# PIX/ASA 7.x: إضافة نفق جديد أو وصول عن بعد إلى شبكة L2L VPN موجودة

## المحتويات



## المقدمة

يقدم هذا المستند الخطوات المطلوبة لإضافة نفق VPN جديد أو شبكة VPN للوصول عن بعد إلى تكوين L2L VPN موجود بالفعل. ارجع إلى أجهزة الأمان المعدلة Cisco ASA 5500 Series - أمثلة التكوين و TechNotes للحصول على معلومات حول كيفية إنشاء أنفاق الشبكة الخاصة الظاهرية (VPN) الأولية من IPSec ولمزيد من أمثلة التكوين.

## المتطلبات الأساسية

### المتطلبات

تأكد من تكوين نفق VPN ل L2L IPsec بشكل صحيح والذي يعمل حاليا قبل أن تحاول إجراء هذا التكوين.

### المكونات المستخدمة

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

- جهازا أمان ASA يركزان على الرمز x.7
- جهاز أمان PIX واحد يشغل الرمز x.7

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

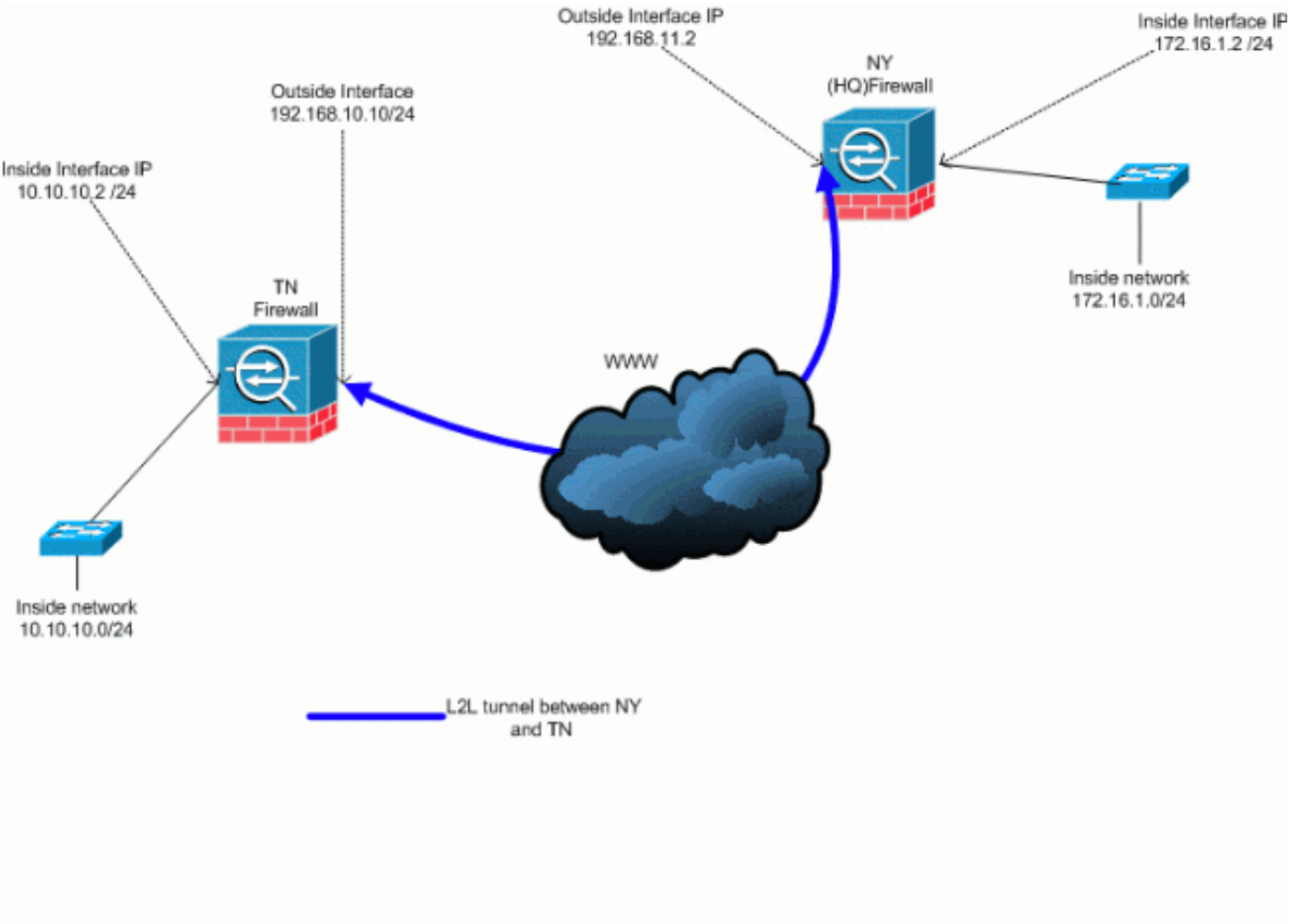
المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

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

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:




هذا المخرج هو التكوين الجاري تشغيله الحالي لجهاز أمان NY (HUB). في هذا التكوين، هناك نفق IPSec L2L تم تكوينه بين NY(HQ) و TN.

**تكوين جدار حماية NY (HQ) الحالي**

```
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
                                                    shutdown
                                                  no nameif
                                             no security-level
                                                 no ip address
                                                                !
                                        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
                                    255.255.255.0 10.10.10.0
        access-list outside_20_cryptomap extended permit ip
                                    172.16.1.0 255.255.255.0
                                    255.255.255.0 10.10.10.0

 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 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 * telnet timeout 1440 ssh timeout 5
      console timeout 0 ! class-map inspection_default match
      default-inspection-traffic ! ! policy-map type inspect
```

```
dns preset_dns_map parameters message-length maximum 512
       policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
    inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
     policy global_policy global prompt hostname context
   Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end
                                                #ASA-NY-HQ
```

## معلومات أساسية

حاليا، هناك نفق L2L موجود تم إعداده بين مكتب NY(HQ) ومكتب TN. قامت شركتك مؤخرا بفتح مكتب جديد موجود في TX. ويتطلب هذا المكتب الجديد الاتصال بالموارد المحلية الموجودة في مكتبي نيويورك وتشرين. بالإضافة إلى ذلك، هناك حاجة إضافية للسماح للموظفين بفرصة العمل من المنزل والوصول الآمن إلى الموارد الموجودة على الشبكة الداخلية عن بعد. في هذا المثال، تم تكوين نفق VPN جديد بالإضافة إلى خادم VPN للوصول عن بعد موجود في مكتب نيويورك.

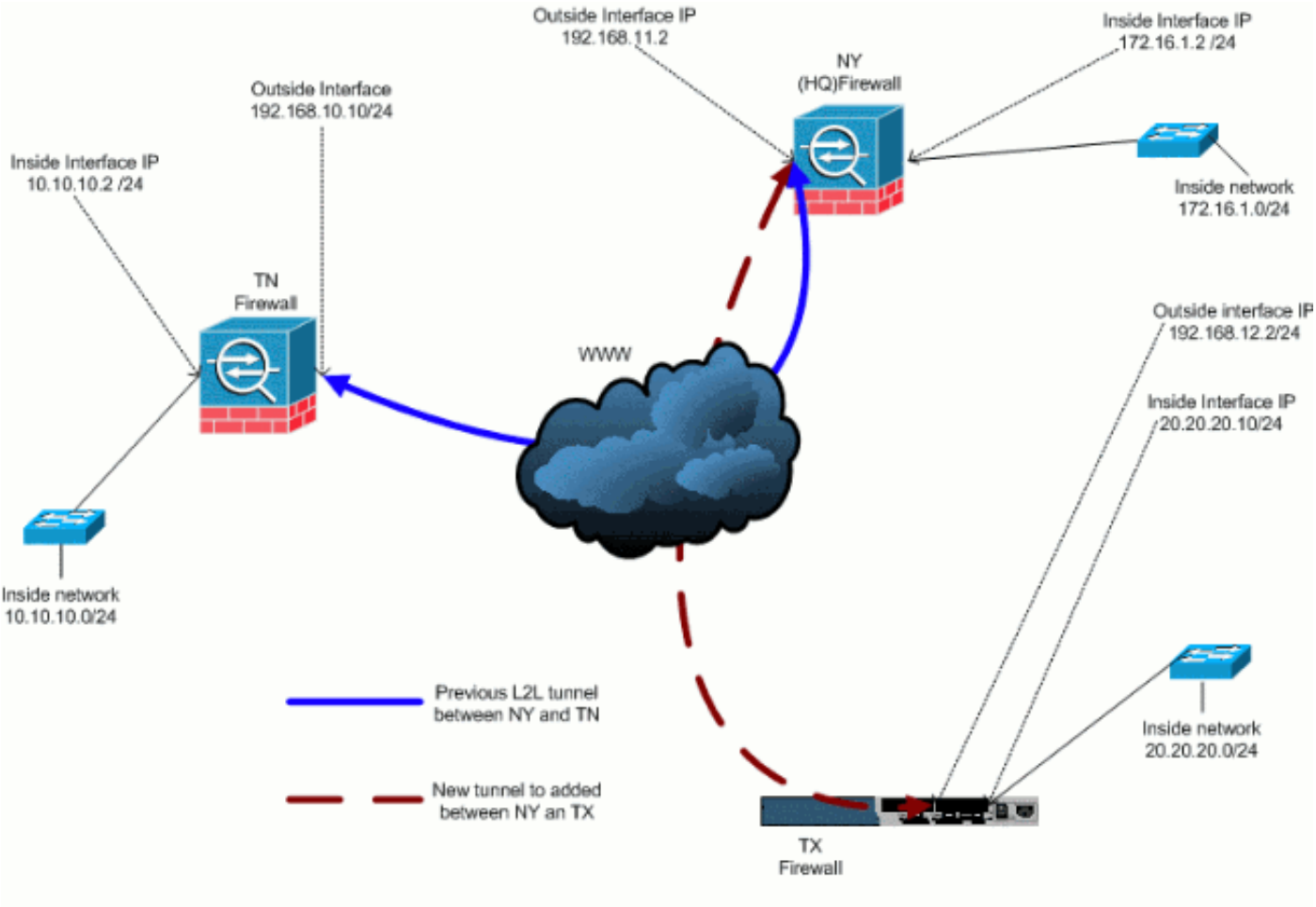
في هذا المثال، يتم إستخدام أمرين للسماح بالاتصال بين شبكات VPN وتحديد حركة مرور البيانات التي يجب إنشاء قنوات لها أو تشفيرها. وهذا يتيح لك إمكانية الوصول إلى الإنترنت دون الاضطرار إلى إرسال حركة مرور البيانات هذه عبر نفق الشبكة الخاصة الظاهرية (VPN). أصدرت in order to شكلت هذا إثنان خيار، **ال split-tunnel** و**نفسه-security-traffic** أمر.

يسمح تقسيم الاتصال النفقي لعميل IPSec للوصول عن بعد إلى الحزم ذات الشروط عبر نفق IPSec في شكل مشفر، أو إلى واجهة شبكة في شكل نص واضح. مع تمكين تقسيم النفقي، لا يجب تشفير الحزم غير المرتبطة بالوجهات على الجانب الآخر من نفق IPSec، وإرسالها عبر النفق، وفك تشفيرها، ثم توجيهها إلى وجهة نهائية. يطبق هذا الأمر نهج تقسيم الاتصال النفقي هذا على شبكة محددة. التقصير أن ينفق كل حركة مرور. لتعيين سياسة تقسيم نفق، قم بإصدار الأمر **split-tunnel-policy** في وضع تكوين نهج المجموعة. قم بإصدار نموذج **no** من هذا الأمر لإزالة نهج تقسيم الاتصال النفقي من التكوين.

يتضمن جهاز الأمان ميزة تتيح لعميل الشبكة الخاصة الظاهرية (VPN) إرسال حركة مرور البيانات المحمية من بروتوكول IPSec إلى مستخدمي الشبكة الخاصة الظاهرية (VPN) الآخرين من خلال السماح بحركة مرور البيانات هذه بالدخول والخروج من الواجهة نفسها. كما يطلق عليها أيضا تسمية التصغير، ويمكن التفكير في هذه الميزة كخوادم VPN (عملاء) تتصل من خلال محور VPN (جهاز أمان). في تطبيق آخر، يمكن أن تعيد هذه الميزة توجيه حركة مرور VPN الواردة من خلال نفس الواجهة مثل حركة المرور غير المشفرة. وهذا مفيد، على سبيل المثال، لعميل شبكة VPN ليس لديه اتصال tunneling منقسم ولكنه يحتاج إلى كل من الوصول إلى شبكة VPN وتصفح الويب. أصدرت in order to شكلت هذا سمة، **ال نفسه أمن-حركة مرور *intra-interface*** أمر في التشكيل عام أسلوب.

## إضافة نفق L2L إضافي إلى التكوين

هذا هو الرسم التخطيطي للشبكة لهذا التكوين:




## التعليمات بالتفصيل

يوفر هذا القسم الإجراءات المطلوبة التي يجب تنفيذها على جهاز الأمان (NY Firewall) HUB). ارجع إلى مثال تكوين نفق PIX/ASA 7.x: Simple PIX-to-PIX VPN Tunnel Configuration Example للحصول على مزيد من المعلومات حول كيفية تكوين العميل المتصل (جدار حماية TX).

أكمل الخطوات التالية:

1. قم بإنشاء قائمتي الوصول الجديدتين هاتين ليتم إستخدامهما من قبل خريطة التشفير لتحديد حركة المرور المفيدة:

```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
      extended permit ip 172.16.1.0 255.255.255.0
                        255.255.255.0 20.20.20.0


ASA-NY-HQ(config)#access-list outside_30_cryptomap
      extended permit ip 10.10.10.0 255.255.255.0
                        255.255.255.0 20.20.20.0
```

**تحذير:** لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة التحكم في الوصول (ACL) هذا الخاص بتلك الشبكة المحددة.

2. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 172.16.1.0 255.255.255.0
                        255.255.255.0 20.20.20.0


ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 10.10.10.0 255.255.255.0
                        255.255.255.0 20.20.20.0
```

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 20.20.20.0 255.255.255.0
                  255.255.255.0 10.10.10.0
```

**تحذير:** لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة التحكم في الوصول هذا للشبكة المحددة.

3. أصدرت هذا أمر in order to مكنت مضيف على ال TX VPN شبكة أن يتلقى منفذ إلى ال TN VPN نفق:

```
ASA-NY-HQ(config)#same-security-traffic permit
                    intra-interface
```

وهذا يسمح لنظراء الشبكات الخاصة الظاهرية (VPN) بالتحدث فيما بينهم.

4. قم بإنشاء تكوين خريطة التشفير لنفق VPN الجديد. استعملت ال نفسه تحويل مجموعة أن كان استعملت في أول VPN تشكيل، بما أن all the مرحلة 2 عملية إعداد ال نفس.

```
ASA-NY-HQ(config)#crypto map outside_map 30 match
                    address outside_30_cryptomap

ASA-NY-HQ(config)#crypto map outside_map 30 set
                              peer 192.168.12.2

ASA-NY-HQ(config)#crypto map outside_map 30 set
                          transform-set
                           ESP-3DES-SHA
```

5. قم بإنشاء مجموعة النفق المحددة لهذا النفق مع السمات المطلوبة للاتصال بالمضيف البعيد.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
                              ipsec-l2l

ASA-NY-HQ(config)#tunnel-group 192.168.12.2
                    ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
                              cisco123
```

**ملاحظة:** يجب أن يتطابق المفتاح المشترك مسبقا تماما على كلا جانبي النفق.

6. والآن بعد ان انتهيت من تكوين النفق الجديد، يجب ان ترسل حركة مرور مثيرة للاهتمام عبر النفق لكي ترفعه. ولتنفيذ هذا الإجراء، قم بإصدار الأمر **source ping** للاتصال بمضيف على الشبكة الداخلية للنفق البعيد.في هذا المثال، يتم سحب محطة عمل على الجانب الآخر من النفق بعنوان 20.20.20.16. وهذا يجعل النفق يصل بين نيويورك و tx. الآن، هناك نفقين متصلان بمكتب المقر الرئيسي. إذا لم يكن لديك حق الوصول إلى نظام خلف النفق، فارجع إلى حلول أستكشاف أخطاء IPSec VPN وإصلاحها للعثور على حل بديل فيما يتعلق باستخدام .

## مثال على التكوين

**مثال تشكيل 1**

