VPN Availability Configuration Guide, Cisco IOS Release 12.4T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

Reverse Route Injection

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.

Enhancements to the default behavior of RRI, the addition of a route tag value, and enhancements to how RRI is configured were added to the Reverse Route Injection feature in Cisco IOS Release 12.3(14)T.

An enhancement was added in Cisco IOS Release 12.4(15)T that allows a distance metric to be set for routes that are created by a VPN process so that the dynamically learned route on a router can take precedence over a locally configured static route.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Reverse Route Injection

- IP routing should be enabled and static routes should be redistributed if dynamic routing protocols are to be used to propagate RRI-generated static routes.

Restrictions for Reverse Route Injection

- If RRI is applied to a crypto map, that map must be unique to one interface on the router. In other words, the same crypto map cannot be applied to multiple interfaces. If more than one crypto map is applied to multiple interfaces, routes may not be cleaned up correctly. If multiple interfaces require a crypto map, each must use a uniquely defined map. This restriction applies only to RRI before Cisco IOS Release 12.3(14)T.
- For static crypto maps, routes are always present if RRI is configured on an applied crypto map. In Cisco IOS Release 12.3(14)T, the default behavior--of routes always being present for a static map--will not apply unless the **static**keyword is added to the **reverse-route** command.

Information About Reverse Route Injection

Reverse Route Injection

RRI is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN router as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN router, this information is propagated to upstream devices, allowing them to determine the appropriate VPN router to which to send returning traffic in order to maintain IPsec state flows. Being able to determine the appropriate VPN router is particularly useful if multiple VPN routers are used at a site to provide load balancing or failover or if the remote VPN devices are not accessible via a default route. Routes are created in either the global routing table or the appropriate virtual route forwarding (VRF) table.

RRI is applied on a per-crypto map basis, whether this is via a static crypto map or a dynamic crypto map template. The default behavior for the two map types is as follows:

- In the case of a dynamic crypto map, routes are created upon the successful establishment of IPsec security associations (SAs) for those remote proxies. The next hop back to those remote proxies is via the remote VPN router whose address is learned and applied during the creation of the dynamic crypto map template. The routes are deleted after the SAs are deleted. In Cisco IOS Release 12.3(14)T, the creation of routes on the basis of IPsec source proxies on static crypto maps was added. This behavior became the default behavior on static maps and overrode the creation of routes on the basis of crypto ACLs (see the next bullet).
- For static crypto maps, routes are created on the basis of the destination information defined in the crypto access list. The next hop is taken from the first set peer statement that is attached to the crypto map. If at any time, RRI, the peer, or the access list is removed from the crypto map, routes will be deleted. This behavior changes with the addition of the RRI enhancements, as explained in the sections below.

Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T

RRI Distance Metric

In general, a static route is created having an administrative distance of 1, which means that static routes always have precedence in the routing table. In some scenarios, however, it is required that dynamically learned routes take precedence over static routes, with the static route being used in the absence of a dynamically learned route. The addition of the **set reverse-route distance** command under either a crypto map or IPsec profile allows you to specify a different distance metric for VPN-created routes so that those routes will be in effect only if a dynamic or more favored route becomes unavailable.

Gateway Option

This RRI gateway option is relevant to the crypto map only.

This option allows you to configure unique next hops or gateways for remote tunnel endpoints. The option is identical to the way the **reverse-route remote-peer**{*ip-address*} command worked prior to Cisco IOS Release 12.3(14)T in that two routes are created for each VPN tunnel. The first route is to the destination-protected subnet via the remote tunnel endpoint. The second route specifies the next hop to be taken to reach this tunnel endpoint. This RRI gateway option allows specific default paths to be specified for specific groups of VPN connections on platforms that support recursive route lookups.

Note In 12.4(15)T and later releases, the **gateway** keyword option replaces the **reverse-route remote-peer** command (with no *ip-address*). Due to changes to Cisco Express Forwarding (CEF), an interface as a next-hop cannot be used without also adding a next-hop IP address.

Support for RRI on IPsec Profiles

Previously RRI was available for crypto map configurations only. Cisco IOS Release 12.4(15)T introduces support for relevant RRI options on IPsec profiles that are predominantly used for virtual tunnel interfaces. On tunnel interfaces, only the distance metric and tag options are useful with the generic RRI capability.

Note It is not necessary to specifically enable RRI on dynamic virtual interfaces for Easy VPN clients. Route support is enabled by default. It is necessary to specify tag or distance metric values if these are required.

Tag Option Configuration Changes

The tag option was introduced in 12.3(14)T for crypto maps. This option is now supported with IPsec profiles under the **set reverse-route tag** command syntax. The **set reverse-route tag** command is also available under the crypto map for uniformity although the legacy **reverse-route tag** command is no longer supported.

show crypto route Command

The **show crypto route** command displays routes that are created through IPsec via RRI or Easy VPN virtual tunnel interfaces (VTIs). The routes are displayed in one table. To see sample output for the **show crypto route** command, see the "show crypto route Command Output Example" section.

How to Configure Reverse Route Injection

Configuring RRI Under Static Crypto Maps

To configure RRI under a static crypto map for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map {** *map-name* } **{** *seq-name*} **ipsec-isakmp**
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto map {** *map-name* } **{** *seq-name*} **ipsec-isakmp** **Example:** `Router (config)# crypto map mymap 1 ipsec-isakmp`	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]] **Example:** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.

Configuring RRI Under a Dynamic Map Template for Cisco

To configure RRI under a dynamic map template for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Router (config)# crypto dynamic-map mymap 1`	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]] **Example:** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.

Configuring RRI with Enhancements Under a Static Crypto Map

To configure RRI with enhancements under a static crypto map (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-name* **ipsec-isakmp**
4. **reverse-route** [**static** | **remote-peer** *ip-address* **[gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto map** *map-name seq-name* **ipsec-isakmp** **Example:** `Router (config)# crypto map mymap 1 ipsec-isakmp`	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	**reverse-route** [**static** | **remote-peer** *ip-address* **[gateway**] [**static**]] **Example:** `Router (config-crypto-map)# reverse-route`	Creates source proxy information for a crypto map entry. **Note** The **gateway** keyword can be added to enable the dual route functionality for default gateway support.
Step 5	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **Example:** `Router (config-crypto-map)# set reverse-route distance 20`	Specifies a distance metric to be used or a tag value to be associated with these routes.

Configuring RRI with Enhancements Under a Dynamic Map Template

To configure RRI with enhancements under a dynamic map template (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **remote-peer** *ip-address* **[gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Router (config)# crypto dynamic-map mymap 1`	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	**reverse-route** [**static** | **remote-peer** *ip-address* **[gateway**] [**static**]] **Example:** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1 gateway`	Creates source proxy information for a crypto map entry.
Step 5	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **Example:** `Router (config-crypto-map)# set reverse-route distance 20`	Specifies a distance metric to be used or a tag value to be associated with these routes.

Configuring an RRI Distance Metric Under an IPsec Profile

To configure a RRI distance metric under an IPsec profile for Cisco IOS Release 12.4(15)T and later releases, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec profile** *name* **Example:** `Router (config)# crypto ipsec profile myprofile`	Creates or modifies an IPsec profile and enters IPsec profile configuration mode.
Step 4	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **Example:** `Router (config-crypto-profile)# set reverse-route distance 20`	Defines a distance metric for each static route or tags a reverse route injection- (RRI-) created route. • **distance** --Defines a distance metric for each static route. • **tag** --Sets a tag value that can be used as a “match” value for controlling distribution using route maps.

Displaying Routes Created through IPsec Using RRI or Easy VPN VTIs

To display routes that are created through IPsec via RRI or Easy VPN VTIs, perform the following steps. To observe the behavior of RRI and its relationship to the creation and deletion of an IPsec SA, you can use the **debug crypto ipsec** command

SUMMARY STEPS

1. **enable**
2. **show crypto route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto route** **Example:** `Router# show crypto route`	Displays routes that are created through IPsec via RRI or Easy VPN VTIs.

Configuration Examples for Reverse Route Injection

Configuring RRI Prior to Cisco IOS Release 12.3(14)T Examples

Configuring RRI When Crypto ACLs Exist Example

The following example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto access control list (ACL):

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

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

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

Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

VPNSM

ip route 10.1.1.1 255.255.255.255 vlan0.1

Configuring RRI for an Remote Endpoint and a Route Recursion Route Example

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

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

Configuring RRI with Enhancements Added in Cisco IOS Release 12.3(14)T Examples

- Configuring RRI When Crypto ACLs Exist Example, page 11
- Configuring RRI with Route Tags Example, page 11
- Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop Example, page 12

Configuring RRI When Crypto ACLs Exist Example

The following example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
   match address 101
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

Configuring RRI with Route Tags Example

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

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1
Router# show ip eigrp topology
P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
     via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop Example

Note This option is applicable only to crypto maps.

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

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

The preceding example yields the following prior to Cisco IOS Release 12.3(14)T:

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

And this result occurs with RRI enhancements:

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

Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T Examples

- Configuring a RRI Distance Metric Under a Crypto Map Example, page 12
- Configuring RRI with Route Tags Example, page 13
- debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map Example, page 13
- Configuring a RRI Distance Metric for a VTI Example, page 14
- debug and show Command Output for a RRI Metric Configuration Having a VTI Example, page 14
- show crypto route Command Output Example, page 15

Configuring a RRI Distance Metric Under a Crypto Map Example

The following configuration shows a server and client configuration for which a RRI distance metric has been set under a crypto map:

Server

```
crypto dynamic-map mymap
 set security-association lifetime seconds 300
 set transform-set 3dessha
 set isakmp-profile profile1
 set reverse-route distance 20
 reverse-route
```

Client

```
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 mode client
 peer 10.0.0.119
 username XXX password XXX
 xauth userid mode local
```

Configuring RRI with Route Tags Example

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

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1
Router# show ip eigrp topology
P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map Example

The following are **debug** and **show** command output for a RRI distance metric configuration under a crypto map on a server:

```
Router# debug crypto ipsec
00:23:37: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.0.14 to network 0.0.0.0
C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 10.0.0.14
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

Configuring a RRI Distance Metric for a VTI Example

The following configuration shows a server and client configuration in which a RRI distance metric has been set for a VTI:

Server Configuration

```
crypto isakmp profile profile1
 keyring mykeyring
 match identity group cisco
 client authentication list authenlist
 isakmp authorization list autholist
 client configuration address respond
 virtual-template 1
crypto ipsec profile vi
 set transform-set 3dessha
 set reverse-route distance 20
 set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
 ip unnumbered
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

Client Configuration

```
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 mode client
 peer 10.0.0.119
 username XXX password XXX
 virtual-interface 1
```

debug and show Command Output for a RRI Metric Configuration Having a VTI Example

The following are **debug** and **show** command output for a RRI metric configuration for a VTI on a server:

```
Router# debug crypto ipsec
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: Crypto mapdb : proxy_match
        src addr     : 0.0.0.0
        dst addr     : 192.168.6.1
        protocol     : 0
        src port     : 0
        dst port     : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same pro
xies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtua
l-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0
00:47:56: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.110, sa_proto= 50,
    sa_spi= 0x19E1175C(434181980),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.14, sa_proto= 50,
    sa_spi= 0xADC90C5(182227141),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, chang
ed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
```

```
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outb
ound sa to SPI ADC90C5
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.0.14 to network 0.0.0.0
C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

show crypto route Command Output Example

The following output example displays routes, in one table, that are created through IPsec via RRI or Easy VPN VTIs:

```
Router# show crypto route
VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs
Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Security commands	*Cisco IOS Security Command Reference*
Other Cisco IOS commands	Cisco IOS Master Command List

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Reverse Route Injection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Reverse Route Injection

Feature Name	Releases	Feature Information
Reverse Route Injection	12.1(9)E 12.2(8)T 12.2(8)YE 15.1(3)S	Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted. The following commands were introduced or modified by this feature: **reverse-route**.
Reverse Route Remote Peer Options	12.2(13)T 12.2(14)S	An enhancement was added to RRI to allow you to specify an interface or address as the explicit next hop to the remote VPN device. This functionality allows the overriding of a default route to properly direct outgoing encrypted packets.

