

	Command	Purpose
Step 4	`Router(config-if)# tunnel destination {hostname | ip-address}`	Sets the IP address of the destination of the tunnel interface. The destination address is the switch that transfers packets into the receiving customer network. • *hostname*—Name of the host destination. • *ip-address*—IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	`Router(config-if)# exit`	Exits interface configuration mode.

Verifying the GRE Tunneling Configuration

To verify that the IPsec VPN SPA has seized the GRE tunnel, enter the **show crypto vlan** command:

```
Router# show crypto vlan

Interface VLAN 101 on IPSec Service Module port 7/1/1 connected to AT4/0/0.101
    Tunnel101 is accelerated via IPSec SM in subslot 7/1
Router#
```

For complete configuration information about GRE tunneling, refer to this URL:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

For GRE tunneling configuration examples, see the "GRE Tunneling in Crypto-Connect Mode Configuration Example" section on page 21-41.

Configuring the GRE Takeover Criteria

You can configure the takeover criteria for Generic Routing Encapsulation (GRE) processing by using the **crypto engine gre supervisor** or **crypto engine gre vpnblade** commands. These two commands allow you to specify whether the GRE processing should be done by the supervisor engine hardware or the route processor or the IPsec VPN SPA.

Note The GRE takeover criteria commands are supported only in Cisco IOS Release 12.2(18)SXE5 and later. In releases prior to Cisco IOS Release 12.2SXE1, the crypto-related GRE tunnels are always taken over by the VPN SPA. In Cisco IOS Release 12.2SXE1, the GRE tunnels are taken over by the VPN SPA only if the supervisor engine hardware cannot do the processing.

To configure a switch to process GRE using the supervisor engine hardware or the route processor (RP), use the **crypto engine gre supervisor** command. When this command is specified, GRE processing by the supervisor engine hardware takes precedence over processing by the route processor (unless the tunnels are from duplicate sources); the RP only takes over GRE processing if the supervisor engine hardware cannot do the processing. If this command is configured, duplicate source GREs will be processed by the route processor.

To configure a switch to process GRE using the IPsec VPN SPA, use the **crypto engine gre vpnblade** command. If the IPsec VPN SPA cannot take over the GRE processing, the GRE processing will be handled either by supervisor engine hardware (which has precedence) or the route processor.

Both of these commands can be configured globally or at an individual tunnel.

Individual tunnel configuration takes precedence over the global configuration. For example, when the **crypto engine gre supervisor** command is configured at the global configuration level, the command will apply to all tunnels except those tunnels that have been configured individually using either a **crypto engine gre supervisor** command or a **crypto engine gre vpnblade** command.

At any time, only one of the two commands (**crypto engine gre supervisor** or **crypto engine gre vpnblade**) can be configured globally or individually at a tunnel. If either command is already configured, configuring the second command will overwrite the first command, and only the configuration applied by the second command will be used.

GRE Takeover Configuration Guidelines and Restrictions

When configuring GRE takeover on the IPsec VPN SPA, follow these guidelines and restrictions:

- For a GRE tunnel to be taken over by the IPsec VPN SPA, it must first satisfy the following criteria:
  - The GRE tunnel interface must be up.
  - The route to the tunnel destination must go through the IPsec VPN SPA.
  - The Address Resolution Protocol (ARP) entry for the next hop must exist.
  - The tunnel mode must be GRE.
  - The only supported options are **tunnel ttl** and **tunnel tos**. If any of the following command options are configured, then the tunnel will not be taken over:
    - **tunnel key**
    - **tunnel sequence-datagrams**
    - **tunnel checksum**

