Configure a Multi-SA Virtual Tunnel Interface on a Cisco IOS XE Router

Contents

Introduction

This document describes how to configure a multi-security association (Multi-SA) Virtual Tunnel Interface (VTI) on Cisco routers with Cisco IOS® XE software. The migration process is also described. Multi-SA VTI is a replacement for the crypto map-based (policy-based) VPN configuration. It is backwards compatible with crypto map-based and other policy-based implementations. Support for this feature is available in Cisco IOS XE Release 16.12 and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of an IPsec VPN configuration on Cisco IOS XE routers.

Components Used

The information in this document is based on an Integrated Services Router (ISR) 4351 with Cisco IOS XE Release 16.12.01a .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Advantages of VTIs over Crypto Maps

A crypto map is an output feature of the physical interface. Tunnels to different peers are configured under the same crypto map. The crypto map Access Control List (ACL) entries are used to match the traffic to be sent to a specific VPN peer. This type of configuration is also called a policy-based VPN.

In the case of VTIs, each VPN tunnel is represented by a separate logical tunnel interface. The routing table decides to which VPN peer the traffic is sent. This type of configuration is also called a route-based VPN.

In releases earlier than Cisco IOS XE Release 16.12, the VTI configuration was not compatible with the crypto map configuration. Both ends of the tunnel had to be configured with the same type of VPN in order to interoperate.

In Cisco IOS XE Release 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 properties of the tunnel interface.

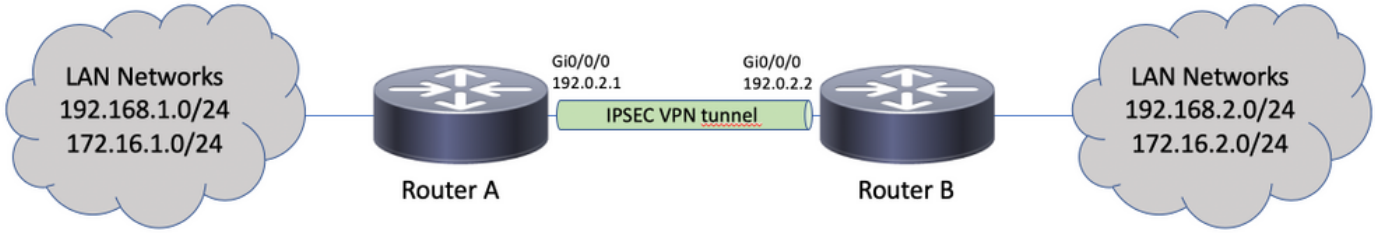
Cisco announced the end-of-life dates for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map feature in Cisco IOS XE Release 17.6.

The advantages of VTI over crypto map include:

- It is easier to determine the tunnel up/down status.
- It is easier to troubleshoot.
- It has the ability to apply features like Quality of Service (QoS), Zone-Based Firewall (ZBF), Network Address Translation (NAT), and Netflow on a per-tunnel basis.
- It has a streamlined configuration for all types of VPN tunnels.

Configure

Network Diagram



Routing Considerations

The administrator must ensure that the routing for remote networks points towards the tunnel interface. The **reverse-route** option under the IPsec profile can be used to automatically create static routes for the networks specified in the crypto ACL. Such routes can also be added manually. If

there are previously configured more specific routes, that point towards a physical interface instead of the tunnel interface, these must be removed.

Configuration Examples

Migration of a Crypto Map-Based IKEv1 Tunnel to a Multi-SA sVTI

Both routers are preconfigured with the Internet Key Exchange Version 1 (IKEv1) crypto map-based solution:

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
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
```

In order to migrate Router A to a multi-SA VTI configuration, complete these steps. Router B can remain with the old configuration or it can be reconfigured similarly:

1. Remove the crypto map from the interface:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Create the IPsec profile. Reverse-route is optionally configured to have the static routes for remote networks automatically added to the routing table:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configure the tunnel interface. The crypto ACL is attached to the tunnel configuration as an IPsec policy. The IP address configured on the tunnel interface is irrelevant, but it must be configured with some value. The IP address can be borrowed from the physical interface with the **ip unnumbered** command:
   ```
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   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
   ```
4. The crypto map entry can be removed completely afterwards:
   ```
   no crypto map CMAP 10
   ```

   Final Router A Configuration

   ```
   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
   !
   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 unnumbered GigabitEthernet0/0/0
   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
   ```

Migration of a Crypto Map Based IKEv2 Tunnel to a Multi-SA sVTI

Both routers are preconfigured with the Internet Key Exchange Version 2 (IKEv2) crypto map-

based solution:

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
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
```

In order to migrate Router A to a multi-SA VTI configuration, complete these steps. Router B can remain with the old configuration or it can be reconfigured similarly.

