VPN Availability Configuration Guide, Cisco IOS Release 15S

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

CONTENTS

Reverse Route Injection

Reverse route injection (RRI) is the ability to automatically insert static routes in 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 a remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN device 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 device can take precedence over a locally configured static route.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the *Next Generation Encryption* (NGE) white paper.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 route 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 device as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN device, this information is propagated to upstream devices, allowing them to determine the appropriate VPN device to which the returning traffic must be sent to maintain IPsec state flows. Being able to determine the appropriate VPN device is particularly useful if multiple VPN devices are used at a site to provide load balancing or failover or if the remote VPN devices are not accessible via a default route. Depending on the scenario, routes are created in the global routing table and/or the appropriate virtual route forwarding (VRF) table.

Note The **remote-peer** keyword is required in the **reverse-route** command to “leak” the routes.

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 device 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 access control lists (ACL) (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 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 with 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

The 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 (formerly known as 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 Cisco IOS Release 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 section "Example: show crypto route Command Output, page 15."

How to Configure Reverse Route Injection

Configuring RRI Under Static Crypto Maps

To configure RRI under a static crypto map for software prior to Cisco IOS 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**]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-name* **ipsec-isakmp** **Example:** `Device(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:** `Device(config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.
Step 5	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

Configuring RRI Under a Dynamic Map Template for Cisco

To configure RRI under a dynamic map template for software prior to Cisco IOS 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**]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Device(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:** `Device(config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.
Step 5	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

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*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-name* **ipsec-isakmp** **Example:** `Device(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:** `Device(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:** `Device(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.
Step 6	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

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*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Device(config)# crypto dynamic-map mymap 1`	Creates a dynamic crypto map entry and enters crypto map configuration command mode.
Step 4	**reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]] **Example:** `Device(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:** `Device(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.
Step 6	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

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 security association (SA), you can use the **debug crypto ipsec** command.

SUMMARY STEPS

1. **enable**
2. **show crypto router**

DETAILED STEPS

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

Configuration Examples for Reverse Route Injection

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

Example: Configuring RRI When Crypto ACLs Exist

The following example shows how to connect all remote VPN gateways to the device 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
 crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac
 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 the 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 CLI (**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
```

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

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
```

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

Example: Configuring RRI When Crypto ACLs Exist

The following example shows how to configure RRI for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac
   match address 101
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

Example: Configuring RRI with Route Tags

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
```

```
Device# 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
```

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

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)
```

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

Example: Configuring an RRI Distance Metric Under a Crypto Map

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

Server

```
crypto dynamic-map mymap
 set security-association lifetime seconds 300
 Crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac
 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
```

Example: Configuring RRI with Route Tags

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
Device# 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
```

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

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

```
Device# 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-aes 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

Device# 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
```

Example: Configuring an RRI Distance Metric for a VTI

The following configuration shows a server and client configuration in which an 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 aes-sha
 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
```

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

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

```
Device# 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-aes 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-aes 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 outbound sa
to SPI ADC90C5

Device# 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
```

Example: show crypto route Command Output

The following is sample output from the show crypto route command that 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 commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Recommended cryptographic algorithms	*Next Generation Encryption*

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 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 to automatically insert static routes in 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 VPN router as the next hop, the traffic is forced through the crypto process to be encrypted. The following commands were introduced or modified: **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	12.2(33)SRA 12.2(33)SXH 12.3(14)T	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: **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: Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP) with IPsec. When used together, these two features provide you with a simplified network design for VPNs and reduced configuration complexity on remote peers when defining gateway lists.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the *Next Generation Encryption* (NGE) white paper.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

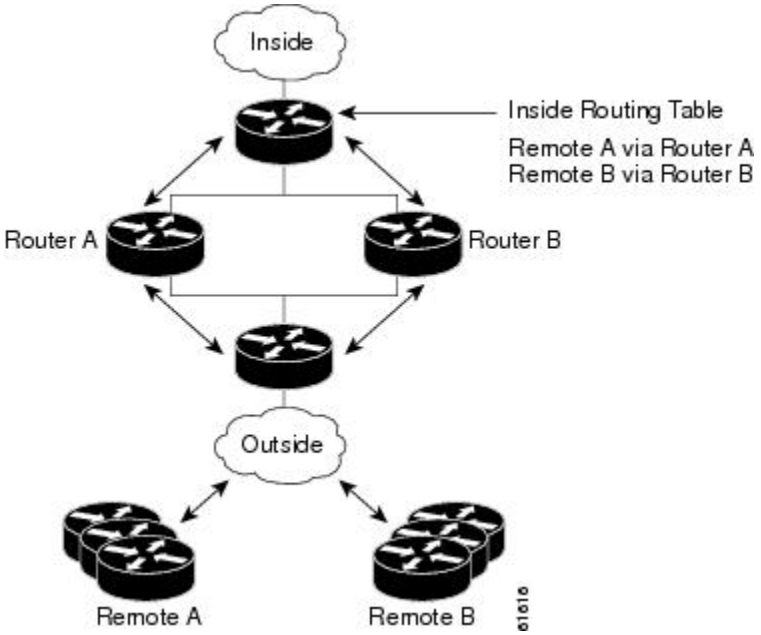
Note The use of any keyword in ACLs with RRI is not supported.