```
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 192.168.11.1 255.255.255.0
```

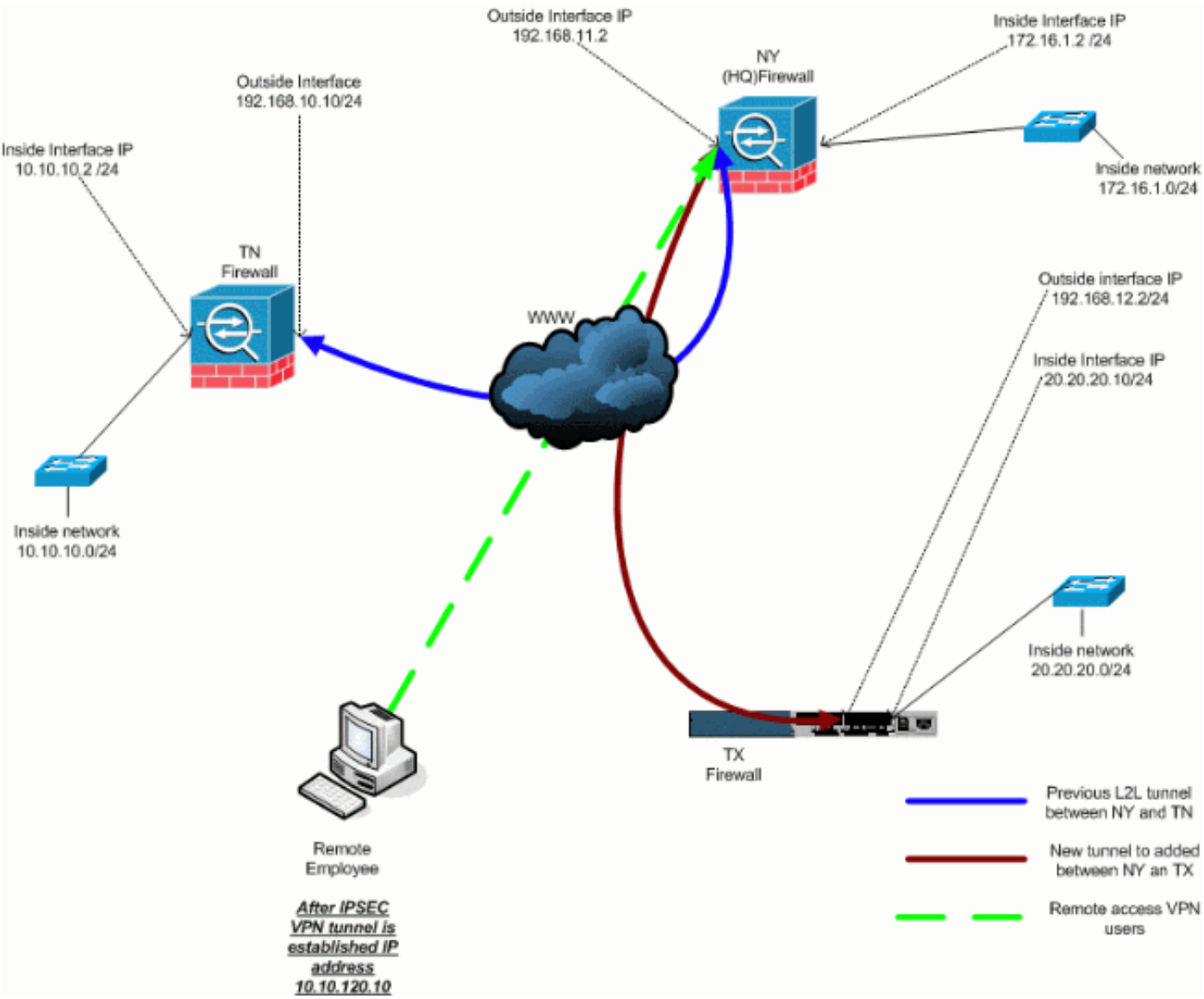
```
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp2.com
same-security-traffic permit intra-interface
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
            route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
     username sidney password 3xsopMX9gN5Wnf1W encrypted
                                          privilege 15
                aaa authentication telnet console LOCAL
                                  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 30 match address
                                    outside_30_cryptomap
          crypto map outside_map 30 set peer 192.168.12.2
crypto map outside_map 30 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
              tunnel-group 192.168.12.2 type ipsec-l2l
             tunnel-group 192.168.12.2 ipsec-attributes
                                        * pre-shared-key
                                    telnet timeout 1440
                                          ssh timeout 5
                                   console timeout 0
                                                      !
                             class-map inspection_default
                        match default-inspection-traffic
                                                      !
                                                      !
             policy-map type inspect dns preset_dns_map
                                           parameters
                          message-length maximum 512
                              policy-map global_policy
                             class inspection_default
                           inspect dns preset_dns_map
                                        inspect ftp
                                 inspect h323 h225
                                  inspect h323 ras
                                   inspect netbios
                                       inspect rsh
                                     inspect rtsp
                                   inspect skinny
```

