L2TPv3 over FlexVPN 컨피그레이션 가이드

목차

소개

이 문서에서는 Cisco IOS® 소프트웨어를 실행하는 두 라우터 간의 Cisco IOS FlexVPN VTI(Virtual Tunnel Interface) 연결을 통해 실행되도록 L2TPv3(Layer 2 Tunneling Protocol version 3) 링크를 구성하는 방법에 대해 설명합니다.이 기술을 사용하면 여러 레이어 3 홉을 통해 IPsec 터널 내에서 레이어 2 네트워크를 안전하게 확장할 수 있으므로 물리적으로 분리된 디바이스가 동일한 로컬 LAN에 있는 것처럼 보일 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS FlexVPN VTI(Virtual Tunnel Interface)
- 레이어 2 터널링 프로토콜(L2TP)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 보안 및 데이터 라이센스가 포함된 Cisco Integrated Services Router Generation 2(G2)
- FlexVPN을 지원하는 Cisco IOS 릴리스 15.1(1)T 이상자세한 내용은 Cisco Feature Navigator를 참조하십시오.

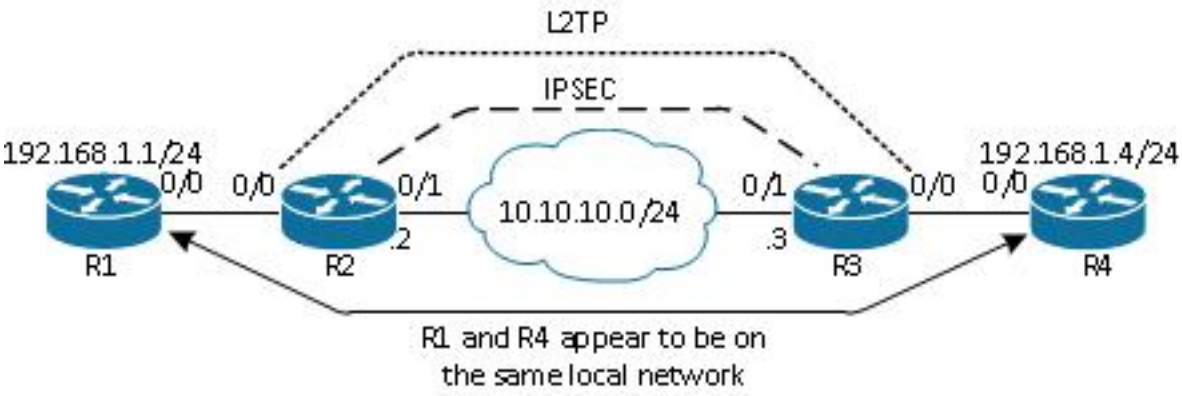
이 FlexVPN 컨피그레이션에서는 설명을 단순화하기 위해 스마트 기본값 및 사전 공유 키 인증을 사용합니다.보안을 극대화하려면 차세대 암호화를 사용합니다.자세한 내용은 차세대 암호화를 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 토폴로지

이 컨피그레이션에서는 이 이미지의 토폴로지를 사용합니다.설치에 필요한 IP 주소를 변경합니다.



참고:이 설정에서 라우터 R2와 R3은 직접 연결되지만 여러 홉으로 분리될 수 있습니다.라우터 R2와 R3이 분리되어 있는 경우 피어 IP 주소로 연결되는 경로가 있는지 확인합니다.

라우터 R1

라우터 R1에는 인터페이스에 구성된 IP 주소가 있습니다.

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

라우터 R2

FlexVPN

이 절차에서는 라우터 R2에서 FlexVPN을 구성합니다.

1. 피어에 대한 IKEv2(Internet Key Exchange Version 2) 키 만들기:

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

2. 피어 라우터와 일치하고 사전 공유 키 인증을 사용하는 IKEv2 기본 프로필을 생성합니다.

```
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. VTI를 생성하고 기본 프로필로 보호합니다.

```
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

이 절차는 라우터 R2에서 L2TPv3을 구성합니다.

1. 캡슐화(L2TPv3)를 정의하고 L2TPv3 연결에서 피어 라우터에 연결하기 위해 사용하는 FlexVPN 터널 인터페이스를 정의하는 의사 유선 클래스를 생성합니다.

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

2. L2TP 터널을 구성하려면 관련 인터페이스에서 xconnectcommand를 사용합니다.터널 인터페이스의 피어 주소를 제공하고 캡슐화 유형을 지정합니다.

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

라우터 R3

FlexVPN

이 절차에서는 라우터 R3에서 FlexVPN을 구성합니다.

1. 피어에 대한 IKEv2 키링을 생성합니다.

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

2. 피어 라우터와 일치하는 IKEv2 기본 프로필을 생성하고 사전 공유 키 인증을 사용합니다.

```
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. VTI를 생성하고 기본 프로필로 보호합니다.

```
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

이 절차는 라우터 R3에서 L2TPv3을 구성합니다.

1. 캡슐화(L2TPv3)를 정의하고 L2TPv3 연결에서 피어 라우터에 연결하기 위해 사용하는 FlexVPN 터널 인터페이스를 정의하는 의사 유선 클래스를 생성합니다.

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

2. L2TP 터널을 구성하려면 관련 인터페이스에서 xconnectcommand를 사용합니다.터널 인터페이스의 피어 주소를 제공하고 캡슐화 유형을 지정합니다.

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

라우터 R4

라우터 R4에는 인터페이스에 구성된 IP 주소가 있습니다.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

IPsec 보안 연결 확인

이 예에서는 인터페이스 Tunnel1을 사용하여 라우터 R2에 IPsec 보안 연결이 성공적으로 생성되었는지 확인합니다.

```
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"
```

IKEv2 SA 생성 확인

이 예에서는 라우터 R2에 IKEv2 SA(보안 연결)가 성공적으로 생성되었는지 확인합니다.

```
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
```

L2TPv3 터널 확인

이 예에서는 라우터 R2에서 L2TPv3 터널의 형식이 올바른지 확인합니다.

```
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
```

R1 네트워크 연결 및 모양 확인

이 예에서는 라우터 R1에 라우터 R4에 대한 네트워크 연결이 있고 동일한 로컬 네트워크에 있는 것으로 나타나는지 확인합니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- **debug crypto ikev2** - IKEv2 디버깅을 활성화합니다.
- **debug xconnect event -** xconnect 이벤트 디버깅을 활성화합니다.
- **show crypto ikev2 진단 오류** - IKEv2 종료 경로 데이터베이스를 표시합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- **기술 지원 및 문서 – Cisco Systems**