مثال تكوين FlexVPN من موقع إلى موقع

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين نفق أمان بروتوكول الإنترنت (IPsec)/تضمين التوجيه العام (GRE) من موقع إلى موقع FlexVPN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

أمر.

الاصطلاحات

أحلت ال cisco في طرف إتفاق لمعلومة على وثيقة إتفاق.

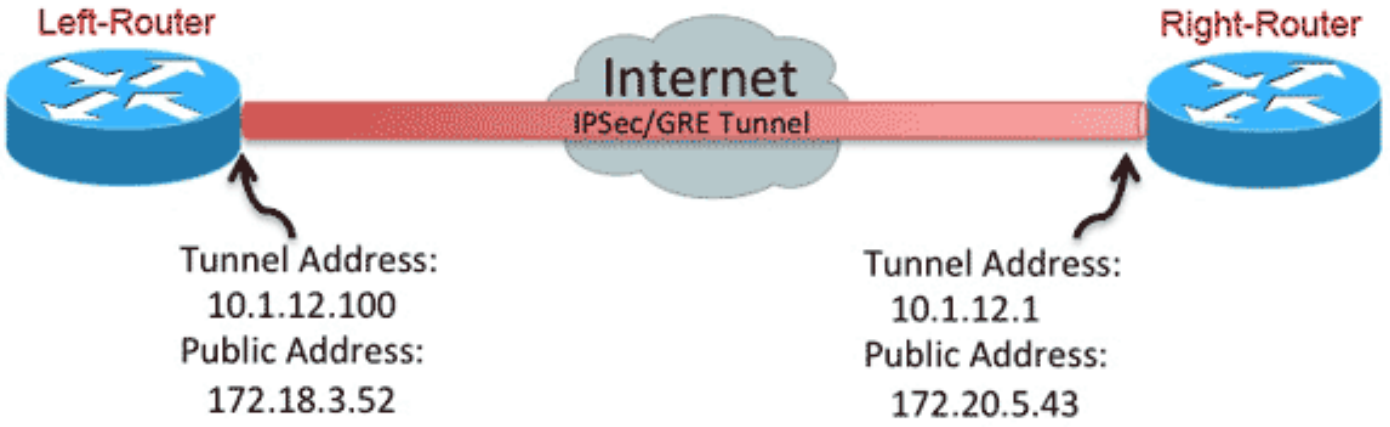
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين نفق PSK

يصف الإجراء الوارد في هذا القسم كيفية إستخدام مفتاح مشترك مسبقا (PSK) لتكوين الأنفاق في بيئة الشبكة هذه.

الموجه الأيسر

1. تكوين حلقة المفاتيح الخاصة ب Internet Key Exchange الإصدار 2 (IKEv2):

```
crypto ikev2 keyring mykeys
 peer Right-Router
  address 172.20.5.43
  pre-shared-key Cisco123
 !
```

2. أعد تكوين ملف التعريف الافتراضي IKEv2 من أجل:
المطابقة على معرف IKEتعيين أساليب المصادقة للمحلي والبعيدالإشارة إلى حلقة المفاتيح المدرجة في الخطوة السابقة

```
crypto ikev2 profile default
match identity remote address 172.20.5.43 255.255.255.255
authentication local pre-share
authentication remote pre-share
keyring local mykeys
dpd 60 2 on-demand
!
```

3. أعد تكوين ملف تعريف IPsec الافتراضي للإشارة إلى ملف تعريف IKEv2 الافتراضي:

```
crypto ipsec profile default
set ikev2-profile default
!
interface Tunnel0
ip address 10.1.12.100 255.255.255.0
tunnel source Ethernet0/0
tunnel destination 172.20.5.43
tunnel protection ipsec profile default
!
```

4. قم بتكوين واجهات LAN و WAN:

```
interface Ethernet0/0
description WAN
ip address 172.18.3.52 255.255.255.0
!
interface Ethernet0/1
description LAN
ip address 192.168.100.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.18.3.1 name route_to_internet
```

موجه أيمن

كرر الخطوات من تكوين الموجه الأيسر، ولكن مع التغييرات الضرورية التالية:

```
crypto ikev2 keyring mykeys
peer Left-Router
address 172.18.3.52
pre-shared-key Cisco123
!
crypto ikev2 profile default
match identity remote address 172.18.3.52 255.255.255.255
authentication local pre-share
authentication remote pre-share
keyring local mykeys
dpd 60 2 on-demand
!
crypto ipsec profile default
set ikev2-profile default
!
interface Tunnel0
ip address 10.1.12.1 255.255.255.0
tunnel source Ethernet0/0
tunnel destination 172.18.3.52
tunnel protection ipsec profile default
!
interface Ethernet0/0
description WAN
ip address 172.20.5.43 255.255.255.0
```

```
!
interface Ethernet0/1
 description LAN
 ip address 192.168.200.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.20.5.1 name route_to_internet
```

تكوين نفق PKI

بعد اكتمال النفق من القسم السابق مع PSK، يمكن تغييره بسهولة لاستخدام البنية الأساسية للمفتاح العام (PKI) للمصادقة. في هذا المثال، يقوم الموجه الأيسر بمصادقة نفسه باستخدام شهادة إلى الموجه الأيمن. يستمر الموجه الأيمن في إستخدام PSK لمصادقة نفسه على الموجه الأيسر. وقد تم القيام بذلك لإظهار المصادقة غير المتماثلة، ومع ذلك، فمن الطبيعي أن يتم تبديل كلا المحولين لاستخدام مصادقة الشهادة.

الموجه الأيسر

1. تكوين المرجع المصدق CA) IOS®) من Cisco على الموجه:

```
Left-Router#config t
Left-Router(config)#ip http server
Left-Router(config)#crypto pki server S2S-CA
"Left-Router(cs-server)#issuer-name cn="S2S-CA
Left-Router(cs-server)#grant auto
Left-Router(cs-server)#no shut
.Some server settings cannot be changed after CA certificate generation%
Please enter a passphrase to protect the private key %
or type Return to exit %
:Password

:Re-enter password
...Generating 1024 bit RSA keys, keys will be non-exportable %
(OK] (elapsed time was 0 seconds]
...Exporting Certificate Server signing certificate and keys %
```

2. مصادقة TrustPoint ID وتسجيله:

```
Left-Router#config t
Left-Router(config)#ip domain name cisco.com
Left-Router(config)#crypto pki trustpoint S2S-ID
Left-Router(ca-trustpoint)#enrollment url http://172.18.3.52:80
Left-Router(ca-trustpoint)#subject-name cn=Left-Router.cisco.com
Left-Router(ca-trustpoint)#exit
Left-Router(config)#crypto pki authenticate S2S-ID
:Certificate has the following attributes
Fingerprint MD5: C11CD575 EC2DEACD 97E9AA3A 2DACFCAB
Fingerprint SHA1: A8A6E79B D1932175 F12652F1 4F967077 3AEFAF08

Do you accept this certificate? [yes/no]: yes %
.Trustpoint CA certificate accepted
#(Left-Router(config
Left-Router(config)#crypto pki enroll S2S-ID
%
.. Start certificate enrollment %
Create a challenge password. You will need to verbally provide this %
.password to the CA Administrator in order to revoke your certificate
.For security reasons your password will not be saved in the configuration
.Please make a note of it

:Password
```

```
                                                                :Re-enter password
                Oct 29 15:15:50.287: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*

                    The subject name in the certificate will include: cn=R1.cisco.com %
                       The subject name in the certificate will include: R1.cisco.com %
                  Include the router serial number in the subject name? [yes/no]: no %
                                Include an IP address in the subject name? [no]: no %
                                          Request certificate from CA? [yes/no]: yes
                                       Certificate request sent to Certificate Authority %
.The 'show crypto pki certificate verbose S2S-ID' command will show the fingerprint %

                     :Oct 29 15:15:57.722: CRYPTO_PKI: Certificate Request Fingerprint MD5*
                                                        CA34FD51 A85007EF A785E058 60D8877D
                    :Oct 29 15:15:57.722: CRYPTO_PKI: Certificate Request Fingerprint SHA1*
                                                    E37AAE3C 851953C3 9FABE1FD 2F0EACD5 566F361E
                                                                Left-Router(config)#exit
                                                                        #Left-Router
Oct 29 15:16:57.829: %PKI-6-CERTRET: Certificate received from Certificate Authority*
```

