L2TPv3 по руководству по конфигурации FlexVPN

Содержание

Введение

Этот документ описывает, как настроить ссылку версии 3 (L2TPv3) Протокола туннелирования Уровня 2 для работания на основе соединения виртуального туннельного интерфейса (VTI) Cisco IOS FlexVPN между двумя маршрутизаторами, которые выполняют программное обеспечение Cisco IOS. С этой технологией сети Уровня 2 могут быть расширены надежно в Туннеле IPSec по нескольким уровням 3 перехода, который обеспечивает физически отдельные устройства, чтобы казаться, быть на той же локальной сети.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Виртуальный туннельный интерфейс (VTI) Cisco IOS FlexVPN

- Протокол туннелирования уровня 2 (L2TP)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Поколение 2 Cisco ISR (G2), с безопасностью и лицензией данных.
- Cisco IOS Release 15.1 (1) T или позже поддерживать FlexVPN. Для получения дополнительной информации обратитесь к Cisco Feature Navigator.

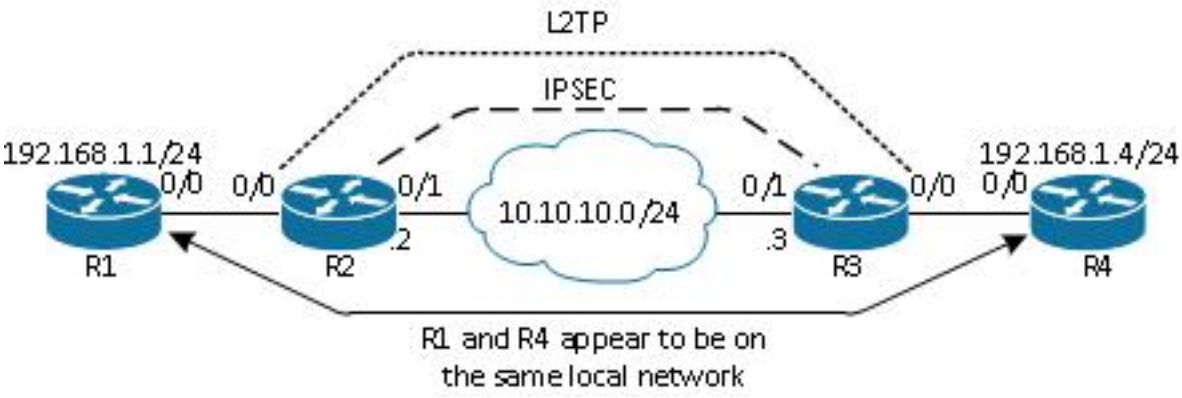
Эта конфигурация FlexVPN использует умные настройки по умолчанию и аутентификацию предварительного общего ключа для упрощения пояснения. Для максимальной безопасности используйте Шифрование Следующего поколения; обратитесь к Шифрованию Следующего поколения для получения дополнительной информации.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Топология сети

Эта конфигурация использует топологию в этом образе. IP-адреса изменения по мере необходимости для вашей установки.



Примечание: В этой настройке напрямую подключаются маршрутизаторы R2 и R3, но они могли быть разделены многими переходами. Если маршрутизаторы R2 и R3 разделены, гарантируют, что существует маршрут для получения до IP - адреса адресуемого точки.

Маршрутизатор M1

Маршрутизатору R1 настроили IP-адрес на интерфейсе:

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

Маршрутизатор M2

FlexVPN

Эта процедура настраивает FlexVPN на маршрутизаторе R2.

1. Создайте брелок второй версии протокола Internet Key Exchange (IKEv2) для узла:

   ```
   crypto ikev2 keyring key1
    peer 10.10.10.3
    address 10.10.10.3
    pre-shared-key ciscol
   ```
2. Создайте профиль по умолчанию IKEv2, который совпадает с равным маршрутизатором и использует аутентификацию предварительного общего ключа:

   ```
   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. Создайте VTI и защитите его с профилем по умолчанию:

   ```
   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

Эта процедура настраивает L2TPv3 на маршрутизаторе R2.

1. Создайте класс pseudowire, чтобы определить инкапсуляцию (L2TPv3) и определить туннельный интерфейс FlexVPN что использование соединения L2TPv3 для достижения равного маршрутизатора:

   ```
   pseudowire-class l2tp1
    encapsulation l2tpv3
    ip local interface Tunnel1
   ```
2. Используйте **xconnectcommand** на соответствующем интерфейсе для настройки туннеля L2TP; предоставьте адрес партнера (peer) туннельного интерфейса и задайте тип инкапсуляции:

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

Маршрутизатор R3

FlexVPN

Эта процедура настраивает FlexVPN на маршрутизаторе R3.

1. Создайте брелок IKEv2 для узла:

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

2. Создайте профиль по умолчанию IKEv2, который совпадает с равным маршрутизатором и использует аутентификацию предварительного общего ключа:

```
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. Создайте VTI и защитите его с профилем по умолчанию:

```
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

Эта процедура настраивает L2TPv3 на маршрутизаторе R3.

1. Создайте класс pseudowire, чтобы определить инкапсуляцию (L2TPv3) и определить туннельный интерфейс FlexVPN что использование соединения L2TPv3 для достижения равного маршрутизатора:

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

2. Используйте **xconnectcommand** на соответствующем интерфейсе для настройки туннеля L2TP; предоставьте адрес партнера (peer) туннельного интерфейса и задайте тип инкапсуляции:

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

Маршрутизатор R4

Маршрутизатору R4 настроили IP-адрес на интерфейсе:

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

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Проверьте сопоставление безопасности IPSec

Данный пример проверяет, что Сопоставление безопасности IPSec успешно создано на маршрутизаторе R2 с интерфейсным 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"
```

Проверьте создание IKEv2 SA

Данный пример проверяет, что сопоставление безопасности (SA) IKEv2 успешно создано на маршрутизаторе 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
```

Проверьте туннель L2TPv3

Данный пример проверяет, что туннель L2TPv3 правильно сформировался на маршрутизаторе 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
```

Проверьте сетевое подключение R1 и появление

Данный пример проверяет, что маршрутизатор R1 имеет сетевое подключение к маршрутизатору R4 и, кажется, находится на той же локальной сети.

```
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
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации:

- **debug crypto ikev2** - включает отладку IKEv2.

- **событие debug xconnect -** включает отладку событий xconnect.
- **покажите, что крипто-ikev2 диагностируют ошибку** - отображают выходную базу данных пути IKEv2.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация