

# L2TPv3 over FlexVPN コンフィギュレーションガイド

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク トポロジ](#)

[ルータ R1](#)

[ルータ R2](#)

[ルータ R3](#)

[ルータ R4](#)

[確認](#)

[IPSec セキュリティ アソシエーションの確認](#)

[IKEv2 SA の作成の確認](#)

[L2TPv3 トンネルの確認](#)

[R1 のネットワーク接続と存在の確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、レイヤ 2 トンネリング プロトコル バージョン 3 ( L2TPv3 ) リンクを設定し、Cisco IOS<sup>®</sup> ソフトウェアが稼働する 2 台のルータ間の Cisco IOS FlexVPN 仮想トンネル インターフェイス ( VTI ) 接続で動作するようにする方法について説明します。このテクノロジーを使用すると、複数のレイヤ 3 ホップを経由する IPSec トンネル内でレイヤ 2 ネットワークを安全に拡張できます。これにより、物理的に離れたデバイスが同じローカル LAN 上にあるように見えます。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS FlexVPN 仮想トンネル インターフェイス ( VTI )

- レイヤ 2 トンネリング プロトコル ( L2TP )

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- セキュリティおよびデータ ライセンス付属の第 2 世代 Cisco サービス統合型ルータ ( G2 )。
- FlexVPN をサポートする Cisco IOS リリース 15.1(1)T 以降。詳細については、[Cisco Feature Navigator](#) を参照してください。

この FlexVPN 設定では、説明を分かりやすくするために、スマート デフォルトおよび事前共有キー認証を使用します。セキュリティを最大にするため、次世代の暗号化を使用します。詳細については、『[次世代の暗号化](#)』を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 設定

### ネットワーク トポロジ

この設定では、次の図に示すトポロジを使用します。実際の設置状況に合わせて IP アドレスを変更してください。

注: このセットアップでは、ルータ R2 と R3 が直接接続されていますが、複数のホップで分けることができます。ルータ R2 と R3 を離す場合は、ピア IP アドレスへのルートを確認してください。

### ルータ R1

ルータ R1 はインターフェイスに IP アドレスが設定されています。

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

### ルータ R2

#### FlexVPN

次の手順でルータ R2 の FlexVPN を設定します。

1. ピアのインターネット キー エクスチェンジ バージョン 2 ( IKEv2 ) キーリングを作成します。

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

2. ピア ルータに一致し、事前共有キー認証を使用する IKEv2 デフォルト プロファイルを作成します。

```
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. VTI を作成し、デフォルト プロファイルでこれを保護します。

```
interface Tunnell1
 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

次の手順でルータ R2 の L2TPv3 を設定します。

1. 疑似回線クラスを作成してカプセル化 ( L2TPv3 ) を定義し、ピア ルータにアクセスするために L2TPv3 接続が使用する FlexVPN トンネル インターフェイスを定義します。

```
pseudowire-class l2tp1
 encapsulation l2tpv3
 ip local interface Tunnell1
```

2. 関連するインターフェイスで **xconnect** コマンドを使用して L2TP トンネルを設定します。また、トンネル インターフェイスのピア アドレスを入力して、カプセル化タイプを指定します。

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

## ルータ R3

### FlexVPN

次の手順でルータ R3 の FlexVPN を設定します。

1. ピアの IKEv2 キーリングを作成します。

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

2. ピア ルータに一致し、事前共有キー認証を使用する、IKEv2 デフォルト プロファイルを作成します。

```
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. VTI を作成し、デフォルト プロファイルでこれを保護します。

```
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

次の手順でルータ R3 の L2TPv3 を設定します。

1. 疑似回線クラスを作成してカプセル化 ( L2TPv3 ) を定義し、ピア ルータにアクセスするために L2TPv3 接続が使用する FlexVPN トンネル インターフェイスを定義します。

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

2. 関連するインターフェイスで **xconnect** コマンドを使用して L2TP トンネルを設定します。また、トンネル インターフェイスのピア アドレスを入力して、カプセル化タイプを指定します。

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

## ルータ R4

ルータ R4 はインターフェイスに IP アドレスが設定されています。

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

## 確認

ここでは、設定が正常に動作していることを確認します。

## IPSec セキュリティ アソシエーションの確認

この例では、IPSec セキュリティ アソシエーションが、インターフェイス Tunnel1 を持つルータ R2 で正常に作成されることを確認します。

```
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"

### IKEv2 SA の作成の確認

この例では、IKEv2 セキュリティ アソシエーション ( SA ) がルータ R2 で正常に作成されることを確認します。

R2#show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/f/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

### L2TPv3 トンネルの確認

この例では、L2TPv3 トンネルがルータ R2 で正しく形成されたことを確認します。

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

### R1 のネットワーク接続と存在の確認

この例では、ルータ R1 がルータ R4 にネットワーク接続し、同じローカル ネットワーク上に存在することを確認します。

```
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
<b>Internet</b>	<b>192.168.1.4</b>	<b>4</b>	<b>aabb.cc00.0400</b>	<b>ARPA</b>	<b>Ethernet0/0</b>

```
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
<b>R4</b>	<b>Eth 0/0</b>	<b>142</b>	<b>R B</b>	<b>Linux Uni</b>	<b>Eth 0/0</b>

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報について説明します。

- **debug crypto ikev2** : IKEv2 デバッグを有効にします。
- **debug xconnect event** : xconnect イベントのデバッグを有効にします。
- **show crypto ikev2 diagnose error** : IKEv2 終了パスのデータベースを表示します。

特定の show コマンドが [アウトプット インタープリタ ツール \(登録ユーザ専用\)](#) でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

## 関連情報

- [テクニカルサポートとドキュメント - Cisco Systems](#)