    All other options configured are ignored.
- If the GRE tunnels have the same source and destination addresses, then the IPsec VPN SPA will, at most, take over only one of them, and the determination of which specific tunnel is taken over is random.
- The IPsec VPN SPA will not take over GRE processing if any of the following features are configured on the tunnel interface:
  - DMVPN
  - NAT
- In crypto-connect mode, the IPsec VPN SPA will not take over GRE processing when the interface VLAN has no crypto map attached. The crypto map must be applied to the interface VLAN and not to the tunnel interface.
- If the IPsec VPN SPA cannot take over the GRE processing, the GRE processing will be handled either by the supervisor engine hardware (which has precedence) or the route processor.
- When neither the **crypto engine gre supervisor** command nor the **crypto engine gre vpnblade** command is specified globally or individually for a tunnel, the IPsec VPN SPA will only attempt to take over GRE processing if the following conditions apply:
  - The supervisor engine hardware does not take over GRE processing.
  - Protocol Independent Multicast (PIM) is configured on the tunnel.
  - Multiple tunnels share the same tunnel source interface and more than one tunnel is up. (If only one tunnel is up, the supervisor engine hardware can still perform the GRE processing.)

- When a new configuration file is copied to the running configuration, the new configuration will overwrite the old configuration for the **crypto engine gre vpnblade** and **crypto engine gre supervisor** commands. If the new configuration does not specify a GRE takeover criteria globally or for an individual tunnel, the existing old configuration will be used.
- GRE keepalives are not supported if **crypto engine gre vpnblade** is configured.

Configuring the GRE Takeover Criteria Globally

To configure the GRE takeover criteria globally (so that it affects all tunnels except those tunnels that have been configured individually using either a **crypto engine gre supervisor** command or a **crypto engine gre vpnblade** command), perform this task beginning in global configuration mode:

	Command	Purpose

Step 1	`Router(config)# crypto engine gre supervisor`
	or
	`Router(config)# crypto engine gre vpnblade`
		Configures a router to process GRE using the supervisor engine hardware or the route processor.
		
		Configures a router to process GRE using the IPsec VPN SPA.

Configuring the GRE Takeover Criteria at an Individual Tunnel

To configure the GRE takeover criteria at an individual tunnel (so that it affects only a specific tunnel), perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface tunnel` *number*	Creates the tunnel interface if it does not exist and enters interface configuration mode. • *number*—Number of the tunnel interface to be configured.

Step 2	`Router(config-if)# crypto engine gre supervisor`
	or
	`Router(config-if)# crypto engine gre vpnblade`
		Configures a router to process GRE using the supervisor engine hardware or the route processor.
		or
		Configures a router to process GRE using the IPsec VPN SPA.

For GRE takeover criteria configuration examples, see the "GRE Takeover Criteria Configuration Examples" section on page 21-43.

Configuring IP Multicast over a GRE Tunnel

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to multiple recipients. GRE is a tunneling protocol developed by Cisco and commonly used with IPsec that encapsulates 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 network.

In some network scenarios, you might want to configure your network to use GRE tunnels to send Protocol Independent Multicast (PIM) and multicast traffic between routers. Typically, this occurs when the multicast source and receiver are separated by an IP cloud that is not configured for IP multicast routing. In such network scenarios, configuring a tunnel across an IP cloud with PIM-enabled transports multicast packets toward the receiver. The configuration of IP multicast over a GRE tunnel using the IPsec VPN SPA involves three key steps:

- Configuring single-SPA mode (if supported) for multicast traffic
- Configuring multicast globally
- Configuring PIM at the tunnel interfaces

IP Multicast over a GRE Tunnel Configuration Guidelines and Restrictions

When configuring IP multicast over a GRE tunnel, follow these guidelines:

- When the **hw-module slot subslot only** command is executed, it automatically resets the Cisco 7600 SSC-400 card and displays the following prompt on the console:

  ```
  Module n will be reset? Confirm [n]:
  ```

  The prompt will default to N (no). You must type Y (yes) to activate the reset action.

  Note The **hw-module slot subslot only** command is not supported in Cisco IOS Release 12.2(33)SXI and later releases.

- When in single-SPA mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **no hw-module subslot shutdown** command, for example), a message is displayed on the router console that refers you to the customer documentation.
- If PIM is configured, and the GRE tunnel interface satisfies the rest of the tunnel takeover criteria, the GRE processing of the multicast packets will be taken over by the IPsec VPN SPA.
- GRE processing of IP multicast packets will be taken over by the IPsec VPN SPA if the GRE tunnel interface satisfies the following tunnel takeover criteria:
  - The tunnel is up.
  - There are no other tunnels with the same source destination pair.
  - The tunnel is not an mGRE tunnel.
  - PIM is configured on the tunnel.
  - None of the following features are configured on the tunnel: tunnel key, tunnel sequence-datagrams, tunnel checksum, tunnel udlr address-resolution, tunnel udlr receive-only, tunnel udlr send-only, ip proxy-mobile tunnel reverse, or NAT. If any of these options are specified, the IPsec VPN SPA will not seize the GRE tunnel.
- When a tunnel is configured for multicast traffic, the **crypto engine gre supervisor** command should not be applied to the tunnel.

Configuring Single-SPA Mode for IP Multicast Traffic

Note Single-SPA mode is not supported in Cisco IOS Release 12.2(33)SXI and later releases.

Before you configure IP multicast on the IPsec VPN SPA, you should change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot using the Before you configure IP multicast on the IPsec VPN SPA, you should change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot using the **hw-module slot subslot only** command. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400 card.

To allocate full buffers to the specified subslot, use the **hw-module slot subslot only** command as follows:

```
Router(config)# hw-module slot slot subslot subslot only
```

slot specifies the slot where the Cisco 7600 SSC-400 card is located.

subslot specifies the subslot where the IPsec VPN SPA is located.

If the **hw-module slot subslot only** command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400 card.

Configuring IP Multicast Globally

You must enable IP multicast routing globally before you can enable PIM on the router interfaces.

To enable IP multicast routing globally, use the **ip multicast-routing** command.

Configuring PIM at the Tunnel Interfaces

You must enable PIM on all participating router interfaces before IP multicast will function.

To enable PIM, use the **ip pim** command as follows:

```
Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}
```

dense-mode enables dense mode of operation.

sparse-mode enables sparse mode of operation.

sparse-dense-mode enables the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.

For IP multicast over GRE tunnels configuration examples, see the "IP Multicast over a GRE Tunnel Configuration Example" section on page 21-44.

Verifying the IP Multicast over a GRE Tunnel Configuration

To verify the IP multicast over a GRE tunnel configuration, enter the **show crypto vlan** and **show ip mroute** commands.

To verify that the tunnel has been taken over by the IPsec VPN SPA, enter the **show crypto vlan** command:

```
Router# show crypto vlan

Interface VLAN 100 on IPSec Service Module port Gi7/0/1 connected to Po1 with crypto map
set map_t3
Tunnel15 is accelerated via IPSec SM in subslot 7/0
```

To verify that the IP multicast traffic is hardware-switched, enter the **show ip mroute** command and look for the **H** flag:

```
Router# show ip mroute 230.1.1.5
```

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 230.1.1.5), 01:23:45/00:03:16, RP 15.15.1.1, flags: SJC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16
(120.1.0.3, 230.1.1.5), 01:23:46/00:03:25, flags: T
Incoming interface: GigabitEthernet8/1, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16, H
```

For IP multicast over GRE tunnels configuration examples, see the "IP Multicast over a GRE Tunnel Configuration Example" section on page 21-44.

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/subslot* {**inside** | **outside**}). The **crypto engine subslot** command is no longer supported. When upgrading, ensure that this command has been modified in your start-up configuration to avoid extended maintenance time.

Access Port in Crypto-Connect Mode Configuration Example

This section provides an example of the access port configuration with switch 1 shown in Figure 21-2 on page 21-8:

Switch 1 (Access Port)

```
!
hostname router-1
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.1
!
!
crypto ipsec transform-set proposal1 esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
  !switch inside port
  ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 502
 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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk

interface Vlan2
 !interface vlan
 ip address 11.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0
```

```
!
interface Vlan502
 !port vlan
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 12.0.0.0 255.0.0.0 11.0.0.1
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
!
end
```

Switch 2 (Access Port)

```
!
hostname router-2
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.2
!
!
crypto ipsec transform-set proposal1 esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
  !switch inside port
  ip address 12.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 502
 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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
```

```
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 !interface vlan
 ip address 11.0.0.1 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0
!
interface Vlan502
 !port vlan
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 13.0.0.0 255.0.0.0 11.0.0.2
!
access-list 101 permit ip host 12.0.0.2 host 13.0.0.2
!
end
```

Routed Port in Crypto-Connect Mode Configuration Example

This section provides an example of the routed port configuration with switch 1 shown in Figure 21-3 on page 21-12:

Switch 1 (Routed Port)

```
!
hostname router-1
!
vlan 2
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 crypto isakmp key 12345 address 11.0.0.2
!
!
crypto ipsec transform-set proposal1 esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 12.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 no ip address
 crypto connect vlan 2
!
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 Vlan2
 !interface vlan
 ip address 11.0.0.1 255.255.255.0
 no mop enabled
 crypto map testtag
 crypto engine slot 4/0
!
ip classless
ip route 13.0.0.0 255.0.0.0 11.0.0.2
!
access-list 101 permit ip host 12.0.0.2 host 13.0.0.2
!
end
```

Switch 2 (Routed Port)

```
!
hostname router-2
!
vlan 2
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.1
!
!
crypto ipsec transform-set proposal1 esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 no ip address
 crypto connect vlan 2
!
```

```
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 Vlan2
 !interface vlan
 ip address 11.0.0.2 255.255.255.0
 no mop enabled
 crypto map testtag
 crypto engine slot 4/0
!
ip classless
ip route 12.0.0.0 255.0.0.0 11.0.0.1
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
!
end
```

Trunk Port in Crypto-Connect Mode Configuration Example

This section provides an example of the trunk port configuration with switch 1 shown in Figure 21-4 on page 21-16:

Switch 1 (Trunk Port)

```
!
hostname router-1
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.2
!
!
crypto ipsec transform-set proposal1  esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal1
 match address 101
```

```
!
!
interface GigabitEthernet1/1
  !switch inside port
  ip address 12.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 502
 switchport mode trunk
!
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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 !interface vlan
 ip address 11.0.0.1 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0
!
interface Vlan 502
 !port vlan
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 13.0.0.0 255.0.0.0 11.0.0.2
!
access-list 101 permit ip host 12.0.0.2 host 13.0.0.2
!
end
```

Switch 2 (Trunk Port)

```
!
hostname router-2
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
```

```
crypto isakmp key 12345 address 11.0.0.1
!
!
crypto ipsec transform-set proposal1  esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
  !switch inside port
  ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 502
 switchport mode trunk
!
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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk

interface Vlan2
 !interface vlan
 ip address 11.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0
!
interface Vlan502
 !port vlan
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 12.0.0.0 255.0.0.0 11.0.0.1
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
!
end
```

IPsec VPN SPA Connections to WAN Interfaces Configuration Examples

The following are configuration examples of IPsec VPN SPA connections to WAN interfaces:

IPsec VPN SPA Connection to an ATM Port Adapter Configuration Example

The following example shows the configuration of an IPsec VPN SPA connection to an ATM port adapter:

```
!
hostname router-1
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set proposal esp-3des esp-sha-hmac
!
crypto map testtag_1 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal
 match address acl_1
!
interface GigabitEthernet1/1
 ip address 12.0.0.2 255.255.255.0
!
interface ATM2/0/0
 no ip address
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/0/0.1 point-to-point
 atm pvc 20 0 20 aal5snap
 no atm enable-ilmi-trap
 crypto connect vlan 2
!
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 Vlan2
 ip address 11.0.0.1 255.255.255.0
 crypto map testtag_1
 crypto engine slot 4/0
!
ip classless
ip route 13.0.0.1 255.255.255.255 11.0.0.2
!
ip access-list extended acl_1
 permit ip host 12.0.0.1 host 13.0.0.1
!
```

IPsec VPN SPA Connection to a POS Port Adapter Configuration Example

The following example shows the configuration of an IPsec VPN SPA connection to a POS port adapter:

```
!

hostname router-1
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set proposal esp-3des esp-sha-hmac
!
crypto map testtag_1 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal
 match address acl_1
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 12.0.0.2 255.255.255.0
!
interface POS2/0/0
 no ip address
 encapsulation frame-relay
 clock source internal
!
interface POS2/0/0.1 point-to-point
 frame-relay interface-dlci 16
 crypto connect vlan 2
!
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 Vlan2
 ip address 11.0.0.1 255.255.255.0
 crypto map testtag_1
 crypto engine slot 4/0
!
ip classless
ip route 13.0.0.1 255.255.255.255 11.0.0.2
!
ip access-list extended acl_1
 permit ip host 12.0.0.1 host 13.0.0.1
```

IPsec VPN SPA Connection to a Serial Port Adapter Configuration Example

The following example shows the configuration of an IPsec VPN SPA connection to a serial port adapter:

```
!
hostname router-1
!
controller T3 2/1/0
 t1 1 channel-group 0 timeslots 1
 t1 2 channel-group 0 timeslots 1
 t1 3 channel-group 0 timeslots 1
 t1 4 channel-group 0 timeslots 1
 t1 5 channel-group 0 timeslots 1
 t1 6 channel-group 0 timeslots 1
 t1 7 channel-group 0 timeslots 1
 t1 8 channel-group 0 timeslots 1
 t1 9 channel-group 0 timeslots 1
 t1 10 channel-group 0 timeslots 1
 t1 11 channel-group 0 timeslots 1
 t1 12 channel-group 0 timeslots 1
 t1 13 channel-group 0 timeslots 1
 t1 14 channel-group 0 timeslots 1
 t1 15 channel-group 0 timeslots 1
 t1 16 channel-group 0 timeslots 1
 t1 17 channel-group 0 timeslots 1
 t1 18 channel-group 0 timeslots 1
 t1 19 channel-group 0 timeslots 1
 t1 20 channel-group 0 timeslots 1
 t1 21 channel-group 0 timeslots 1
 t1 22 channel-group 0 timeslots 1
 t1 23 channel-group 0 timeslots 1
 t1 24 channel-group 0 timeslots 1
 t1 25 channel-group 0 timeslots 1
 t1 26 channel-group 0 timeslots 1
 t1 27 channel-group 0 timeslots 1
 t1 28 channel-group 0 timeslots 1
!
crypto isakmp policy 1
```

```
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set proposal esp-3des esp-sha-hmac
!
crypto map testtag_1 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal
 match address acl_1
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 12.0.0.2 255.255.255.0
!
interface Serial2/1/0/1:0
 ip unnumbered Null0
 encapsulation ppp
 no fair-queue
 no cdp enable
 crypto connect vlan 2
!
!
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 Vlan2
 ip address 11.0.0.1 255.255.255.0
 crypto map testtag_1
 crypto engine slot 4/0
!
ip classless
ip route 13.0.0.1 255.255.255.255 11.0.0.2
!
ip access-list extended acl_1
 permit ip host 12.0.0.1 host 13.0.0.1
```

GRE Tunneling in Crypto-Connect Mode Configuration Example

This section provides an example of GRE tunneling configurations.

Switch 1 (GRE Tunneling)

The following example shows the configuration of GRE tunneling for switch 1:

```
!
hostname router-1
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.2
!
!
crypto ipsec transform-set proposal1 ah-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal1
 match address 101
!
!
!
!
interface Tunnel1
 ip address 1.0.0.1 255.255.255.0
 tunnel source Vlan2
 tunnel destination 11.0.0.2
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 12.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 502
 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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
```

