

XE SD-WANの同じトンネルインターフェイスでのIPsecおよびGREの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[使用例](#)

[シナリオ1](#)

[シナリオ2](#)

[コンフィギュレーション](#)

[vManage機能テンプレートを使用](#)

[CLIの場合](#)

[検証](#)

[関連情報](#)

概要

このドキュメントでは、Cisco IOS XE® SD-WANルータの同じトンネルインターフェイスでIPsecおよびGREカプセル化を有効にする設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco SD-WAN
- 基本的なCisco IOS XEコマンドラインインターフェイス(CLI)

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.6.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco IOS XE SD-WANルータには、トンネルインターフェイスごとに少なくとも1つのカプセル化、つまりInternet Protocol Security(IPsec)またはGeneric Routing Encapsulation(GRE)が必要です。

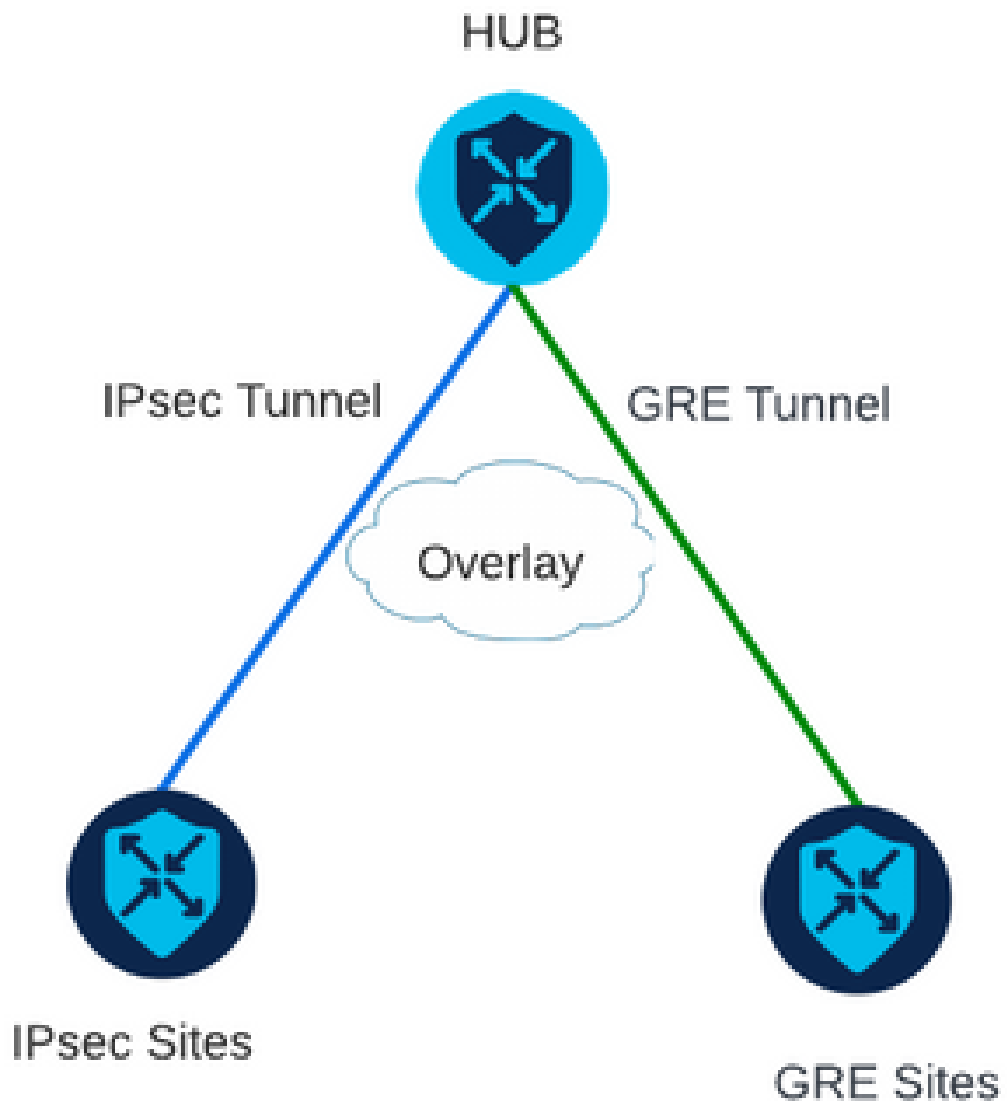
両方のカプセル化が必要になる場合があります。

使用例

シナリオ 1

このシナリオでは、同じトンネルインターフェイスに、1つのトランスポートと両方のカプセル化を持つハブがあります。

これにより、2つのTLOCが作成され、IPSecのみを使用するリモートエッジデバイスとGREのみを使用するリモートエッジデバイスとのトンネルの形成が許可されます。



シナリオ 2

このシナリオでは、1つのトランスポートを持つ2つのエッジデバイスがあります。このトランスポートは、両方のエンドポイントで両方のカプセル化を使用して設定されます。

これは、GRE経由で送信する必要があるトラフィックとIPsec経由で送信するトラフィックがある場合に便利です。



コンフィギュレーション

この設定は、ルータのCLIまたはvManage機能テンプレートを使用して実行できます。

vManage機能テンプレートを使用

VPN 0のCisco VPN Interface Ethernet機能テンプレートで、Tunnel > Advanced Options > Encapsulationの順に移動し、On GREとIPsecをオンにします。

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

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

CLI の場合

両方のcEdgeデバイスで両方のカプセル化を使用してトンネルインターフェイスを設定します。

```
<#root>
```

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

```
encapsulation gre
```

```
encapsulation ipsec
```

検証

検証コマンドを使用して、制御接続の状態を確認します。

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

シナリオ2の例：

TLOCがOMPに再配布されていることを確認します。

```
Edge_A#show sdwan omp tlocs table | i 10.2.2.2
ipv4  10.2.2.2  mp1s  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  mp1s  ipsec  0.0.0.0  C,Red,R  1  172.16.1.30  12346  172.16.1.30  12346  :: 0  :: 0
```

両方のTLOCでEdge_BへのBFDセッションを確認します。

```
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	DETE MULT
10.4.4.4	4	up	mp1s	mp1s	172.16.1.30	172.16.1.32	0	gre	7
10.4.4.4	4	up	mp1s	mp1s	172.16.1.30	172.16.1.32	12366	ipsec	7

両方のトンネルへのパスを確認します。 show sdwan policy service path vpn <vpn-number>

interface <interface> source-ip <source-ip> dest-ip <dest-ip> protocol <protocol> allコマンドを使用します。

```
Edge_A#show sdwan policy service-path vpn 10 interface Loopback 20 source-ip 10.40.40.40 dest-ip 10.50.
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.
Next Hop: IPsec
Source: 172.16.1.30 12346 Destination: 172.16.1.32 12366 Local Color: mpls Remote Color: mpls Remote Sy
```

関連情報

- [Cisco SD-WANシステムおよびインターフェイス設定ガイド、Cisco IOS XEリリース17.x](#)
- [Cisco SD-WANコマンドリファレンス](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。