The bridge to possible

White paper
Cisco public

Migration from IPsec Static Crypto Maps and Dynamic Crypto Map to IPsec Virtual Tunnel Interface – Cisco IOS XE

Contents

1. Why migrate to IPsec virtual tunnel interface?

If you are reading this document, you're either already convinced or curious about the potential advantages that Cisco's IPsec Virtual Tunnel Interface (VTI) will bring.

This is a normal transition, and some new platforms and software releases will exclusively support IPsec VTIs.

As time goes on, we at Cisco will cease using the Cisco IPsec Static Crypto Map (SCM) and Dynamic Crypto Map (DCM) features of Cisco® IOS XE, so it's better to get prepared for the transition.

Cisco Static Crypto Map has been a legacy way to provision IPsec sessions for decades. It identifies peer and traffic to be encrypted explicitly using Access Control Lists (ACLs). This type of configuration is also called policy-based VPN. The original use case was to accommodate a few tunnels with different profiles and characteristics (partners, sites, locations). When we have the information of both peers about what policies they are going to use and what the IP addresses are of both devices, we normally use Static Crypto Map. Dynamic Crypto Map was developed to accommodate peers that share the same characteristics (for example, multiple branch offices sharing the same configuration) or peers that have dynamic IP addressing (DHCP, etc.).

But as IPsec use cases and scalability grow significantly, the legacy crypto map features have been shown to have many limitations and problems. Let's take a look at the following example.

A new subnet 10.220.220.0/24 is added to Site A LAN side. 2 Access Control Entries (ACEs) need to be updated in the routers in both sites.

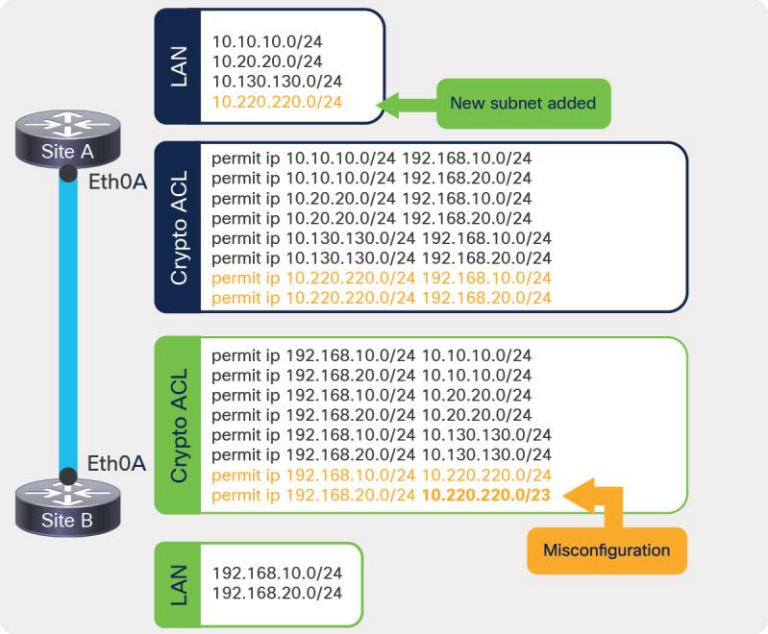

Figure 1.
Static crypto map misconfiguration example

Now scale it up to thousands of sites and tens of thousands of ACEs in each site. It is intuitive to understand that crypto map is facing the challenges of:

- Combinatory explosion of source/destination pairs
- Need for crypto ACLs to be updated whenever networks are added or removed
- Complexity of configurations when you have long crypto ACLs
- Proneness to mismatching of ACL configurations
- And, for the router itself to manage crypto map with large-scale configuration changes of ACLs/ACEs, session creations, churn, and rekeying can expose the system to heavy utilization of system resources, potentially leading to traffic outage or even system failure.

Because crypto map is directly attached to physical interfaces, there is no clear feature separation in the underlay transport vs. overlay IPsec session. This adds complexity to the support features that deal with both pre- and post-encapsulated traffic; for example, QoS pre-classify and IP access-group. And there are features that work only with either pre- or post-encapsulated traffic but not with both; for example, embedded packet capture and NetFlow. There is lack of support for multicast traffic, non-IP traffic, and equal-cost multipath (ECMP) traffic. And there is no crypto map support for certain interface types such as Bridge Domain Interface (BDI) and port channel.

