L2TPv3 over FlexVPN配置指南

目錄

簡介 必要條件 需求 採用元件 設定 網路拓撲 路由器R1 路由器R2 路由器R3 路由器R4 驗證 驗證IPsec安全關聯 驗證IKEv2 SA建立 <u>驗證L2TPv3隧道</u> <u>檢驗R1的網路連通</u>性和外觀 疑難排解 相關資訊

簡介

本文說明如何設定第2層通道通訊協定第3版(L2TPv3)連結,以在執行Cisco IOS^{®軟體的兩台路由器之間 ^{執行}Cisco IOS FlexVPN虛擬通道介面(VTI)連接。利用此技術,第2層網路可以在通過多個第3層躍 點的IPsec隧道內進行安全擴展,這允許物理上獨立的裝置出現在同一個本地LAN上。}

必要條件

需求

思科建議您瞭解以下主題:

- Cisco IOS FlexVPN虛擬通道介面(VTI)
- 第2層通道通訊協定(L2TP)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

思科第2代整合多業務路由器(G2),具有安全性和資料許可證。

• Cisco IOS版本15.1(1)T或更高版本支援FlexVPN。有關詳細資訊,請參閱<u>思科功能導航器</u>。 此FlexVPN配置使用智慧預設設定和預共用金鑰身份驗證以簡化說明。為了獲得最大的安全性,請 使用下一代加密;如需詳細資訊,請參閱<u>下一代加密</u>。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

網路拓撲

此配置使用此映像中的拓撲。根據安裝需要更改IP地址。



附註:在此設定中,路由器R2和R3是直接連線的,但它們之間可以有多個跳數分隔。如果路 由器R2和R3是分開的,請確儲存在到達對等IP地址的路由。

路由器R1

路由器R1在介面上配置了IP地址:

interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0

路由器R2

FlexVPN

此過程在路由器R2上配置FlexVPN。

1. 為對等項建立網際網路金鑰交換版本2(IKEv2)金鑰環:

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

2. 建立與對等路由器匹配並使用預共用金鑰身份驗證的IKEv2預設配置檔案:

```
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. 建立VTI, 並使用預設配置檔案對其進行保護:

```
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

此過程在路由器R2上配置L2TPv3。

1. 建立偽線類以定義封裝(L2TPv3),並定義L2TPv3連線用於到達對等路由器的FlexVPN隧道介面:

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

 在相關介面上使用xconnectcommand以設定L2TP通道;提供通道介面的對等位位址,並指定 封裝型別:

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

路由器R3

FlexVPN

此過程在路由器R3上配置FlexVPN。

1. 為對等項建立IKEv2金鑰環:

```
crypto ikev2 keyring key1
peer 10.10.10.2
address 10.10.10.2
```

pre-shared-key cisco

2. 建立與對等路由器匹配的IKEv2預設配置檔案,並使用預共用金鑰身份驗證:

```
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. 建立VTI, 並使用預設配置檔案對其進行保護:

```
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

此過程在路由器R3上配置L2TPv3。

1. 建立偽線類以定義封裝(L2TPv3),並定義L2TPv3連線用於到達對等路由器的FlexVPN隧道介 面:

```
pseudowire-class l2tpl
encapsulation l2tpv3
ip local interface Tunnel1
```

 在相關介面上使用xconnectcommand以設定L2TP通道;提供通道介面的對等位位址,並指定 封裝型別:

```
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的介面上配置了IP地址:

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

驗證

使用本節內容,確認您的組態是否正常運作。

驗證IPsec安全關聯

此示例驗證是否已在路由器R2上通過介面Tunnel1成功建立IPsec安全關聯。

```
R2#show crypto sockets
Number of Crypto Socket connections 1
Tul 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: "Tunnell-head-0"
```

驗證IKEv2 SA建立

此示例驗證在路由器R2上成功建立了IKEv2安全關聯(SA)。

R2#show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tun	nel-id Local	Remote		fvrf/iv	rf	Status
2	10.10.10.2/500	10.10.10	.3/500	none/no	one	READY
	Encr: AES-CBC, keysize:	256, Hash:	SHA512,	DH Grp:5, A	Auth sign:	PSK,
	Auth verify: PSK					
	Life/Active Time: 86400/562 sec					

IPv6 Crypto IKEv2 SA

驗證L2TPv3隧道

此示例驗證路由器R2上已正確形成L2TPv3隧道。

R2#show xconnect all

Legend: 2	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

UP pri ac Et0/0:3(Ethernet) UP l2tp 172.16.1.3:1001

UΡ

檢驗R1的網路連通性和外觀

此示例驗證路由器R1與路由器R4之間具有網路連線,並且似乎位於同一個本地網路中。

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: 11111 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

Eth 0/0 142 R B Linux Uni Eth 0/0 R4

疑難排解

本節提供的資訊可用於對組態進行疑難排解:

- debug crypto ikev2 啟用IKEv2調試。
- debug xconnect event 啟用xconnect事件調試。
- show crypto ikev2 diagnose error 顯示IKEv2退出路徑資料庫。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸 出的分析。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊。</u>

相關資訊

• 技術支援與文件 - Cisco Systems