Guida alla configurazione di L2TPv3 over FlexVPN

Sommario

Introduzione

In questo documento viene descritto come configurare un collegamento Layer 2 Tunneling Protocol versione 3 (L2TPv3) in modo che venga eseguito su una connessione Cisco IOS FlexVPN Virtual Tunnel Interface (VTI) tra due router con software Cisco IOS®. Con questa tecnologia, le reti di layer 2 possono essere estese in modo sicuro all'interno di un tunnel IPsec su più hop di layer 3, consentendo a dispositivi fisicamente separati di apparire sulla stessa LAN locale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS FlexVPN Virtual Tunnel Interface (VTI)

- L2TP (Layer 2 Tunneling Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Integrated Services Router generazione 2 (G2), con la licenza per la sicurezza e i dati.
- Cisco IOS versione 15.1(1)T o successive per supportare FlexVPN. Per ulteriori informazioni, consultare Cisco Feature Navigator.

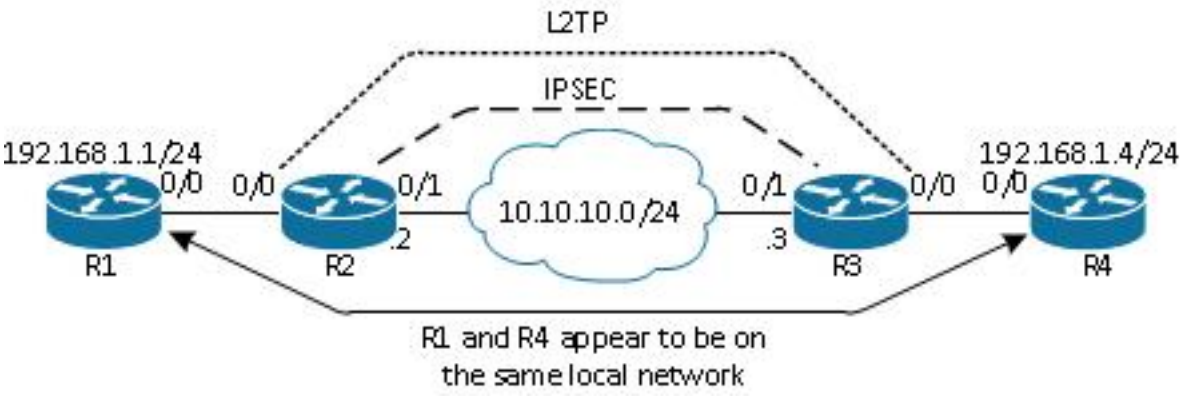
Questa configurazione di FlexVPN usa i valori predefiniti intelligenti e l'autenticazione a chiave precondivisa per semplificare la spiegazione. Per la massima protezione, utilizzare la crittografia di nuova generazione. per ulteriori informazioni, fare riferimento a Crittografia di nuova generazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Topologia della rete

Questa configurazione utilizza la topologia dell'immagine. Modificare gli indirizzi IP in base alle esigenze dell'installazione.



Nota: In questa configurazione, i router R2 e R3 sono collegati direttamente, ma potrebbero essere separati da più hop. Se i router R2 e R3 sono separati, verificare che sia disponibile una route per raggiungere l'indirizzo IP del peer.

Router R1

Il router R1 ha un indirizzo IP configurato sull'interfaccia:

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

Router R2

FlexVPN

Questa procedura consente di configurare FlexVPN sul router R2.

1. Creare un keyring di Internet Key Exchange versione 2 (IKEv2) per il peer:

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

2. Creare un profilo predefinito IKEv2 corrispondente al router peer e che utilizzi l'autenticazione con chiave già condivisa:

```
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. Creare la VTI e proteggerla con il profilo predefinito:

```
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

Questa procedura consente di configurare L2TPv3 sul router R2.

1. Creare una classe di pseudonimo per definire l'incapsulamento (L2TPv3) e definire l'interfaccia del tunnel FlexVPN usata dalla connessione L2TPv3 per raggiungere il router peer:

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

2. Per configurare il tunnel L2TP, usare il comando xconnect sull'interfaccia interessata; fornire l'indirizzo del peer dell'interfaccia del tunnel e specificare il tipo di incapsulamento:

```
interface Ethernet0/0
 no ip address
```

```
 xconnect 172.16.1.3 1001 encapsulation l2tpv3 pw-class l2tp1
```

Router R3

FlexVPN

Questa procedura consente di configurare FlexVPN sul router R3.

1. Creare un keyring IKEv2 per il peer:

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

2. Creare un profilo predefinito IKEv2 che corrisponda al router peer e utilizzi l'autenticazione a chiave già condivisa:

```
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. Creare la VTI e proteggerla con il profilo predefinito:

```
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

Questa procedura consente di configurare L2TPv3 sul router R3.

1. Creare una classe di pseudonimo per definire l'incapsulamento (L2TPv3) e definire l'interfaccia del tunnel FlexVPN usata dalla connessione L2TPv3 per raggiungere il router peer:

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

2. Per configurare il tunnel L2TP, usare il comando xconnect sull'interfaccia interessata; fornire l'indirizzo del peer dell'interfaccia del tunnel e specificare il tipo di incapsulamento:

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

Router R4

Il router R4 ha un indirizzo IP configurato sull'interfaccia:

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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica associazione di sicurezza IPSec

In questo esempio viene verificato che l'associazione di sicurezza IPsec sia stata creata correttamente sul router R2 con interfaccia Tunnel1.

```
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"
```

Verifica creazione SA IKEv2

In questo esempio viene verificato che l'associazione di sicurezza (SA) IKEv2 sia stata creata correttamente sul router R2.

```
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
```

Verifica tunnel L2TPv3

In questo esempio viene verificato che il tunnel L2TPv3 sia stato formattato correttamente sul router R2.

```
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
```

Verifica della connettività e dell'aspetto della rete R1

Nell'esempio viene verificato che il router R1 disponga della connettività di rete al router R4 e che si trovi sulla stessa rete locale.

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione:

- **debug crypto ikev2**: abilita il debug IKEv2.
- **debug evento xconnect -** abilita il debug degli eventi xconnect.
- **show crypto ikev2 diagnose error** - visualizza il database dei percorsi di uscita IKEv2.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems