L2TPv3 over FlexVPN Configuration Guide

Document ID: 116207

Contributed by Graham Bartlett, Cisco TAC Engineer.
Jun 06, 2013

Contents

Introduction

This document describes how to configure a Layer 2 Tunnelling Protocol version 3 (L2TPv3) link to run over a Cisco IOS FlexVPN Virtual Tunnel Interface (VTI) connection between two routers that run Cisco IOS® Software. With this technology, Layer 2 networks can be extended securely within an IPsec tunnel over multiple layer 3 hops, which allows for physically separate devices to appear to be on the same local LAN.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS FlexVPN Virtual Tunnel Interface (VTI)
- Layer 2 Tunnelling Protocol (L2TP)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Integrated Services Router Generation 2 (G2), with the security and data license.
- Cisco IOS Release 15.1(1)T or later to support FlexVPN. For details, refer to the Cisco Feature Navigator.

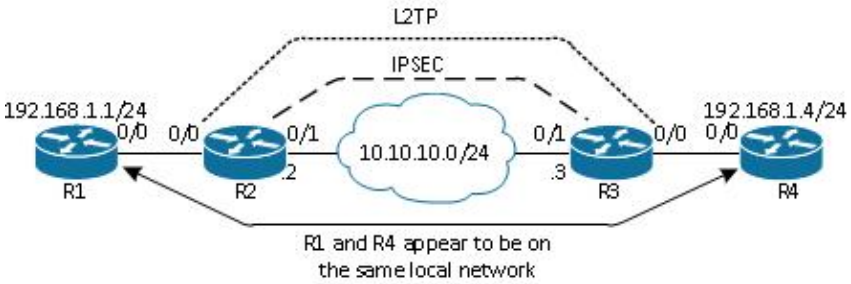
This FlexVPN configuration uses smart defaults and pre−shared−key authentication in order to simplify the explanation. For maximum security, use Next−Generation Encryption; refer to Next−Generation Encryption for more information.

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.

Configure

Network Topology

This configuration uses the topology in this image. Change IP addresses as needed for your installation.



Note: In this setup, routers R2 and R3 are directly connected, but they could be separated by many hops. If routers R2 and R3 are separated, ensure that there is a route to get to the peer IP address.

Router R1

Router R1 has an IP address configured on the interface:

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

Router R2

FlexVPN

This procedure configures the FlexVPN on router R2.

1. Create an Internet Key Exchange Version 2 (IKEv2) keyring for the peer:

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

2. Create an IKEv2 default profile that matches the peer router and uses pre−shared−key authentication:

```
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. Create the VTI, and protect it with the default profile:

```
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

This procedure configures L2TPv3 on router R2.

1. Create a pseudowire class to define the encapsulation (L2TPv3), and define the FlexVPN tunnel interface that the L2TPv3 connection uses to reach the peer router:

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

2. Use the ***xconnect***command on the relevant interface in order to configure the L2TP tunnel; provide the peer address of the tunnel interface, and specify the encapsulation type:

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

Router R3

FlexVPN

This procedure configures the FlexVPN on router R3.

1. Create an IKEv2 keyring for the peer:

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

2. Create an IKEv2 default profile that matches the peer router, and uses pre-shared-key authentication:

```
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. Create the VTI, and protect it with the default profile:

```
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

This procedure configures L2TPv3 on router R3.

1. Create a pseudowire class to define the encapsulation (L2TPv3), and define the FlexVPN tunnel interface that the L2TPv3 connection uses to reach the peer router:

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

2. Use the ***xconnect***command on the relevant interface in order to configure the L2TP tunnel; provide the peer address of the tunnel interface, and specify the encapsulation type:

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

Router R4

Router R4 has an IP address configured on the interface:

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

Verify

Use this section to confirm that your configuration works properly.

Verify IPsec Security Association

This example verifies that the IPsec security association is successfully created on router R2 with 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"
```

Verify IKEv2 SA Creation

This example verifies that IKEv2 security association (SA) is successfully created on router 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
```

Verify L2TPv3 Tunnel

This example verifies that L2TPv3 tunnel has correctly formed on router 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
```

Verify R1 Network Connectivity and Appearance

This example verifies that router R1 has network connectivity to router R4 and appears to be on the same local network.

```
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration:

- ***debug crypto ikev2*** − enable IKEv2 debugging.
- ***debug xconnect event*** − enable xconnect event debugging.
- ***show crypto ikev2 diagnose error*** − display the IKEv2 exit path database.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

Related Information

- ***Technical Support & Documentation − Cisco Systems***

Updated: Jun 06, 2013 Document ID: 116207