L2TPv3 sobre o manual de configuração de FlexVPN

Índice

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)

- Protocolo da escavação de um túnel da camada 2 (L2TP)

Componentes Utilizados

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

- A geração 2 do roteador dos Serviços integrados de Cisco (G2), com a Segurança e os dados licenciam.
- Cisco IOS Release 15.1(1)T ou Mais Recente para apoiar FlexVPN. Para detalhes, refira o Cisco Feature Navigator.

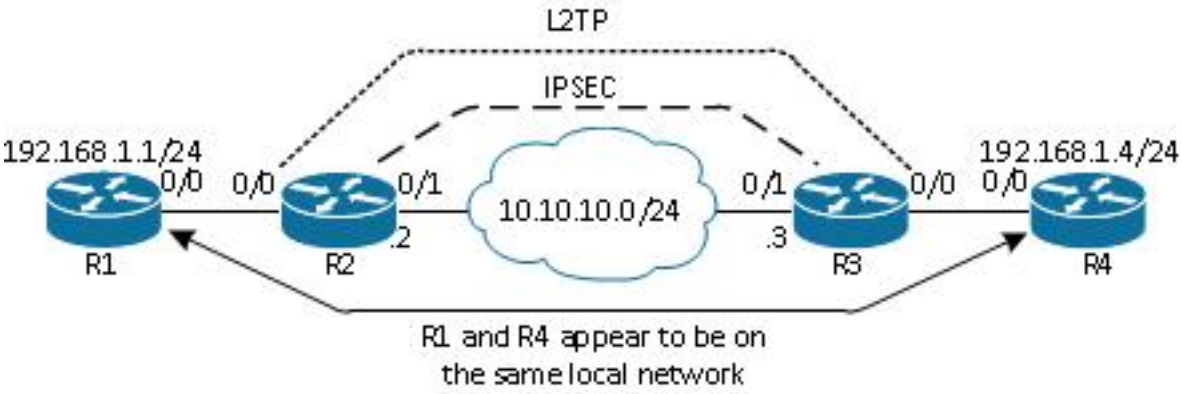
Esta configuração de FlexVPN usa padrões e a autenticação espertos da chave pré-compartilhada a fim simplificar a explicação. Para a segurança máxima, use a criptografia da próxima geração; refira a criptografia da próxima geração para mais informação.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Topologia de rede

Esta configuração usa a topologia nesta imagem. Mude endereços IP de Um ou Mais Servidores Cisco ICM NT como necessários para sua instalação.



> Nota: Nesta instalação, o Roteadores R2 e o R3 são conectados diretamente, mas poderia ser separado por muitos saltos. Se o Roteadores R2 e R3 é separado, assegure-se de que haja uma rota a obter ao endereço IP do peer.

R1 do roteador

O r1 do roteador tem um endereço IP de Um ou Mais Servidores Cisco ICM NT configurado na relação:

```
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 ciscol
```

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 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 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 Tunnel1
```

2. Use o **xconnectcommand 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 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 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 Tunnel1
```

2. Use o **xconnectcommand 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

  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"
```

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                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
```

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
```

```
 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
```

Verifique a conectividade de rede e a aparência do r1

Este exemplo verifica que o r1 do roteador tem a conectividade de rede ao 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
```

Troubleshooting

Esta seção fornece a informação que você pode se usar para pesquisar defeitos sua configuração:

- **o debug crypto ikev2** - permita a eliminação de erros IKEv2.
- **debugar o evento do xconnect -** permita o event debugging do xconnect.
- **a mostra ikev2 cripto diagnostica a exibição de erros o** base de dados do trajeto da saída

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