الموجه IOS VPN: إضافة شبكة أو إزالتها على نفق L2L VPN مثال تكوين

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل ل كيف أن يضيف أو يزيل شبكة على موجود lan إلى VPN (L2L) lan نفق.

المتطلبات الأساسية

المتطلبات

تأكد من تكوين نفق VPN الحالي بشكل صحيح ل L2L IPsec قبل محاولة هذا التكوين.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى موجهات Cisco IOS® التي تشغل الإصدار T1(15)12.4 من البرنامج.

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

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يوجد حاليا نفق L2L VPN بين المكتب الرئيسي (HQ) والمكتب الفرعي (BO). قام مكتب المقر الرئيسي بإضافة شبكة جديدة ليتم إستخدامها من قبل فريق المبيعات. يحتاج هذا الفريق إلى الوصول إلى الموارد الموجودة في مكتب مكتب عمليات حفظ السلام. تتمثل المهمة الحالية في إضافة شبكة جديدة إلى نفق L2L VPN الموجود بالفعل.

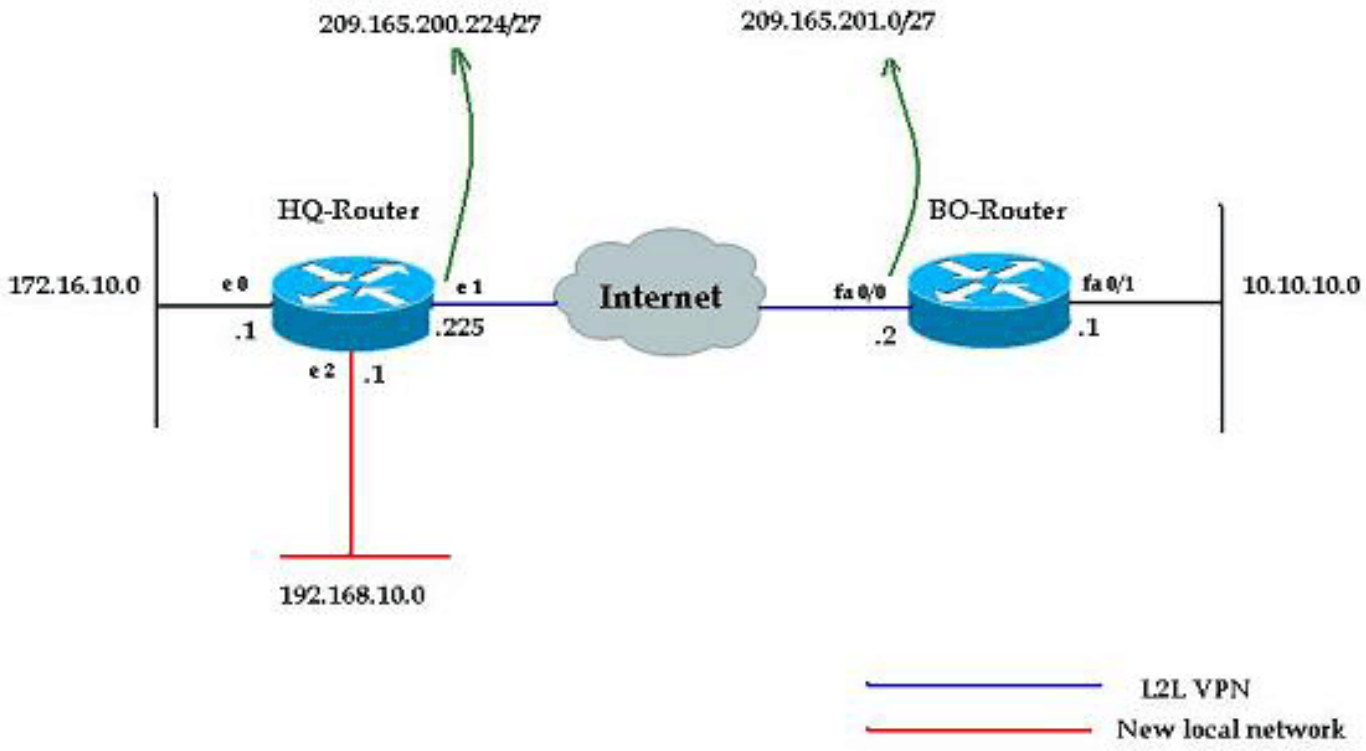
التكوين

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:



التكوينات

يستخدم هذا المستند التكوينات الموضحة في هذا القسم. تتضمن هذه التكوينات شبكة VPN L2L التي يتم تشغيلها بين شبكة 172.16.10.0 من مكتب HQ وشبكة 10.10.10.0 من مكتب BO. يوضح الإخراج المعروض بنص غامق التكوين المطلوب لدمج الشبكة الجديدة 192.168.10.0 من مكتب HQ في نفق VPN نفسه مع 10.10.10.0 كشبكة الوجهة.

