دليل التكوين FlexVPN عبر L2TPv3

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
مخطط الشبكة
الموجه R1
الموجه R2
الموجه R3
الموجه R4
التحقق من الصحة
التحقق من اقتران أمان IPsec
التحقق من إنشاء IKEv2 SA
التحقق من نفق L2TPv3
التحقق من اتصال شبكة R1 ومظهرها
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين إرتباط الإصدار 3 (L2TPv3) لبروتوكول نفق الطبقة 2 للتشغيل عبر اتصال واجهة النفق الظاهرية (VTI) Cisco IOS FlexVPN بين موجهين يعملان ببرنامج Cisco IOS® Software. باستخدام هذه التقنية، يمكن توسيع شبكات الطبقة 2 بشكل آمن داخل نفق IPsec عبر نقلات متعددة من الطبقة 3، مما يتيح للأجهزة المنفصلة ماديا أن تظهر على شبكة LAN المحلية نفسها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- واجهة النفق الظاهري (VTI) IOS FlexVPN من Cisco
- بروتوكول الاتصال النفقي للطبقة 2 (L2TP)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الجيل 2 من موجه الخدمات المدمجة (G2) من Cisco، مع الأمان وترخيص البيانات.
- برنامج Cisco IOS الإصدار 15.1(1)T أو إصدار أحدث لدعم FlexVPN. أحلت لتفاصيل، ال cisco سمة متصفح.

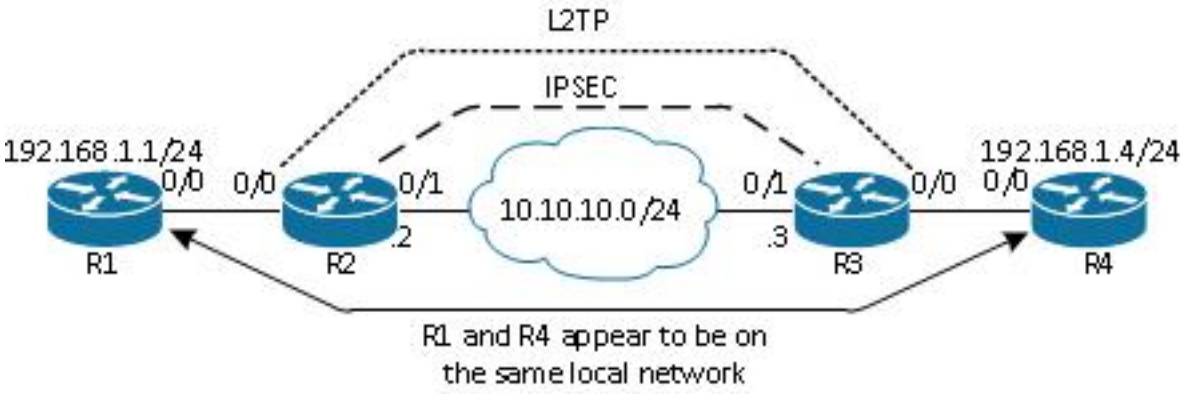
يستخدم تكوين FlexVPN هذا إعدادات افتراضية ذكية ومصادقة مفاتيح مشتركة مسبقا من أجل تبسيط التفسير. للحصول على أقصى قدر من الأمان، أستخدم تشفير الجيل التالي، ارجع إلى تشفير الجيل التالي للحصول على مزيد من المعلومات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

مخطط الشبكة

يستخدم هذا التكوين المخطط في هذه الصورة. قم بتغيير عناوين IP حسب الحاجة للتثبيت.



ملاحظة: في هذا الإعداد، يتم توصيل الموجهين R2 و R3 مباشرة، ولكن يمكن فصلهما بواسطة العديد من الخطوات. إذا تم فصل الموجهين R2 و R3، فتأكد من وجود مسار للوصول إلى عنوان IP النظير.

الموجه R1

يحتوي الموجه R1 على عنوان IP تم تكوينه على الواجهة:

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

الموجه R2

FlexVPN

يقوم هذا الإجراء بتكوين FlexVPN على الموجه R2.

1. إنشاء حلقة مفاتيح Internet Key Exchange الإصدار 2 (IKEv2) للنظير:

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

2. إنشاء ملف تعريف افتراضي IKEv2 يطابق موجه النظير ويستخدم مصادقة مفتاح مشترك مسبقا:

```
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. قم بإنشاء VTI، وأحميه باستخدام ملف التخصيص الافتراضي:

```
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

يقوم هذا الإجراء بتكوين L2TPv3 على الموجه R2.

1. قم بإنشاء فئة pseudowire لتحديد التضمين (L2TPv3)، وتحديد واجهة نفق FlexVPN التي يستخدمها اتصال L2TPv3 للوصول إلى الموجه النظير:

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

2. أستخدم xconnectCommand على الواجهة ذات الصلة لتكوين نفق L2TP؛ وتقديم عنوان النظير لواجهة النفق، وتحديد نوع التضمين:

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

الموجه R3

FlexVPN

يقوم هذا الإجراء بتكوين FlexVPN على الموجه R3.

1. إنشاء حلقة مفاتيح IKEv2 للنظير:

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

2. قم بإنشاء ملف تعريف افتراضي IKEv2 يطابق موجه النظير، ويستخدم مصادقة مفتاح مشترك مسبقا:

```
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. قم بإنشاء VTI، وأحميه باستخدام ملف التخصيص الافتراضي:

```
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

يقوم هذا الإجراء بتكوين L2TPv3 على الموجه R3.

1. قم بإنشاء فئة pseudowire لتحديد التضمين (L2TPv3)، وتحديد واجهة نفق FlexVPN التي يستخدمها اتصال L2TPv3 للوصول إلى الموجه النظير:

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

2. أستخدم xconnectCommand على الواجهة ذات الصلة لتكوين نفق L2TP؛ وتقديم عنوان النظير لواجهة النفق، وتحديد نوع التضمين:

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

الموجه R4

يحتوي الموجه R4 على عنوان IP تم تكوينه على الواجهة:

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

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

التحقق من اقتران أمان IPsec

يتحقق هذا المثال من إنشاء اقتران أمان IPsec بنجاح على الموجه R2 باستخدام نفق الواجهة 1.

```
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
```

التحقق من إنشاء IKEv2 SA

يتحقق هذا المثال من إنشاء اقتران أمان IKEv2 (SA) بنجاح على الموجه R2.

```
R2#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
none/none            READY      10.10.10.3/500      10.10.10.2/500          2
   ,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
```

التحقق من نفق L2TPv3

يتحقق هذا المثال من تكوين نفق L2TPv3 بشكل صحيح على الموجه 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
```

التحقق من اتصال شبكة R1 ومظهرها

يتحقق هذا المثال من أن الموجه R1 لديه اتصال شبكة بالموجه R4 ويبدو أنه على الشبكة المحلية نفسها.

```
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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها:

- **debug crypto ikev2** - قم بتمكين تصحيح أخطاء IKEv2.
- **debug xconnect event** - تمكين تصحيح أخطاء حدث xconnect.
- **إظهار خطأ تشخيص IKEV2** - عرض قاعدة بيانات مسار الخروج من IKEv2.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).