3. إعادة تكوين ملف تعريف IKEv2:

```
                                                    crypto ikev2 profile default
                                                     authentication local rsa-sig
                                                                identity local dn
                                                            pki trustpoint S2S-ID
```

موجه أيمن

1. مصادقة نقطة ثقة CA بحيث يمكن للموجه التحقق من شهادة الموجه الأيسر:

```
                                                                Right-Router#config t
                                                    Right-Router(config)#ip domain name cisco.com
                                                Right-Router(config)#crypto pki trustpoint S2S-ID
                                    Right-Router(ca-trustpoint)#enrollment url http://172.18.3.52:80
                                                Right-Router(ca-trustpoint)#revocation-check none
                                                            Right-Router(ca-trustpoint)#exit
Right-Router(config)#crypto pki authenticate S2S-IDCertificate has the following
                                                                                    :attributes
                                                Fingerprint MD5: C11CD575 EC2DEACD 97E9AA3A 2DACFCAB
                                            Fingerprint SHA1: A8A6E79B D1932175 F12652F1 4F967077 3AEFAF08

                                                    Do you accept this certificate? [yes/no]: yes %
                                                                .Trustpoint CA certificate accepted
                                                                        #(Right-Router(config
```

2. أعد تكوين ملف تعريف IKEv2 لمطابقة الاتصال الوارد:

```
                                                  crypto pki certificate map S2S-Cert-Map 10
                                                                  issuer eq cn=S2S-CA
                                                        crypto ikev2 profile default
                                                      match certificate S2S-Cert-Map
                                                       authentication remote rsa-sig
```

التحقق من الصحة

أستخدم الأمر **show crypto ikev2 sa detail** للتحقق من التكوين.

يظهر الموجه الأيمن ما يلي:

- علامة المصادقة = كيفية مصادقة هذا الموجه لنفسه على الموجه الأيسر = مفتاح مشترك مسبقا

- التحقق من المصادقة = كيفية مصادقة الموجه الأيسر مع هذا الموجه = RSA (الشهادة)
- معرف محلي/بعيد = هويات ISAKMP المتبادلة

```
IPv4 Crypto IKEv2  SA

Tunnel-id Local Remote fvrf/ivrf Status
none/none READY 172.18.3.52/500 172.20.5.43/500 1
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: RSA
Life/Active Time: 86400/3165 sec
CE id: 1043, Session-id: 22
Status Description: Negotiation done
Local spi: 3443E884EB151E8D Remote spi: 92779BC873F58132
Local id: 172.20.5.43
Remote id: hostname=Left-Router.cisco.com,cn=Left-Router.cisco.com
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 60 seconds, retry 2
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

تكوين التوجيه

يتيح مثال التكوين السابق إنشاء النفق، ولكنه لا يوفر أي معلومات حول التوجيه (أي الوجهات المتاحة عبر النفق). باستخدام IKEv2، هناك طريقتان لتبادل هذه المعلومات: بروتوكولات التوجيه الديناميكية ومسارات IKEv2.

بروتوكولات التوجيه الديناميكية

بما أن النفق هو نفق GRE من نقطة إلى نقطة، فإنه يتصرف مثل أي واجهة أخرى من نقطة إلى نقطة (على سبيل المثال: تسلسلي، متصل)، ومن الممكن تشغيل أي بروتوكول العبارة الداخلية (IGP)/بروتوكول العبارة الخارجية (EGP) عبر الارتباط لتبادل معلومات التوجيه. هنا مثال من يحسن داخلي مدخل تحشد بروتوكول (EIGRP):

1. قم بتكوين الموجه الأيسر لتمكين EIGRP والإعلان عنه على واجهات الشبكة المحلية (LAN) والنفق:

```
router eigrp 100
 no auto-summary
network 10.1.12.0 0.0.0.255
network 192.168.100.0 0.0.0.255
```

2. قم بتكوين الموجه الأيمن لتمكين EIGRP والإعلان عنه على واجهات الشبكة المحلية (LAN) والنفق:

