

VPN Gateway Router Configuration Using Static And Dynamic Crypto Maps

Michael J. Martin

Implementing IPsec VPNs on IOS routers involves a number of different configuration elements. In addition to the ISAKMP/IKE configuration and transform set definitions, crypto maps are part of configuring gateways that will support Cisco software VPN client connections.

When we look at the VPN gateway router configuration, it's immediately evident that IPsec policy configuration is involved. The crypto map (CM) serves as the convergence point for the many elements involved. It serves as the interface that interacts with all of the different configuration components, security protocols and algorithms and applies them to support IPsec services on the router. For an IPsec peering relationship to exist, the two peers involved must agree exactly on a set of security parameters to be used in order for the Phase 1 and Phase 2 negotiations to be successful. If a common protocol set cannot be agreed upon, then the IPsec peering negotiation will fail. So it is critical that the CM configuration provides the protocol diversity needed to support your remote peer needs.

IOS supports two different types of CMs: static and dynamic. Static CMs are used to define remote peering relationships when all of the variables needed to establish an IPsec peering relationship are known prior to any negotiation between the VPN gateway and the remote peer taking place. Dynamic CMs are used when only some of the remote peer parameters are known prior to negotiation with the VPN gateway. Another way of looking at this is that static CMs are used when the peering relationship will be permanent, for example, when using VPNs to support a network-to-network topology between fixed locations. Dynamic CMs are most commonly used to support client-to-network topologies. The most common problem with client-to-network IPsec VPN configurations is that the client IP address is either unknown or always changing, and/or the peering relationship will be temporary.

The construction of both maps is a lot like writing a newspaper story, in which you need to get the five Ws (Who, What, Where, When, and Why) straight in order for the story to make sense (or work in this case). So let's take a look at different elements of the CM story:

- **Who:** The configuration starts with the CM definition. A CM needs at least one entry to be valid. The CM is created using this global configuration command: `<crypto map {static map name} {1-65535} {ipsec-isakmp}>`. A CM is a series of entries with the same name but a different sequence number. CM entries are evaluated from the lowest numbered entry to the highest. The syntax above is used for creating or adding a static CM entry.

Dynamic CMs are anchored to a static CM; they are not directly applied to a router interface. The dynamic CM is created with a different command: `<crypto dynamic-map {dynamic map name} {1-65535}>`. Once created, it is added to the static CM using some options on the static CM command: `<crypto map {static map name} {1-65535} {ipsec-isakmp} {dynamic} {dynamic map name}>`. A static CM can have multiple dynamic CMs. A dynamic CM must be created before it can be anchored to the static CM.

A CM sequence definition is typically created for each remote peer or for each traffic policy associated with a peer. Each Static CM remote peer entry is defined with the `<set peer {x.x.x.x | hostname}>` sub-command. For redundancy, it is possible to have multiple remote peers defined within a CM sequence. When defining redundant remote peers, each remote peer must support the same mirror policy.

VPN Gateway Router Configuration Using Static And Dynamic Crypto Maps

Michael J. Martin

- **What:** A CM sequence needs to have a traffic match policy. The match policy defines the source-to-destination traffic flow that will be secured. The match policy is defined using the <match address {access-list-id}> sub-command. Each match ACL entry must have a mirror match policy map ACL entry on the remote peer's CM definition. The CM match policy ACL can be created using named or numbered extended ACLs. Within the ACL, network-to-network, host-to-host, or a combination of host and network patterns can be defined. The most critical aspect of the traffic match policy is that each sequence needs to have its own unique ACL, and -- most important -- the ACLs should not duplicate match traffic entries. If possible, crossover definitions should be avoided.

If different sequences use the same traffic ACLs, or if a crossover traffic definition is less specific than a following sequence definition, the lower-numbered sequence will always qualify the traffic first. Mapping out traffic flows and greater-to-least specific traffic crossovers is very important when constructing an IPsec peer topology. If the sequence ordering is incorrect, the traffic will not be secured properly and could be dropped entirely.

- **Where:** The placement of the CM is critical to ensure that the security policy operates properly. The CM is applied to the interface using the <crypto map {static map name}> interface sub-command. Remember, all traffic that traverses the interface the CM is applied to will be qualified against the CM. This way the CM can open or respond to IKE requests and secure traffic destined to established peers. In addition to the CM, if the router interface is connected to an unsecured network, a traffic filtering ACL is also a requirement. This ACL should permit IP traffic to the "unsecured" interface IP address, for UDP 500 (IKE) or UDP 4500 (NAT traversal) for ISAKMP, ESP IP, and any ports for which you may be supporting Compound TCP tunneling.
- **When:** To ensure communications integrity, SAs between peers must be refreshed at periodic intervals. The expiration interval can be based on time or volume of data. The SA lifetime is defined using the sub-command . Additionally, a timer to delete an idle SA can be set (in seconds) using <set security-association idle-time {60-86400}>.
- **Why:** Why secure the traffic? There are lots of reasons. In order for peers to establish an SA, they must both agree on what traffic will be protected and how they will secure it. What will be protected is defined by the traffic qualification policy. How it is protected is defined by the transform sets associated with the CM entry. The protocols and algorithms that are actually used between the two peers are agreed upon during the ISAKMP Phase 2 negotiation. In order for the Phase 2 negotiation to work at all, at least one transform set definition must be defined, but you can have up to six. The definitions are set using the sub-command <set transform-set transform-set-name1 {transform-set-name2...transform-set-name6}>.

Here is a basic CM configuration example:

```
outlan-rt02(config)#crypto map VPN_Gateway 10 ipsec-isakmp
```

NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

VPN Gateway Router Configuration Using Static And Dynamic Crypto Maps

Michael J. Martin

```
outlan-rt02(config-crypto-map)#set peer 172.30.60.2
outlan-rt02(config-crypto-map)#match address norlan-peer
outlan-rt02(config-crypto-map)#set transform-set 3DES-SHA no-crypt-MD5
outlan-rt02(config-crypto-map)#set security-association lifetime seconds 600
```

In terms of monitoring, there are a number of show commands to retrieve information about the IPsec policy. The most commonly used command is <show crypto ipsec sa>, which provides information and statistics on the active SAs