

L2TPv3 au-dessus de guide de configuration de FlexVPN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Topologie du réseau](#)

[Routeur R1](#)

[Routeur R2](#)

[Routeur R3](#)

[Routeur R4](#)

[Vérifiez](#)

[Vérifiez l'association de sécurité IPSec](#)

[Vérifiez la création d'IKEv2 SA](#)

[Vérifiez le tunnel L2TPv3](#)

[Vérifiez la connexion réseau R1 et l'apparence](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un lien de la version 3 de Layer 2 Tunneling Protocol (L2TPv3) pour exécuter plus d'une connexion virtuelle de l'interface de tunnel de FlexVPN de Cisco IOS (VTI) entre deux Routeurs qui exécutent le logiciel de Cisco IOS®. Avec cette technologie, posez 2 réseaux peut être étendu sécurisé dans un tunnel d'IPsec au-dessus de plusieurs sauts de la couche 3, qui tient compte pour que physiquement les périphériques distincts semblent être sur le même réseau local.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Interface de tunnel virtuelle de FlexVPN de Cisco IOS (VTI)

- Layer 2 Tunneling Protocol (L2TP)

Composants utilisés

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

- La génération 2 (G2) d'Integrated Services Router de Cisco, avec la Sécurité et les données autorisent.
- Cisco IOS version 15.1(1)T ou ultérieures pour prendre en charge FlexVPN. Pour des détails, référez-vous au [navigateur de caractéristique de Cisco](#).

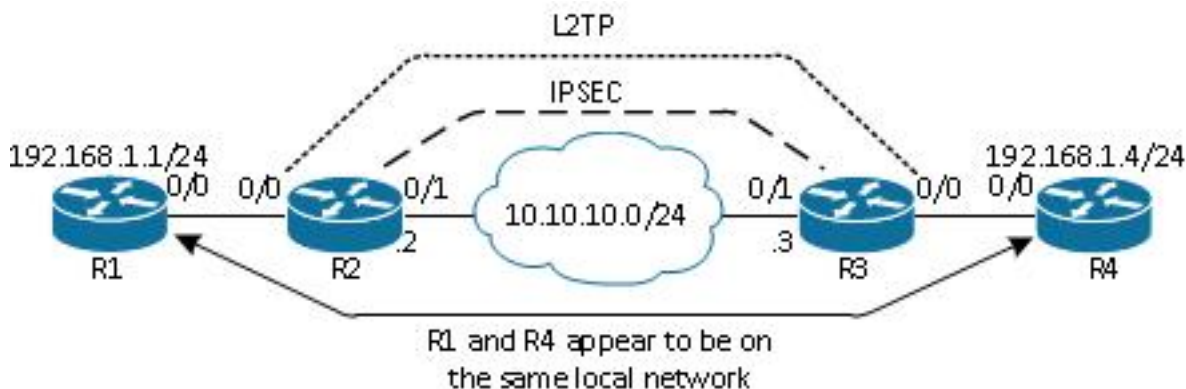
Cette configuration de FlexVPN emploie des par défaut et l'authentification intelligents de pre-shared-key afin de simplifier l'explication. Pour la sécurité maximale, utilisez le cryptage de la deuxième génération ; référez-vous au pour en savoir plus [de la deuxième génération de cryptage](#).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Topologie du réseau

Cette configuration utilise la topologie dans cette image. Adresses IP de modification comme nécessaires pour votre installation.



Remarque: Dans cette installation, les Routeurs R2 et les R3 sont directement connectés, mais ils pourraient être séparés par beaucoup de sauts. Si les Routeurs R2 et R3 sont séparés, assurez-vous qu'il y a une artère à obtenir à l'adresse IP de pair.

Routeur R1

Le routeur R1 a une adresse IP configurée sur l'interface :

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

Routeur R2

FlexVPN

Cette procédure configure le FlexVPN sur le routeur R2.

1. Créez un keyring de la version 2 d'échange de clés Internet (IKE) (IKEv2) pour le pair :

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

2. Créez un profil IKEv2 par défaut qui apparie le routeur de pair et utilise l'authentification de pre-shared-key :

```
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 le VTI, et protégez-le avec le profil par défaut :

```
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

Cette procédure configure L2TPv3 sur le routeur R2.

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

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

2. Employez le **xconnect** command sur l'interface appropriée afin de configurer le tunnel L2TP ; fournissez l'adresse de pair 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 le FlexVPN sur le routeur R3.

1. Créez un keyring IKEv2 pour le pair :

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

2. Créez un profil IKEv2 par défaut qui apparie le routeur de pair, et utilisez l'authentification de pre-shared-key :

```
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 le VTI, et protégez-le avec le profil par défaut :

```
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

Cette procédure configure L2TPv3 sur le routeur R3.

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

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

2. Employez le **xconnectcommand** sur l'interface appropriée afin de configurer le tunnel L2TP ; fournissez l'adresse de pair 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

Le routeur R4 a une adresse IP configurée sur l'interface :

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

Vérifiez

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

Vérifiez l'association de sécurité IPSec

Cet exemple vérifie que l'association de sécurité d'IPsec est avec succès créée sur le routeur R2 avec l'interface 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"
```

Vérifiez la création d'IKEv2 SA

Cet exemple vérifie que l'association de sécurité IKEv2 (SA) est avec succès créée sur le routeur R2.

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

```
IPv4 Crypto IKEv2 SA
```

Tunnel-id	Local	Remote	fvr/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
```

Vérifiez le tunnel L2TPv3

Cet exemple vérifie que le tunnel L2TPv3 a correctement formé 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
```


- **l'exposition crypto ikev2 diagnostiquent l'erreur** - affichez la base de données de chemin de la sortie IKEv2.

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Remarque: 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](#)