

Reverse Route Injection

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

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

- Prerequisites for Reverse Route Injection, on page 1
- Restrictions for Reverse Route Injection, on page 1
- Information About Reverse Route Injection, on page 2
- How to Configure Reverse Route Injection, on page 2
- Configuration Examples for Reverse Route Injection, on page 4
- Additional References, on page 5
- Feature Information for Reverse Route Injection, on page 5

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

- RRI is not supported for IPv6 crypto maps.
- For static crypto maps, routes are always present if RRI is configured on an applied crypto map. 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.
- For a prefix in the RIB, if you have manually configured a static route with a tag and a route without a tag inserted through RRI, the route selection may be inconsistent. In this scenario, either the manually configured route or the RRI route may be chosen. To prevent such an inconsistency, perform one of the following actions:
  - Disable RRI by removing reverse route configuration from the crypto map, if you are manually configuring static routes to all the peer VPN networks of the router.

- Set an identical tag in the crypto map for the route inserted through RRI.

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. Routes created on the basis of IPsec source proxies on static crypto maps is the default behavior on static maps and overrides 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.

How to Configure Reverse Route Injection

Configuring RRI Under a Static Crypto Map

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

Procedure

	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

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

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* **Example:** `Router (config)# crypto dynamic-map mymap 1`	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	**reverse-route** [**static** | **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.

Configuration Examples for Reverse Route Injection

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 0/0/1
 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
```

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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
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	Cisco IOS XE Release 2.1	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: The following commands were introduced or modified by this feature: **reverse-route**.