IPsec Virtual Tunnel Interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. This type of configuration is also called route-based VPN.

IPsec VTIs simplify the configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing. If we were using VTI in the previous example, to add a new subnet 10.220.220.0/24 in the Site A LAN side, we would only require the routing configuration to add a new RIB entry in Site B to route the subnet over the tunnel interface:

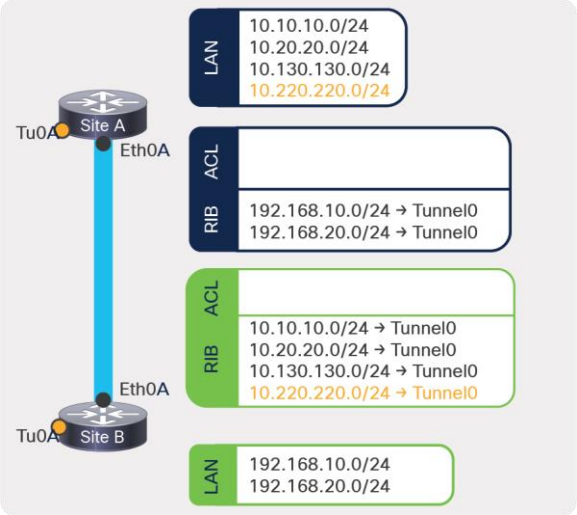

Figure 2.
IPsec VTI route-based VPN example

The benefits of VTI are significant:

- Provides flexibility to send and receive encrypted traffic on any physical interface, including multipath and port channel.
- Traffic is encrypted/decrypted when forwarding to/from the tunnel interface and is managed by the IP routing table.
- Rich services can be applied to VTI; for example, VRF, QoS, Network Address Translation (NAT), v6 overlay, Zone Based Firewall (ZBFW), NetFlow, and multicast.
- Features can be applied either to clear-text packets on the VTI or to encrypted packets on the physical interface.
- Minimal configuration as on-demand virtual access is cloned from a virtual-template interface in a Dynamic Virtual Tunnel Interface (DVTI).
- Easy to determine a tunnels up/down status

2. IPsec virtual tunnel interface migration in practice

Let's take the following network diagram as an example:

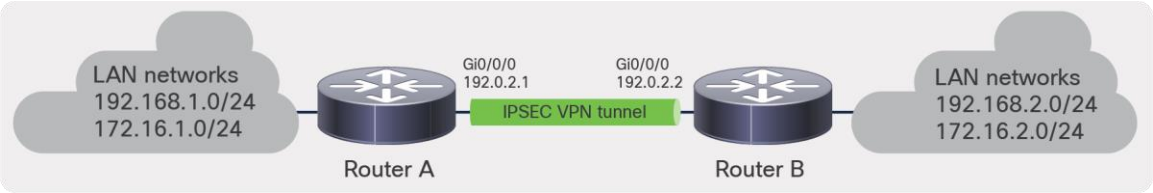

Figure 3.
IPsec VTI migration example

2.1 Migrate both router A and router B to VTI – IKEv1

Crypto map – IKEv1	VTI – IKEv1
Router A: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.2 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.2 set transform-set TSET match address CACL ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255	Router A: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.2 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ipsec profile PROF set transform-set TSET ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 ! interface Tunnel0

Crypto map – IKEv1	VTI – IKEv1
192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 crypto map CMAP Router B: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.1 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.1 set transform-set TSET match address CACL ! ip access-list extended CACL permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 crypto map CMAP	ip address 100.0.2.1 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.2 tunnel protection ipsec profile PROF ! static routes can be replaced by dynamic routing protocols such as EIGRP, BGP or OSPF ip route 192.168.2.0 255.255.255.0 Tunnel0 ip route 172.16.2.0 255.255.255.0 Tunnel0 Router B: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.1 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ipsec profile PROF set transform-set TSET ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 ! interface Tunnel0 ip address 100.0.2.2 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.1 tunnel protection ipsec profile PROF ! ip route 192.168.1.0 255.255.255.0 Tunnel0 ip route 172.16.1.0 255.255.255.0 Tunnel0

2.2 Migrate both router A and router B to VTI – IKEv2

Crypto map – IKEv2	VTI – IKEv2
Router A: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.2 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.2 set transform-set TSET set ikev2-profile PROF match address CACL ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 crypto map CMAP	Router A: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.2 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto ipsec profile PROF set transform-set TSET set ikev2-profile PROF ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 ! interface Tunnel0 ip address 100.0.2.1 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.2 tunnel protection ipsec profile PROF ! static routes can be replaced by dynamic routing protocols such as EIGRP, BGP or OSPF ip route 192.168.2.0 255.255.255.0 Tunnel0 ip route 172.16.2.0 255.255.255.0 Tunnel0
Router B: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.1 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.1 set transform-set TSET set ikev2-profile PROF match address CACL	Router B: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.1 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto ipsec profile PROF set transform-set TSET

Crypto map – IKEv2	VTI – IKEv2
! ip access-list extended CACL permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 crypto map CMAP	set ikev2-profile PROF ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 ! interface Tunnel0 ip address 100.0.2.2 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.1 tunnel protection ipsec profile PROF ! ip route 192.168.1.0 255.255.255.0 Tunnel0 ip route 172.16.1.0 255.255.255.0 Tunnel0

Prior to Cisco IOS-XE Release 16.12, the VTI configuration was not compatible with a crypto map configuration. Both ends of the tunnel had to be configured with the same type of VPN to interoperate.

In IOS-XE 16.12, new configuration options have been added that allow the tunnel interface to act as a policy-based VPN on the protocol level but have all the properties of a tunnel interface. This means that even if router B is a third-party device that cannot be migrated to VTI, router A, which is a Cisco® device, can still be migrated to a VTI configuration.

2.3 Migrate only router A to VTI – IKEv1

Crypto map – IKEv1	VTI – IKEv1
Router A: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.2 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.2 set transform-set TSET match address CACL ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface GigabitEthernet0/0/0	Router A: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.2 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ipsec profile PROF set transform-set TSET reverse-route ! reverse-route option under ipsec profile can be used to automatically create static routes for networks specified in crypto ACL (CACL) referenced in ipsec policy ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0

Crypto map – IKEv1	VTI – IKEv1
ip address 192.0.2.1 255.255.255.0 crypto map CMAP Router B: crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 192.0.2.1 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.1 set transform-set TSET match address CACL ! ip access-list extended CACL permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 crypto map CMAP	0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 ! interface Tunnel0 ip address 100.0.2.1 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.2 Tunnel protection ipsec policy ipv4 CACL tunnel protection ipsec profile PROF ! Router B: ! remain with old configuration

2.4 Migrate only router A to VTI – IKEv2

Crypto map – IKEv2	VTI – IKEv2
Router A: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.2 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.2 set transform-set TSET set ikev2-profile PROF match address CACL ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 crypto map CMAP Router B: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.1 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.1 set transform-set TSET	Router A: crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ikev2 profile PROF match identity remote address 192.0.2.2 255.255.255.255 authentication remote pre-share key cisco123 authentication local pre-share key cisco123 ! crypto ipsec profile PROF set transform-set TSET set ikev2-profile PROF reverse-route ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.1 255.255.255.0 ! interface Tunnel0 ip address 100.0.2.1 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.2 tunnel protection ipsec policy ipv4 CACL tunnel protection ipsec profile PROF ! Router B: ! remain with old configuration

Crypto map - IKEv2	VTI - IKEv2
set ikev2-profile PROF match address CACL ! ip access-list extended CACL permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 crypto map CMAP	

2.5 Migrate only router A to VTI - VRF-aware

Crypto map - IKEv1	VTI - IKEv1
Router A: ip vrf fvrf ip vrf ivrf ! crypto keyring KEY vrf fvrf pre-shared-key address 192.0.2.2 key cisco123 ! crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp profile PROF vrf ivrf keyring KEY match identity address 192.0.2.2 255.255.255.255 fvrf ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.2 set transform-set TSET set isakmp-profile PROF match address CACL ! interface GigabitEthernet0/0/0 ip vrf forwarding fvrf ip address 192.0.2.1 255.255.255.0 crypto map CMAP ! interface GigabitEthernet0/0/1 ip vrf forwarding ivrf ip address 192.168.1.1 255.255.255.0	Router A: ip vrf fvrf ip vrf ivrf ! crypto keyring KEY vrf fvrf pre-shared-key address 192.0.2.2 key cisco123 ! crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp profile PROF keyring KEY match identity address 192.0.2.2 255.255.255.255 fvrf ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto ipsec profile PROF set transform-set TSET set isakmp-profile PROF reverse-route ! interface GigabitEthernet0/0/0 ip vrf forwarding fvrf ip address 192.0.2.1 255.255.255.0 ! interface GigabitEthernet0/0/1 ip vrf forwarding ivrf ip address 192.168.1.1 255.255.255.0 ! ip access-list extended CACL

Crypto map – IKEv1	VTI – IKEv1
! ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2 ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2 ! ip access-list extended CACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 Router B: ip vrf fvrf ip vrf ivrf ! crypto keyring KEY vrf fvrf pre-shared-key address 192.0.2.1 key cisco123 ! crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp profile PROF vrf ivrf keyring KEY match identity address 192.0.2.1 255.255.255.255 fvrf ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto map CMAP 10 ipsec-isakmp set peer 192.0.2.1 set transform-set TSET set isakmp-profile PROF match address CACL ! interface GigabitEthernet0/0/0 ip vrf forwarding fvrf ip address 192.0.2.2 255.255.255.0 crypto map CMAP ! interface GigabitEthernet0/0/1 ip vrf forwarding ivrf ip address 192.168.2.1 255.255.255.0 ! ip route vrf ivrf 172.16.1.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.1 ip route vrf ivrf 192.168.1.0 255.255.255.0	permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! interface tunnel0 ip vrf forwarding ivrf ip address 100.0.2.1 255.255.255.252 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel destination 192.0.2.2 tunnel vrf fvrf tunnel protection ipsec policy ipv4 CACL tunnel protection ipsec profile PROF Router B: ! remain with old configuration

Crypto map - IKEv1	VTI - IKEv1
GigabitEthernet0/0/0 192.0.2.1 ! ip access-list extended CACL permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255	

2.6 Migrate dynamic crypto map to dynamic VTI

Dynamic crypto map	DVTI
crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! ip access-list extended SiteB permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ! crypto map VPN 1 ipsec-isakmp dynamic HQ ! crypto dynamic-map HQ 10 set security-association lifetime seconds 86400 set transform-set TSET match address SiteB ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 crypto map VPN	crypto isakmp policy 10 encryption aes hash sha256 authentication pre-share group 14 ! crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 ! crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac ! crypto isakmp profile VPN keyring default match identity address 0.0.0.0 virtual-template 1 ! crypto ipsec profile TP set transform-set TSET set isakmp-profile VPN ! interface GigabitEthernet0/0/0 ip address 192.0.2.2 255.255.255.0 ! interface Virtual-Template1 type tunnel ip unnumbered Loopback1 tunnel source GigabitEthernet0/0/0 tunnel mode ipsec ipv4 tunnel protection ipsec profile TP

2.7 Migration when crypto map ACL use protocol or deny entries

There are cases where, instead of matching on an IP subnet, the crypto map ACL uses the match protocol (tcp, udp, icmp). In that scenario, IKEv2 routing will not work, and the ACL will have deny entries. In such cases, the migration plan is to enable Policy-Based Routing (PBR) on the LAN-facing interface, where the traffic that passed the ACL classification will be routed to the VTI, and other traffic will follow the default routing decision.

Crypto map ACL match protocol	VTI w/ PBR on LAN

`crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac`
`  mode tunnel`
`!`
`crypto map CMAP 10 ipsec-isakmp`
`  set peer 170.69.8.2`
`  set transform-set TSET`
`  set ikev2-profile PROF`
`  match address CACL`
`!`
`interface GigabitEthernet0/0/0`
`  description Connected to Internet`
`  ip address 209.22.2.21 255.255.255.224`
`  negotiation auto`
`  crypto map CMAP`
`!`
`interface GigabitEthernet0/0/1`
`  description Connected to LAN`
`  ip address 10.12.4.11 255.255.255.224`
`  negotiation auto`
`!`
`ip access-list extended CACL`
`  permit tcp host 10.12.100.111 host 192.240.110.98 eq 22`
`  permit icmp host 10.12.100.111 host 192.240.110.98`
`  permit tcp host 192.240.110.98 host 10.12.100.111 eq 22`
`  permit icmp host 192.240.110.98 host 10.12.100.111`
	`crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac`
	`!`
	`crypto ipsec profile PROF`
	`  set transform-set TSET`
	`  set ikev2-profile PROF`
	`!`
	`route-map PBR2VTI permit 110`
	`  match ip address CACL`
	`  set interface tunnel0`
	`!`
	`ip access-list extended CACL`
	`  permit tcp host 10.12.100.111 host 192.240.110.98 eq 22`
	`  permit icmp host 10.12.100.111 host 192.240.110.98`
	`  permit tcp host 192.240.110.98 host 10.12.100.111 eq 22`
	`  permit icmp host 192.240.110.98 host 10.12.100.111`
	`!`
	`interface GigabitEthernet0/0/0`
	`  description Connected to Internet`
	`  ip address 209.221.12.21 255.255.255.224`
	`  negotiation auto`
	`!`
	`interface GigabitEthernet0/0/1`
	`  description Connected to LAN`
	`  ip address 10.12.4.11 255.255.255.224`
	`  ip policy route-map PBR2VTI`
	`  negotiation auto`
	`!`
	`interface Tunnel0`
	`  ip  address 100.0.2.1 255.255.255.252`
	`  tunnel source GigabitEthernet0/0/0`
	`  tunnel mode ipsec ipv4`
	`  tunnel destination 170.69.8.2`
	`  tunnel protection ipsec profile PROF`

Crypto map ACL deny entries	VTI w/ PBR on LAN

`crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac`
`  mode tunnel`
`!`
`crypto map CMAP 10 ipsec-isakmp`
`  set peer 170.69.8.2`
`  set transform-set TSET`
`  set ikev2-profile PROF`
`  match address CACL`
`!`
`interface GigabitEthernet0/0/0`
`  description Connected to Internet`
`  ip address 209.22.2.21 255.255.255.224`
`  negotiation auto`
`  crypto map CMAP`
`!`
`interface GigabitEthernet0/0/1`
`  description Connected to LAN`
`  ip address 10.12.4.11 255.255.255.224`
`  negotiation auto`
`!`
`ip access-list extended CACL`
`  remark ** TCP exclusions **`
`  deny  tcp any any eq 1494`
`  deny  tcp any any eq 2598`
`  deny  tcp any any eq 22`
`  deny  tcp any eq 1494 any`
`  deny  tcp any eq 2598 any`
`  deny  tcp any eq 22 any`
`  remark ** Encrypted all other IP **`
`  permit ip any any`
	`crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac`
	`!`
	`crypto ipsec profile PROF`
	`  set transform-set TSET`
	`  set ikev2-profile PROF`
	`!`
	`route-map PBR2VTI permit 110`
	`  match ip address CACL`
	`  set interface tunnel0`
	`!`
	`ip access-list extended CACL`
	`  remark ** TCP exclusions **`
	`  deny  tcp any any eq 1494`
	`  deny  tcp any any eq 2598`
	`  deny  tcp any any eq 22`
	`  deny  tcp any eq 1494 any`
	`  deny  tcp any eq 2598 any`
	`  deny  tcp any eq 22 any`
	`  remark ** Encrypted all other IP **`
	`  permit ip any any`
	`!`
	`interface GigabitEthernet0/0/0`
	`  description Connected to Internet`
	`  ip address 209.221.12.21 255.255.255.224`
	`  negotiation auto`
	`!`
	`interface GigabitEthernet0/0/1`
	`  description Connected to LAN`
	`  ip address 10.12.4.11 255.255.255.224`
	`  ip policy route-map PBR2VTI`
	`  negotiation auto`
	`!`
	`interface Tunnel0`
	`  ip  address 100.0.2.1 255.255.255.252`
	`  tunnel source GigabitEthernet0/0/0`
	`  tunnel mode ipsec ipv4`
	`  tunnel destination 170.69.8.2`
	`  tunnel protection ipsec profile PROF`

3. Migration considerations

3.1 Be fully aware of existing restrictions on crypto map

- This migration is applicable to the Static Crypto Map and Dynamic Crypto Map, but not to the GDOI Crypto Map, which is used by GETVPN.
- Crypto map is not supported on Bridge Domain Interfaces (BDIs).
- Crypto map is not supported on tunnel interfaces. As an exception, crypto map for GDOI is supported on tunnel interfaces.
- Crypto map is not supported on a port-channel interface.
- Cryoto map is not supported on a VASI interface.
- If a transport profile is enabled on a tunnel, crypto map is not supported on the tunnel source interfaces.
- Crypto map is not supported on a tunnel interface of Multilink Frame Relay.
- Crypto map is not supported on loopback interfaces.
- Crypto maps are not supported on VASI interfaces. As an exception, crypto maps for GDOI are supported on VASI interfaces.
- Tunnel interfaces with tunnel protection sourced from an interface that has crypto map are not supported:

```
interface Tunnel1
 tunnel source GigabitEthernet0/0/0
 tunnel protection ipsec profile TAC
!
interface GigabitEthernet0/0/0
 crypto map CMAP
```

3.2 Dual stack consideration

Dual stack is possible with crypto maps. Use two different crypto maps, one for IPv4 and one for IPv6, then apply both crypto maps on the interface:

```
interface GigabitEthernet0/0/0
 crypto map CMAP1
 ipv6 crypto map CMAP2
```

The IPsec mixed mode support for VTI and DVTI provides support for carrying IPv4 traffic over IPv6 transport or IPv6 traffic over IPv4 transport. This implementation does not support using a single IPsec Security Association (SA) pair for both IPv4 and IPv6 traffic:

```
interface Tunnel0
 tunnel mode ipsec ipv4 v6-overlay
or
 tunnel mode ipsec ipv6 v4-overlay
```

In DVI configuration:

```
crypto ipsec profile dVTI_profile
 set mixed-mode
```

For true dual stack support, the recommendation is to deploy Cisco FlexVPN, which supports dual stack FlexVPN over IPv4 or IPv6 transport.

3.3 High availability

Static Crypto Map (SCM) or Dynamic Crypto Map (DCM) IPsec high availability (SCM or DCM IPsec HA) may have been deployed with Reverse Route Injection (RRI) and Hot Standby Router Protocol (HSRP). The migration path for such deployments is FlexVPN HA Dual Hub design.

3.4 Scalability

Be aware of scalability differences for SCM and VTI on the platform you plan to migrate. There are platforms that may claim to support up to 8000 IPsec sessions with SCM, but only 4000 IPsec VTI tunnels. It is recommended to migrate to FlexVPN, which is designed to support high scale deployments; up to 10,000 FlexVPN (IKEv2/DVTI) tunnels can be supported. DCM can only scale up to 500 IPsec sessions; migrating to FlexVPN will provide a significant scalability improvement for the deployment.

3.5 Crypto map on a physical source interface of a tunnel-protection interface

In Cisco IOS XE, we do not support having a crypto map on a physical source interface of a tunnel protection interface. In classic Cisco IOS®, it is fully supported.

```
interface Tunnel1
  tunnel source GigabitEthernet0/0/0
  tunnel protection ipsec profile PROF
!
interface GigabitEthernet0/0/0
   crypto map CMAP
```

In such a configuration, a third-party device cannot use a VTI. An incoming packet should go onto physical or tunnel interface. What is to be expected? The answer is to look specifically at the ACL; if the packet matches on the physical ACL, as well as with the Security Parameter Index (SPI), the packet will be encrypted over the crypto map IPsec session; if not, the packet will be encrypted over the tunnel interface if the tunnel SPI picks it up. With Cisco IOS XE Release16.12, such a configuration can be migrated to multi-SA VTIs.

4. Conclusion

We have made everything possible to help you transition from your current SCM and DCM environment. Multi-SA VTI is a replacement for a crypto map based (or policy based) virtual private network configuration. It is backward compatible with crypto-map-based and other policy-based implementations. Support for this feature is available from Cisco IOS XE Release 16.12.

While you work that way in backward-compatibility mode, you know you're safe and can start exploring new VPN technology, such as FlexVPN, which is the new, unified VPN solution offered by Cisco. FlexVPN takes advantage of the IKEv2 protocol and combines remote access, site-to-site, hub and spoke, and partial mesh VPN deployments.

So, whenever you feel comfortable, you can make the switch.

Welcome to the VTI and FlexVPN.

References

IPsec Virtual Tunnel Interfaces

Configuring Security for VPN with IPsec

FlexVPN HA Dual Hub Configuration Example

FlexVPN Site-to-Site Configuration Example

FlexVPN VRF-Aware Remote Access Configuration Example

EIGRP on SVTI, DVTI, and IKEv2 FlexVPN with the " IP[v6] Unnumbered" Command Configuration Example

End-of-Sale and End-of-Life Announcement for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map Feature in IOS XE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-744879-00 03/21