```
router eigrp 100
 no auto-summary
network 10.1.12.0 0.0.0.255
network 192.168.200.0 0.0.0.255
```

3. تأكد من أن المسار إلى 24/192.168.200.0 يتم تعلمه عبر النفق عبر EIGRP:

```
Left-Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
                    E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
                                replicated route, % - next hop override - +

                        Gateway of last resort is 172.18.3.1 to network 0.0.0.0

                                                S* 0.0.0.0/0 [1/0] via 172.18.3.1
                           is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                                 C 10.1.12.0/24 is directly connected, Tunnel0
                                L 10.1.12.100/32 is directly connected, Tunnel0
                        is variably subnetted, 2 subnets, 2 masks 172.18.0.0/16
                             C 172.18.3.0/24 is directly connected, Ethernet0/0
                            L 172.18.3.52/32 is directly connected, Ethernet0/0
                     is variably subnetted, 2 subnets, 2 masks 192.168.100.0/24
                          C 192.168.100.0/24 is directly connected, Ethernet0/1
                          L 192.168.100.1/32 is directly connected, Ethernet0/1
        D 192.168.200.0/24 [90/27008000] via 10.1.12.1, 00:00:22, Tunnel0
```

مسارات بروتوكول IKEv2

وبدلا من إستخدام مسارات بروتوكول التوجيه الديناميكي للتعرف على الوجهات عبر النفق، يمكن تبادل المسارات أثناء إنشاء رابطة أمان IKEv2 (SA).

1. على الموجه الأيسر، قم بتكوين قائمة بالشبكات الفرعية التي أعلن عنها الموجه الأيسر إلى الموجه الأيمن:

```
ip access-list standard Net-List
  permit 192.168.100.0 0.0.0.255
```

2. على الموجه الأيسر، قم بتكوين سياسة تفويض لتحديد الشبكات الفرعية التي سيتم الإعلان عنها: /32 التي تم تكوينها على واجهة النفق/24 المسار المشار إليه في قائمة التحكم في الوصول (ACL)

```
crypto ikev2 authorization policy default
                                route set interface
                          route set access-list Net-List
```

3. على الموجه الأيسر، قم بإعادة تكوين ملف تعريف IKEv2 للإشارة إلى سياسة التخويل عند إستخدام المفاتيح المشتركة مسبقا:

```
crypto ikev2 profile default
aaa authorization group psk list default default
```

4. على الموجه الأيمن، كرر الخطوات 1 و 2 واضبط توصيف IKEv2 للإشارة إلى سياسة التخويل عند إستخدام الشهادات:

```
ip access-list standard Net-List
  permit 192.168.200.0 0.0.0.255

crypto ikev2 authorization policy default
                                route set interface
                          route set access-list Net-List

                                crypto ikev2 profile default
aaa authorization group cert list default default
```

5. أستخدم الأوامر **shutdown** و**no shutdown** على واجهة النفق لإجبار تنفيذ IKEv2 SA جديد.

6. تحقق من تبادل مسارات IKEv2. راجع "الشبكات الفرعية البعيدة" في إخراج هذا النموذج:

```
Right-Router#show crypto ikev2 sa detailed
                                IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
```

```
                                    none/none READY 172.18.3.52/500 172.20.5.43/500 1
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: RSA
                                                  Life/Active Time: 86400/3165 sec
                                                       CE id: 1043, Session-id: 22
                                                Status Description: Negotiation done
                                Local spi: 3443E884EB151E8D Remote spi: 92779BC873F58132
                                                          Local id: 172.20.5.43
                                Remote id: hostname=R100.cisco.com,cn=R100.cisco.com
                                                Local req msg id: 0 Remote req msg id: 4
                                              Local next msg id: 0 Remote next msg id: 4
                                                Local req queued: 0 Remote req queued: 4
                                                        Local window: 5 Remote window: 5
                                                DPD configured for 60 seconds, retry 2
                                                          NAT-T is not detected
                                Cisco Trust Security SGT is disabled Initiator of SA : No

                                                                  :Remote subnets
                                                              255.255.255.255 10.1.12.100
                                                              255.255.255.0 192.168.100.0

                                                                 IPv6 Crypto IKEv2 SA
```

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).