Feature Name	Releases	Feature Information
Reverse Route Injection Enhancements	12.3(14)T 12.2(33)SRA 12.2(33)SXH	The following enhancements were added to the Reverse Route Injection feature: • The default behavior of static crypto maps will be the same as that of dynamic crypto maps unless the **reverse-route** command and **static** keyword are used. • A route tag value was added for any routes that are created using RRI. • RRI can be configured on the same crypto map that is applied to multiple router interfaces. • RRI configured with the **reverse-route remote-peer** {*ip-address*} command, keyword, and argument will create one route instead of two. The following command was modified by these feature enhancements: **reverse-route**.
Gateway Option	12.4(15)T 15.1(3)S	This option allows you to configure unique next hops or gateways for remote tunnel endpoints.
RRI Distance Metric	12.4(15)T 15.1(3)S	This enhancement allows you to define a metric distance for each static route. The following commands were introduced or modified by this feature: **reverse-route**, **set reverse-route**.
show crypto route Command	12.4(15)T 15.1(3)S	This command displays routes that are created through IPsec via RRI or Easy VPN VTIs.
Support for RRI on IPsec Profiles	12.4(15)T 15.1(3)S	This feature provides support for relevant RRI options on IPsec profiles that are predominantly used by VTIs.

Feature Name	Releases	Feature Information
Tag Option Configuration Changes	12.4(15)T 15.1(3)S	The tag option is now supported with IPsec profiles under the **set reverse-route tag** command.

IPsec VPN High Availability Enhancements

The IPsec VPN High Availability Enhancements feature consists of two features--Reverse Route Injection (RRI) and Hot Standby Router Protocol and IPsec (HSRP). When used together, these two features work together to provide users with a simplified network design for VPNs and reduced configuration complexity on remote peers with respect to defining gateway lists.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPsec VPN High Availability Enhancements

Reverse Route Injection

Reverse Route Injection (RRI) simplifies network design for Virtual Private Networks (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

RRI provides the following benefits:

- Enables routing of IPsec traffic to a specific VPN headend device in environments that have multiple (redundant) VPN headend devices.
- Ensures predictable failover time of remote sessions between headend devices when using IKE keepalives, especially in environments in which remote device route flapping is common (not taking

into consideration the effects of route convergence, which may vary depending on the routing protocol used and the size of the network).

- Eliminates the need for the administration of static routes on upstream devices, as routes are dynamically learned by these devices.

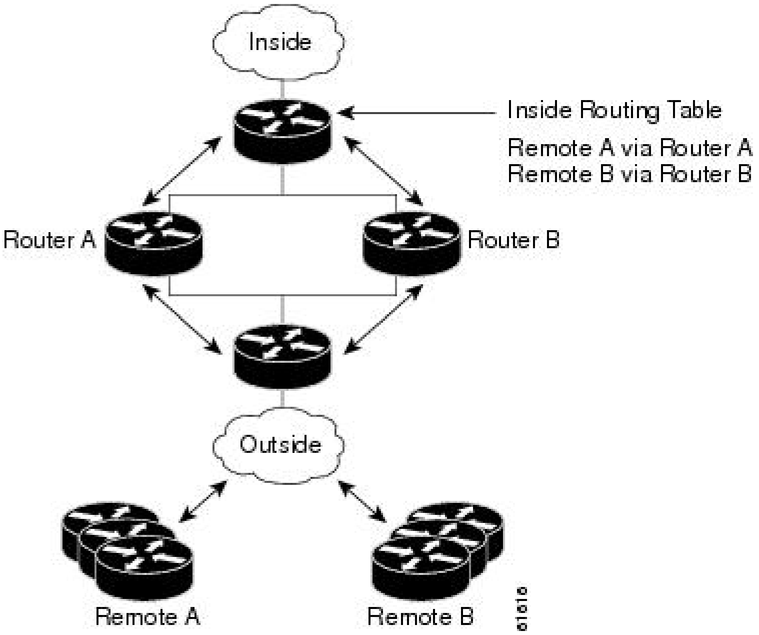
In the dynamic case, as remote peers establish IPsec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access list rule. When RRI is used on a static crypto map with an access control list (ACL), routes will always exist, even without the negotiation of IPsec SAs.

Note Use of any keyword in ACLs with RRI is not supported.

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPsec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPsec policy mismatches and possible packet loss.

The figure below shows a RRI configuration functionality topology. Remote A is being serviced by Router A and Remote B connected to Router B, providing load balancing across VPN gateways at the central site. RRI on the central site devices ensures that the other router on the inside of the network can automatically make the correct forwarding decision. RRI also eliminates the need to administer static routes on the inside router.

Figure 1 Topology Showing Reverse Route Injection Configuration Functionality



Hot Standby Router Protocol and IPsec

Hot Standby Router Protocol (HSRP) provides high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP) and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure cannot communicate with the network.

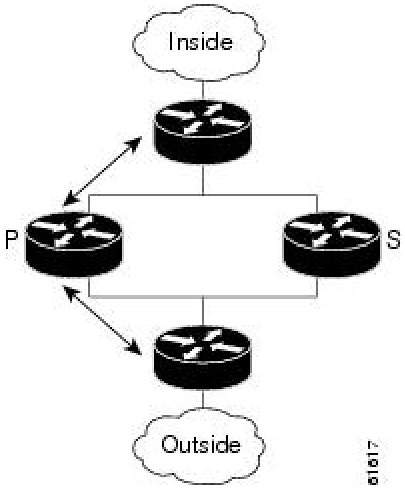
HSRP is configurable on LAN interfaces using standby command-line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPsec identity or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN gateways.

Failover can be applied to VPN routers through the use of HSRP. Remote VPN gateways connect to the local VPN router through the standby address that belongs to the active device in the HSRP group. This functionality reduces configuration complexity on remote peers with respect to defining gateway lists, because only the HSRP standby address needs to be defined.

The figure below shows the enhanced HSRP functionality topology. Traffic is serviced by the active Router P, the active device in the standby group. In the event of failover, traffic is diverted to Router S, the original standby device. Router S assumes the role of the new active router and takes ownership of the standby IP address.

Figure 2 *Topology Showing Hot Standby Router Protocol Functionality*



Note In case of a failover, HSRP does not facilitate IPsec state information transference between VPN routers. This means that without this state transference, SAs to remotes will be deleted, requiring Internet Key Exchange (IKE) and IPsec SAs to be reestablished. To make IPsec failover more efficient, it is recommended that IKE keepalives be enabled on all routers.

How to Configure IPsec VPN High Availability Enhancements

This section contains the following procedures:

- Configuring Reverse Route Injection on a Dynamic Crypto Map, page 24
- Configuring Reverse Route Injection on a Static Crypto Map, page 25

- Configuring HSRP with IPsec, page 26
- Verifying VPN IPsec Crypto Configuration, page 28

Configuring Reverse Route Injection on a Dynamic Crypto Map

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic map name, but each with a different dynamic sequence number. Each member of the set may be configured for RRI.

To create a dynamic crypto map entry and enable RRI, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *map-name seq-num*
4. **set transform-set**
5. **reverse-route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *map-name seq-num* **Example:** `Router (config)#` **crypto dynamic-map mymap 2**	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 4	**set transform-set** **Example:** `Router (config-crypto-m)#` **set transform-set**	Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first). This entry is the only configuration statement required in dynamic crypto map entries.

	Command or Action	Purpose
Step 5	**reverse-route** **Example:** `Router (config-crypto-m)#` **reverse-route**	Creates source proxy information.

Configuring Reverse Route Injection on a Static Crypto Map

Before configuring RRI on a static crypto map, note that:

- Routes are not created based on access list 102, as reverse-route is not enabled on mymap 2. RRI is not enabled by default and is not displayed in the router configuration.
- Enable a routing protocol to distribute the VPN routes to upstream devices.
- If Cisco Express Forwarding (CEF) is run on a VPN router configured for RRI, adjacencies need to be formed for each RRI injected network through the next hop device. As the next hop is not explicitly defined in the routing table for these routes, proxy-ARP should be enabled on the next hop router, which allows the CEF adjacency to be formed using the layer two addresses of that device. In cases where there are many RRI injected routes, adjacency tables may become quite large, as an entry is created for each device from each of the subnets represented by the RRI route. This issue is to be resolved in a future release.

To add RRI to a static crypto map set, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set peer** *ip-address*
5. **reverse-route**
6. **match address**
7. **set transform-set**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* **ipsec-isakmp** **Example:** `Router (config)#` **crypto map mymap 3 ipsec-isakmp**	Adds a dynamic crypto map set to a static crypto map set and enters interface configuration mode.
Step 4	**set peer** *ip-address* **Example:** `Router (config-if)#` **set peer 209.165.200.248**	Specifies an IPsec peer IP address in a crypto map entry.
Step 5	**reverse-route** **Example:** `Router (config-if)#` **reverse-route**	Creates dynamically static routes based on crypto access control lists (ACLs).
Step 6	**match address** **Example:** `Router (config-if)#` **match address**	Specifies an extended access list for a crypto map entry.
Step 7	**set transform-set** **Example:** `Router (config-if)#` **set transform-set**	Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first).

Configuring HSRP with IPsec

When configuring HSRP with IPsec, the following conditions may apply:

- When HSRP is applied to a crypto map on an interface, the crypto map must be reapplied if the standby IP address or the standby name is changed on that interface.
- If HSRP is applied to a crypto map on an interface, and the user deletes the standby IP address or the standby name from that interface, the crypto tunnel endpoint is reinitialized to the actual IP address of that interface.

- If a user adds the standby IP address and the standby name to an interface with the requirement IPsec failover, the crypto map must be reapplied with the appropriate redundancy information.
- Standby priorities should be equal on active and standby routers. If they are not, the higher priority router takes over as the active router. If the old active router comes back up and immediately assumes the active role before having time to report itself standby and sync, connections will be dropped.
- The IP addresses on the HSRP-tracked interfaces on the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state-based IP address. If an addressing scheme exists so that the public IP address of router A is lower than the public IP address of router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could exist, which will break connectivity.

Note To configure HSRP without IPsec, refer to the “Configuring IP Services“ module in the *Cisco IOS IP Application Services Configuration Guide*

To apply a crypto map set to an interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **standby name** *group-name*
5. **standby ip** *ip-address*
6. **crypto map** *map-name* **redundancy** [*standby-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Router (config)#` **interface GigabitEthernet 0/0**	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**standby name** *group-name* **Example:** `Router (config-if)#` **standby name mygroup**	Specifies the standby group name (required).
Step 5	**standby ip** *ip-address* **Example:** `Router (config-if)#` **standby ip 209.165.200.249**	Specifies the IP address of the standby groups (required for one device in the group).
Step 6	**crypto map** *map-name* **redundancy** [*standby-name*] **Example:** `Router (config-if)#` **crypto map mymap redundancy**	Specifies IP redundancy address as the tunnel endpoint for IPsec.

Verifying VPN IPsec Crypto Configuration

To verify your VPN IPsec crypto configuration, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **show crypto ipsec transform-set**
3. **show crypto map** [**interface** *interface* | **tag** *map-name*]
4. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]
5. **show crypto dynamic-map** [**tag** *map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show crypto ipsec transform-set** **Example:** `Router#` **show crypto ipsec transform-set**	Displays your transform set configuration.
Step 3	**show crypto map** [**interface** *interface* | **tag** *map-name*] **Example:** `Router#` **show crypto map tag mycryptomap**	Displays your crypto map configuration.
Step 4	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**] **Example:** `Router#` **show crypto ipsec sa address detail**	Displays information about IPsec SAs.
Step 5	**show crypto dynamic-map** [**tag** *map-name*] **Example:** `Router#` **show crypto dynamic-map tag mymap**	Displays information about dynamic crypto maps.

Configuration Examples for IPsec VPN High Availability Enhancements

Example Reverse Route Injection on a Dynamic Crypto Map

In the following example, using the **reverse-route** command in the definition of the dynamic crypto map template ensures that routes are created for any remote proxies (subnets or hosts), protected by the connecting remote IPsec peers.

```
crypto dynamic mydynmap 1
    set transform-set esp-3des-sha
    reverse-route
```

This template is then associated with a “parent” crypto map statement and then applied to an interface.

```
crypto map mymap 3 ipsec-isakmp dynamic mydynmap
```

```
interface FastEthernet 0/0
crypto map mymap
```

Example Reverse Route Injection on a Static Crypto Map

RRI is a good solution for topologies that require encrypted traffic to be diverted to a VPN router and all other traffic to a different router. In these scenarios, RRI eliminates the need to manually define static routes on devices.

RRI is not required if a single VPN router is used, and all traffic passes through the VPN router during its path in to and out of the network.

If the user chooses to manually define static routes on the VPN router for remote proxies, and has these routes permanently installed in the routing table, RRI should not be enabled on the crypto map instance that covers the same remote proxies. In this case, there is no possibility of user-defined static routes being removed by RRI.

Routing convergence can affect the success of a failover based on the routing protocol used to advertise routes (link state versus periodic update). It is recommended that a link state routing protocol such as OSPF be used to help speed convergence time by ensuring that routing updates are sent as soon as a change in routing state is detected.

In the following example, RRI is enabled for mymap 1, but not for mymap 2. Upon the application of the crypto map to the interface, a route is created based on access-list 101 analogous to the following:

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route
   set transform-set esp-3des-sha
   match address 101
crypto map mymap 2 ipsec-isakmp
   set peer 10.1.1.1
   set transform-set esp-3des-sha
   match address 102
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
interface FastEthernet 0/0
    crypto map mymap
```

Example HSRP and IPsec

The following example shows how all remote VPN gateways connect to the router via 192.168.0.3. The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of *mymap* and at the same time ensures that HSRP failover is facilitated between an active and standby device belonging to the same standby group, group1.

Note that RRI also provides the ability for only the active device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If there is a failover, routes are deleted on the formerly active device and created on the newly active device.

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

The standby name needs to be configured on all devices in the standby group, and the standby address needs to configured on at least one member of the group. If the standby name is removed from the router, the IPsec SAs will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the redundancy option) will have to be reapplied to the interface.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring HSRP without IPsec	“ Configuring IP Services “ module in the *Cisco IOS IP Application Services Configuration Guide*
Configuring stateful failover for IP security (IPsec)	“ Stateful Failover for IPsec ” module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
Removing and installing a Service Adapter VPN Acceleration Module 2 (SA-VAM2)	*VAM2 Installation and Configuration Guide*
Initial hardware installation and basic configuration procedures for the Cisco 7100 Series VPN routers	*Cisco 7100 Series VPN Router Installation and Configuration Guide*
Replacing, installing, configuring, or maintaining the the Cisco 7200 VXR Series router hardware	*Cisco 7200 VXR Installation and Configuration Guide*
Initial hardware installation and basic configuration procedures for the Cisco 7401ASR router	*Cisco 7401ASR Installation and Configuration Guide*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPsec VPN High Availability Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for IPsec VPN High Availability Enhancements

Feature Name	Releases	Feature Information
IPsec VPN High Availability Enhancements	12.1(9)E 12.2(8)T 12.2(11)T 12.2(9)YE 12.2(14)S Cisco IOS XE 3.1.0SG	The IPsec VPN High Availability Enhancements feature consists of two features--Reverse Route Injection (RRI) and Hot Standby Router Protocol and IPsec (HSRP). When used together, these two features work together to provide users with a simplified network design for VPNs and reduced configuration complexity on remote peers with respect to defining gateway lists. In 12.2(11)T, this feature was introduced on the Cisco AS5300 and Cisco AS5800 platforms. The following sections provide information about this feature: The following commands were introduced or modified: **crypto map** (interface IPsec), **reverse-route**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Stateful Failover for IPsec

Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent to the user and does not require adjustment or reconfiguration of any remote peer.

Stateful failover for IPsec is designed to work in conjunction with stateful switchover (SSO) and Hot Standby Routing Protocol (HSRP). HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. That is, HSRP monitors both the inside and outside interfaces so that if either interface goes down, the whole router is deemed to be down and ownership of Internet Key Exchange (IKE) and IPsec security associations (SAs) is passed to the standby router (which transitions to the HSRP active state). SSO allows the active and standby routers to share IKE and IPsec state information so that each router has enough information to become the active router at any time. To configure stateful failover for IPsec, a network administrator should enable HSRP, assign a virtual IP address, and enable the SSO protocol.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Stateful Failover for IPsec

Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices

This document assumes that you have a complete IKE and IPsec configuration. (This document describes only how to add stateful failover to a working IPsec configuration.)

The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on the crypto map sets, all AAA configurations used for crypto, client configuration groups, ip local pools used for crypto, and ISAKMP profiles.

Note None of the configuration information between the active and standby device is automatically transferred; the user is responsible for ensuring that the crypto configurations match on both devices. If the crypto configurations on both devices do not match, failover from the active device to the standby device will not be successful.

Device Requirements

- Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.
- This feature is currently supported only on a limited number of platforms. To check the latest platform support, go to Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp .

Restrictions for Stateful Failover for IPsec

When configuring redundancy for a virtual private network (VPN), the following restrictions exist:

- Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via hub or switch.
- The Cisco Integrated Services Routers (ISRs) and the VPN modules that support stateful failover for IPsec are as follows:
    - The AIM-VPN/BPII-PLUS and AIM-VPN/SSL-1 hardware encryption modules are supported in a Cisco 1841 router.
    - The AIM-VPN/EPII-Plus and AIM-VPN/SSL-2 hardware encryption modules are supported in Cisco 2801, 2811, 2821 and 2851 routers.
    - The AIM-VPN/EPII+ and AIM-VPN/SSL-3 hardware encryption modules are supported in a Cisco 3825 router.
    - The AIM-VPN/HPII+ and AIM-VPN/SSL3 hardware encryption modules are supported in a Cisco 3845 router.
    - The VPN Acceleration Module (VAM) and VAM2 hardware encryption modules are supported in a Cisco 7200 series router.
- Only “box-to-box” failover is supported; that is, intrachassis failover is currently not supported.
- WAN interfaces between the active (primary) router and the standby (secondary) router are not supported. (HSRP requires inside interfaces and outside interfaces to be connected via LANs.)
- Load balancing is not supported; that is, no more than one device in a redundancy group can be active at any given time.

- Stateful failover of IPsec with Layer 2 Tunneling Protocol (L2TP) i s not supported.
- Public key infrastructure (PKI) is not supported when used with stateful failover. (Only preshared keys for IKE are supported.)
- IKE keepalives are not supported. (Enabling this functionality will cause the connection to be torn down after the standby router assumes ownership control.) However, dead peer detection (DPD) and periodic DPD are supported.
- IPsec idle timers are not supported when used with stateful failover.
- A stateful failover crypto map applied to an interface in a virtual route forwarding (VRF) instance is not supported. However, VRF-aware IPsec features are supported when a stateful failover crypto map is applied to an interface in the global VRF.
- Stateful failover is not compatible or interoperable with the State Synchronization Protocol (SSP) version of stateful failover (which is available in Cisco IOS Release 12.2YX1 and Cisco IOS Release 12.2SU).

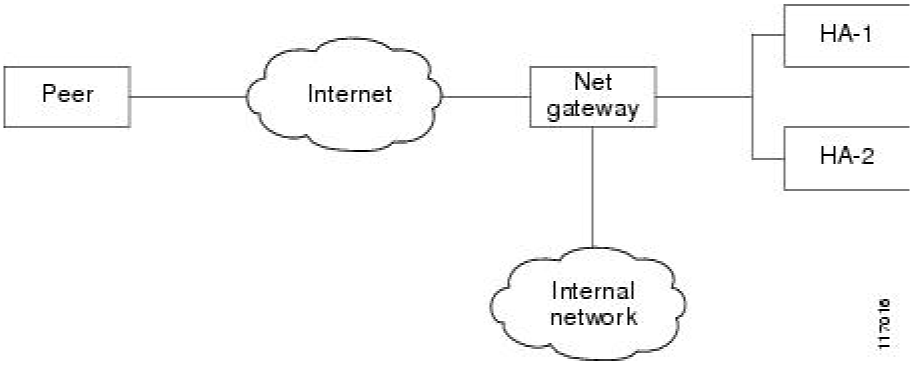
Information About Stateful Failover for IPsec

Supported Deployment Scenarios Stateful Failover for IPsec

It is recommended that you implement IPsec stateful failover in one of the following recommended deployment scenarios--a single interface scenario or a dual interface scenario.

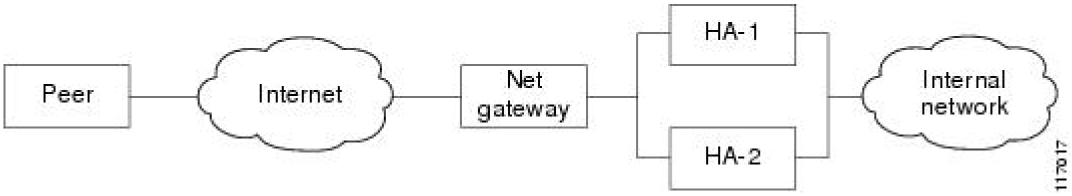
In a single interface scenario, the VPN gateways use one LAN connection for both encrypted traffic arriving from remote peers and decrypted traffic flowing to inside hosts (see the figure below). The single interface design allows customers to save money on router ports and subnets. This design is typically used if all traffic flowing in and out of the organization does not traverse the VPN routers.

Figure 3 *Single Interface Network Topology*



In a dual interface scenario, a VPN gateway has more than one interface, enabling traffic to flow in and out of the router via separate interfaces (see the figure below). This scenario is typically used if traffic flowing in and out of a site must traverse the routers, so the VPN routers will provide the default route out of the network.

Figure 4 Dual Interface Network Topology



The table below lists the functionality available in both a single interface scenario and a dual interfaces scenario.

Table 3 IPsec StateFul Failover: Single and Dual Interface Functionality Overview

Single Interface	Dual Interface
Route Injection	
Routes must be injected to provide the devices that are behind the VPN gateways with a next hop for traffic that requires encryption. Stateful failover for IPsec typically requires routes to be injected for this network topology.	If the VPN gateways are not the logical next hop for devices inside the network, the routes must be created and injected into the routing process. Thus, traffic that is returning from inside the network can be sent back to the VPN routers for IPsec services before it is sent out. A virtual IP (VIP) address cannot be used as the advertiser of routing updates, so flows must be synchronized via the injected routes. If the VPN gateways are the next hop (default route) for all devices inside the network, the VIP address that is used on the inside interfaces can be used as the next hop. Thus, injection of the VPN routes is not required. However, static routes on inside hosts must be used to direct the routes to the next hop VIP address.
HSRP Configuration	
The role of HSRP is simplified in a single interface design because if the only interface is disabled, the entire device is deemed unavailable. This functionality helps to avoid some of the routing considerations to be discussed in the next scenario.	Because each interface pair functions independently, you should configure HSRP so that multiple pairs of interfaces can be tracked. (That is, HSRP should not be configured on only one pair of interfaces or on both pairs of interfaces without each pair mutually tracking each other.) Mutual tracking means that if the outside interface does fail, the inside interface on the same router will also be deemed down, allowing for complete router failover to the secondary router.
Secure State Information	

Single Interface	Dual Interface
If secured-state information is passed between routers, the information is passed over the same interface as all other traffic.	The router has a separate inside and outside interface; thus, the inside interface can be used as a more secure channel for the exchange of state information.
Firewall Configuration	
The VPN gateways can sit in front of the firewall or behind the firewall.	VPN gateways may sit behind or in front of a firewall, a firewall can be installed in parallel to the VPN gateways.

IPsec Stateful Failover for Remote Access Connections

The main difference between a remote access and a LAN-to-LAN connection is the use of Xauth and mode-config. IKE Xauth is often used to authenticate the user. IKE mode-config is often used to push security policy from the hub (concentrator) router to the user’s IPsec implementation. Mode-config is also typically used to assign an internal company network IP address to a user.

In addition to the differences between a remote access configuration and a LAN-to-LAN configuration, you should note the following remote-access-server-specific functions:

- Assigned IP address--The IP address can be assigned to the client via one of the following options:
    - Local IP pools. For local IP pools, the administrator must first configure identical local IP address pools on each router in the high availability (HA) pair (via the **ip local pool** *client-address-pool*command). This pool name can be applied in one of two places--in a group policy via the **crypto isakmp client configuration group** *group-name* (and the submode command **pool** *pool-name*) or in a client configuration via the **crypto isakmp client configuration address-pool local** *local-pool* command.
    - RADIUS-assigned address. If you are using RADIUS authentication and the RADIUS server returns the Framed-IP-Address attribute, the concentrator will always assign that address to the client. It is recommended that you refer to your RADIUS server vendor’s documentation, especially for vendors that allow you to configure address pools on the RADIUS server. Typically those servers require crypto accounting to work properly.

To enable accounting on the HA pair, you should issue the following commands on both Active and Standby devices: **aaa accounting network radius-accounting start-stop group radius** then apply radius-accounting either to the crypto isakmp profile or the crypto map set.

- RADIUS NAS-IP address--The HA pair should appear as a single device to the RADIUS server. Thus, both HA routers must communicate with the RADIUS server using the same IP address. However, when communicating with the RADIUS server, the router must use a physical IP address, not a virtual IP (VIP) address as the NAS-IP address of the router. To configure the RADIUS NAS-IP address for the HA pair, you must configure the same loopback address in the HA pair via **interface loopback ip address**command; thereafter, you must issue the **ip radius source-interface loopback** command in the HA pair. Finally, add the new loopback IP address to the RADIUS servers configuration so the RADIUS server can process requests from the HA pair.

For additional information on how to configure IPsec stateful failover for a remote access connection, see the section “ Configuring IPSec Stateful Failover for an Easy VPN Server: Example ” in this document.

Dead Peer Detection with IPsec High Availability

To configure Dead Peer Detection (DPD) with IPsec High Availability (HA), it is recommended that you use a value other than the default (2 seconds). A keepalive time of 10 seconds with 5 retries seems to work well with HA because of the time it takes for the router to get into active mode.

To configure DPD with IPsec HA, use the **crypto isakmp keepalive** command.

How to Use Stateful Failover for IPsec

This section contains the following procedures:

- Enabling HSRP: IP Redundancy and a Virtual IP Address, page 6 (required)
- Enabling SSO, page 9 (required)
- Configuring Reverse Route Injection on a Crypto Map, page 13 (required)
- Enabling Stateful Failover for IKE and IPSec, page 15 (required)
- Protecting SSO Traffic, page 18 (optional)
- Managing and Verifying High Availability Information, page 20 (optional)

Enabling HSRP IP Redundancy and a Virtual IP Address

HSRP provides two services--IP redundancy and a VIP address. Each HSRP group may provide either or both of these services. IPsec stateful failover uses the IP redundancy services from only one HSRP standby group. It can use the VIP address from one or more HSRP groups. Use the following task to configure HSRP on the outside and inside interfaces of the router.

Note Perform this task on both routers (active and standby) and of both interfaces on each router.

Note You must perform at least one of the prerequisite steps for correct HSRP operation.

Note Each time an active device relinquishes control to become the standby device, the active device will reload. This functionality ensures that the state of the new standby device synchronizes correctly with the new active device.

If a switch connects the active and standby routers, you must perform one of the following steps to ensure that the correct settings are configured on that switch:

- Enable the **spanning-tree portfast** command on every switch port that connects to a HSRP-enabled router interface.
- Disable the Spanning Tree Protocol (STP) on the switch only if your switch does not connect to other switches. Disabling spanning tree in a multi-switch environment may cause network instability.
- Enable the **standby delay minimum** [*min-delay*] **reload** [*reload-delay*] command if you do not have access to the switch. The *reload-delay* argument should be set to a value of at least 120 seconds. This command must be applied to all HSRP interfaces on both routers.

For more information on HSRP instability, see the "Avoiding HSRP Instability in a Switching Environment with Various Router Platforms" technical note.

Note

- Both the inside (private) interface and the outside (public) interface must belong to separate HSRP groups, but the HSRP group number can be the same.
- The state of the inside interface and the outside interface must be the same--both interfaces must be in the active state or standby state; otherwise, the packets will not have a route out of the private network.
- Standby priorities should be equal on both active and standby routers. If the priorities are not equal, the higher priority router will unnecessarily take over as the active router, negatively affecting uptime.
- The IP addresses on the HSRP-tracked interfaces of the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state on the basis of the IP address. If an addressing scheme exists so that the public IP address of Router A is lower than the public IP address of Router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could exist which will break connectivity.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface *typenumber*
4. standby standby-group-number name standby-group-name
5. standby standby-group-number ip ip-address
6. standby standby-group-number track interface-name
7. **standby** [*group-number*] **preempt**
8. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
9. **standby delay minimum** [*min-delay*] **reload** [*reload-delay*]
10. Repeat.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface *typenumber* **Example:** `Router(config)# interface Ethernet 0/0`	Configures an interface type for the router and enters interface configuration mode.
Step 4	standby standby-group-number name standby-group-name **Example:** `Router(config-if)# standby 1 name HA-out`	Assigns a user-defined group name to the HSRP redundancy group. **Note** The *standby-group-number* argument should be the same for both routers that are on directly connected interfaces. However, the *standby-group-name* argument should be different between two (or more) groups on the same router. The *standby-group-number* argument can be the same on the other pair of interfaces as well.
Step 5	standby standby-group-number ip ip-address **Example:** `Router(config-if)# standby 1 ip 209.165.201.1`	Assigns an IP address that is to be “shared” among the members of the HSRP group and owned by the primary IP address. **Note** The virtual IP address must be configured identically on both routers (active and standby) that are on directly connected interfaces.
Step 6	standby standby-group-number track interface-name **Example:** `Router(config-if)# standby 1 track Ethernet1/0`	Configures HSRP to monitor the second interface so that if either of the two interfaces goes down, HSRP causes failover to the standby device. **Note** Although this command is not required, it is recommended for dual interface configurations.

	Command or Action	Purpose
Step 7	**standby** [*group-number*] **preempt** **Example:** `Router(config-if)# standby 1 preempt`	Enables the active device to relinquish control because of an interface tracking event.
Step 8	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* **Example:** `Router(config-if)# standby 1 timers 1 5`	(Optional) Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down. • *holdtime* --Amount of time the routers take to detect types of failure. A larger hold time means that failure detection will take longer. For the best stability, it is recommended that you set the hold time between 5 and 10 times the hello interval time; otherwise, a failover could falsely occur when no actual failure has happened.
Step 9	**standby delay minimum** [*min-delay*] **reload** [*reload-delay*] **Example:** `Router(config-if)# standby delay minimum reload 120`	Configures the delay period before the initialization of HSRP groups. **Note** It is suggested that you enter 120 as the value for the *reload-delay* argument and leave the *min-delay*argument at the preconfigured default value.
Step 10	Repeat.	Repeat this task on both routers (active and standby) and on both interfaces of each router.

- Troubleshooting Tips, page 43
- Examples, page 43
- What to Do Next, page 44

Troubleshooting Tips

To help troubleshoot possible HSRP-related configuration problems, issue any of the following HSRP-related debug commands--**debug standby errors**, **debug standby events**, and **debug standby packets** [**terse**].

Examples

The following example shows how to configure HSRP on a router:

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
```

What to Do Next

After you have successfully configured HSRP on both the inside and outside interfaces, you should enable SSO as described the in the "Enabling SSO” section.

Enabling SSO

Use this task to enable SSO, which is used to transfer IKE and IPsec state information between two routers.

SSO Interacting with IPsec and IKE

SSO is a method of providing redundancy and synchronization for many Cisco IOS applications and features. SSO is necessary for IPsec and IKE to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

- You should configure HSRP before enabling SSO.
- To avoid losing SCTP communication between peers, be sure to include the following commands to the local address section of the SCTP section of the IPC configuration:
  - **retransmit-timeout** *retran-min* [*msec*] *retra-max* [*msec*]
  - **path-retransmit** *max-path-retries*
  - **assoc-retransmit** *retries*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy inter-device**
4. **scheme standby** *standby-group-name*
5. **exit**
6. **ipc zone default**
7. **association 1**
8. **protocol sctp**
9. **local-port** *local-port-number*
10. **local-ip** *device-real-ip-address* [*device-real-ip-address2*
11. **retransmit-timeout** *retran-min* [*msec*] *retra-max* [*msec*]
12. **path-retransmit** *max-path-retries*
13. **assoc-** retransmit retries
14. **exit**
15. **remote-port** *remote-port-number*
16. **remote-ip** *peer-real-ip-address* [*peer-real-ip-address2*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy inter-device** **Example:** `Router(config)# redundancy inter-device`	Configures redundancy and enters inter-device configuration mode. To exit inter-device configuration mode, use the **exit** command. To remove all inter-device configuration, use the **no** form of the command.
Step 4	**scheme standby** *standby-group-name* **Example:** `Router(config-red-interdevice)# scheme standby HA-out`	Defines the redundancy scheme that is to be used. Currently, “standby” is the only supported scheme. • *standby-group-name* --Must match the standby name specified in the **standby name** interface configuration command. Also, the standby name should be the same on both routers. **Note** Only the active or standby state of the standby group is used for SSO. The VIP address of the standby group is not required or used by SSO. Also, the standby group does not have to be part of any crypto map configuration.
Step 5	**exit** **Example:** `Router(config-red-interdevice)# exit`	Exits inter-device configuration mode.
Step 6	**ipc zone default** **Example:** `Router(config)# ipc zone default`	Configures the inter-device communication protocol, Inter-Process Communication (IPC), and enters IPC zone configuration mode. Use this command to initiate the communication link between the active router and standby router.

	Command or Action	Purpose
Step 7	**association 1** **Example:** `Router(config-ipczone)# association 1`	Configures an association between the two devices and enters IPC association configuration mode.
Step 8	**protocol sctp** **Example:** `Router(config-ipczone-assoc)# protocol sctp`	Configures Stream Control Transmission Protocol (SCTP) as the transport protocol and enters SCTP protocol configuration mode.
Step 9	**local-port** *local-port-number* **Example:** `Router(config-ipc-protocol-sctp)# local-port 5000`	Defines the local SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport - SCTP local configuration mode. • *local-port-number* --There is not a default value. This argument must be configured for the local port to enable inter-device redundancy. Valid port values: 1 to 65535. The local port number should be the same as the remote port number on the peer router.
Step 10	**local-ip** *device-real-ip-address* [*device-real-ip-address2* **Example:** `Router(config-ipc-local-sctp)# local-ip 10.0.0.1`	Defines at least one local IP address that is used to communicate with the redundant peer. The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global VRF. A virtual IP address cannot be used.
Step 11	**retransmit-timeout** *retran-min* [*msec*] *retra-max* [*msec*] **Example:** `Router(config-ipc-local-sctp)# retransmit-timeout 300 10000`	Configures the maximum amount of time, in milliseconds, that SCTP will wait before retransmitting data. • *retran-min* : 300 to 60000; default: 300 • *retran-max* : 300 to 60000; default: 600
Step 12	**path-retransmit** *max-path-retries* **Example:** `Router(config-ipc-local-sctp)# path-retransmit 10`	Configures the number of consecutive retransmissions SCTP will perform before failing a path within an association. • *max-path-retries* : 2 to 10; default: 4 retries

	Command or Action	Purpose

Step 13	**assoc-** retransmit retries
	Example:
	`Router(config-ipc-local-sctp)#`
	`assoc`
	`-retransmit 10`
		Configures the number of consecutive retransmissions SCTP will perform before failing an association.
		• *max-association-retries* : 2 to 10; default: 4 retries

Step 14	**exit** **Example:** `Router(config-ipc-local-sctp)# exit`	Exits IPC transport - SCTP local configuration mode.

Step 15	**remote-port** *remote-port-number*
	Example:
	`Router(config-ipc-protocol-sctp)#`
	`remote-port 5000`
		Defines the remote SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport - SCTP remote configuration mode.
		Note *remote-port-number* --There is not a default value. This argument must be configured for the remote port to enable inter-device redundancy. Valid port values: 1 to 65535. The remote port number should be the same as the local port number on the peer router.

Step 16	**remote-ip** *peer-real-ip-address* [*peer-real-ip-address2*
	Example:
	`Router(config-ipc-remote-sctp)#`
	`remote-ip 10.0.0.2`
		Defines at least one remote IP address of the redundant peer that is used to communicate with the local device.
		All remote IP addresses must refer to the same device.
		A virtual IP address cannot be used.

Troubleshooting Tips

To help troubleshoot possible SSO-related configuration problems, issue the **debug redundancy** command.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
 scheme standby HA-out
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 10
   remote-port 5000
    remote-ip 10.0.0.2
!
```

What to Do Next

After you have enabled SSO, you should configure reverse route injection (RRI) on a crypto map as shown in the following section.

Configuring Reverse Route Injection on a Crypto Map

You should configure RRI on all existing crypto maps that you want to use with stateful failover. RRI is used with stateful failover so routers on the inside network can learn about the correct path to the current active device. When failover occurs, the new active device injects the RRI routes into its IP routing table and sends out routing updates to its routing peers.

Use one of the following tasks to configure RRI on a dynamic or static crypto map.

- Configuring RRI on Dynamic Crypto Map, page 13
- Configuring RRI on a Static Crypto Map, page 14

- Configuring RRI on Dynamic Crypto Map, page 48
- Configuring RRI on a Static Crypto Map, page 49
- What to Do Next, page 50

Configuring RRI on Dynamic Crypto Map

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic map name but each with a different dynamic sequence number. Each member of the set may be configured for RRI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *map-name seq-num*
4. **reverse-route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *map-name seq-num* **Example:** `Router(config)# crypto dynamic-map mymap 10`	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 4	**reverse-route** **Example:** `Router(config-crypto-map)# reverse-route`	Enables RRI for a dynamic crypto map.

Configuring RRI on a Static Crypto Map

Static crypto map entries are grouped into sets. A set is a group of static crypto map entries all with the same static map name but each with a different sequence number. Each static crypto map in the map set can be configured for RRI. Use this task to configure RRI on a static crypto map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **reverse-route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* **ipsec-isakmp** **Example:** `Router(config)# crypto map to-peer-outside 10 ipsec-isakmp`	Enters crypto map configuration mode and creates or modifies a crypto map entry.
Step 4	**reverse-route** **Example:** `Router(config-crypto-map)# reverse-route`	Dynamically creates static routes based on crypto ACLs.

Examples

The following example shows how to configure RRI on the static crypto map “to-peer-outside”:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
 reverse-route
```

What to Do Next

After you have configured RRI, you can enable stateful failover for IPsec and IKE.

Enabling Stateful Failover for IKE and IPsec

Use the following tasks to configure stateful failover for IPsec, IKE, and tunnel protection:

- Enabling Stateful Failover for IKE, page 15
- Enabling Stateful Failover for IPSec, page 15
- Enabling Stateful Failover for Tunnel Protection, page 17

- Enabling Stateful Failover for IKE, page 51
- Enabling Stateful Failover for IPsec, page 51
- Enabling Stateful Failover for Tunnel Protection, page 52
- What to Do Next, page 54

Enabling Stateful Failover for IKE

There is no specific command-line interface (CLI) necessary to enable stateful failover for IKE. It is enabled for a particular VIP address when a stateful failover crypto map is applied to an interface.

Enabling Stateful Failover for IPsec

Use this task to enable stateful failover for IPsec. All IPsec state information is transferred from the active router to the standby router via the SSO redundancy channel that was specified in the task “ Enabling SSO .”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface *typenumber*
4. crypto map map-name [redundancy standby-group-name [stateful]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface *typenumber* **Example:** `Router(config)# interface Ethernet 0/0`	Defines an interface that has already been configured for redundancy and enters interface configuration mode.
Step 4	crypto map map-name [redundancy standby-group-name [stateful]] **Example:** `Router(config-if)# crypto map to-peer-outside redundancy HA-out stateful`	Binds the crypto map on the specified interface to the redundancy group. **Note** Although the standby group does not have to be the same group that was used when enabling SSO, it does have to be the same group that was used with the **standby ip** command on this interface. This crypto map will use the same VIP address for both IKE and IPsec to communicate with peers.

- Troubleshooting Tips, page 52
- Examples, page 52

Troubleshooting Tips

To help troubleshoot possible IPsec HA-related problems, issue the **debug crypto ipsec ha** [**detail**] [**update**] command.

Examples

The following example shows how to configure IPsec stateful failover on the crypto map “to-peer-outside”:

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

Enabling Stateful Failover for Tunnel Protection

Use an existing IPsec profile to configure stateful failover for tunnels using IPsec. (You do not configure the tunnel interface as you would with a crypto map configuration.)

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

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. crypto ipsec profile name
4. redundancy standby-group-name stateful
5. **exit**
6. **interface tunnel** *number*
7. **tunnel protection ipsec profile** *name*
8. **tunnel source** *virtual ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	crypto ipsec profile name **Example:** `Router(config)# crypto ipsec profile peer-profile`	Defines the IPsec parameters that are to be used for IPsec encryption between two routers and enters crypto map configuration mode.

Step 4	redundancy standby-group-name stateful
	Example:
	`Router(`
	`config-crypto-map`
	`)#`
	`redundancy HA-out stateful`
		Configures stateful failover for tunnels using IPsec.

Step 5	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode.
Step 6	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 5`	Configures a tunnel interface and enters interface configuration mode • *number* --Specifies the number of the interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 7	**tunnel protection ipsec profile** *name* **Example:** `Router(config-if)# tunnel protection ipsec profile catprofile`	Associates a tunnel interface with an IPsec profile. *name* --Specifies the name of the IPsec profile; this value must match the name specified in the **crypto ipsec profile name**command.

	Command or Action	Purpose
Step 8	**tunnel source** *virtual ip-address* **Example:** `Router(config-if)# tunnel source 10.1.1.1`	Sets source address for a tunnel interface. • *virtual-ip-address* -- Must be a VIP address. **Note** Do not use the interface name as the tunnel source.

- Examples, page 54

Examples

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

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

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

What to Do Next

After you have configured stateful failover, you can use the CLI to protect, verify, and manage your configurations. For more information on completing these tasks, see the sections “ Protecting SSO Traffic ” and “ Managing and Verifying High Availability Information .”

Protecting SSO Traffic

Use this task to secure a redundancy group via an IPsec profile. To configure SSO traffic protection, the active and standby devices must be directly connected to each other via Ethernet networks.

The crypto maps that are automatically generated when protecting SSO traffic are applied to each interface, which corresponds to an IP address that was specified via the **local-ip** command. Traffic that is destined for an IP address that was specified via the **remote-ip** command is forced out of the crypto-map-configured interface via an automatically created static host route.

Note If you are certain that the SSO traffic between the redundancy group runs on a physically secure interface, you do not have to configure SSO traffic protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. crypto isakmp key keystring address peer-address
4. crypto ipsec transform-set transform-set-name transform-set-list
5. crypto ipsec profile profile-name
6. **set transform-set** *transform-set-name*
7. **exit**
8. **redundancy inter-device**
9. security ipsec *profile-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	crypto isakmp key keystring address peer-address **Example:** `Router(config)# crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0`	Configures a preshared authentication key. • *peer-address* --The SCTP remote IP address.
Step 4	crypto ipsec transform-set transform-set-name transform-set-list **Example:** `Router(config)# crypto ipsec transform-set trans2 ah-md5-hmac esp-aes`	Configures a transform set that defines the packet format and cryptographic algorithms used for IPsec.
Step 5	crypto ipsec profile profile-name **Example:** `Router(config)# crypto ipsec profile sso-secure`	Defines an IPsec profile that describes how the traffic will be protected.

	Command or Action	Purpose
Step 6	**set transform-set** *transform-set-name* **Example:** `Router(config-crypto-map)# set transform-set trans2`	Specifies which transform sets can be used with the IPsec profile.
Step 7	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode.
Step 8	**redundancy inter-device** **Example:** `Router(config)# redundancy inter-device`	Configures redundancy and enters inter-device configuration mode.
Step 9	security ipsec *profile-name* **Example:** `Router(config-red-interdevice)# security ipsec sso-secure`	Applies the IPsec profile to the redundancy group communications, protecting all SSO traffic that is passed between the active and standby device.

