Reverse Route Injection

First Published: August 16, 2001
Last Updated: April 5, 2011

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

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

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

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

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Reverse Route Injection" section on page 19.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Contents

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

Prerequisites for Reverse Route Injection

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

Restrictions for Reverse Route Injection

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

Information About Reverse Route Injection

Reverse Route Injection

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

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

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

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

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

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

RRI Distance Metric

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

Gateway Option

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

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

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

Support for RRI on IPsec Profiles

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

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

Tag Option Configuration Changes

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

show crypto route Command

The **show crypto route** command displays routes that are created through IPsec via RRI or Easy VPN virtual tunnel interfaces (VTIs). The routes are displayed in one table. To see sample output for the **show crypto route** command, see the "show crypto route Command Output: Example" section on page 16.

How to Configure Reverse Route Injection

Configuring RRI Under Static Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** {*map-name*} {*seq-name*} **ipsec-isakmp** **Example:** `Router (config)# crypto map mymap 1 ipsec-isakmp`	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]] **Example:** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.

Configuring RRI Under a Dynamic Map Template for Cisco IOS Releases Prior to 12.4(15)T

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Router (config)# crypto dynamic-map mymap 1`	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]] **Example:** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	Creates source proxy information for a crypto map entry.

Configuring RRI with Enhancements Under a Static Crypto Map for Cisco IOS Release 12.4(15)T and Later Releases

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-name* **ipsec-isakmp** **Example:** `Router (config)# crypto map mymap 1 ipsec-isakmp`	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	**reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]] **Example:** `Router (config-crypto-map)# reverse-route`	Creates source proxy information for a crypto map entry. **Note** The **gateway** keyword can be added to enable the dual route functionality for default gateway support.
Step 5	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **Example:** `Router (config-crypto-map)# set reverse-route distance 20`	Specifies a distance metric to be used or a tag value to be associated with these routes.

Configuring RRI with Enhancements Under a Dynamic Map Template For Cisco IOS Release 12.4(15)T and Later Releases

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

SUMMARY STEPS

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

DETAILED STEPS

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

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.

To display routes that are created through IPsec via RRI or Easy VPN VTIs, perform the following steps.

SUMMARY STEPS

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

DETAILED STEPS

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

To observe the behavior of RRI and its relationship to the creation and deletion of an IPsec SA, you can use the **debug crypto ipsec** command (see the *Cisco IOS Debug Command Reference*.

Configuration Examples for Reverse Route Injection

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

Configuring RRI When Crypto ACLs Exist: Example

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

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

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

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

Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

VPNSM

ip route 10.1.1.1 255.255.255.255 vlan0.1

Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example

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

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

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

Configuring RRI When Crypto ACLs Exist: Example

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

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
   match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

Configuring RRI with Route Tags: Example

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

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip eigrp topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
     via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

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

Note This option is applicable only to crypto maps.

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

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

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

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

And this result occurs with RRI enhancements:

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

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

Configuring a RRI Distance Metric Under a Crypto Map: Example

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

Server

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

Client

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

Configuring RRI with Route Tags: Example

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

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip eigrp topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

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

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

```
Router# debug crypto ipsec

00:23:37: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 10.0.0.14
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
```

```
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

Configuring a RRI Distance Metric for a VTI: Example

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

Server Configuration

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

Client Configuration

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

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

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

```
Router# debug crypto ipsec

00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: Crypto mapdb : proxy_match
        src addr     : 0.0.0.0
        dst addr     : 192.168.6.1
        protocol     : 0
        src port     : 0
        dst port     : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same pro
xies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtua
l-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

00:47:56: IPSEC(create_sa): sa created,
```

```
  (sa) sa_dest= 10.0.0.110, sa_proto= 50,
    sa_spi= 0x19E1175C(434181980),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.14, sa_proto= 50,
    sa_spi= 0xADC90C5(182227141),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, chang
ed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outb
ound sa to SPI ADC90C5

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

show crypto route Command Output: Example

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

```
Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                  on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

Additional References

The following sections provide references related to Reverse Route Injection enhancements.

Related Documents

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

Standards

Standards	Title
None	—

MIBs

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

RFCs

RFCs	Title
None	—

Technical Assistance

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

Feature Information for Reverse Route Injection

Table 1 lists the features in this module and provides links to specific configuration information.

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

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 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	Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted. The following sections provide information about this feature: • "Reverse Route Injection" section on page 2 The following commands were introduced or modified by this feature: **reverse-route**.
Reverse Route Remote Peer Options	12.2(13)T 12.2(14)S	An enhancement was added to RRI to allow you to specify an interface or address as the explicit next hop to the remote VPN device. This functionality allows the overriding of a default route to properly direct outgoing encrypted packets. The following sections provide information about the remote peer options: • "Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T" section on page 3.

Table 1 Feature Information for Reverse Route Injection (continued)

Feature Name	Releases	Feature Information
Reverse Route Injection Enhancements	12.3(14)T 12.2(33)SRA 12.2(33)SXH	The following enhancements were added to the Reverse Route Injection feature: • The default behavior of static crypto maps will be the same as that of dynamic crypto maps unless the **reverse-route** command and **static** keyword are used. • A route tag value was added for any routes that are created using RRI. • RRI can be configured on the same crypto map that is applied to multiple router interfaces. • RRI configured with the **reverse-route remote-peer** {*ip-address*} command, keyword, and argument will create one route instead of two. The following sections provide information about the Reverse Route Injection enhancements: • "Reverse Route Injection" section on page 2 • "Configuring RRI Under Static Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T" section on page 5 • "Configuring RRI with Enhancements Under a Static Crypto Map for Cisco IOS Release 12.4(15)T and Later Releases" section on page 7 • "Configuring RRI When Crypto ACLs Exist: Example" section on page 11 • "Configuring RRI with Route Tags: Example" section on page 12 • "Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example" section on page 12 The following command was modified by these feature enhancements: **reverse-route**.
Gateway Option	12.4(15)T	This option allows you to configure unique next hops or gateways for remote tunnel endpoints. The following section provides information about the Gateway Option: • "Gateway Option" section on page 3

Table 1 Feature Information for Reverse Route Injection (continued)

Feature Name	Releases	Feature Information
RRI Distance Metric	12.4(15)T	This enhancement allows you to define a metric distance for each static route. The following sections provide information about the RRI distance metric enhancement. • "RRI Distance Metric" section on page 3 • "Configuring a RRI Distance Metric Under a Crypto Map: Example" section on page 13 • "debug and show Command Output for a RRI Metric Configuration Having a VTI: Example" section on page 15 The following commands were introduced or modified by this feature: **reverse-route**, **set reverse-route**.
show crypto route Command	12.4(15)T	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	This feature provides support for relevant RRI options on IPsec profiles that are predominantly used by VTIs. The following section provides information about the Support for RRI on IPsec Profiles feature: • "Support for RRI on IPsec Profiles" section on page 4
Tag Option Configuration Changes	12.4(15)T	The tag option is now supported with IPsec profiles under the **set reverse-route tag** command. The following section provides information about this feature enhancement: • "Tag Option Configuration Changes" section on page 4