



IPSec VPN High Availability Enhancements

Feature History

Release	Modification
12.1(9)E	This feature was introduced in Cisco IOS Release 12.1(9)E.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This feature was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the IPSec VPN High Availability Enhancements. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 10](#)

Feature Overview

The IPSec VPN High Availability Enhancements feature consists of two new features—[Reverse Route Injection \(RRI\)](#) and [Hot Standby Router Protocol and IPSec \(HSRP\)](#)—that work together to provide users with a simplified network design for VPNs, and reduced configuration complexity on remote peers with respect to defining gateway lists. When used together, RRI and HSRP provide a more reliable network design for VPNs and reduce configuration complexity on remote peers.

Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify 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.

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

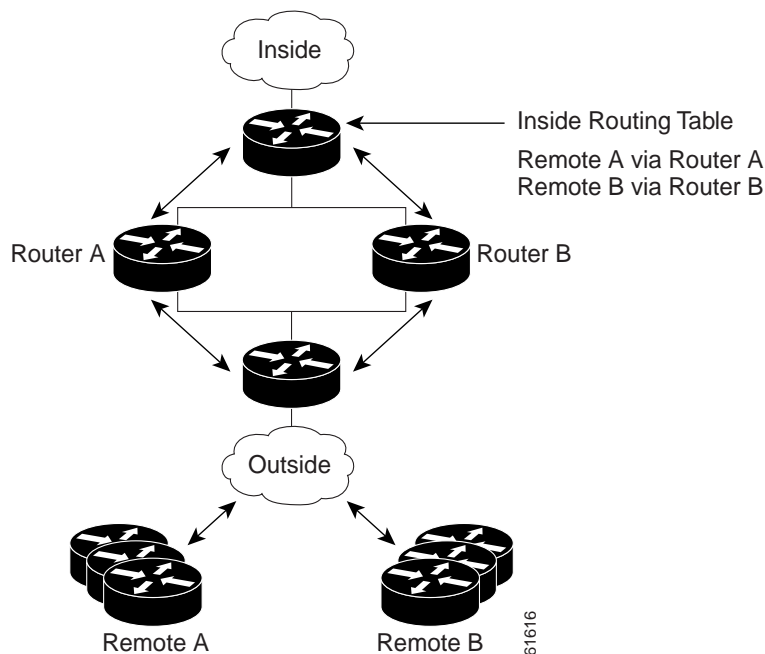
**Note**

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

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

Figure 1 shows a RRI configuration functionality topology. Remote A is being serviced by Router A and Remote B connected to Router B, providing load balancing across VPN gateways at the central site. RRI on the central site devices will ensure 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

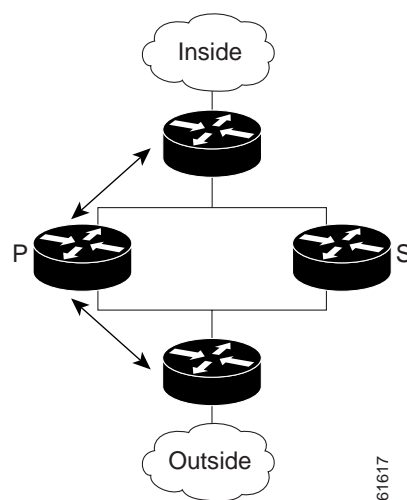
Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router 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 is unable to communicate with the network.

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

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

Figure 2 shows the enhanced HSRP functionality topology. Traffic is serviced by the active Router P, the active device in the standby group. In the event of failover, traffic is diverted to Router S, the original standby device. Router S assumes the role of the new active router and takes ownership of the standby IP address.

Figure 2 Topology Showing Hot Standby Router Protocol Functionality



Note

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

Benefits

Reverse Route Injection

- 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.

Hot Standby Router Protocol with IPSec

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.

Related Documents

- [Stateful Failover for IPSec](#)
- [Cisco IOS Security Configuration Guide](#), Release 12.2
- [Cisco IOS IP Configuration Guide](#), Release 12.2 (Configuring IP Services chapter)
- [VPN Acceleration Module Installation and Configuration Guide](#)
- [SA-VAM2 Installation and Configuration Guide](#)
- [Release Notes for the SA-VAM2](#)
- [Cisco 7100 Series VPN Router Installation and Configuration Guide](#)
- [Cisco 7200 VXR Installation and Configuration Guide](#)
- [Cisco 7401ASR Installation and Configuration Guide](#)

Supported Platforms

Cisco IOS Release 12.1(9)E and Cisco IOS Release 12.2(8)T

- Cisco 7100 series
- Cisco 7200VXR series

Cisco IOS Release 12.2(8)T Only

- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco uBR7200
- Cisco uBR925

Cisco IOS Release 12.2(11)T Only

- Cisco AS5300 series
- Cisco AS5800 series

Cisco IOS Release 12.2(9)YE

- Cisco 7401ASR router

Cisco IOS Release 12.2(14)S

- Cisco 7200 series
- Cisco 7400 series

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the IPSec VPN High Availability Enhancements feature. Each task in the list is identified as either required or optional.

- [Configuring Reverse Route Injection on a Dynamic Crypto Map](#) (required)
- [Configuring Reverse Route Injection on a Static Crypto Map](#) (required)
- [Configuring HSRP with IPSec](#) (required)
- [Verifying VPN IPSec Crypto Configuration](#) (optional)

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, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto dynamic map-name seq-num	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 2	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 3	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, please note the following items:

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

To add RRI to a static crypto map set, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto map map-name seq-num ipsec-isakmp	Adds a dynamic crypto map set to a static crypto map set and enters interface configuration mode.
Step 2	Router (config-if)# set peer ip address	Specifies an IPSec peer IP address in a crypto map entry.
Step 3	Router (config-if)# reverse-route	Creates dynamically static routes based on crypto access control lists (ACLs).
Step 4	Router (config-if)# match address	Specifies an extended access list for a crypto map entry.
Step 5	Router (config-if)# set transform-set	Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first).

Configuring HSRP with IPSec

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

- When HSRP is applied to a crypto map on an interface, the crypto map must be reapplied if the standby IP address or the standby name is changed on that interface.
- If HSRP is applied to a crypto map on an interface, and the user deletes the standby IP address or the standby name from that interface, the crypto tunnel endpoint is reinitialized to the actual IP address of that interface.
- If a user adds the standby IP address and the standby name to an interface with the requirement IPSec failover, the crypto map must be reapplied with the appropriate redundancy information.
- Standby priorities should be equal on active and standby routers. If they are not, the higher priority router takes over as the active router. When that occurs, the active router goes into a cycle where it continuously goes down and comes back up.
- 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](#)” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

To apply a crypto map set to an interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# interface <i>type slot/port</i>	Specifies an interface and enters interface configuration mode.
Step 2	Router (config-if)# standby name <i>group-name</i>	Specifies the standby group name (required).
Step 3	Router (config-if)# standby ip <i>ip-address</i>	Specifies the IP address of the standby groups (required for one device in the group).
Step 4	Router (config-if)# crypto map <i>map-name</i> redundancy [<i>standby-name</i>]	Specifies IP redundancy address as the tunnel endpoint for IPSec.

Verifying VPN IPSec Crypto Configuration

To verify your VPN IPSec crypto configuration, use the following EXEC commands:

Command	Purpose
Router# show crypto ipsec transform-set	Displays your transform set configuration.
Router# show crypto map [interface <i>interface</i> tag <i>map-name</i>]	Displays your crypto map configuration.
Router# show crypto ipsec sa [map <i>map-name</i> address identity] [detail]	Displays information about IPSec SAs.
Router# show crypto dynamic-map [tag <i>map-name</i>]	Displays information about dynamic crypto maps.

Configuration Examples

This section provides the following configuration examples:

- [Reverse Route Injection on a Dynamic Crypto Map Example](#)
- [Reverse Route Injection on a Static Crypto Map Example](#)
- [HSRP and IPSec Example](#)

Reverse Route Injection on a Dynamic Crypto Map Example

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

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

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

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

interface FastEthernet 0/0
crypto map mymap
```

Reverse Route Injection on a Static Crypto Map Example

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 and out of the network.

If the user chooses 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). It is recommended that a link state routing protocol such as OSPF be used to help speed convergence time by ensuring that routing updates are sent as soon as a change in routing state is detected.

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

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0

crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route
  set transform-set esp-3des-sha
  match address 101
crypto map mymap 2 ipsec-isakmp
  set peer 10.1.1.1
  set transform-set esp-3des-sha
  match address 102

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255

interface FastEthernet 0/0
  crypto map mymap
```

HSRP and IPsec Example

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

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

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

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

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

The standby name needs to be configured on all devices in the standby group and the standby address needs to be 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.

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the [Cisco IOS Release 12.2 command reference](#) publications.

- [crypto map \(interface IPSec\)](#)
- [reverse-route](#)

crypto map (interface IPSec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

```
crypto map map-name [redundancy standby-name]
```

```
no crypto map map-name [redundancy standby-name]
```

Syntax Description		
<i>map-name</i>	The name which identifies the crypto map set. This is the name assigned when the crypto map was created.	
	When the no form of the command is used, this argument is optional. Any value supplied for the argument is ignored.	
redundancy	(Optional) Defines a backup IP Security peer. Both routers in the standby group are defined by the redundancy <i>standby name</i> and share the same virtual IP address.	
<i>standby-name</i>	(Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands.	

Defaults	
None.	

Command Modes	
Interface configuration	

Command History	Release	Modification
	11.2	This command was introduced.
	12.1(9)E	The redundancy keyword and <i>standby-name</i> argument were integrated into Cisco IOS Release 12.1(9)E.
	12.2(8)T	The redundancy keyword and <i>standby-name</i> argument were integrated into Cisco IOS Release 12.2(8)T.
	12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
	12.2(9)YE	The redundancy keyword and <i>standby-name</i> argument were integrated into Cisco IOS Release 12.2(9)YE.
	12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines	
Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPSec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of cisco , ipsec-isakmp , and ipsec-manual crypto map entries.	

The standby name needs to be configured on all devices in the standby group, and the standby address needs to be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (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.

Examples

The following example shows how all remote Virtual Private Network (VPN) gateways connect to the router via 192.168.0.3:

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

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

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

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of *mymap* and at the same time ensures that HSRP failover is facilitated between an active and standby device belonging to the same standby group, group1.

Note that Reverse Route Injection (RRI) is also enabled to provide 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 a failover occurs, routes are deleted on the former active device and created on the new active device.

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

reverse-route

no reverse-route

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Crypto map configuration

Release	Modification
12.1(9)E	This command was introduced in Cisco IOS Release 12.1(9)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines This command can be applied on a per crypto basis.

Reverse route injection (RRI) is a good solution for topologies that require encrypted traffic to be diverted to a virtual private network (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 and out of the network.

If the user chooses 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.

Set peer statements in crypto maps must use IP addresses only for this release. Support for host name resolution with RRI is not yet available.

Routing convergence can affect the success of a failover based on the routing protocol used to advertise routes (link state versus periodic update). It is recommended that a link state routing protocol such as Open Shortest Path First (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.

Examples

The following example shows how all remote VPN gateways connect to the router via 192.168.0.3:

```
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
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.