Guía de Configuración de L2TPv3 over FlexVPN

Contenido

Introducción

Este documento describe cómo configurar un enlace L2TPv3 del Protocolo de túnel de capa 2 para que se ejecute sobre una conexión de Cisco IOS FlexVPN Virtual Tunnel Interface (VTI) entre dos routers que ejecutan Cisco IOS® Software. Con esta tecnología, las redes de capa 2 se pueden ampliar de forma segura dentro de un túnel IPsec a través de varios saltos de capa 3, lo que permite que los dispositivos físicamente separados parezcan estar en la misma LAN local.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Interfaz de túnel virtual (VTI) de Cisco IOS FlexVPN
- Protocolo de túnel de capa 2 (L2TP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router de servicios integrados de segunda generación (G2) de Cisco, con licencia de datos y seguridad.
- Cisco IOS Release 15.1(1)T o posterior para soportar FlexVPN. Para obtener más información, consulte Cisco Feature Navigator.

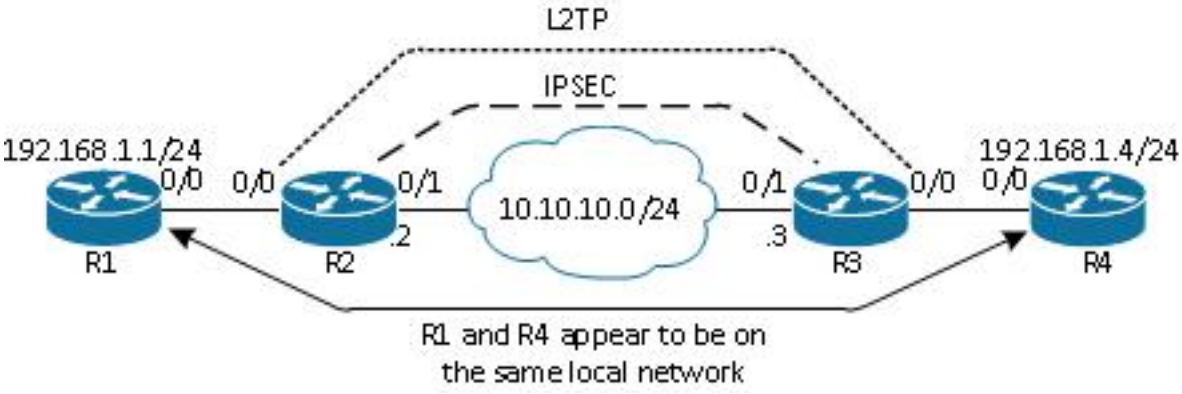
Esta configuración de FlexVPN utiliza valores predeterminados inteligentes y autenticación de clave previamente compartida para simplificar la explicación. Para obtener la máxima seguridad, utilice el cifrado Next-Generation; consulte Encriptación de última generación para obtener más información.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Topología de red

Esta configuración utiliza la topología en esta imagen. Cambie las direcciones IP según sea necesario para la instalación.



Nota: En esta configuración, los routers R2 y R3 están conectados directamente, pero podrían estar separados por muchos saltos. Si los routers R2 y R3 están separados, asegúrese de que haya una ruta para llegar a la dirección IP de peer.

Router R1

El router R1 tiene una dirección IP configurada en la interfaz:

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

Router R2

FlexVPN

Este procedimiento configura FlexVPN en el router R2.

1. Cree un llavero de intercambio de claves de Internet versión 2 (IKEv2) para el par:

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

2. Cree un perfil predeterminado IKEv2 que coincida con el router del par y utilice autenticación de clave previamente compartida:

```
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. Cree el VTI y protéjalo con el perfil predeterminado:

```
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

Este procedimiento configura L2TPv3 en el router R2.

1. Cree una clase de pseudowire para definir la encapsulación (L2TPv3), y defina la interfaz de túnel FlexVPN que la conexión L2TPv3 utiliza para alcanzar el router peer:

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

2. Utilice el comando xconnecten la interfaz relevante para configurar el túnel L2TP; proporcione la dirección de peer de la interfaz de túnel y especifique el tipo de encapsulación:

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

Router R3

FlexVPN

Este procedimiento configura FlexVPN en el router R3.

1. Cree un llavero IKEv2 para el par:

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

2. Cree un perfil predeterminado IKEv2 que coincida con el router del par y utilice autenticación de clave previamente compartida:

```
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. Cree el VTI y protéjalo con el perfil predeterminado:

```
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

Este procedimiento configura L2TPv3 en el router R3.

1. Cree una clase de pseudowire para definir la encapsulación (L2TPv3), y defina la interfaz de túnel FlexVPN que la conexión L2TPv3 utiliza para alcanzar el router peer:

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

2. Utilice el comando xconnecten la interfaz relevante para configurar el túnel L2TP; proporcione la dirección de peer de la interfaz de túnel y especifique el tipo de encapsulación:

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

Router R4

El router R4 tiene una dirección IP configurada en la interfaz:

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

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificación de la Asociación de Seguridad IPsec

Este ejemplo verifica que la asociación de seguridad IPSec se haya creado correctamente en el router R2 con la interfaz 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"
```

Verificación de la Creación de IKEv2 SA

Este ejemplo verifica que la asociación de seguridad (SA) IKEv2 se haya creado correctamente en el 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
```

Verificación del Túnel L2TPv3

Este ejemplo verifica que el túnel L2TPv3 se haya formado correctamente en el 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
```

Verificación de la Apariencia y Conectividad de Red R1

Este ejemplo verifica que el router R1 tenga conectividad de red con el router R4 y parece estar en la misma red local.

```
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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración:

- **debug crypto ikev2** - habilitar debugging IKEv2.
- **debug xconnect event -** habilitar depuración de eventos xconnect.
- **show crypto ikev2 diagnose error** - muestra la base de datos de trayectoria de salida IKEv2.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems