

Configure IPsec and GRE in the Same Tunnel Interface on XE SD-WAN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Use Cases](#)

[Scenario 1](#)

[Scenario 2](#)

[Configuration](#)

[Via vManage Feature template](#)

[Via CLI](#)

[Verification](#)

[Related Information](#)

Introduction

This document describes the configuration to enable IPsec and GRE encapsulation for the same tunnel interface on a Cisco IOS XE® SD-WAN Router.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco SD-WAN
- Basic Cisco IOS-XE Command Line Interface (CLI)

Components Used

This document is based on these software and hardware versions:

- C8000V version 17.6.2

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

Cisco IOS-XE SD-WAN Routers need at least one encapsulation; Internet Protocol Security (IPsec) or Generic Routing Encapsulation (GRE) for each tunnel interface.

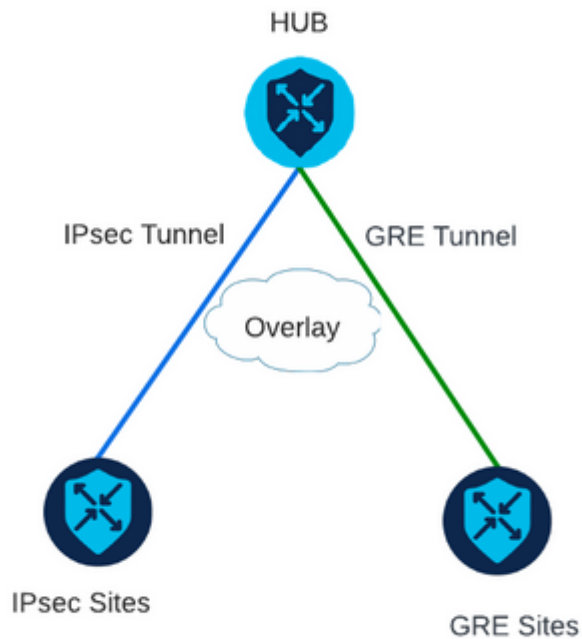
There are use cases when both encapsulations are needed.

Use Cases

Scenario 1

In this scenario, there is a Hub with one transport and both encapsulations for the same tunnel interface.

This creates two TLOCs and permits to form tunnels with remote edge devices that only use IPsec and remote edge devices that only use GRE.



Scenario 2

In this scenario, there are two edge devices with one transport. This transport is configured with both encapsulation on both endpoints.

This is useful if there is traffic that needs to be sent via GRE and traffic to be sent via IPsec.









Configuration

This configuration can be performed through the router CLI or through a vManage feature template.

Via vManage Feature template

On the Cisco VPN Interface Ethernet feature template for VPN 0, navigate to **Tunnel > Advanced Options > Encapsulation** and turn **On GRE** and **IPsec**:

[Feature Template](#) > [Cisco VPN Interface Ethernet](#) > VPN-0-INTERFACE_cEdge

Basic Configuration	<u>Tunnel</u>	NAT	VRRP	ACL/QoS	ARP
Encapsulation					
GRE		<input checked="" type="radio"/> On	<input type="radio"/> Off		
Preference					
Weight		1			
IPsec		<input checked="" type="radio"/> On	<input type="radio"/> Off		
Preference					
Weight		1			

Via CLI

Configure the tunnel interface with both encapsulations on both cEdge devices:

```
<#root>
```

```
sdwan
```

```
interface <WAN Interface>  
  tunnel-interface
```

```
  encapsulation gre
```

```
  encapsulation ipsec
```

Verification

Verify the state of the control connections with the verification commands.

```
show sdwan omp tlocs table | i <system-ip>
show sdwan bfd sessions
```

Example for Scenario 2:

Verify the TLOCs are redistributed into OMP:

```
Edge_A#show sdwan omp tlocs table | i 10.2.2.2
ipv4 10.2.2.2 mpls gre 0.0.0.0 C,Red,R 1 172.16.1.30 0 172.16.1.30 0 :: 0 :: 0
      10.2.2.2 mpls ipsec 0.0.0.0 C,Red,R 1 172.16.1.30 12346 172.16.1.30 12346 :: 0 :: 0
```

Verify the BFD sessions to Edge_B on both TLOCs:

```
Edge_A#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	DETECT MULTIPLE
10.4.4.4	4	up	mpls	mpls	172.16.1.30	172.16.1.32	0	gre	7
10.4.4.4	4	up	mpls	mpls	172.16.1.30	172.16.1.32	12366	ipsec	7

Verify the path toward both tunnels. Use the command **show sdwan policy service path vpn <vpn-number> interface <interface> source-ip <source-ip> dest-ip <dest-ip> protocol <protocol> all**.

```
Edge_A#show sdwan policy service-path vpn 10 interface Loopback 20 source-ip 10.40.40.40 dest-ip 10.50.50.50
Number of possible next hops: 2
Next Hop: GRE
Source: 172.16.1.30 Destination: 172.16.1.32 Local Color: mpls Remote Color: mpls Remote System IP: 10.40.40.40
Next Hop: IPsec
Source: 172.16.1.30 12346 Destination: 172.16.1.32 12366 Local Color: mpls Remote Color: mpls Remote System IP: 10.40.40.40
```

Related Information

- [Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x](#)
- [Cisco SD-WAN Command Reference](#)