



Reverse Route Injection

Last Updated: October 15, 2012

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, page 1](#)
- [Prerequisites for Reverse Route Injection, page 2](#)
- [Restrictions for Reverse Route Injection, page 2](#)
- [Information About Reverse Route Injection, page 2](#)
- [How to Configure Reverse Route Injection, page 4](#)
- [Configuration Examples for Reverse Route Injection, page 10](#)
- [Additional References, page 15](#)
- [Feature Information for Reverse Route Injection, page 16](#)

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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, page 2](#)
- [Enhancements to Reverse Route Injection in Cisco IOS Release 12.4\(15\)T, page 3](#)

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, page 3](#)
- [Gateway Option, page 3](#)
- [Support for RRI on IPsec Profiles, page 4](#)
- [Tag Option Configuration Changes, page 4](#)
- [show crypto route Command, page 4](#)

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, page 4](#)
- [Configuring RRI Under a Dynamic Map Template for Cisco, page 5](#)
- [Configuring RRI with Enhancements Under a Static Crypto Map, page 6](#)
- [Configuring RRI with Enhancements Under a Dynamic Map Template, page 8](#)
- [Configuring an RRI Distance Metric Under an IPsec Profile, page 9](#)
- [Displaying Routes Created Through IPsec Using RRI or Easy VPN VTIs, page 10](#)

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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 crypto map <i>map-name seq-name ipsec-isakmp</i> 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 <i>tag-id</i> [static] remote-peer [static] remote-peer <i>ip-address</i> [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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-name</i> 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 <i>tag-id</i> [static] remote-peer [static] remote-peer <i>ip-address</i> [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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 crypto map <i>map-name seq-name ipsec-isakmp</i> 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 [<i>static</i> <i>remote-peer ip-address</i> [<i>gateway</i>] [<i>static</i>]] 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 [<i>distance number</i> <i>tag tag-id</i>] 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-name</i> 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 <i>ip-address</i> [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 <i>number</i> tag <i>tag-id</i>] 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.

Command or Action	Purpose
Step 6 <code>end</code> Example: <code>Device(config-crypto-map)# end</code>	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 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3 <code>crypto ipsec profile name</code> Example: <code>Router (config)# crypto ipsec profile myprofile</code>	Creates or modifies an IPsec profile and enters IPsec profile configuration mode.
Step 4 <code>set reverse-route [distance number tag tag-id]</code> Example: <code>Router (config-crypto-profile)# set reverse-route distance 20</code>	Defines a distance metric for each static route or tags a reverse route injection- (RRI-) created route. <ul style="list-style-type: none"> • 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	Enables privileged EXEC mode.
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show crypto router	Displays routes that are created through IPsec via RRI or Easy VPN VTIs.
	Example: Device# show crypto route	

Configuration Examples for Reverse Route Injection

- [Example: Configuring RRI Prior to Cisco IOS Release 12.3\(14\)T, page 10](#)
- [Example: Configuring RRI with Enhancements Added in Cisco IOS Release 12.3\(14\)T, page 11](#)
- [Example: Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T, page 12](#)

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

- [Example: Configuring RRI When Crypto ACLs Exist, page 10](#)
- [Example: Configuring RRI for a Remote Endpoint and a Route Recursion Route, page 11](#)

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, page 11](#)
- [Example: Configuring RRI with Route Tags, page 11](#)
- [Example: Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop, page 12](#)

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
```

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

```

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

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 typel
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 (type=4),
remote_proxy= 192.168.6.1/255.255.255.0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysz= 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
```

Example: Configuring an RRI Distance Metric for a VTI

```

      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-Templat1 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 Virtual-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, changed 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
Security commands	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p> <p>The following commands were introduced or modified: reverse-route.</p>
Reverse Route Remote Peer Options	12.2(13)T 12.2(14)S	<p>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.</p>

Feature Name	Releases	Feature Information
Reverse Route Injection Enhancements	12.2(33)SRA 12.2(33)SXH 12.3(14)T	<p>The following enhancements were added to the Reverse Route Injection feature:</p> <ul style="list-style-type: none"> 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. <p>The following command was modified by these feature enhancements: reverse-route.</p>
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	<p>This enhancement allows you to define a metric distance for each static route.</p> <p>The following commands were introduced or modified: reverse-route, set reverse-route.</p>
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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2011 Cisco Systems, Inc. All rights reserved.

© 2012 Cisco Systems, Inc. All rights reserved.