L2TPv3 over FlexVPN-configuratiegids

Inhoud

Inleiding

Dit document beschrijft hoe u een Layer 2 Tunneling Protocol, versie 3 (L2TPv3)-link kunt configureren om een Cisco IOS FlexVPN Virtual Tunnel Interface (VTI)-verbinding tussen twee routers die Cisco IOS® software uitvoeren. Dankzij deze technologie kunnen Layer 2-netwerken veilig worden uitgebreid binnen een IPsec-tunnel boven meerdere laag 3-poorten, waardoor fysieke afzonderlijke apparaten op hetzelfde lokale LAN kunnen lijken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS FlexVPN Virtual Tunnel Interface (VTI)
- Layer 2 Tunneling Protocol (L2TP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco geïntegreerde services router Generation 2 (G2), met de security en gegevenslicentie.
- Cisco IOS release 15.1(1)T of hoger om FlexVPN te ondersteunen. Raadpleeg de Cisco Functie Navigator voor meer informatie.

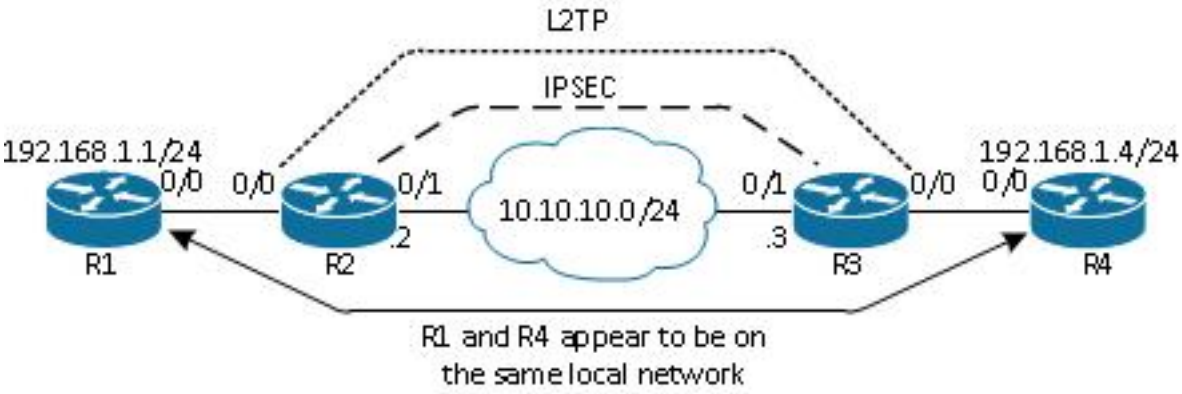
Deze FlexVPN-configuratie maakt gebruik van slimme standaardinstellingen en pre-Shared Key authenticatie om de verklaring te vereenvoudigen. Gebruik encryptie van de volgende generatie voor een maximale beveiliging; Raadpleeg de next-generation encryptie voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerktopologie

Deze configuratie gebruikt de topologie in dit beeld. Verandert IP-adressen waar dit nodig is voor uw installatie.



> Opmerking: In deze opstelling worden de routers R2 en R3 direct verbonden, maar zij zouden door vele sprongen kunnen worden gescheiden. Als de routers R2 en R3 worden gescheiden, zorg er dan voor dat er een route is om naar het IP-adres van de peer te gaan.

router R1

router R1 heeft een IP adres ingesteld op de interface:

```
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
```

router R2

FlexVPN

Deze procedure vormt FlexVPN op router R2.

1. Maak een Internet Key Exchange Versie 2 (IKEv2)-toets voor de peer:

```
crypto ikev2 keyring key1
 peer 10.10.10.3
 address 10.10.10.3
 pre-shared-key ciscol
```

2. Maak een IKEv2 standaard profiel dat overeenkomt met de peer router en gebruik van pre-Shared-key verificatie:

```
crypto ikev2 profile default
 match identity remote address 10.10.10.3 255.255.255.255
 identity local address 10.10.10.2
 authentication remote pre-share
 authentication local pre-share
 keyring local key1
```

3. Maak het VTI en bescherm het met het standaardprofiel:

```
interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 tunnel source 10.10.10.2
 tunnel destination 10.10.10.3
 tunnel protection ipsec profile default
```

L2TPv3

Deze procedure vormt L2TPv3 op router R2.

