

# L2TPv3 sobre o manual de configuração de FlexVPN

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Topologia de rede](#)

[R1 do roteador](#)

[Roteador R2](#)

[Roteador R3](#)

[Roteador R4](#)

[Verificar](#)

[Verifique a associação de segurança IPsec](#)

[Verifique a criação IKEv2 SA](#)

[Verifique o túnel do L2TPv3](#)

[Verifique a conectividade de rede e a aparência do r1](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como configurar um link da versão do protocolo 3 da escavação de um túnel da camada 2 (L2TPv3) para executar sobre uma conexão virtual da interface de túnel de FlexVPN do Cisco IOS (VTI) entre dois Roteadores que executa o Cisco IOS ® Software. Com esta tecnologia, mergulhe 2 redes pode ser estendido firmemente dentro de um túnel de IPsec sobre saltos da camada múltipla 3, que permita fisicamente dispositivos separados parecer estar no mesmo LAN local.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Interface de túnel virtual de FlexVPN do Cisco IOS (VTI)



```
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 da versão 2 do intercâmbio de chave de Internet (IKEv2) para o par:

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

2. Crie um perfil padrão IKEv2 que combine o roteador de peer e use a autenticação da 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 Tunnell
 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 do pseudowire para definir o encapsulamento (L2TPv3), e defina a interface de túnel de FlexVPN que a conexão do L2TPv3 se usa para alcançar o roteador de peer:

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

2. Use o **xconnect** command na interface relevante a fim configurar o túnel L2TP; forneça o endereço de peer da interface de 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 par:

```
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 combine o roteador de peer, e use a autenticação da 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 Tunnell
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 do pseudowire para definir o encapsulamento (L2TPv3), e defina a interface de túnel de FlexVPN que a conexão do L2TPv3 se usa para alcançar o roteador de peer:

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

2. Use o **xconnect** na interface relevante a fim configurar o túnel L2TP; forneça o endereço de peer da interface de 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 de Um ou Mais Servidores Cisco ICM NT configurado na relação:

```
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.

## Verifique a associação de segurança IPSec

Este exemplo verifica que a associação de segurança IPSec está criada com sucesso no roteador R2 com a relação Tunnel1.

```
R2#show crypto sockets
```

```
Number of Crypto Socket connections 1
```

```
Tun1 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"
```

## Verifique a criação IKEv2 SA

Este exemplo verifica que a associação de segurança IKEv2 (SA) está criada com sucesso no roteador R2.

```
R2#show crypto ikev2 sa
```

```
IPv4 Crypto IKEv2 SA
```

Tunnel-id	Local	Remote	fvr/ivrf	Status
<b>2</b>	<b>10.10.10.2/500</b>	<b>10.10.10.3/500</b>	<b>none/none</b>	<b>READY</b>

```
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
```

## Verifique o túnel do L2TPv3

Este exemplo verifica que o túnel do L2TPv3 formou 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
```



IKEv2.

[A ferramenta Output Interpreter \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

## Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)