Guide de configuration de L2TPv3 sur FlexVPN

Contenu

Introduction

Ce document décrit comment configurer une liaison L2TPv3 (Layer 2 Tunneling Protocol version 3) pour s'exécuter sur une connexion VTI (Virtual Tunnel Interface) Cisco IOS FlexVPN entre deux routeurs qui exécutent le logiciel Cisco IOS®. Grâce à cette technologie, les réseaux de couche 2 peuvent être étendus en toute sécurité dans un tunnel IPsec sur plusieurs sauts de couche 3, ce qui permet à des périphériques physiquement séparés de paraître sur le même réseau local.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Interface de tunnel virtuel Cisco IOS FlexVPN (VTI)
- Protocole L2TP (Layer 2 Tunneling Protocol)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur à services intégrés Cisco de 2e génération (G2), avec licence de sécurité et de données.
- Cisco IOS version 15.1(1)T ou ultérieure pour prendre en charge FlexVPN. Pour plus d'informations, reportez-vous au Navigateur de fonctions Cisco.

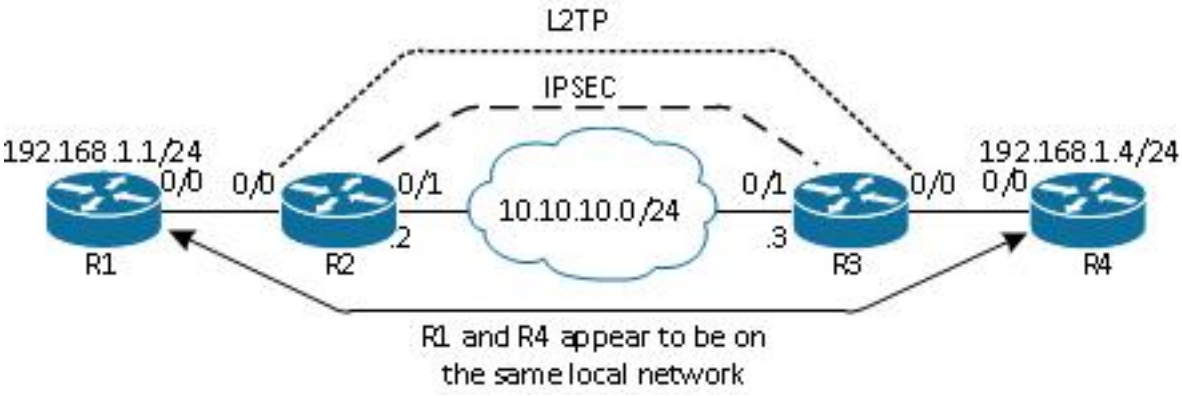
Cette configuration FlexVPN utilise les paramètres par défaut intelligents et l'authentification par clé prépartagée afin de simplifier l'explication. Pour une sécurité maximale, utilisez le chiffrement de nouvelle génération ; référez-vous à Cryptage nouvelle génération pour plus d'informations.

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.

Configuration

Topologie du réseau

Cette configuration utilise la topologie de cette image. Modifiez les adresses IP selon les besoins de votre installation.



Note: Dans cette configuration, les routeurs R2 et R3 sont directement connectés, mais ils peuvent être séparés par de nombreux sauts. Si les routeurs R2 et R3 sont séparés, assurez-vous qu'il existe une route pour accéder à l'adresse IP de l'homologue.

Routeur R1

Une adresse IP du routeur R1 est configurée sur l'interface :

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

Routeur R2

FlexVPN

Cette procédure configure FlexVPN sur le routeur R2.

1. Créez une clé IKEv2 (Internet Key Exchange Version 2) pour l'homologue :

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

2. Créez un profil par défaut IKEv2 qui correspond au routeur homologue et utilise l'authentification à clé pré-partagée :

```
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. Créez la VTI et protégez-la avec le profil par défaut :

```
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

Cette procédure configure L2TPv3 sur le routeur R2.

1. Créez une classe pseudowire pour définir l'encapsulation (L2TPv3) et définir l'interface de tunnel FlexVPN que la connexion L2TPv3 utilise pour atteindre le routeur homologue :

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

2. Utilisez la commande xconnectsur l'interface appropriée afin de configurer le tunnel L2TP ; fournissez l’adresse homologue de l’interface de tunnel et spécifiez le type d’encapsulation :

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

Routeur R3

FlexVPN

Cette procédure configure FlexVPN sur le routeur R3.

1. Créez une clé IKEv2 pour l'homologue :

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

2. Créez un profil par défaut IKEv2 qui correspond au routeur homologue et utilise l'authentification à clé pré-partagée :

```
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. Créez la VTI et protégez-la avec le profil par défaut :

```
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

Cette procédure configure L2TPv3 sur le routeur R3.

1. Créez une classe pseudowire pour définir l'encapsulation (L2TPv3) et définir l'interface de tunnel FlexVPN que la connexion L2TPv3 utilise pour atteindre le routeur homologue :

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

2. Utilisez la commande xconnectsur l'interface appropriée afin de configurer le tunnel L2TP ; fournissez l’adresse homologue de l’interface de tunnel et spécifiez le type d’encapsulation :

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

Routeur R4

Une adresse IP est configurée sur l’interface du routeur R4 :

```
interface Ethernet0/0
```

```
 ip address 192.168.1.4 255.255.255.0
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérifier l'association de sécurité IPsec

Cet exemple montre comment vérifier que l'association de sécurité IPsec a bien été créée sur le routeur R2 avec l'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"
```

Vérifier la création de SA IKEv2

Cet exemple montre comment vérifier que l'association de sécurité (SA) IKEv2 est correctement créée sur le routeur 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
```

Vérification du tunnel L2TPv3

Cet exemple vérifie que le tunnel L2TPv3 s'est formé correctement sur le routeur 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
```

Vérification de la connectivité et de l'apparence du réseau de R1

Cet exemple montre comment vérifier que le routeur R1 dispose d'une connectivité réseau au routeur R4 et semble se trouver sur le même réseau 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration:

- **debug crypto ikev2** - enable IKEv2 debugging.
- **debug xconnect event -** enable xconnect event debugging.
- **show crypto ikev2 diagnose error** - affiche la base de données du chemin de sortie IKEv2.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Informations connexes

- Support et documentation techniques - Cisco Systems