1. Remove the crypto map from the interface:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Create the IPsec profile. The **reverse-route** command is optionally configured to have the static routes for remote networks automatically added to the routing table:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
   reverse-route
   ```

3. Configure the tunnel interface. The crypto ACL is attached to the tunnel configuration as an IPsec policy. The IP address configured on the tunnel interface is irrelevant, but it must be configured with some value. The IP address can be borrowed from the physical interface with the **ip unnumbered** command:

```
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
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
```

4. Remove the crypto map completely afterwards:

```
no crypto map CMAP 10
```

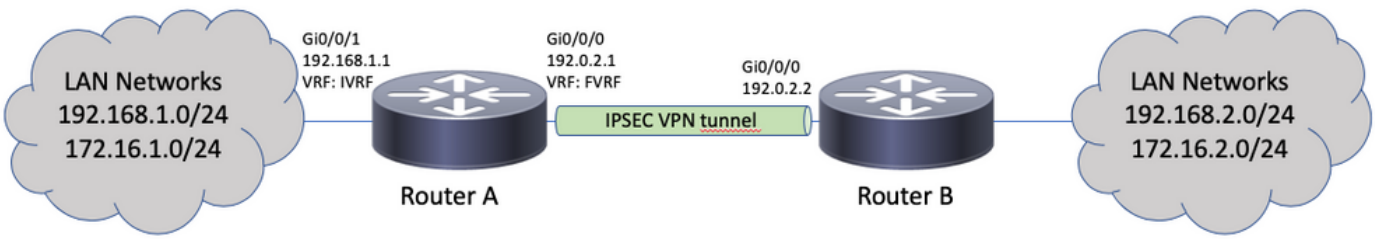
Final Router A Configuration

```
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 unnumbered GigabitEthernet0/0/0
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
```

Migration of a VRF-Aware Crypto Map to a Multi-SA VTI

This example shows how to migrate the VRF-aware crypto map configuration.

Topology



Crypto Map Configuration

```
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
!
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
```

These are the steps required to migrate to multi-SA VTI:

```
! vrf configuration under isakmp profile is only for crypto map based configuration
!
crypto isakmp profile PROF
no vrf ivrf
!
interface GigabitEthernet0/0/0
no crypto map
!
no crypto map CMAP 10
!
no ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
no ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
```

```
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
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
```

Final VRF-Aware Configuration

```
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
!
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
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 ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
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
```

Verify

Use this section in order to confirm that your configuration works properly.

The Cisco CLI Analyzer (registered customers only) supports certain **show** commands. Use the

Cisco CLI Analyzer in order to view an analysis of **show** command output.

In order to verify if the tunnel has been negotiated successfully, the tunnel interface status can be checked. The last two columns - Status and Protocol - show a status of up when the tunnel is operational:

```
RouterA#show ip interface brief | include Interface|Tunnel0
Interface IP-Address OK? Method Status Protocol
Tunnel0 192.0.2.1 YES TFTP up                    up
```

More details about the current crypto session status can be found in the **show crypto session** output. The Session status of UP-ACTIVE indicates that the IKE session has been negotiated properly:

```
RouterA#show crypto session interface tunnel0
Crypto session current status

Interface: Tunnel0
Profile: PROF
Session status: UP-ACTIVE
Peer: 192.0.2.2 port 500
Session ID: 2
IKEv2 SA: local 192.0.2.1/500 remote 192.0.2.2/500 Active
IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 172.16.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

Verify that the routing to the remote network points over the correct tunnel interface:

```
RouterA#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Tunnel0
Route metric is 0, traffic share count is 1

RouterA#show ip cef 192.168.2.100
192.168.2.0/24
attached to Tunnel0
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

In order to troubleshoot the IKE protocol negotiation, use these debugs:

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands.

```
! For IKEv1-based scenarios:
debug crypto isakmp
debug crypto ipsec

! For IKEv2-based scenarios:
debug crypto ikev2
debug crypto ipsec
```

Frequently Asked Questions

Does the tunnel come up automatically or is traffic needed to bring up the tunnel?

Unlike with crypto maps, the multi-SA VTI tunnels come up automatically regardless of whether data traffic that matches the crypto ACL flows over the router or not. The tunnels stay up all the time, even if there is no interesting traffic.

What happens if traffic is routed through the VTI, but the source or destination of the traffic does not match the crypto ACL configured as an IPsec policy for this tunnel?

Such a scenario is not supported. Only the traffic intended to be encrypted must be routed to the tunnel interface. Policy-based routing (PBR) can be used to route only specific traffic to the VTI. PBR can use the IPsec policy ACL to match the traffic to be routed to the VTI.

Each packet is checked against the configured IPsec policy and must match the crypto ACL. If it does not match, it is not encrypted and is sent in clear text out of the tunnel source interface.

In case the same internal VRF (iVRF) and front VRF (fVRF) is used (iVRF = fVRF), this results in a routing loop and the packets are dropped with a reason **Ipv4RoutingErr**. Statistics for such drops can be seen with the **show platform hardware qfp active statistics drop** command:

```
RouterA#show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

---------------------------------------------------------------------
Global Drop Stats Packets Octets
---------------------------------------------------------------------
Ipv4RoutingErr 5 500
```

In case iVRF is different than fVRF, the packets that enter the tunnel in iVRF, and do not match the IPsec policy, exit the tunnel source interface in fVRF in clear text. They are not dropped, as there is no routing loop between the VRFs.

Are features like VRF, NAT, QoS, and so on, supported on multi-SA VTI?

Yes, all of those features are supported the same way as on regular VTI tunnels.