```
                                                inspect esmtp
                                               inspect sqlnet
                                               inspect sunrpc
                                                 inspect tftp
                                                  inspect sip
                                                inspect xdmcp
                                                            !
                                    service-policy global_policy global
                                                prompt hostname context
                                Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae
                                                          end :
                                                     #ASA-NY-HQ
```

## إضافة شبكة VPN للوصول عن بعد إلى التكوين

هذا هو الرسم التخطيطي للشبكة لهذا التكوين:




## التعليمات بالتفصيل

يوفر هذا القسم الإجراءات المطلوبة لإضافة إمكانية الوصول عن بعد والسماح للمستخدمين عن بعد بالوصول إلى كافة المواقع. ارجع إلى PIX/ASA 7.x ASDM: تقييد الوصول إلى الشبكة لمستخدمي VPN للوصول عن بعد للحصول على مزيد من المعلومات حول كيفية تكوين خادم الوصول عن بعد وتقييد الوصول.

أكمل الخطوات التالية:

1. خلقت عنوان بركة أن يكون استعملت لزبون أن يربط عن طريق ال VPN نفق. خلقت أيضا، مستعمل أساسي in order to نفذت ال VPN ما إن التشكيل أتمت.

```
ASA-NY-HQ(config)#ip local pool Hill-V-IP
mask 255.255.255.0 10.10.120.10-10.10.120.100

ASA-NY-HQ(config)#username cisco password
cisco111
```

2. إستثناء حركة مرور معينة من كونها غير محددة.

```
ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.120.0 255.255.255.0

ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0

ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0
```

لاحظ أن اتصال NAT بين أنفاق الشبكة الخاصة الظاهرية (VPN) معفى في هذا المثال.

3. السماح بالاتصال بين أنفاق L2L التي تم إنشاؤها بالفعل.

```
ASA-NY-HQ(config)#access-list
outside_20_cryptomap extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0

ASA-NY-HQ(config)#access-list
outside_30_cryptomap extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0
```

وهذا يتيح لمستخدمي الوصول عن بعد إمكانية الاتصال بالشبكات خلف الأنفاق المحددة.**تحذير:** لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة التحكم في الوصول هذا للشبكة المحددة.

4. قم بتكوين حركة مرور البيانات التي سيتم تشفيرها وإرسالها عبر نفق VPN.

```
ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 172.16.1.0
255.255.255.0

ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 10.10.10.0
255.255.255.0

ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 20.20.20.0
255.255.255.0
```

5. قم بتكوين المصادقة المحلية ومعلومات السياسة، مثل بروتوكولات WINS و DNS و IPSec، لعملاء VPN.

```
ASA-NY-HQ(config)#group-policy Hillvalley
internal

ASA-NY-HQ(config)#group-policy Hillvalley
attributes

ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20

ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20
```

```
ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. قم بتعيين IPSec والسمات العامة، مثل المفاتيح المشتركة مسبقا وتجمعات عناوين IP، التي سيتم إستخدامها بواسطة نفق VPN الخاص بوادي تل.