الموجه من HQ
HQ-Router#**show running-config** ...Building configuration Current configuration : 1439 bytes

```
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname HQ-Router
Output suppressed. ! crypto isakmp policy 1 hash ---!!
md5 authentication pre-share crypto isakmp key cisco123
address 209.165.200.225 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.200.225 set transform-set rtpset
match address 115 ! interface Ethernet0 ip address
172.16.10.1 255.255.255.0 ip nat inside ! interface
Ethernet1 ip address 209.165.201.2 255.255.255.224 ip
nat outside crypto map rtp ! interface Ethernet2 ip
address 192.168.10.1 255.255.255.0 ip nat inside !
interface Serial0 no ip address shutdown no fair-queue !
interface Serial1 no ip address shutdown ! ip nat inside
source route-map nonat interface Ethernet1 overload ip
classless ip route 0.0.0.0 0.0.0.0 209.165.201.1 ! !---
Output suppressed. access-list 110 deny ip 172.16.10.0
0.0.0.255 10.10.10.0 0.0.0.255 access-list 110 permit ip
172.16.10.0 0.0.0.255 any ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
rule. access-list 110 deny   ip 192.168.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 192.168.10.0 0.0.0.255 any
access-list 115 permit ip 172.16.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
Add this ACL entry to include 192.168.10.0 !--- ---!
network into the crypto map. access-list 115 permit ip
192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255
route-map nonat permit 10
match ip address 110
!
Output suppressed. end ---!
```

موجه Bo

```
BO-Router#show running-config
...Building configuration

Current configuration : 2836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BO-Router
Output suppressed. ! crypto isakmp policy 1 hash ---!!
md5 authentication pre-share crypto isakmp key cisco123
address 209.165.201.2 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.201.2 set transform-set rtpset
match address 115 ! !--- Output suppressed. interface
FastEthernet0/0 ip address 209.165.200.225
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.10.10.1 255.255.255.0 ip
nat inside ip virtual-reassembly duplex auto speed auto
```

```
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 ! !--- Output
suppressed. ! ip http server no ip http secure-server ip
                nat inside source route-map nonat interface
   FastEthernet0/0 overload ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
    rule. access-list 110 deny   ip 10.10.10.0 0.0.0.255
                                      192.168.10.0 0.0.0.255
          access-list 110 deny   ip 10.10.10.0 0.0.0.255
                                      172.16.10.0 0.0.0.255
     access-list 110 permit ip 10.10.10.0 0.0.0.255 any
         access-list 115 permit ip 10.10.10.0 0.0.0.255
                                      172.16.10.0 0.0.0.255
                                                          !
   Add this ACL entry to include 192.168.10.0 !--- ---!
  network into the crypto map. access-list 115 permit ip
              10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
                                                          !
                                   route-map nonat permit 10
                                       match ip address 110
                                                          !
                                 Output suppressed. ! end ---!
```

إزالة شبكة من نفق IPsec

أكمل الخطوات الموضحة في هذا القسم لإزالة الشبكة من تكوين نفق IPsec. لاحظ أنه تمت إزالة الشبكة 24/192.168.10.0 من تكوين موجه HQ.

1. أستخدم هذا الأمر لقطع اتصال IPsec:
```
HQ-Router#clear crypto sa
```

2. أستخدم هذا الأمر لمسح اقترانات أمان (ISAKMPSecurity (SAs:
```
HQ-Router#clear crypto isakmp
```

3. أستخدم هذا الأمر لإزالة قائمة التحكم في الوصول (ACL) لحركة المرور المفيدة لنفق IPsec:
```
HQ-Router(config)#no access-list 115 permit ip
0.0.0.255 10.10.10.0 0.0.0.255 192.168.10.0
```

4. أستخدم هذا الأمر لإزالة بيان قائمة التحكم في الوصول (ACL) المعفاة من nat لشبكة 192.168.10.0:
```
HQ-Router(config)#no access-list 110 deny ip
0.0.0.255 10.10.10.0 0.0.0.255 192.168.10.0
```

5. استعملت هذا أمر in order to يمسح ال nat ترجمة:
```
* HQ-Router#clear ip nat translation
```

6. أستخدم هذه الأوامر لإزالة خريطة التشفير وإعادة تطبيقها على الواجهة لضمان تأثير تكوين التشفير الحالي:
```
HQ-Router(config)#int ethernet 1

HQ-Router(config-if)#no crypto map rtp

May 25 10:35:12.153: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF*

HQ-Router(config-if)#crypto map rtp

May 25 10:36:09.305: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON*
```

ملاحظة: تؤدي إزالة خريطة التشفير من الواجهة إلى إزالة جميع إتصالات VPN الموجودة المقترنة بخريطة التشفير هذه. قبل القيام بذلك، يرجى التأكد من أنك قمت بإلغاء الوقت المطلوب واتبعت سياسة التحكم في التغيير الخاصة بمؤسستك وفقا لذلك.

7. أستخدم الأمر **write memory** لحفظ التكوين النشط في ذاكرة Flash (الذاكرة المؤقتة) .
8. أتمت هذا steps على الآخر نهاية من ال VPN نفق (in order to BO-Router) أزلت التشكيل.
9. ابدأ نفق IPsec وتحقق من الاتصال.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

أستخدم تسلسل إختبار الاتصال هذا لضمان إمكانية تمرير الشبكة الجديدة للبيانات من خلال نفق VPN:

```
HQ-Router#clear crypto sa
#HQ-Router
HQ-Router#ping 10.10.10.1 source 172.16.10.1

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds
Packet sent with a source address of 172.16.10.1
!!!!.
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms
HQ-Router#ping 10.10.10.1 source 192.168.10.1

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds
Packet sent with a source address of 192.168.10.1
!!!!.
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms
HQ-Router#ping 10.10.10.1 source 192.168.10.1

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

show crypto ipsec sa

```
HQ-Router#show crypto ipsec sa

interface: Ethernet1
    Crypto map tag: rtp, local addr. 209.165.201.2

   local  ident (addr/mask/prot/port):
          ((192.168.10.0/255.255.255.0/0/0
   remote ident (addr/mask/prot/port):
          ((10.10.10.0/255.255.255.0/0/0
     current_peer: 209.165.200.225
       {,PERMIT, flags={origin_is_acl
  pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9#
  pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9#
     pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts compr. failed: 0,#
                  #pkts decompress failed: 0
   send errors 1, #recv errors 0#

  local crypto endpt.: 209.165.201.2, remote crypto
                       endpt.: 209.165.200.225
    path mtu 1500, ip mtu 1500, ip mtu interface
                                    Ethernet1
     current outbound spi: FB52B5AB
```

```
                                    :inbound esp sas
                          (spi: 0x612332E(101856046
              , transform: esp-des esp-md5-hmac
                    { ,in use settings ={Tunnel
slot: 0, conn id: 2002, flow_id: 3, crypto map:
                                                rtp
     sa timing: remaining key lifetime (k/sec):
                                          ((4607998/3209
                                IV size: 8 bytes
                    replay detection support: Y

                                     :inbound ah sas

                                    :inbound pcp sas

                                   :outbound esp sas
                       (spi: 0xFB52B5AB(4216501675
              , transform: esp-des esp-md5-hmac
                    { ,in use settings ={Tunnel
slot: 0, conn id: 2003, flow_id: 4, crypto map:
                                                rtp
     sa timing: remaining key lifetime (k/sec):
                                          ((4607998/3200
                                IV size: 8 bytes
                    replay detection support: Y

                                     :outbound ah sas

                                    :outbound pcp sas


                local  ident (addr/mask/prot/port):
                       ((172.16.10.0/255.255.255.0/0/0
                remote ident (addr/mask/prot/port):
                        ((10.10.10.0/255.255.255.0/0/0
                          current_peer: 209.165.200.225
                    {,PERMIT, flags={origin_is_acl
  pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4#
  pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4#
         pkts compressed: 0, #pkts decompressed: 0#
   pkts not compressed: 0, #pkts compr. failed: 0,#
                               #pkts decompress failed: 0
                     send errors 1, #recv errors 0#

 local crypto endpt.: 209.165.201.2, remote crypto
                                  endpt.: 209.165.200.225
      path mtu 1500, ip mtu 1500, ip mtu interface
                                                Ethernet1
                    current outbound spi: C9E9F490

                                    :inbound esp sas
                       (spi: 0x1291F1D3(311554515
              , transform: esp-des esp-md5-hmac
                    { ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map:
                                                rtp
     sa timing: remaining key lifetime (k/sec):
                                          ((4607999/3182
                                IV size: 8 bytes
                    replay detection support: Y

                                     :inbound ah sas
```

```
                                    :inbound pcp sas

                                   :outbound esp sas
                        (spi: 0xC9E9F490(3387552912
                , transform: esp-des esp-md5-hmac
                     { ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map:
                                                rtp
     sa timing: remaining key lifetime (k/sec):
                                            ((4607999/3182
                                  IV size: 8 bytes
                       replay detection support: Y

                                    :outbound ah sas

                                   :outbound pcp sas
```

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

استكشاف الأخطاء وإصلاحها

استخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

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

- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto engine**—يعرض الجلسات المشفرة.

معلومات ذات صلة

- مقدمة عن تشفير أمان IP (IPSec)
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- تكوين نظير شبكة LAN إلى شبكة LAN الديناميكية لموجه IPsec وعملاء شبكة VPN الديناميكية
- 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).