L2TPv3 over FlexVPN配置指南

目录

简介

本文档介绍如何配置第2层隧道协议第3版(L2TPv3)链路，以在运行Cisco IOS®软件的两台路由器之间的Cisco IOS FlexVPN虚拟隧道接口(VTI)连接上运行。利用此技术，第2层网络可以在IPsec隧道内通过多个第3层跳安全地扩展，这允许物理上独立的设备看起来位于同一本地LAN中。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IOS FlexVPN虚拟隧道接口(VTI)
- 第2层隧道协议(L2TP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科第2代集成多业务路由器(G2)，带安全和数据许可证。
- Cisco IOS版本15.1(1)T或更高版本，支持FlexVPN。有关详细信息，请参阅Cisco Feature Navigator。

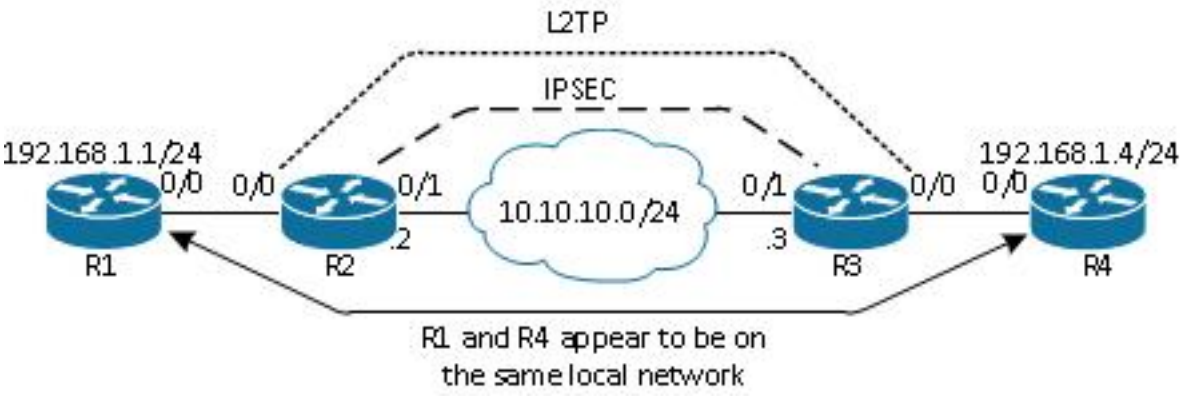
此FlexVPN配置使用智能默认值和预共享密钥身份验证，以简化说明。为获得最高安全性，请使用下一代加密；有关详细信息，请参阅下一代加密。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络拓扑

此配置使用此映像中的拓扑。根据安装需要更改IP地址。



注意：在此设置中，路由器R2和R3直接相连，但它们之间可以分隔许多跳。如果路由器R2和R3分开，请确保有到达对等IP地址的路由。

路由器 R1

路由器R1在接口上配置了IP地址：

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

路由器 R2

FlexVPN

此过程在路由器R2上配置FlexVPN。

1. 为对等体创建互联网密钥交换版本2(IKEv2)密钥环：

```
crypto ikev2 keyring key1
 peer 10.10.10.3
 address 10.10.10.3
 pre-shared-key cisco1
```

2. 创建与对等路由器匹配并使用预共享密钥身份验证的IKEv2默认配置文件：

```
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. 创建VTI，并使用默认配置文件对其进行保护：

```
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

此过程在路由器R2上配置L2TPv3。

1. 创建伪线类以定义封装(L2TPv3)，并定义L2TPv3连接用于到达对等路由器的FlexVPN隧道接口：

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

2. 在相关接口上使用xconnect命令以配置L2TP隧道；提供隧道接口的对等地址，并指定封装类型：

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

路由器 R3

FlexVPN

此过程在路由器R3上配置FlexVPN。

1. 为对等体创建IKEv2密钥环：

```
crypto ikev2 keyring key1
```

```
 peer 10.10.10.2
 address 10.10.10.2
 pre-shared-key cisco
```

2. 创建与对等路由器匹配的IKEv2默认配置文件，并使用预共享密钥身份验证：

```
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. 创建VTI，并使用默认配置文件对其进行保护：

```
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

此过程在路由器R3上配置L2TPv3。

1. 创建伪线类以定义封装(L2TPv3)，并定义L2TPv3连接用于到达对等路由器的FlexVPN隧道接口：

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

2. 在相关接口上使用xconnect命令以配置L2TP隧道；提供隧道接口的对等地址，并指定封装类型：

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

路由器R4

路由器R4的接口上配置了IP地址：

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

验证

使用本部分可确认配置能否正常运行。

检验IPsec安全关联

本示例验证在路由器R2上与接口Tunnel1成功创建IPsec安全关联。

```
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"
```

验证IKEv2 SA的创建

本示例验证在路由器R2上已成功创建IKEv2安全关联(SA)。

```
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
```

检验L2TPv3隧道

本示例检验路由器R2上的L2TPv3隧道是否已正确形成。

```
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
```

检验R1的网络连接和外观

本示例检验路由器R1是否与路由器R4具有网络连接，并且似乎位于同一本地网络中。

```
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
```

故障排除

本节提供可用于排除配置故障的信息：

- **debug crypto ikev2** — 启用IKEv2调试。
- **debug xconnect event** — 启用xconnect事件调试。
- **show crypto ikev2 diagnose error** — 显示IKEv2退出路径数据库。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

相关信息

- 技术支持和文档 - Cisco Systems