1. Maak een pseudodraadklasse om de insluiting (L2TPv3) te definiëren en de FlexVPN tunnelinterface te definiëren die de L2TPv3 verbinding gebruikt om de peer router te bereiken:

```
pseudowire-class l2tp1
 encapsulation l2tpv3
 ip local interface Tunnel1
```

2. Gebruik de verbindingsopdracht op de relevante interface om de L2TP-tunnel te configureren; geef het peer adres van de tunnelinterface op en specificeer het insluitingstype:

```
interface Ethernet0/0
 no ip address
 xconnect 172.16.1.3 1001 encapsulation l2tpv3 pw-class l2tp1
```

router R3

FlexVPN

Deze procedure vormt FlexVPN op router R3.

1. Maak een IKEv2-toets voor de peer:

```
crypto ikev2 keyring key1
 peer 10.10.10.2
 address 10.10.10.2
 pre-shared-key cisco
```

2. Maak een IKEv2-standaardprofiel dat overeenkomt met de peer router en gebruik van pre-Shared-key verificatie:

```
crypto ikev2 profile default
 match identity remote address 10.10.10.2 255.255.255.255
 identity local address 10.10.10.3
 authentication remote pre-share
 authentication local pre-share
 keyring local key1
```

3. Maak het VTI en bescherm het met het standaardprofiel:

```
interface Tunnel1
 ip address 172.16.1.3 255.255.255.0
 tunnel source 10.10.10.3
 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

L2TPv3

Deze procedure vormt L2TPv3 op router R3.

1. Maak een pseudodraadklasse om de insluiting (L2TPv3) te definiëren en de FlexVPN tunnelinterface te definiëren die de L2TPv3 verbinding gebruikt om de peer router te bereiken:

```
pseudowire-class l2tp1
 encapsulation l2tpv3
 ip local interface Tunnel1
```

2. Gebruik de verbindingsopdracht op de relevante interface om de L2TP-tunnel te configureren; geef het peer adres van de tunnelinterface op en specificeer het insluitingstype:

```
interface Ethernet0/0
 no ip address
 xconnect 172.16.1.2 1001 encapsulation l2tpv3 pw-class l2tp1
```

router R4

router R4 heeft een IP adres ingesteld op de interface:

```
interface Ethernet0/0
 ip address 192.168.1.4 255.255.255.0
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer de IPsec-beveiligingsassociatie

Dit voorbeeld verifieert dat de IPsec security associatie met succes op router R2 met interface Tunnel1 is gecreëerd.

```
R2#show crypto sockets

 Number of Crypto Socket connections 1

  Tu1 Peers (local/remote): 10.10.10.2/10.10.10.3

      Local Ident  (addr/mask/port/prot): (10.10.10.2/255.255.255.255/0/47)

      Remote Ident (addr/mask/port/prot): (10.10.10.3/255.255.255.255/0/47)

      IPSec Profile: "default"

      Socket State: Open

      Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "default" Map-name: "Tunnel1-head-0"
```

Controleer de oprichting van IKEv2 SA

Dit voorbeeld verifieert dat IKEv2 security association (SA) met succes op router R2 wordt gecreëerd.

```
R2#show crypto ikev2 sa

 IPv4 Crypto IKEv2  SA

 Tunnel-id Local                 Remote                fvrf/ivrf            Status

2          10.10.10.2/500        10.10.10.3/500        none/none            READY

      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,

      Auth verify: PSK

      Life/Active Time: 86400/562 sec


 IPv6 Crypto IKEv2  SA
```

Controleer L2TPv3-tunnels

Dit voorbeeld verifieert dat L2TPv3 tunnel correct op router R2 gevormd heeft.

```
R2#show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State

 UP=Up       DN=Down             AD=Admin Down      IA=Inactive

 SB=Standby  HS=Hot Standby      RV=Recovering      NH=No Hardware


XC ST  Segment 1                         S1 Segment 2                          S2

------+---------------------------------+--+---------------------------------+--

UP pri   ac Et0/0:3(Ethernet)            UP l2tp 172.16.1.3:1001               UP
```

Controleer de R1-netwerkconnectiviteit en -aanwezigheid

Dit voorbeeld verifieert dat router R1 netwerkconnectiviteit op router R4 heeft en op hetzelfde lokale netwerk lijkt te zijn.

```
R1#ping 192.168.1.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms

R1#show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface

Internet  192.168.1.1            -   aabb.cc00.0100  ARPA   Ethernet0/0

Internet  192.168.1.4            4   aabb.cc00.0400  ARPA   Ethernet0/0


R1#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

                  D - Remote, C - CVTA, M - Two-port Mac Relay


Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

R4               Eth 0/0           142              R B   Linux Uni Eth 0/0
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen:

- **debug van crypto ikev2** - schakelt het debuggen van IKEv2 in.
- **debug xconnect gebeurtenis -** maakt het debuggen van gebeurtenissen mogelijk.
- **tonen crypto ikev2 diagnostische fout** - toon de IKEv2 exit path database.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems