PIX/ASA 7.x: إضافة/إزالة شبكة على مثال دوجوم L2L VPN تكوين نفق

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل ل كيف أن يضيف شبكة جديد إلى موجود VPN نفق.

المتطلبات الأساسية

المتطلبات

تأكد من وجود جهاز أمان PIX/ASA لديك الذي يشغل الرمز 7.x قبل أن تحاول إجراء هذا التكوين.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهازي أمان Cisco 5500.

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان PIX 500.

الاصطلاحات

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

معلومات أساسية

هناك حاليا نفق VPN لشبكة LAN إلى شبكة LAN (L2L) يقع بين مكتب NY و TN. لقد أضاف مكتب نيويورك شبكة جديدة ستستخدمها مجموعة تطوير مبادرة أمن الحاويات. تتطلب هذه المجموعة الوصول إلى الموارد الموجودة في مكتب TN. تتمثل المهمة الحالية في إضافة الشبكة الجديدة إلى نفق VPN الموجود بالفعل.

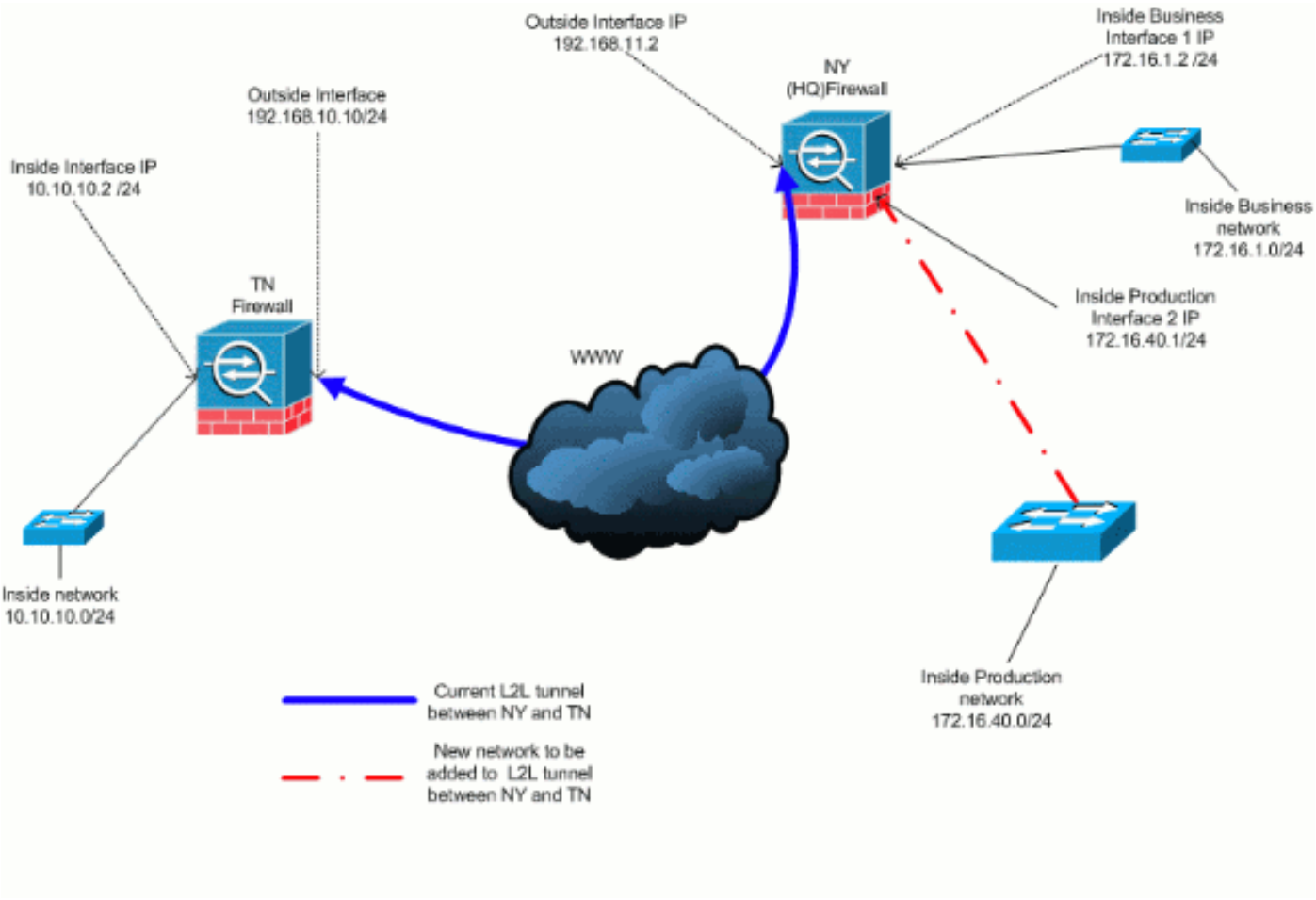
التكوين

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:



إضافة شبكة إلى نفق IPSec

يستعمل هذا وثيقة هذا تشكيل:

تكوين جدار حماية (HQ NY)

```
ASA-NY-HQ#show running-config

Saved :
:
(ASA Version 7.2(2
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 192.168.11.2 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
nameif Cisco
security-level 70
ip address 172.16.40.2 255.255.255.0
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp2.com
access-list inside_nat0_outbound extended permit ip
172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0

   You must be sure that you configure the !--- ---!
opposite of these access control lists !--- on the other
 end of the VPN tunnel. access-list inside_nat0_outbound
extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0

access-list outside_20_cryptomap extended permit ip
172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0

   You must be sure that you configure the !--- ---!
opposite of these access control lists !--- on the other
 end of the VPN tunnel. access-list outside_20_cryptomap
extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

```
Output is suppressed. nat-control global (outside) ---!
                1 interface nat (inside) 0 access-list
        inside_nat0_outbound nat (inside) 1 172.16.1.0
 255.255.255.0 !--- The new network is also required to
have access to the Internet. !--- So enter an entry into
 the NAT statement for this new network. nat (inside) 1
                                 172.16.40.0 255.255.255.0

        route outside 0.0.0.0 0.0.0.0 192.168.11.100 1
                                    timeout xlate 3:00:00
   timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                              icmp 0:00:02
  timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
                                   0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                  sip-disconnect 0:02:00
                          timeout uauth 0:05:00 absolute
                                 no snmp-server location
                                 no snmp-server contact
    snmp-server enable traps snmp authentication linkup
                                        linkdown coldstart
  crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
                                                sha-hmac
              crypto map outside_map 20 match address
                                  outside_20_cryptomap
      crypto map outside_map 20 set peer 192.168.10.10
crypto map outside_map 20 set transform-set ESP-3DES-SHA
              crypto map outside_map interface outside
                           crypto isakmp enable outside
                                crypto isakmp policy 10
                             authentication pre-share
                                     encryption 3des
                                            hash sha
                                             group 2
                                        lifetime 86400
                        crypto isakmp nat-traversal  20
            tunnel-group 192.168.10.10 type ipsec-l2l
          tunnel-group 192.168.10.10 ipsec-attributes
                                        * pre-shared-key
          #Output is suppressed. : end ASA-NY-HQ ---!
```

إزالة الشبكة من نفق IPSec

أستخدم هذه الخطوات لإزالة الشبكة من تكوين نفق IPSec.هنا، ضع في الاعتبار إزالة الشبكة 24/172.16.40.0 من تكوين جهاز أمان HQ) NY).

1. قبل إزالة الشبكة من النفق، قم بإزالة اتصال IPSec، والذي يعمل أيضا على مسح اقترانات الأمان المتعلقة بالمرحلة 2.

```
ASA-NY-HQ# clear crypto ipsec sa
```

يمحي الرابطات الأمنية ذات الصلة بالمرحلة الأولى على النحو التالي

```
ASA-NY-HQ# clear crypto isakmp sa
```

2. قم بإزالة قائمة التحكم في الوصول (ACL) الخاصة بحركة المرور المثيرة للاهتمام لأنفاق IPSec.

```
ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0
                                  255.255.255.0 10.10.10.0 255.255.255.0
```

3. قم بإزالة قائمة التحكم في الوصول (inside_nat0_outbound)، نظرا لاستثناء حركة المرور من nat.

```
ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

4. مسح ترجمة NAT كما هو موضح

```
ASA-NY-HQ# clear xlate
```

5. عند قيامك بتعديل تكوين النفق، قم بإزالة أوامر التشفير هذه وإعادة تطبيقها لأخذ أحدث تكوين في الواجهة الخارجية

```
ASA-NY-HQ(config)# crypto map outside_map interface outside
ASA-NY-HQ(config)# crypto isakmp enable outside
```

6. حفظ التكوين النشط في ذاكرة الفلاش **"write memory"**.
7. اتبع نفس الإجراء للطرف الآخر - جهاز أمان TN لإزالة التكوينات.
8. أدخل نفق IPSec وتحقق من الاتصال.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

- **إختبار الاتصال داخل 172.16.40.20**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.40.20, timeout is 2 seconds:
?!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

- **show crypto isakmp sa**

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.10.10
Type    : L2L             Role    : initiator
Rekey   : no              State   : MM_ACTIVE
```

- **show crypto ipsec sa**

```
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

      access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 172.16.40.0 255.255.255.0
      local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.40.0/255.255.255.0/0/0)
      current_peer: 192.168.10.10

      #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: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 4C0547DE

    inbound esp sas:
      spi: 0x0EB40138 (246677816)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28476)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x4C0547DE (1275414494)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28476)
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

      access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      current_peer: 192.168.10.10

      #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 14, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 5CC4DE89

    inbound esp sas:
      spi: 0xF48286AD (4102194861)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28271)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x5CC4DE89 (1556405897)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274998/28271)
         IV size: 8 bytes
         replay detection support: Y
```

استكشاف الأخطاء وإصلاحها

راجع هذه المستندات للحصول على مزيد من معلومات أستكشاف الأخطاء وإصلاحها:

- حلول أستكشاف أخطاء VPN وإصلاحها ل IPsec
- فهم أوامر تصحيح الأخطاء واستخدامها
- أستكشاف أخطاء الاتصالات وإصلاحها من خلال كل من PIX و ASA

معلومات ذات صلة

- مقدمة لتشفير أمان IPsec) IP)
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- مرجع أمر جهاز الأمان
- تكوين قوائم الوصول إلى IP
- 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).