Guia de configuração do L2TPv3 sobre FlexVPN

Contents

Introduction

Este documento descreve como configurar um link da versão 3 (L2TPv3) do Protocolo de Tunelamento de Camada 2 para ser executado em uma conexão Cisco IOS FlexVPN Virtual Tunnel Interface (VTI) entre dois roteadores que executam o Cisco IOS® Software. Com essa tecnologia, as redes de Camada 2 podem ser estendidas com segurança em um túnel IPsec sobre vários saltos de camada 3, o que permite que dispositivos fisicamente separados pareçam estar na mesma LAN local.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) FlexVPN do Cisco IOS
- L2TP (Layer 2 Tunneling Protocol)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Integrated Services Router Generation 2 (G2), com licença de segurança e dados.
- Cisco IOS versão 15.1(1)T ou posterior para oferecer suporte a FlexVPN. Para obter detalhes, consulte o Cisco Feature Navigator.

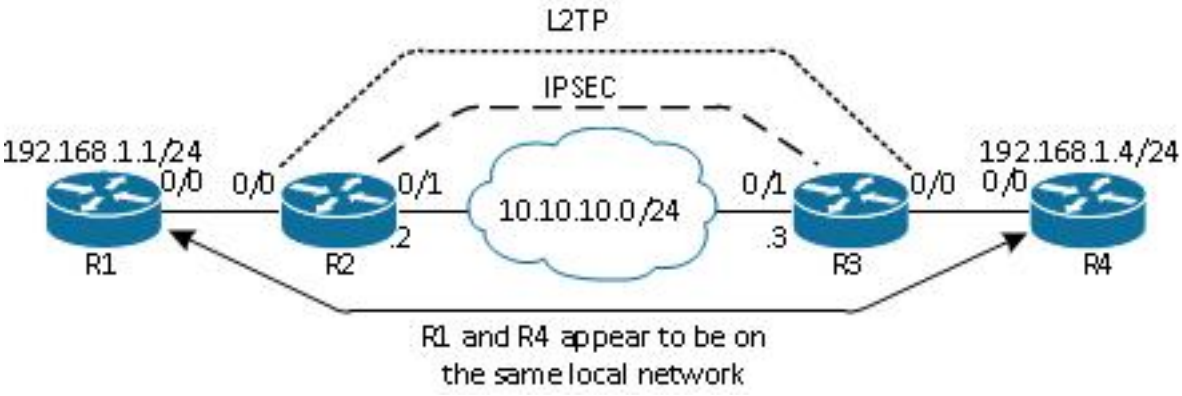
Essa configuração FlexVPN usa padrões inteligentes e autenticação de chave pré-compartilhada para simplificar a explicação. Para máxima segurança, use a criptografia de próxima geração; consulte Criptografia de próxima geração para obter mais informações.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Topologia de rede

Essa configuração usa a topologia nesta imagem. Altere os endereços IP conforme necessário para a instalação.



Note: Nessa configuração, os roteadores R2 e R3 estão diretamente conectados, mas podem ser separados por muitos saltos. Se os roteadores R2 e R3 estiverem separados, certifique-se de que haja uma rota para chegar ao endereço IP do peer.

Roteador R1

O roteador R1 tem um endereço IP configurado na interface:

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

Roteador R2

FlexVPN

Este procedimento configura o FlexVPN no roteador R2.

1. Crie um keyring IKEv2 (Internet Key Exchange Version 2) para o peer:

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

2. Crie um perfil padrão IKEv2 que corresponda ao roteador peer e use a autenticação de chave pré-compartilhada:

```
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. Crie o VTI e proteja-o com o perfil padrão:

```
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 procedimento configura o L2TPv3 no roteador R2.

1. Crie uma classe pseudoire para definir o encapsulamento (L2TPv3) e defina a interface de túnel FlexVPN que a conexão L2TPv3 usa para acessar o roteador peer:

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

2. Use o comando xconnectna interface relevante para configurar o túnel L2TP; forneça o endereço de peer da interface do túnel e especifique o tipo de encapsulamento:

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

Roteador R3

FlexVPN

Este procedimento configura o FlexVPN no roteador R3.

1. Crie um keyring IKEv2 para o peer:

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

2. Crie um perfil padrão IKEv2 que corresponda ao roteador peer e use a autenticação de chave pré-compartilhada:

```
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. Crie o VTI e proteja-o com o perfil padrão:

```
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 procedimento configura o L2TPv3 no roteador R3.

1. Crie uma classe pseudoire para definir o encapsulamento (L2TPv3) e defina a interface de túnel FlexVPN que a conexão L2TPv3 usa para acessar o roteador peer:

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

2. Use o comando xconnectna interface relevante para configurar o túnel L2TP; forneça o endereço de peer da interface do túnel e especifique o tipo de encapsulamento:

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

Roteador R4

O roteador R4 tem um endereço IP configurado na interface:

```
interface Ethernet0/0
```

```
 ip address 192.168.1.4 255.255.255.0
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificar a associação de segurança IPsec

Este exemplo verifica se a associação de segurança IPsec foi criada com êxito no roteador R2 com interface 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"
```

Verificar a criação de SA do IKEv2

Este exemplo verifica se a associação de segurança (SA) IKEv2 foi criada com êxito no roteador R2.

```
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
```

Verificar o túnel L2TPv3

Este exemplo verifica se o túnel L2TPv3 foi formado corretamente no roteador R2.

```
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
```

Verificar a conectividade e a aparência da rede R1

Este exemplo verifica se o roteador R1 tem conectividade de rede com o roteador R4 e parece estar na mesma rede 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
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração:

- **debug crypto ikev2** - enable IKEv2 debugging.
- **debug xconnect event -** enable xconnect event debugging.
- **show crypto ikev2 diagnose error** - exibe o banco de dados do caminho de saída de IKEv2.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems