Konfiguration von IPsec und GRE in derselben Tunnelschnittstelle im XE SD-WAN

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration zum Aktivieren der IPsec- und GRE-Kapselung für dieselbe Tunnelschnittstelle auf einem Cisco IOS XE® SD-WAN-Router beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco SD-WAN
- Grundlegende Cisco IOS-XE Kommandozeile

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- C8000V Version 17.6.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco IOS-XE SD-WAN-Router benötigen mindestens eine Kapselung: IPsec (Internet Protocol Security) oder GRE (Generic Routing Encapsulation) für jede Tunnelschnittstelle.

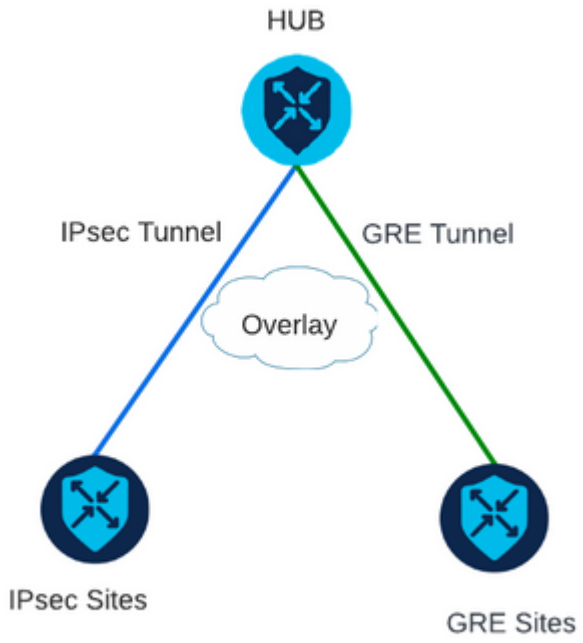
Es gibt Anwendungsfälle, in denen beide Kapselungen erforderlich sind.

Anwendungsfälle

Szenario 1

In diesem Szenario gibt es einen Hub mit einem Transport und beiden Kapselungen für die gleiche Tunnelschnittstelle.

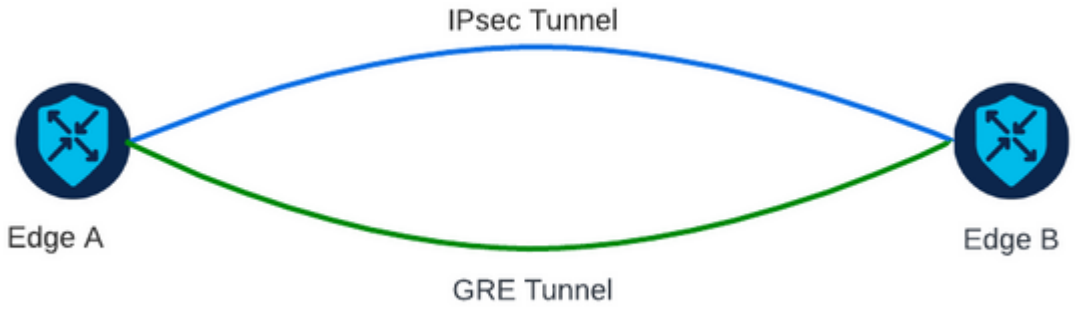
Dadurch werden zwei TLOCs erstellt, und es können Tunnel mit Remote-Edge-Geräten erstellt werden, die nur IPSec verwenden, und mit Remote-Edge-Geräten, die nur GRE verwenden.



Szenario 2

In diesem Szenario gibt es zwei Edge-Geräte mit einem Transport. Dieser Transport wird mit beiden Kapselungen auf beiden Endpunkten konfiguriert.

Dies ist nützlich, wenn Datenverkehr über GRE und Datenverkehr über IPsec gesendet werden muss.