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 an 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. You can to use the standby IP address from an interface as the local IPsec identity or local tunnel endpoint.

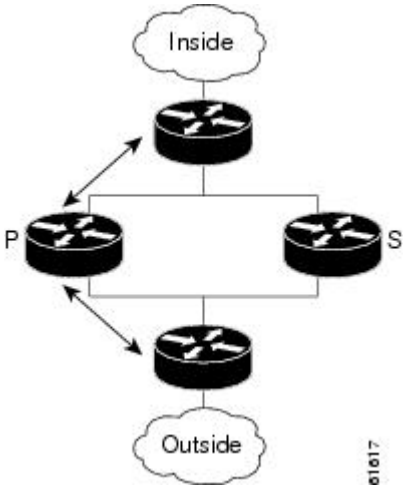
By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership 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, which is the active device in the standby group. In the event of failover, traffic is diverted to Router S,

which is 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

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`	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.
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 2 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.

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** *transform-set-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 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.

	Command or Action	Purpose
Step 5	**reverse-route** **Example:** `Router (config-if)#reverse-route`	Creates dynamic 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** *transform-set-name* **Example:** `Router (config-if)# set transform-set my_t_set1`	Specifies which transform sets are allowed for the crypto map entry. List 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 you delete 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 you add 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 *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.
Step 4	**standby name** *group-name* **Example:** `Router(config-if)#standby name mygroup`	Specifies the standby group name.
Step 5	**standby ip** *ip-address* **Example:** `Router(config-if)#standby ip 209.165.200.249`	Specifies the IP address of the standby groups • This command is required for one device in the group.

	Command or Action	Purpose
Step 6	**crypto map** *map-name* **redundancy** [*standby-name*] **Example:** `Router (config-if)#crypto map mymap redundancy`	Specifies the IP redundancy address as the tunnel endpoint for IPsec.

Verifying VPN IPsec Crypto Configuration

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.
Step 2	**show crypto ipsec transform-set** **Example:** `Router#show crypto ipsec transform-set`	Displays the 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.

	Command or Action	Purpose
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: Configuring 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 my-transform-set
 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: Configuring 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 you choose to manually define static routes on the VPN router for remote proxies and have 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). We recommend 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 my-transform-set
 match address 101
crypto map mymap 2 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set my-transform-set
 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: Configuring HSRP with 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 the crypto map named *mymap* and at the same time ensures that HSRP failover is facilitated between an active and standby device belonging to the same standby group named 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-aes-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 Command List, All Releases*
Configuring HSRP without IPsec	"Configuring IP Services" module in the *IP Application Services Configuration Guide*

Related Topic	Document Title
Configuring stateful failover for IP security (IPsec)	"Stateful Failover for IPsec" module in the *Security Configuration Guide: Secure Connectivity*
Recommended cryptographic algorithms	*Next Generation Encryption*

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	Cisco IOS XE 3.1.0S	The IPsec VPN High Availability Enhancements feature consists of two features:Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP) with IPsec. When used together, these two features provide you with a simplified network design for VPNs and reduced configuration complexity on remote peers when defining gateway lists. The following commands were introduced or modified: **crypto map** (interface IPsec), **reverse-route**.

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 caveats and feature information, see Bug Search Tool and 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 module.

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.

IPsec Failover

IPsec on the Cisco ASR 1000 Series Router supports only stateless failover. IPsec failover is a feature that increases the total uptime (or availability) of an IPsec network. This is accomplished traditionally by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPsec.

IPsec failover falls into two categories: stateless failover and stateful failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary-to-secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

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 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

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.

	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**] [**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 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.
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 3 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.

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 caveats and feature information, see Bug Search Tool and 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 module.

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 48
- What to Do Next, page 48

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.

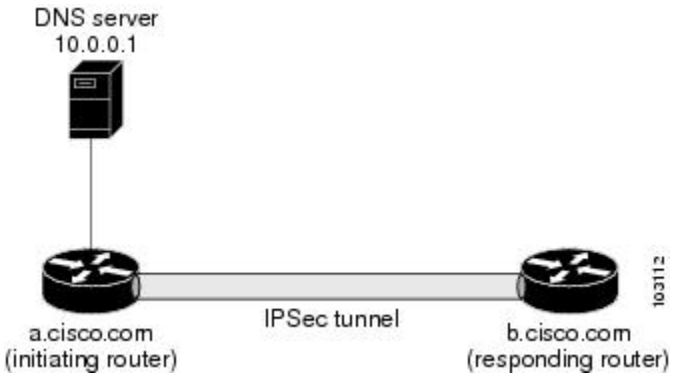
Configuration Examples for Real-Time Resolution

- Configuring Real-Time Resolution for an IPsec Peer Example, page 49

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 3 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 4 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) .**