```
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 11.0.0.1 255.255.255.0
 no mop enabled
 crypto map testtag
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
!
ip classless
ip route 13.0.0.0 255.0.0.0 Tunnel1
!
!
access-list 101 permit gre host 11.0.0.1 host 11.0.0.2
!
```

Switch 2 (GRE Tunneling)

```
!
hostname router-2
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.1
!
!
crypto ipsec transform-set proposal1 ah-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 match address 101
!
!
!
!
interface Tunnel1
 ip address 1.0.0.2 255.255.255.0
 tunnel source Vlan2
 tunnel destination 11.0.0.1
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 502
 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 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 11.0.0.2 255.255.255.0
 no mop enabled
 crypto map testtag
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 12.0.0.0 255.0.0.0 Tunnel1
!
access-list 101 permit gre host 11.0.0.2 host 11.0.0.1
!
```

GRE Takeover Criteria Configuration Examples

The following examples show how to configure the GRE takeover criteria:

- GRE Takeover Criteria Global Configuration Example, page 21-43
- GRE Takeover Criteria Tunnel Configuration Example, page 21-43
- GRE Takeover Verification Example, page 21-44

GRE Takeover Criteria Global Configuration Example

The following example shows that the GRE takeover criteria has been set globally and the supervisor engine hardware or RP always does the GRE processing:

```
Router(config)# crypto engine gre supervisor
```

GRE Takeover Criteria Tunnel Configuration Example

The following example shows that the GRE takeover criteria has been set individually for tunnel interface 3 and the IPsec VPN SPA always does the GRE processing for this tunnel:

```
Router(config)# interface tunnel 3
Router(config-if)# crypto engine gre vpnblade
```

GRE Takeover Verification Example

The following example shows how to verify that the tunnel has been taken over by the IPsec VPN SPA:

```
Router(config)# show crypto vlan 100

Interface VLAN 100 on IPSec Service Module port GigabitEthernet4/0/1 connected to POS8/0/0
with crypto map set MAP_TO_R2
    Tunnel1 is accelerated via IPSec SM in subslot 4/0
```

The following example shows that the tunnel has not been taken over by the IPsec VPN SPA:

```
Router(config)# show crypto vlan 100

Interface VLAN 100 on IPSec Service Module port GigabitEthernet4/0/1 connected to POS8/0/0
with crypto map set MAP_TO_R2
```

IP Multicast over a GRE Tunnel Configuration Example

The following example shows how to configure IP multicast over GRE:

```
hostname router-1
!
vlan 2-1001
ip multicast-routing
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set proposal esp-3des
!
!
crypto map cm_spoke1_1 10 ipsec-isakmp
 set peer 11.1.1.1
 set transform-set proposal
 match address spoke1_acl_1
!
!
interface Tunnel1
 ip address 20.1.1.1 255.255.255.0
 ip mtu 9216
 ip pim sparse-mode
 ip hold-time eigrp 1 3600
 tunnel source 1.0.1.1
 tunnel destination 11.1.1.1
 crypto engine slot 4/0
!
interface GigabitEthernet1/1
 !switch inside port
 mtu 9216
 ip address 50.1.1.1 255.0.0.0
 ip pim sparse-mode
!
interface GigabitEthernet1/2
 !switch outside port
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,252,1002-1005
 switchport mode trunk
 mtu 9216
!
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 1,252,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 mtu 9216
 ip address 1.0.1.1 255.255.255.0
 crypto map cm_spoke1_1
 crypto engine slot 4/0
!
interface Vlan252
 mtu 9216
 no ip address
 crypto connect vlan 2
!
router eigrp 1
 network 20.1.1.0 0.0.0.255
 network 50.1.1.0 0.0.0.255
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 11.1.1.0 255.255.255.0 1.0.1.2
!
ip pim bidir-enable
ip pim rp-address 50.1.1.1
!
ip access-list extended spoke1_acl_1
 permit gre host 1.0.1.1 host 11.1.1.1
!
```