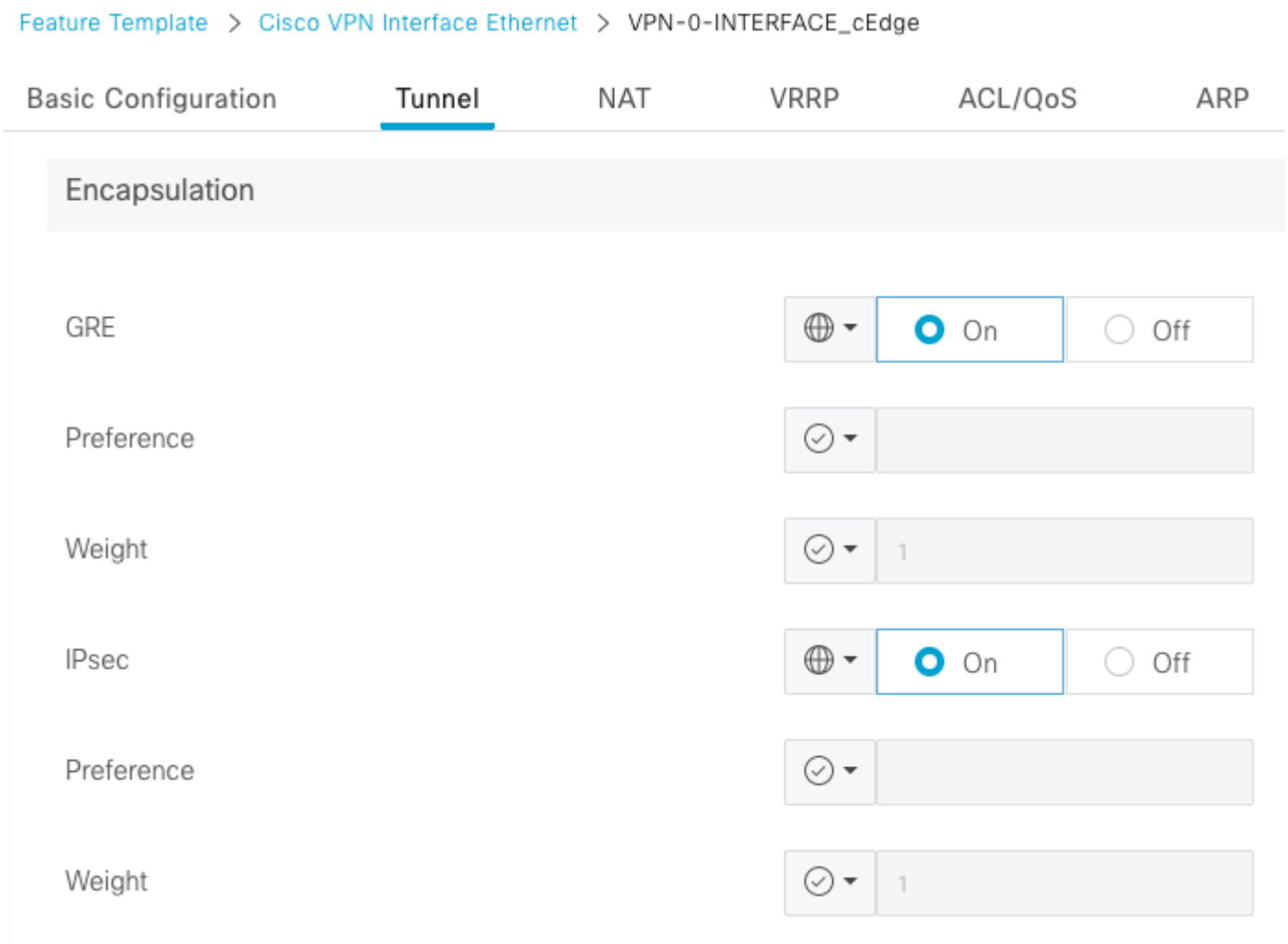


Konfiguration

Diese Konfiguration kann über die Router-CLI oder eine vManage-Funktionsvorlage vorgenommen werden.

Über vManage-Funktionsvorlage

Navigieren Sie in der Cisco VPN Interface Ethernet-Funktionsvorlage für VPN 0 zu **Tunnel > Advanced Options > Encapsulation,** und aktivieren Sie **GRE** und **IPsec**:



Über CLI

Konfigurieren Sie die Tunnelschnittstelle mit beiden Kapselungen auf beiden cEdge-Geräten:

<#root>

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

 encapsulation gre


   encapsulation ipsec
```

Verifizierung

Überprüfen Sie mit den Prüfbefehlen den Zustand der Steuerungsanschlüsse.

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

Beispiel für Szenario 2:

Überprüfen Sie, ob die TLOCs in OMP umverteilt werden:

```
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
```

Überprüfen Sie die BFD-Sitzungen mit Edge_B auf beiden TLOCs:

```
Edge_A#show sdwan bfd sessions
                           SOURCE TLOC  REMOTE TLOC              DST PUBLIC   DST PUBLIC         DETEC
SYSTEM IP    SITE ID  STATE  COLOR        COLOR       SOURCE IP    IP           PORT        ENCAP  MULTI
-------------------------------------------------------------------------------------------------------
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
```

Überprüfen Sie den Pfad zu beiden Tunneln. Verwenden Sie den Befehl **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 10.50.5
```

```
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: 10.4
Next Hop: IPsec
Source: 172.16.1.30 12346 Destination: 172.16.1.32 12366 Local Color: mpls Remote Color: mpls Remote Sys
```

Zugehörige Informationen

- Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Version 17.x
- Cisco SD-WAN-Befehlsreferenz

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.