在FlexVPN配置指南的L2TPv3

目录

简介

本文描述如何配置Layer2隧道协议版本3 (L2TPv3)链路运行Cisco IOS FlexVPN虚拟隧道接口(VTI)连接在运行Cisco IOS软件的两路由器之间。使用此技术， Layer2网络可以在多层3跳的一个IPSec隧道内安全地被扩展，物理的允许独立设备看来在同样本地LAN。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS FlexVPN虚拟隧道接口(VTI)
- Layer2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：

- 思科集成业务路由器生成2 (G2)，以安全和数据准许。
- 支持FlexVPN的Cisco IOS版本15.1(1)T或以上。关于详细信息，参考Cisco Feature Navigator。

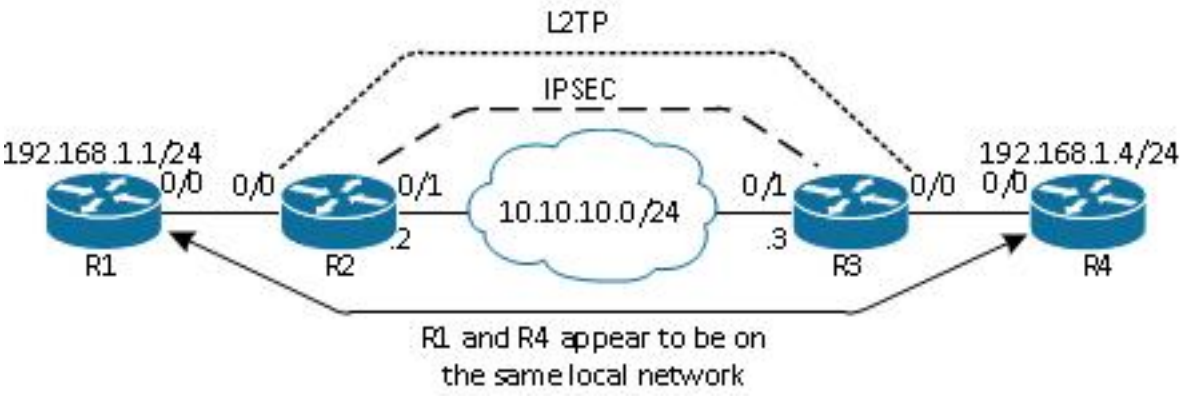
此FlexVPN配置使用聪明的默认和密钥验证为了简化说明。对于最大安全性，请使用下一代加密;参考下一代加密欲知更多信息。

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

此配置在此镜像使用拓扑。崔凡吉莱IP地址当必要时为您的安装。



注意：在此设置，路由器R2和R3直接地连接，但是他们可能由许多跳分离。如果路由器R2和R3被分离，请保证有路由达到对端IP地址。

路由器 R1

路由器R1有在接口配置的一个IP地址：

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

路由器 R2

FlexVPN

此步骤配置在路由器R2的FlexVPN。

1. 创建对等体的一个互联网密钥交换版本2 (IKEv2)钥匙圈：

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

2. 创建匹配对等`路由器并且使用密钥验证的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，并且保护它与默认配置文件：

```
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

此步骤配置在路由器R2的L2TPv3。

1. 创建pseudowire类定义封装(L2TPv3)，并且定义L2TPv3连接使用到达对等`路由器的FlexVPN隧道接口：

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

2. 请使用在相关接口的**xconnectcommand**为了配置L2TP通道;提供隧道接口的对等地址，并且指定封装类型：

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

路由器 R3

FlexVPN

此步骤配置在路由器R3的FlexVPN。

1. 创建对等体的一个IKEv2钥匙圈：

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

2. 创建匹配对等`路由器的IKEv2默认配置文件，并且使用密钥验证：

```
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，并且保护它与默认配置文件：

```
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

此步骤配置在路由器R3的L2TPv3。

1. 创建pseudowire类定义封装(L2TPv3)，并且定义L2TPv3连接使用到达对等`路由器的FlexVPN隧道接口：

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

2. 请使用在相关接口的**xconnectcommand**为了配置L2TP通道;提供隧道接口的对等地址，并且指定封装类型：

```
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有在接口配置的一个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。

验证IPSec安全关联

此示例验证IPSec安全关联在有接口Tunnel1的路由器R2顺利地创建。

```
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SA IKEv2创建

此示例验证IKEv2安全关联(SA)在路由器R2顺利地创建。

```
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
```

验证L2TPv3通道

此示例验证L2TPv3通道在路由器R2正确地形成了。

```
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
```

验证R1网络连通性和外观

此示例验证路由器R1有网络连通性到路由器R4并且看来在同一个本地网络。

```
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

此部分提供您能使用排除故障您的配置的信息：

- **debug crypto ikev2** - enable (event) IKEv2调试。
- **调试xconnect事件-** enable (event) xconnect事件调试。
- **显示crypto ikev2诊断错误**-请显示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。请使用Output Interpreter Tool为了查看show命令输出分析。

> **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