Configure Multi-SA Virtual Tunnel Interface on IOS-XE router

Content

Introduction
Prerequisites
Requirements
Components Used
Advantages of Virtual Tunnel Interfaces over Crypto maps
Configure
Network Diagram
Configurations
IKEv1
IKEv2
Routing considerations
VRF-aware configuration
Verify
Frequently Asked Questions
Troubleshoot

Introduction

This document describes how to configure multi security association Virtual Tunnel Interface on IOS-XE router. Migration process is also described. Multi-SA VTI is a replacement for crypto map based (policy based) virtual private network configuration. It is backwards compatible with crypto map based and other policy based implementations. Support for this features is available since IOS-XE 16.12 release.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IPsec Virtual Private Network configuration on IOS-XE routers

Components Used

The information in this document is based on ISR 4351 routers running IOS-XE 16.12.01a software version.

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.
Advantages of Virtual Tunnel Interfaces over Crypto maps

Crypto map is an output feature of physical interface. Tunnels to different peers are configured under the same crypto map. Access-list entries specify to which peer traffic should be sent to. This type of configuration is also called policy-based VPN.

If Virtual Tunnel Interfaces are utilized, each VPN tunnel is represented by a separate logical tunnel interface. Routing table decides to which peer traffic should be sent to. This type of configuration is also called route-based VPN.

Prior to IOS-XE 16.12 release, the VTI configuration was not compatible with 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 policy-based VPN on the protocol level, but have all properties of tunnel interface.

The advantages of VTI over crypto map include:

- Easier to determine tunnel up/down status
- Easier to troubleshoot
- Ability to apply features like QoS, ZBF, NAT, Netflow on a per-tunnel basis
- Streamlined configuration for all types of VPN tunnels

Configure

Network Diagram

![Network Diagram](image)

Configurations

IKEv1

Both routers are preconfigured with IKEv1 crypto map based solution:

Router A:

crypto isakmp policy 10
cipher aes
hash sha256
authentication pre-share
group 14
In order to migrate the Router A to a multi-SA VTI configuration, the following must be configured:

Router B can remain with old configuraion or can be reconfigured similarly:

1. Remove the crypto map from the interface:

interface GigabitEthernet0/0/0
no crypto map

2. Create 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 tunnel interface. Crypto access-list is attached to the tunnel configuration as ipsec policy. IP address configured on the tunnel interface is irrelevant but it must be configured with some value. IP address can be borrowed from physical interface using "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. Crypto map 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

IKEv2

Both routers are preconfigured with 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
!
In order to migrate the Router A to a multi-SA VTI configuration, the following must be configured. Router B can remain with old configuration or can be reconfigured similarly:

1. Remove the crypto map from the interface:

```
interface GigabitEthernet0/0/0
no crypto map
```

2. Create 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
set ikev2-profile PROF
reverse-route
```

3. Configure tunnel interface. Crypto access-list is attached to the tunnel configuration as ipsec policy. IP address configured on the tunnel interface is irrelevant but it must be configured with some value. IP address can be borrowed from physical interface using "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. Crypto map can be removed 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

**Routing considerations**

Administrator must ensure that the routing for remote networks is pointing towards the tunnel interface. "Reverse-route" option under ipsec profile can be used to automatically create static routes for networks specified in the crypto ACL. Such routes can also be added manually. If there were preexisting more specific routes pointing towards physical interface instead of tunnel interface, these must be removed.

**VRF-aware configuration**

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

**Topology**
Crypto map configuration:

```
ip vrf fvrf

! 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
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip route vrf fvrf 192.168.1.1 255.255.255.0 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
```

In order to migrate to multi-SA VTI, the following steps must be performed:

```
!
! 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

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" columns - should indicated "up" status:

RouterA#show ip interface brief | i Tunnel0
Tunnel0 192.0.2.1 YES TFTP up up

More details about current crypto session status can be found in "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

Frequently Asked Questions

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

A: Unlike with crypto maps, the multi-SA VTI tunnels come up automatically regardless of whether data traffic matching the crypto ACL is currently being routed. The tunnels stay up all the time even if the traffic stops flowing.

Q: 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 ipsec policy for this tunnel?

A: Such traffic will be dropped. Each packet is checked against the configured ipsec policy and must match the crypto ACL. The reason for such drop is registered as "Ipv4RoutingErr". Statistics for such drops can be found through the following command:
RouterA#show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

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

Q: Are features like VRF, NAT, QoS etc. supported on multi-SA VTI?

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

**Troubleshoot**

In order to troubleshoot the IKE protocol negotiation, the following debugs can be used:

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

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