Examples

The following example shows how to configure SSO traffic protection:

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-out
 security ipsec sso-secure
```

Managing and Verifying High Availability Information

Use any of the following optional tasks to secure and manage your high availability configurations:

- Managing Anti-Replay Intervals, page 21
- Managing and Verifying HA Configurations, page 22

- Managing Anti-Replay Intervals, page 57
- Managing and Verifying HA Configurations, page 57

- Examples, page 59

Managing Anti-Replay Intervals

Use this optional task to modify the interval in which an IP redundancy-enabled crypto map forwards anti-replay updates from the active router to the standby router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. crypto map map-name redundancy replay-interval inbound in-value outbound out-value

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	crypto map map-name redundancy replay-interval inbound in-value outbound out-value **Example:** `Router(config)# crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000`	Modifies the interval at which inbound and outbound replay counters are passed from an active device to a standby device. • **inbound** *in-value*-- Number of inbound packets that are processed before an anti-replay update is sent from the active router to the standby router. Default value: one update every 1,000 packets. • **outbound** *out-value*-- Number of outbound packets that are processed before an anti-replay update is sent from the active router to the standby router. Default value: one update every 100,000 packets.

Examples

The following example shows how to modify replay counter intervals between the active and standby devices on the crypto map “to-peer-outside”:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
```

Managing and Verifying HA Configurations

Use any of the steps within this optional task to display and verify the high availability configurations.

SUMMARY STEPS

1. **enable**
2. **show redundancy** [**states** | **inter-device**]
3. **show crypto isakmp sa** [**active** | **standby**]
4. **show crypto ipsec sa** [**active** | **standby**]
5. **show crypto session** [**active** | **standby**
6. **show crypto ha**
7. **clear crypto isakmp** [**active** | **standby**
8. **clear crypto sa** [**active** | **standby**
9. **clear crypto session** [**active** | **standby**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show redundancy** [**states** | **inter-device**] **Example:** `Router# show redundancy states`	Displays the current state of SSO on the configured device. After the two devices have negotiated with each other, one device should show an "ACTIVE" state and the other device should show a "STANDBY HOT" state.
Step 3	**show crypto isakmp sa** [**active** | **standby**] **Example:** `Router# show crypto isakmp sa active`	Displays IKE SAs present on the device. An "ACTIVE" or "STDBY" state is shown for each SA. • The **active** keyword displays only ACTIVE, HA-enabled SAs; The **standby** keyword displays only STDBY, HA-enabled SAs.
Step 4	**show crypto ipsec sa** [**active** | **standby**] **Example:** `Router# show crypto ipsec sa active`	Displays IPsec SAs present on the device. An "ACTIVE" or "STDBY" state is shown for each SA. • The **active** keyword displays only ACTIVE, HA-enabled SAs; The **standby** keyword displays only STDBY, HA-enabled SAs.

	Command or Action	Purpose
Step 5	**show crypto session** [**active** | **standby** **Example:** `Router# show crypto session active`	Displays crypto sessions that are currently present on the device. An “ACTIVE” or “STANDBY” state is shown as part of the state of each session, such as “UP-STANDBY.” Only HA-enabled SAs are shown.
Step 6	**show crypto ha** **Example:** `Router# show crypto ha`	Displays all virtual IP addresses that are currently in use by IPsec and IKE.
Step 7	**clear crypto isakmp** [**active** | **standby** **Example:** `Router# clear crypto isakmp active`	Clears IKE SAs. When this command is issued on the standby device, all standby IKE SAs are resynchronized from the active device. • The **active** keyword clears only IKE HA-enabled SAs in the active state; the **standby** keyword clears only IKE HA-enabled SAs in the standby state.
Step 8	**clear crypto sa** [**active** | **standby** **Example:** `Router# clear crypto sa active`	Clears IPsec SAs. When this command is issued on the standby device, all standby IPsec SAs are resynchronized from the active device. • The **active** keyword clears only IPsec HA-enabled SAs in the active state; the **standby** keyword clears only IPsec HA-enabled SAs in the standby state.
Step 9	**clear crypto session** [**active** | **standby** **Example:** `Router# clear crypto session active`	Clears both IKE and IPsec SAs. Any standby SAs will resynchronize from the active device after they are cleared on the standby. Only HA-enabled SAs are cleared from the device.

Examples

Verifying the Active Device:Examples

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
        Unit ID = 0
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 7
 client_notification_TMR = 30000 milliseconds
```

```
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0
Router# show crypto isakmp sa active
dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              5    0 ACTIVE
Router# show crypto ipsec sa active
interface:Ethernet0/0
    Crypto map tag:to-peer-outside, local addr 209.165.201.3
   protected vrf:(none)
   local  ident (addr/mask/prot/port):(192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):(172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps:3, #pkts encrypt:3, #pkts digest:3
    #pkts decaps:4, #pkts decrypt:4, #pkts verify:4
    #pkts compressed:0, #pkts decompressed:0
    #pkts not compressed:0, #pkts compr. failed:0
    #pkts not decompressed:0, #pkts decompress failed:0
    #send errors 0, #recv errors 0
     local crypto endpt.:209.165.201.3, remote crypto endpt.:209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi:0xD42904F0(3559458032)
     inbound esp sas:
      spi:0xD3E9ABD0(3555306448)
        transform:esp-3des ,
        in use settings ={Tunnel, }
        conn id:2006, flow_id:6, crypto map:to-peer-outside
        sa timing:remaining key lifetime (k/sec):(4586265/3542)
             HA last key lifetime sent(k):(4586267)
        ike_cookies:9263635C CA4B4E99 C14E908E 8EE2D79C
        IV size:8 bytes
        replay detection support:Y
        Status:ACTIVE
inbound ah sas:
      spi: 0xF3EE3620(4092474912)
        transform: ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: 6, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586265/3542)
             HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        replay detection support: Y
        Status: ACTIVE
     inbound pcp sas:
     outbound esp sas:
      spi: 0xD42904F0(3559458032)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: 9, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586266/3542)
             HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
      spi: 0x75251086(1965363334)
        transform: ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: 9, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586266/3542)
             HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        replay detection support: Y
        Status: ACTIVE
     outbound pcp sas:

Router# show crypto session active
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
```

```
Peer: 209.165.200.225 port 500
  IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
  IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
  IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
        Active SAs: 4, origin: crypto map


Router# show crypto ha
IKE VIP: 209.165.201.3
  stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254
```

Verifying the Standby Device: Examples

```
Router# show redundancy states
       my state = 8  -STANDBY HOT
     peer state = 13 -ACTIVE
           Mode = Duplex
        Unit ID = 0
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 7
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 7
           RF debug mask = 0x0

Router# show crypto isakmp sa standby
dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              5    0 STDBY
Router# show crypto ipsec sa standby
interface:Ethernet0/0
    Crypto map tag:to-peer-outside, local addr 209.165.201.3
   protected vrf:(none)
   local  ident (addr/mask/prot/port):(192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):(172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #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 not decompressed:0, #pkts decompress failed:0
    #send errors 0, #recv errors 0
     local crypto endpt.:209.165.201.3, remote crypto endpt.:209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi:0xD42904F0(3559458032)
     inbound esp sas:
      spi:0xD3E9ABD0(3555306448)
        transform:esp-3des ,
        in use settings ={Tunnel, }
        conn id:2012, flow_id:12, crypto map:to-peer-outside
        sa timing:remaining key lifetime (k/sec):(4441561/3486)
             HA last key lifetime sent(k):(4441561)
        ike_cookies:00000000 00000000 00000000 00000000
        IV size:8 bytes
        replay detection support:Y
        Status:STANDBY
     inbound ah sas:
      spi:0xF3EE3620(4092474912)
        transform:ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id:2012, flow_id:12, crypto map:to-peer-outside
        sa timing:remaining key lifetime (k/sec):(4441561/3486)
             HA last key lifetime sent(k):(4441561)
        ike_cookies:00000000 00000000 00000000 00000000
        replay detection support:Y
        Status:STANDBY
     inbound pcp sas:
     outbound esp sas:
      spi:0xD42904F0(3559458032)
        transform:esp-3des ,
        in use settings ={Tunnel, }
        conn id:2011, flow_id:11, crypto map:to-peer-outside
        sa timing:remaining key lifetime (k/sec):(4441561/3485)
             HA last key lifetime sent(k):(4441561)
        ike_cookies:00000000 00000000 00000000 00000000
        IV size:8 bytes
        replay detection support:Y
        Status:STANDBY
     outbound ah sas:
      spi:0x75251086(1965363334)
        transform:ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id:2011, flow_id:11, crypto map:to-peer-outside
        sa timing:remaining key lifetime (k/sec):(4441561/3485)
             HA last key lifetime sent(k):(4441561)
        ike_cookies:00000000 00000000 00000000 00000000
        replay detection support:Y
        Status:STANDBY
     outbound pcp sas:
```

```
Router# show crypto session standby
Crypto session current status
Interface:Ethernet0/0
Session status:UP-STANDBY
Peer:209.165.200.225 port 500
  IKE SA:local 209.165.201.3/500 remote 209.165.200.225/500 Active
  IPSEC FLOW:permit ip host 192.168.0.1 host 172.16.0.1
        Active SAs:4, origin:crypto map
Router# show crypto ha
IKE VIP:209.165.201.3
  stamp:74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IPSec VIP:209.165.201.3
IPSec VIP:255.255.255.253
IPSec VIP:255.255.255.254
ha-R2#
```

Verifying the Active and Standby SAs: Example

The following sample output shows SAs of both the active and standby devices:

```
Router# show crypto isakmp sa
dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              2    0 STDBY
10.0.0.1        10.0.0.2        QM_IDLE              1    0 ACTIVE
```

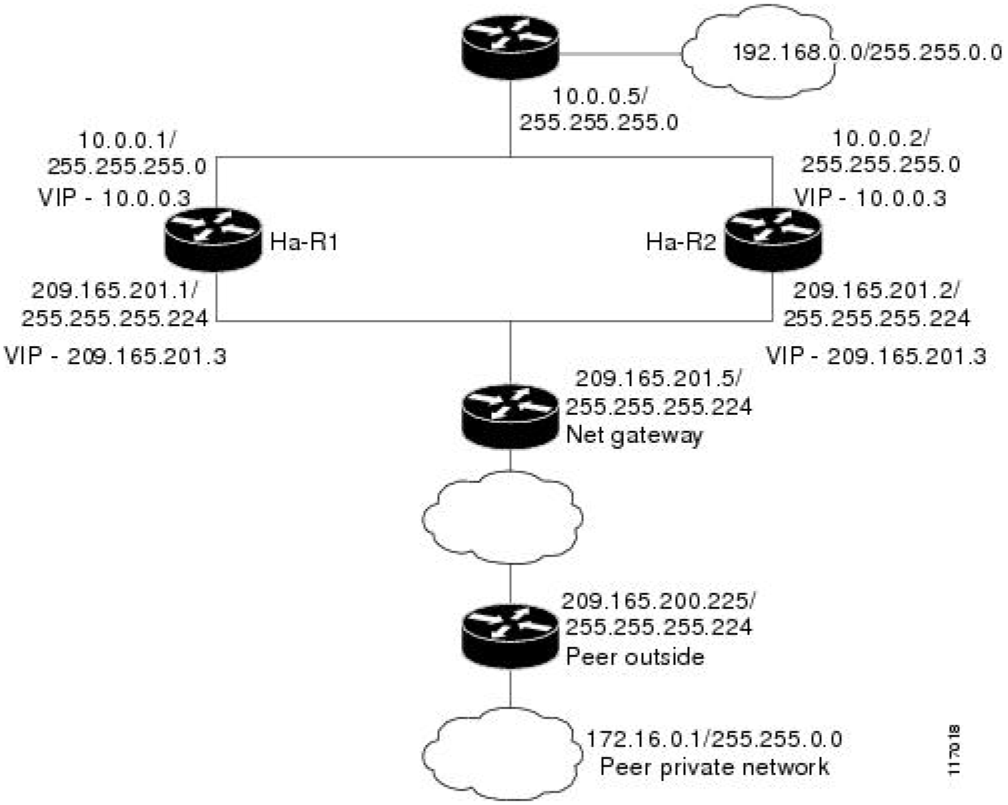
Configuration Examples for Stateful Failover

- Configuring IPsec Stateful Failover Example, page 63
- Configuring IPsec Stateful Failover for an Easy VPN Server Example, page 66

Configuring IPsec Stateful Failover Example

The figure below and the following sample outputs from the show running-config command illustrate how to configure stateful failover on two devices--Ha-R1 and Ha-R2.

Figure 5 IPsec Stateful Failover Sample Topology



Stateful Failover Configuration on Ha-R1

```
Ha-R1# show running-config
Building configuration...
Current configuration :2086 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ha-R1
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby HA-out
 security ipsec sso-secure
!
logging buffered 10000000 debugging
logging rate-limit console 10000
!
```

```
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
!
clock timezone PST 0
no aaa new-model
ip subnet-zero
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set trans1 ah-md5-hmac esp-3des
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
!
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
!
!
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to-peer-outside redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby delay reload 120
 standby 2 track Ethernet0/0
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
no ip http server
no ip http secure-server
!
!
!
ip access-list extended peer-outside
 permit ip host 192.168.0.1 host 172.16.0.1
!
!
```

```
control-plane
!
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

Stateful Failover Configuration on Ha-R2

```
Ha-R2# show running-config
Building configuration...
Current configuration :2100 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ha-R2
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby HA-out
 security ipsec sso-secure
!
logging buffered 10000000 debugging
logging rate-limit console 10000
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.2
   remote-port 5000
    remote-ip 10.0.0.1
!
clock timezone PST 0
no aaa new-model
ip subnet-zero
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 120
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set trans1 ah-md5-hmac esp-3des
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
!
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
```

```
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
!
!
!
interface Ethernet0/0
 ip address 209.165.201.2 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to-peer-outside redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.2 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby delay reload 120
 standby 2 track Ethernet0/0
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
no ip http server
no ip http secure-server
!
!
!
ip access-list extended peer-outside
 permit ip host 192.168.0.1 host 172.16.0.1
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
end
Ha-R2#
```

Configuring IPsec Stateful Failover for an Easy VPN Server Example

The following sample outputs from the **show running-config** command show how to configure stateful failover for a remote access connection via an Easy VPN server:

Stateful Failover for an Easy VPN Server Configuration on RAHA-R1

```
RAHA-R1# show running-config
Building configuration...
Current configuration :3829 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RAHA-R1
!
boot-start-marker
boot-end-marker
!
redundancy inter-device
 scheme standby HA-out
!
username remote_user password 0 letmein
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
!
aaa new-model
!
!
! Enter the following command if you are doing Xauth locally.
aaa authentication login local_xauth local
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa authentication login radius_xauth group radius
!
! Enter the following command if you are not doing Xauth
!aaa authentication login no_xauth none
!
! Enter the following command if you are doing local group authentication.
aaa authorization network local_auth local
!
! Enter the following command if you are doing group authentication remotely via RADIUS.
!aaa authorization network radius_auth group radius
!
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!
aaa accounting network radius_accounting start-stop group radius
aaa session-id common
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
!
! Enter the following command if you are doing group authentication locally.
crypto isakmp client configuration group unity
 key cisco123
 domain cisco.com
 pool client-address-pool
!
!
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map to-remote-client 10
```

```
 set transform-set trans1
 reverse-route remote-peer
!
! Use this map if you want to do local group authentication and Xauth.
crypto map to_peer_outside_local_xauth client authentication list local_xauth
crypto map to_peer_outside_local_xauth isakmp authorization list local_auth
crypto map to_peer_outside_local_xauth client configuration address respond
crypto map to_peer_outside_local_xauth 10 ipsec-isakmp dynamic to-remote-client
!
! Use this map if you want to use Radius for group authentication and Xauth.
!crypto map to_peer_outside_radius_xauth isakmp client authentication list radius_xauth
!crypto map to_peer_outside_radius_xauth client accounting list radius_accounting
!crypto map to_peer_outside_radius_xauth isakmp authorization list radius_auth
!crypto map to_peer_outside_radius_xauth isakmp client configuration address respond
!crypto map to_peer_outside_radius_xauth isakmp 10 ipsec-isakmp dynamic to-remote-client
!
! Use this map if you want to do local group authentication and no Xauth
!crypto map to_peer_outside_no_xauth isakmp authorization list local_auth
!crypto map to_peer_outside_no_xauth configuration address respond
!crypto map to_peer_outside_no_xauth 10 ipsec-isakmp dynamic to-remote-client
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to_peer_outside_local_xauth redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby 2 track Ethernet0/0
 standby delay reload 120
!
! Enable loopback0 if you are using radius for Xauth, group auth, or accounting with !
crypto HA
!interface loopback0
! ip address 192.168.100.1 255.255.255.255
!
! Enable this command if you are using radius for Xauth, group auth, or accounting with !
crypto HA
!ip radius source-interface loopback0
!
ip local pool client-address-pool 50.0.0.1 50.0.0.254
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.255.0 10.0.0.5
!
radius-server host 192.168.0.0 255.255.0.0 auth-port 1845 acct-port 1846
radius-server key radius123
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

Stateful Failover for an Easy VPN Server Configuration on RAHA-R2

```
RAHA-R2# show running-config
Building configuration...
Current configuration :3829 bytes
!
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RAHA-R2
!
boot-start-marker
boot-end-marker
!
redundancy inter-device
 scheme standby HA-out
!
username remote_user password 0 letmein
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.2
   remote-port 5000
    remote-ip 10.0.0.1
!
aaa new-model
!
!
! Enter the following command if you are doing Xauth locally.
aaa authentication login local_xauth local
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa authentication login radius_xauth group radius
!
! Enter the following command if you are not doing Xauth.
!aaa authentication login no_xauth none
!
! Enter the following command if you are doing local group authentication.
aaa authorization network local_auth local
!
! Enter the following command if you are doing group authentication remotely via RADIUS.
!aaa authorization network radius_auth group radius
!
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa accounting network radius_accounting start-stop group radius
aaa session-id common
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
!
! Enter the following commands if you are doing group authentication locally.
crypto isakmp client configuration group unity
 key cisco123
 domain cisco.com
 pool client-address-pool
!
!
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map to-remote-client 10
 set transform-set trans1
 reverse-route remote-peer
!
!
! Use this map if you want to dolocal group authentication and Xauth.
crypto map to_peer_outside_local_xauth client authentication list local_xauth
crypto map to_peer_outside_local_xauth isakmp authorization list local_auth
crypto map to_peer_outside_local_xauth client configuration address respond
crypto map to_peer_outside_local_xauth 10 ipsec-isakmp dynamic to-remote-client
```

```
!
! Use this map if you want to use Radius for group authentication and Xauth.
!crypto map to_peer_outside_radius_xauth isakmp client authentication list radius_xauth
!crypto map to_peer_outside_radius_xauth client accounting list radius_accounting
!crypto map to_peer_outside_radius_xauth isakmp authorization list radius_auth
!crypto map to_peer_outside_radius_xauth isakmp client configuration address respond
!crypto map to_peer_outside_radius_xauth isakmp 10 ipsec-isakmp dynamic to-remote-client
!
!
! Use this map if you want to do local authentication and no Xauth.
!crypto map to_peer_outside_no_xauth isakmp authorization list local_auth
!crypto map to_peer_outside_no_xauth configuration address respond
!crypto map to_peer_outside_no_xauth 10 ipsec-isakmp dynamic to-remote-client
!
interface Ethernet0/0
 ip address 209.165.201.2 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload
 crypto map to_peer_outside_local_xauth redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.2 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby 2 track Ethernet0/0
 standby delay reload
!
! Enable loopback0 if you are using radius for Xauth, group auth, or accounting with !
crypto HA
!interface loopback0
! ip address 192.168.100.1 255.255.255.255
!
! Enable this command if you are using radius for Xauth, group auth, or accounting with !
crypto HA
!ip radius source-interface loopback0
!
ip local pool client-address-pool 50.0.0.1 50.0.0.254
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
!
radius-server host 192.168.0.200 auth-port 1845 acct-port 1846
radius-server key radius123
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Security commands	*Cisco IOS Security Command Reference*
RRI	The section “IPSec VPN High Availability Enhancements” in the *Cisco IOS Security Configuration Guide: Secure Connectivity*.
HSRP	The section “Configuring the Hot Standby Router Protocol” in the Cisco IOS IP Configuration Guide: Secure Connectivity .
Easy VPN Server	The section “Cisco Easy VPN Remote” in t he *Cisco IOS Security Configuration Guide: Secure Connectivity*.
IKE configuration	The section “Configuring Internet Key Exchange for IPsec VPNs” in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
IPsec configuration	The section “Configuring Security for VPNs with IPsec” in the *Cisco IOS Security Configuration Guide* .
IPsec and IKE commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Stateful Failover for IPsec

GUID-095377BC-8C55-4939-B7AE-362481D2A8BB1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note GUID-095377BC-8C55-4939-B7AE-362481D2A8BB1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Stateful Failover for IPsec

Feature Name	Releases	Feature Information
Stateful Failover for IPsec	12.3(11)T	The Stateful Failover for IP Sec feature enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. The following commands were introduced or modified: **clear crypto isakmp , clear crypto sa , clear crypto session , crypto map (interface IPsec) , crypto map redundancy replay-interval , debug crypto ha , debug crypto ipsec ha , debug crypto isakmp ha , local-ip (IPC transport-SCTP local) , local-port , redundancy inter-device , redundancy stateful , remote-ip (IPC transport-SCTP remote) , remote-port , scheme , security ipsec , show crypto ha , show crypto ipsec sa , show crypto isakmp sa , show crypto session , show redundancy .**

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

IPsec Preferred Peer

The IP Security (IPsec) Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario.

This feature includes the following capabilities:

- Default peer configuration
- IPsec idle-timer usage with default peer

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPsec Preferred Peer

- You must have a properly defined, complete crypto map.

Restrictions for IPsec Preferred Peer

Default peer:

- This feature must be used in conjunction with Dead Peer Detection (DPD). It is most effective on a remote site running DPD in periodic mode. DPD detects the failure of a device quickly and resets the peer list so that the default peer is tried for the next attempted connection.
- Only one peer can be designated as the default peer in a crypto map.
- The default peer must be the first peer in the peer list.

IPsec idle-timer usage with default peer:

- This feature works only on the crypto map for which it is configured. You cannot configure the capability globally for all crypto maps.
- If there is a global idle timer, the crypto map idle-timer value must be different from the global value; otherwise, the idle timer is not added to the crypto map.

Information About IPsec Preferred Peer

IPsec

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating Internet Protocol (IP) packets between participating IPsec devices (peers), such as Cisco routers.

IPsec provides the following network security services. These services are optional. In general, local security policy dictates the use of one or more of these services:

- Data Confidentiality--The IPsec sender can encrypt packets before transmitting them across a network.
- Data Integrity--The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication--The IPsec receiver can authenticate the source of the IPsec packets sent.
- Anti-Replay--The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as Virtual Private Networks (VPNs), including intranets, extranets, and remote user access.

IPsec provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying characteristics of these tunnels. When the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

Dead Peer Detection

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPsec tunnel. If the network is unusually busy or unreliable, you can increase the number of seconds that the VPN Client will wait before deciding whether the peer is no longer active.

Keepalive packets are not sent if traffic is received. This lowers the overhead associated with DPD, because on a heavily loaded network very few keepalive packets will be sent because traffic is being received on the tunnels. In addition, DPD sends keepalive packets only if there is user traffic to send (and no user traffic is received).

You can configure Internet Key Exchange (IKE) DPD so that DPD sends the keepalive packets whether or not there is outbound user data. That is, as long as there is no inbound user data, the keepalive packets are sent at the configured keepalive interval.

Default Peer Configuration

If a connection timeout occurs, the connection to the current peer is closed. The **set peer** command allows you to configure the first peer as the default peer. If there is a default peer, the next time a connection is initiated, the connection is directed to the default peer instead of to the next peer in the peer list. If the default peer is unresponsive, the next peer in the peer list becomes the current peer and future connections through the crypto map try that peer.

This capability is useful when traffic on a physical link stops due to the failure of a remote peer. DPD indicates that the remote peer is unavailable, but that peer remains the current peer.

A default peer facilitates the failover to a preferred peer that was previously unavailable, but has returned to service. Users can give preference to certain peers in the event of a failover. This is useful if the original failure was due to a network connectivity problem rather than failure of the remote peer.

Idle Timers

When a router running Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers.

IPsec SA idle timers increase the availability of resources by deleting SAs associated with idle peers. Because IPsec SA idle timers prevent the wasting of resources by idle peers, more resources are available to create new SAs when required.

If IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

IPsec Idle-Timer Usage with Default Peer

If all connections to the current peer time out, the next time a connection is initiated it is directed to the default peer configured in the **set peer** command. If a default peer is not configured and there is a connection timeout, the current peer remains the one that timed out.

This enhancement helps facilitate a failover to a preferred peer that was previously unavailable but is in service now.

Peers on Crypto Maps

A crypto map set can contain multiple entries, each with a different access list. The router searches the crypto map entries in order, and attempts to match the packet to the access list specified in that entry.

When a packet matches a **permit** entry in a particular access list, and the corresponding crypto map entry is tagged as Cisco, connections are established with the remote peer as specified in the set peer statements within the crypto map.

How to Configure IPsec Preferred Peer

- Configuring a Default Peer, page 78
- Configuring the Idle Timer, page 79

Configuring a Default Peer

To configure a default peer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **Example:** `Router(config)# crypto map mymap 10 ipsec-isakmp`	Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.

	Command or Action	Purpose

Step 4	**set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
	Example:
	`Router(config-crypto-map)# set peer 10.0.0.2 default`
		Specifies an IPsec peer in a crypto map entry. Ensures that the first peer specified is defined as the default peer.

Step 5	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode and returns to global configuration mode.

Configuring the Idle Timer

To configure the idle timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set security-association idletime** *seconds* [**default**]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **Example:** `Router(config)# crypto map mymap 10 ipsec-isakmp`	Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
Step 4	**set security-association idletime** *seconds* [**default**] **Example:** `Router(config-crypto-map)# set security-association idletime 120 default`	Specifies the maximum amount of time for which the current peer can be idle before the default peer is used.
Step 5	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode and returns to global configuration mode.

Configuration Examples for IPsec Preferred Peer

Configuring a Default Peer Example

The following example shows that the first peer, at IP address 10.1.1.1, is the default peer:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

Configuring the IPsec Idle Timer Example

In the following example, if the current peer is idle for 120 seconds, the default peer 10.1.1.1 (which was specified in the **set peer**command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idletime 120 default
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPsec	*Security for VPNs with IPsec*
Crypto map	• *Security for VPNs with IPsec* • *Configuring Internet Key Exchange for IPsec VPNs*
DPD	*IPsec Dead Peer Detection Periodic Message Option*
Security commands	*Cisco IOS Security Command Reference*

MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPsec Preferred Peer

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for IPsec Preferred Peer

Feature Name	Releases	Feature Information
IPsec Preferred Peer	12.3(14)T 12.2(33)SRA 12.2(33)SXH	The IPsec Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario. In 12.3(14)T, this feature was introduced. In 12.2(33)SRA, this feature, the **set peer (IPsec)** command, and the **set security-association idle-time** command were integrated into this release.

Glossary

crypto access list --A list that defines which IP traffic will be protected by crypto and which traffic will not be protected by crypto.

crypto map --A map that specifies which traffic should be protected by IPsec, where IPsec-protected traffic should be sent, and what IPsec transform sets should be applied to this traffic.

dead peer detection --A feature that allows the router to detect an unresponsive peer.

keepalive message --A message sent by one network device to inform another network device that the virtual circuit between the two is still active.

peer --Router or other device that participates in IPsec and IKE. In IPsec, peers are devices or entities that communicate securely either through the exchange of keys or the exchange of digital certificates.

SA --security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPsec. A user also can establish IPsec SAs manually. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Payload (ESP) between peers, one ESP SA is required for each direction. SAs are identified uniquely by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

transform set --An acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Real-Time Resolution for IPsec Tunnel Peer

After a user specifies a host name (instead of an IP address) for remote IP Security (IPsec) peer, the Real-Time Resolution for IPsec Tunnel Peer feature allows the host name to be domain name server (DNS) resolved before the router establishes the IPsec tunnel. Thus, the router can immediately discover whether the IP address of the peer has changed.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Real-Time Resolution for IPsec Tunnel Peer

Secure DNS Requirement

It is recommended that you use this feature only with secure DNS and when the DNS responses can be authenticated. Otherwise, an attacker can spoof or forge DNS responses and have access to Internet Key Exchange (IKE) authentication data, such as a certificate. If an attacker has a certificate that is trusted by the initiating host, the attacker can successfully establish Phase 1 IKE security association (SA), or the attacker can try to guess the preshared key that is shared between the initiator and the actual responder.

DNS Initiator

DNS names resolution for remote IPsec peers will work only if they are used as an initiator. The first packet that is to be encrypted will trigger a DNS lookup; after the DNS lookup is complete, subsequent packets will trigger IKE.

Information About Real-Time Resolution for IPsec Tunnel Peer

Real-Time Resolution Via Secure DNS

When specifying the host name of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

DNS resolution assures users that their established IPsec tunnel is secure and authenticated.

How to Configure Real-Time Resolution

Configuring Real-Time Resolution for IPsec Peers

Use this task to configure a router to perform real-time DNS resolution with a remote IPsec peer; that is, the host name of peer is resolved through a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

Before creating a crypto map, you should perform the following tasks:

- Define Internet Security Association Key Management Protocol (ISAKMP) policies.
- Define IPsec transform sets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **match address** *access-list-id*
5. **set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
6. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**crypto map** *map-name seq-num* **ipsec-isakmp**
	Example:
	`Router(config)# crypto map`
	`secure_b 10 ipsec-isakmp`
		Specifies the crypto map entry to create (or modify) and enters crypto map configuration mode.

Step 4	**match address** *access-list-id*
	Example:
	`Router(config-crypto-m)# match`
	`address 140`
		Names an extended access list.
		This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec in the context of this crypto map entry.

Step 5	**set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
	Example:
	`Router(config-crypto-m)#`
	` set peer b.cisco.com dynamic`
		Specifies a remote IPsec peer.
		This is the peer to which IPsec-protected traffic can be forwarded.
		• The *host-name* argument specifies the IPsec peer by its hostname. This is the peer's hostname concatenated with its domain name (for example, myhost.example.com).
		• The optional **dynamic** keyword allows the hostname of the IPsec peer to be resolved through a domain name server (DNS) lookup immediately before the router establishes the IPsec tunnel.
		• The optional **default** keyword designates that the first peer is the default peer if there are multiple IPsec peers.
		• The *ip-address* argument specifies the IPsec peer by its IP address.
		Repeat this step if there are multiple remote peers.

	Command or Action	Purpose
Step 6	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] **Example:** `Router(config-crypto-m)# set transform-set myset`	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).

- Troubleshooting Tips, page 88
- What to Do Next, page 88

Troubleshooting Tips

To display crypto map configuration information, use the **show crypto map** command.

What to Do Next

You need to apply a crypto map set to each interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association (SA) negotiation on behalf of traffic to be protected by crypto.

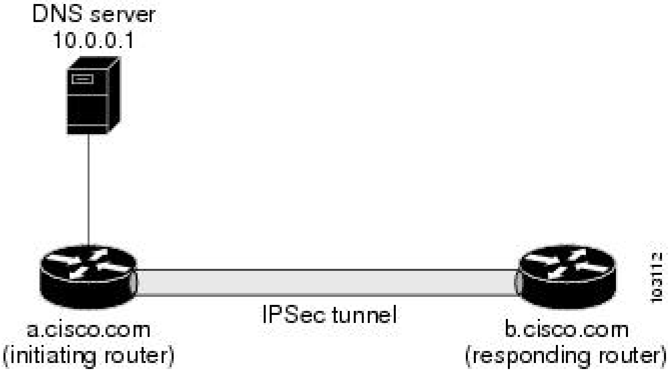
Configuration Examples for Real-Time Resolution

- Configuring Real-Time Resolution for an IPsec Peer Example, page 89

Configuring Real-Time Resolution for an IPsec Peer Example

The figure below and the following example illustrate how to create a crypto map that configures the host name of a remote IPsec peer to DNS resolved through a DNS lookup right before the Cisco IOS software attempts to establish a connection with that peer.

Figure 6 Real-Time Resolution Sample Topology



```
! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPSec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
  match address 150
  set peer 30.0.0.1
  set transform-set
interface serial0/1
  ip address 40.0.0.1
  crypto map secure_a
access-list 150 ...
! DNS server configuration
b.cisco.com    40.0.0.1       # the address of serial0/1 of b.cisco.com
```

Additional References

Related Documents

Related Topic	Document Title
Crypto maps	“Configuring Security for VPNs with IPsec” module in the *Security for VPNs with IPsec Configuration Guide*
ISAKMP policies	“Configuring Internet Key Exchange for IPsec VPNs” module in the *Internet Key Exchange for IPsec VPNs Configuration Guide*
IPsec and IKE configuration commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Real-Time Resolution for IPsec Tunnel Peer

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 *Feature Information for Real-Time Resolution for IPsec Tunnel Peer*

Feature Name	Releases	Feature Information
Real-Time Resolution for IPsec Tunnel Peer	11.2 12.3(4)T 12.2(18)SXD 12.3(14)T 12.2(33)SRA	After a user specifies a host name (instead of an IP address) for remote IP Security (IPsec) peer, the Real-Time Resolution for IPsec Tunnel Peer feature allows the host name to be domain name server (DNS) resolved before the router establishes the IPsec tunnel. Thus, the router can immediately discover whether the IP address of the peer has changed. This feature was introduced in Cisco IOS Release 11.2. In Cisco IOS Release 12.3(4)T, the **dynamic** keyword was added to the **set peer (IPsec)** command. In Cisco IOS Release 12.3(14)T, the **dynamic** keyword was added to the **set peer (IPsec)** command. The following command was introduced or modified: **set peer (IPsec) .**

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.