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234

ASA-NY-HQ(config)#tunnel-group Hillvalley
general-attributes

ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP

ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. قم بإنشاء سياسة النفق المقسم التي ستستخدم قائمة التحكم في الوصول (ACL) التي تم إنشاؤها في الخطوة 4 لتحديد حركة المرور التي سيتم تشفيرها وتمريرها عبر النفق.

```
ASA-NY-HQ(config)#split-tunnel-policy
tunnelspecified

ASA-NY-HQ(config)#split-tunnel-network-list value
Hillvalley_splitunnel
```

8. قم بتكوين معلومات خريطة التبلور المطلوبة لإنشاء نفق VPN.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
Hill-trans esp-3des esp-sha-hmac

ASA-NY-HQ(config)#crypto dynamic-map
outside_dyn_map 20 set transform-set
Hill-trans

ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
set reverse-route

ASA-NY-HQ(config)#crypto map outside_map 65535
ipsec-isakmp dynamic
outside_dyn_map
```

## مثال على التكوين

**مثال تشكيل 2**

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

Saved :

hostname ASA-NY-HQ
(ASA Version 7.2(2

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
                                             shutdown
                                           no nameif
                                    no security-level
                                        no ip address
                                                     !
                                    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
                same-security-traffic permit intra-interface

    This is required for communication between VPN ---!
peers. access-list inside_nat0_outbound extended permit
   ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
    access-list inside_nat0_outbound extended permit ip
      172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0
    access-list inside_nat0_outbound extended permit ip
      10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
    access-list inside_nat0_outbound extended permit ip
      20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0
    access-list inside_nat0_outbound extended permit ip
                    10.10.120.0 255.255.255.0 20.20.20.0
                                          255.255.255.0
    access-list inside_nat0_outbound extended permit ip
                    172.16.1.0 255.255.255.0 10.10.120.0
                                          255.255.255.0
    access-list inside_nat0_outbound extended permit ip
                    10.10.120.0 255.255.255.0 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
    access-list outside_20_cryptomap extended permit ip
                     20.20.20.0 255.255.255.0 10.10.10.0
                                          255.255.255.0
    access-list outside_20_cryptomap extended permit ip
                    10.10.120.0 255.255.255.0 10.10.10.0
                                          255.255.255.0
      access-list Hillvalley_splitunnel standard permit
                                    172.16.1.0 255.255.255.0
      access-list Hillvalley_splitunnel standard permit
                                    10.10.10.0 255.255.255.0
      access-list Hillvalley_splitunnel standard permit
                                    20.20.20.0 255.255.255.0
```

```
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
group-policy Hillvalley internal
group-policy Hillvalley attributes
wins-server value 10.10.10.20
dns-server value 10.10.10.20
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Hillvalley_splitunnel
default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted
aaa authentication telnet console LOCAL
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 ipsec transform-set Hill-trans esp-3des esp-sha-
hmac
crypto dynamic-map outside_dyn_map 20 set transform-set
Hill-trans
crypto dynamic-map dyn_map 20 set reverse-route
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 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.1
crypto map outside_map 30 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic
```

```
outside_dyn_map
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
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
* pre-shared-key
tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes
address-pool Hill-V-IP
default-group-policy Hillvalley
tunnel-group Hillvalley ipsec-attributes
* pre-shared-key
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48
#ASA-NY-HQ
```

## 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 x.x.x.x (عنوان IP للمضيف على الجانب الآخر من النفق)**—يسمح هذا الأمر بإرسال حركة مرور البيانات أسفل النفق باستخدام عنوان المصدر للواجهة الداخلية.

## استكشاف الأخطاء وإصلاحها

ارجع إلى هذه المستندات للحصول على معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها:

- حلول أستكشاف أخطاء IPSec VPN وإصلاحها الأكثر شيوعا
- أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر التصحيح واستخدامها
- أستكشاف أخطاء الاتصالات وإصلاحها من خلال PIX و ASA

## معلومات ذات صلة

- مقدمة عن تشفير أمان IP (IPSec)
- صفحة دعم مفاوضة IKE/بروتوكولات IPSec
- مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances Command References
- 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).