L2TPv3 über FlexVPN - Konfigurationsleitfaden

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Layer 2 Tunneling Protocol Version 3 (L2TPv3)-Verbindung so konfiguriert wird, dass sie über eine Cisco IOS FlexVPN Virtual Tunnel Interface (VTI)-Verbindung zwischen zwei Routern ausgeführt wird, auf denen die Cisco IOS® Software ausgeführt wird. Mit dieser Technologie können Layer-2-Netzwerke innerhalb eines IPsec-Tunnels sicher über mehrere Layer-3-Hops erweitert werden, sodass physisch separate Geräte im selben lokalen LAN erscheinen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Integrated Services Router Generation 2 (G2) mit Sicherheits- und Datenlizenz.
- Cisco IOS Release 15.1(1)T oder höher zur Unterstützung von FlexVPN. Weitere Informationen finden Sie im Cisco Feature Navigator.

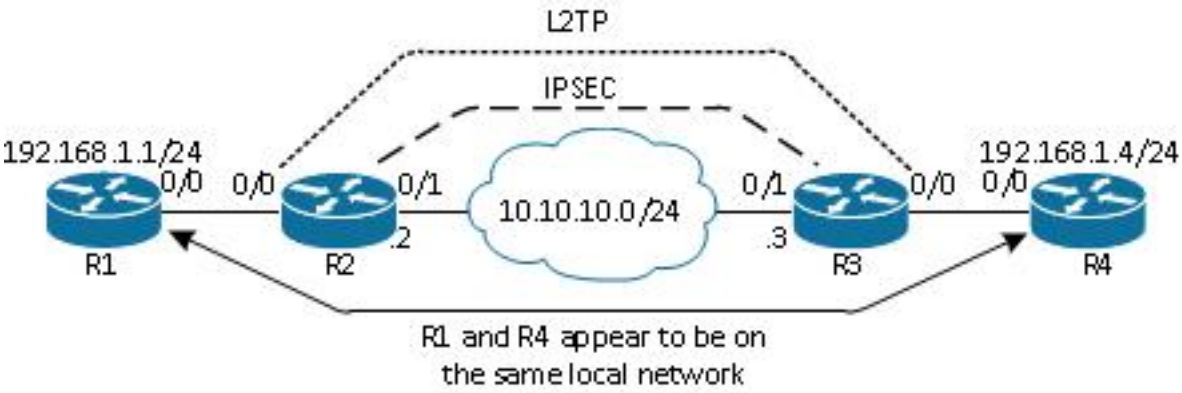
Diese FlexVPN-Konfiguration verwendet intelligente Standardeinstellungen und Pre-Shared-Key-Authentifizierung, um die Erläuterung zu vereinfachen. Verwenden Sie für maximale Sicherheit Verschlüsselungstechnologie der nächsten Generation. Weitere Informationen finden Sie unter Verschlüsselung der nächsten Generation.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerktopologie

Diese Konfiguration verwendet die Topologie in diesem Bild. Ändern Sie die IP-Adressen nach Bedarf für Ihre Installation.



> **Hinweis**: In dieser Konfiguration sind die Router R2 und R3 direkt miteinander verbunden, können aber durch viele Hops getrennt werden. Wenn die Router R2 und R3 voneinander getrennt sind, stellen Sie sicher, dass eine Route zum Peer-IP-Adresse vorhanden ist.

Router R1

Auf dem Router R1 ist eine IP-Adresse für die Schnittstelle konfiguriert:

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

Router R2

FlexVPN

Bei diesem Verfahren wird FlexVPN auf dem Router R2 konfiguriert.

1. Erstellen Sie einen Internet Key Exchange Version 2 (IKEv2)-Keyring für den Peer:

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

2. Erstellen Sie ein IKEv2-Standardprofil, das dem Peer-Router entspricht und die Pre-Shared-Key-Authentifizierung verwendet:

```
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. Erstellen Sie das VTI, und schützen Sie es mit dem Standardprofil:

```
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

Bei diesem Verfahren wird L2TPv3 auf dem Router R2 konfiguriert.

1. Erstellen Sie eine Pseudowire-Klasse, um die Kapselung (L2TPv3) zu definieren, und definieren Sie die FlexVPN-Tunnelschnittstelle, die die L2TPv3-Verbindung verwendet, um den Peer-Router zu erreichen:

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

2. Verwenden Sie den Befehl "xconnect" auf der entsprechenden Schnittstelle, um den L2TP-Tunnel zu konfigurieren. Geben Sie die Peer-Adresse der Tunnelschnittstelle an, und geben Sie den Kapselungstyp an:

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

Router R3

FlexVPN

Bei diesem Verfahren wird FlexVPN auf dem Router R3 konfiguriert.

1. Erstellen Sie einen IKEv2-Keyring für den Peer:

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

2. Erstellen Sie ein IKEv2-Standardprofil, das dem Peer-Router entspricht, und verwenden Sie die Pre-Shared-Key-Authentifizierung:

```
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. Erstellen Sie das VTI, und schützen Sie es mit dem Standardprofil:

```
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

Bei diesem Verfahren wird L2TPv3 auf dem Router R3 konfiguriert.

1. Erstellen Sie eine Pseudowire-Klasse, um die Kapselung (L2TPv3) zu definieren, und definieren Sie die FlexVPN-Tunnelschnittstelle, die die L2TPv3-Verbindung verwendet, um den Peer-Router zu erreichen:

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

2. Verwenden Sie den Befehl "xconnect" auf der entsprechenden Schnittstelle, um den L2TP-Tunnel zu konfigurieren. Geben Sie die Peer-Adresse der Tunnelschnittstelle an, und geben Sie den Kapselungstyp an:

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

Router R4

Auf dem Router R4 ist eine IP-Adresse für die Schnittstelle konfiguriert:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen der IPsec-Sicherheitszuordnung

In diesem Beispiel wird überprüft, ob die IPsec-Sicherheitszuordnung erfolgreich auf Router R2 mit Schnittstelle Tunnel1 erstellt wurde.

```
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"
```

Überprüfen der IKEv2 SA-Erstellung

In diesem Beispiel wird überprüft, ob die IKEv2-Sicherheitszuordnung (SA) erfolgreich auf Router R2 erstellt wurde.

```
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
```

Überprüfen des L2TPv3-Tunnels

In diesem Beispiel wird überprüft, ob der L2TPv3-Tunnel auf dem Router R2 korrekt geformt wurde.

```
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
```

Überprüfung der Netzwerkverbindung und -darstellung des R1

In diesem Beispiel wird überprüft, ob der Router R1 über Netzwerkverbindungen mit dem Router R4 verfügt und sich scheinbar im gleichen lokalen Netzwerk befindet.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration:

- **debug crypto ikev2** - Aktivieren des IKEv2-Debuggens.
- **debug xconnect event -** enable xconnect event debugging.
- **show crypto ikev2 diagnose error** - display the IKEv2 exit path database.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

> **Hinweis**: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems