L2TPv3 sobre la guía de configuración de FlexVPN

Contenido

Introducción

Este documento describe cómo configurar un link del protocolo de túneles de la capa 2 versión 3 (L2TPv3) para ejecutar encima una conexión virtual de la interfaz del túnel de FlexVPN del Cisco IOS (VTI) entre dos Routers que ejecute el Cisco IOS ® Software. Con esta tecnología, acode 2 redes puede ser extendido con seguridad dentro de un túnel IPsec sobre los saltos de la capa múltiple 3, que permite para que físicamente los dispositivos diferentes aparezcan estar en el mismo LAN local.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Interfaz del túnel virtual de FlexVPN del Cisco IOS (VTI)

- Protocolo de túneles de la capa 2 (L2TP)

Componentes Utilizados

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

- La generación 2 (G2) del router de los Servicios integrados de Cisco, con la Seguridad y los datos autorizan.
- Cisco IOS Release 15.1(1)T o Posterior para soportar FlexVPN. Para los detalles, refiera al Cisco Feature Navigator.

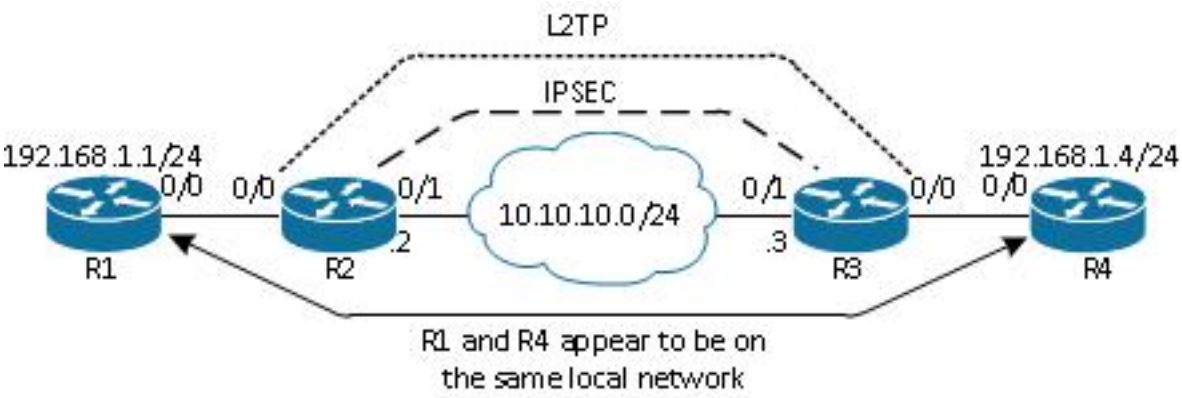
Esta configuración de FlexVPN utiliza los valores por defecto y la autenticación elegantes de la clave previamente compartida para simplificar la explicación. Para la seguridad máxima, utilice el cifrado de la última generación; refiera al cifrado de la última generación para más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Topología de red

Esta configuración utiliza la topología en esta imagen. Cambie los IP Addresses según las necesidades para su instalación.



> Nota: En esta configuración, el r2 del Routers y el R3 están conectados directamente, pero podrían ser separados por muchos saltos. Si se separan el r2 del Routers y el R3, asegúrese de que haya una ruta a conseguir al IP Address de Peer.

R1 del router

El r1 del router tiene una dirección IP configurada en la interfaz:

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

R2 del router

FlexVPN

Este procedimiento configura el FlexVPN en el r2 del router.

1. Cree un llavero del 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 haga juego al router del par y utilice la autenticación de la 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 el L2TPv3 en el r2 del router.

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

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

2. Utilice el **xconnectcommand** en la interfaz pertinente para configurar el túnel L2TP; proporcione a la dirección de peer de la interfaz del 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 el 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 haga juego al router del par, y utiliza la autenticación de la 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 el L2TPv3 en el router R3.

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

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

2. Utilice el **xconnectcommand** en la interfaz pertinente para configurar el túnel L2TP; proporcione a la dirección de peer de la interfaz del 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.

Verifique la asociación de seguridad IPSec

Este ejemplo verifica que creen a la asociación de seguridad IPSec con éxito en el r2 del router 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"
```

Verifique la creación IKEv2 SA

Este ejemplo verifica que creen a la asociación de seguridad IKEv2 (SA) con éxito en el r2 del router.

```
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
```

Verifique el túnel del L2TPv3

Este ejemplo verifica que el túnel del L2TPv3 haya formado correctamente en el r2 del router.

```
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
```

Verifique la conectividad de red y el aspecto del r1

Este ejemplo verifica que el r1 del router tenga conectividad de red al router R4 y aparece 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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración:

- **debug crypto ikev2** - debugging del permiso IKEv2.
- **evento del xconnect del debug -** debugging de evento del xconnect del permiso.
- **la demostración ikev2 crypto diagnostica el error aparece la** base de datos de la trayectoria

de la salida IKEv2.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la 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