تكوين PIX إلى PIX إلى PIX IPSec مع ديفي الكامل

المحتويات

المقدمة

يتيح هذا التكوين للشبكات الخاصة الموجودة خلف ثلاثة مربعات جدار حماية PIX الآمن من Cisco الاتصال بواسطة أنفاق VPN عبر الإنترنت أو أي شبكة عامة تستخدم IPsec. تكون كل شبكة من الشبكات الثلاث متصلة بالشبكتين الأخريين. في هذا السيناريو، يلزم ترجمة عنوان الشبكة (NAT) للاتصالات بالإنترنت العام. ومع ذلك، لا يتطلب NAT حركة مرور البيانات بين الشبكات الداخلية الثلاث، والتي يمكن إرسالها باستخدام نفق VPN عبر الإنترنت العام.

المتطلبات الأساسية

المتطلبات

لكي يعمل IPsec، يجب أن يكون لديك اتصال من نقطة نهاية النفق إلى نقطة نهاية النفق قبل بدء هذا التكوين.

المكونات المستخدمة

تم تطوير هذا التكوين واختباره باستخدام جدار حماية PIX الإصدار 6.1(2).

ملاحظة: يجب أن يوضح الأمر **show version** أن التشفير ممكن.

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.

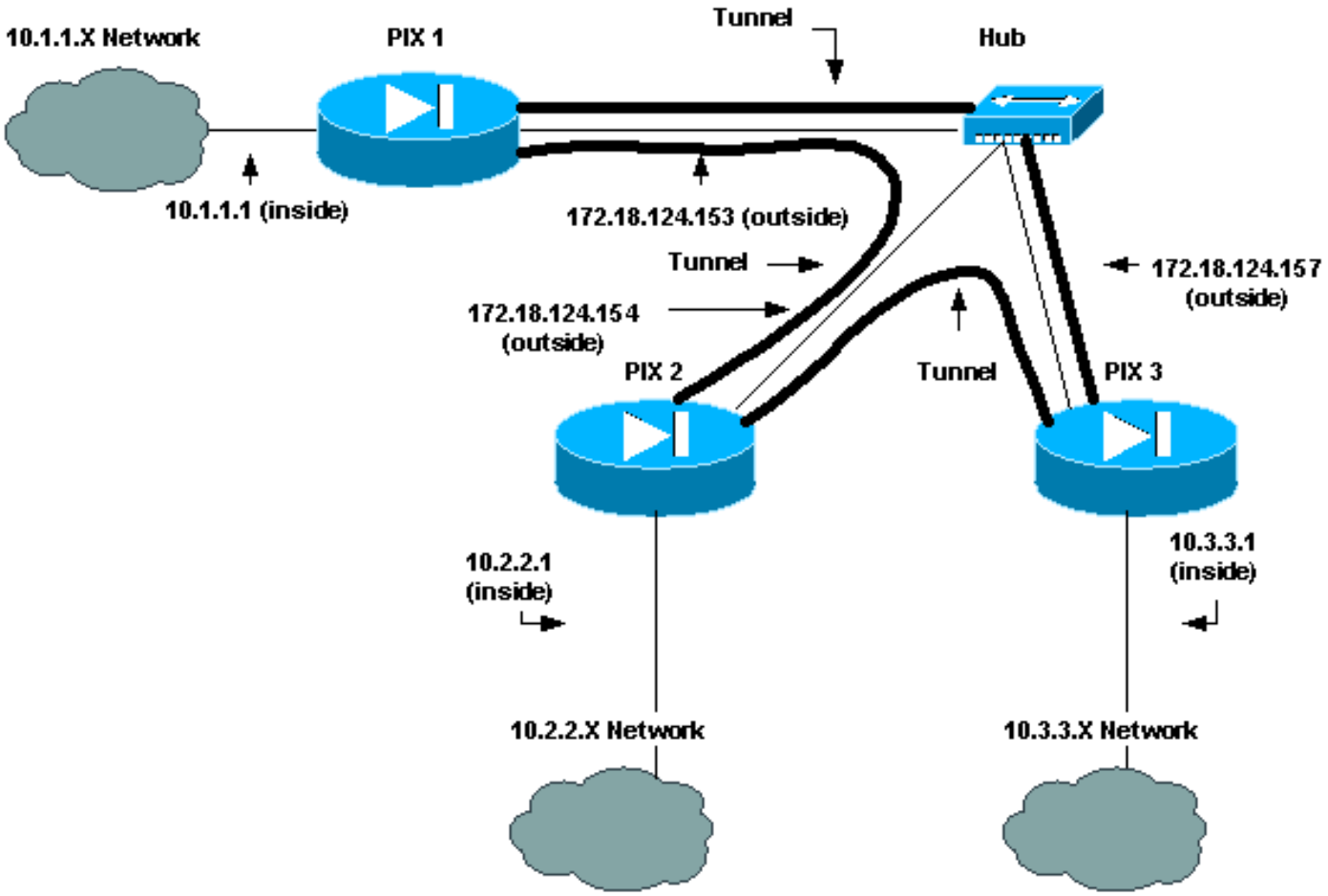
التكوين

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 التالية:

- PIX 1
- PIX 2
- PIX 3

تكوين PIX 1
(PIX Version 6.1(2 nameif ethernet0 outside security0

```
                    nameif ethernet1 inside security100
              enable password 8Ry2YjIyt7RRXU24 encrypted
                      passwd 2KFQnbNIdI.2KYOU encrypted
                                          hostname pix_1
                                    fixup protocol ftp 21
                                   fixup protocol http 80
                                 fixup protocol h323 1720
                                   fixup protocol rsh 514
                                   fixup protocol smtp 25
                                fixup protocol sqlnet 1521
                                  fixup protocol sip 5060
                                                   names
  Traffic to PIX 2 private network: access-list 120 ---!
permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
  Traffic to PIX 3 private network: access-list 130 ---!
permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
    Do not perform NAT for traffic to !--- other PIX ---!
     Firewall private networks: access-list 100 permit ip
            10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
        access-list 100 permit ip 10.1.1.0 255.255.255.0
                                    10.3.3.0 255.255.255.0
                                           pager lines 24
                                              logging on
                                 no logging timestamp
                                   no logging standby
                                   no logging console
                                   no logging monitor
                                 no logging buffered
                                       no logging trap
                                  no logging history
                                 logging facility 20
                                   logging queue 512
                              interface ethernet0 auto
                              interface ethernet1 auto
                                      mtu outside 1500
                                       mtu inside 1500
          ip address outside 172.18.124.153 255.255.255.0
                 ip address inside 10.1.1.1 255.255.255.0
                               ip audit info action alarm
                           ip audit attack action alarm
                                                no failover
                             failover timeout 0:00:00
                                     failover poll 15
                    failover ip address outside 0.0.0.0
                     failover ip address inside 0.0.0.0
                                   arp timeout 14400
        Do not perform NAT for traffic to other PIX ---!
               Firewalls: nat (inside) 0 access-list 100
             route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
                                   timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                           0:10:00 h323
                sip 0:30:00 sip_media 0:02:00 0:05:00
                           timeout uauth 0:05:00 absolute
                +aaa-server TACACS+ protocol tacacs
                  aaa-server RADIUS protocol radius
                                    no snmp-server location
                                     no snmp-server contact
                           snmp-server community public
                               snmp-server enable traps
                                      floodguard enable
                          sysopt connection permit-ipsec
                                 no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

```
IPsec configuration for tunnel to PIX 2: crypto map ---!
                                    newmap 20 ipsec-isakmp
                          crypto map newmap 20 match address 120
                 crypto map newmap 20 set peer 172.18.124.154
                 crypto map newmap 20 set transform-set myset
IPsec configuration for tunnel to PIX 3: crypto map ---!
                                    newmap 30 ipsec-isakmp
                          crypto map newmap 30 match address 130
                 crypto map newmap 30 set peer 172.18.124.157
                 crypto map newmap 30 set transform-set myset
                          crypto map newmap interface outside
                                   isakmp enable outside
      isakmp key ******** address 172.18.124.154 netmask
                                              255.255.255.255
                                 no-xauth no-config-mode
      isakmp key ******** address 172.18.124.157 netmask
                                              255.255.255.255
                                 no-xauth no-config-mode
                                    isakmp identity address
                  isakmp policy 10 authentication pre-share
                           isakmp policy 10 encryption des
                                 isakmp policy 10 hash md5
                                 isakmp policy 10 group 1
                              isakmp policy 10 lifetime 1000
                                                telnet timeout 5
                                                   ssh timeout 5
                                               terminal width 80
        Cryptochecksum:436c96500052d0276324b9ef33221b2d
                                                           end :
                                                          [OK]
```

تكوين PIX 2

```
                                               (PIX Version 6.1(2
                                  nameif ethernet0 outside security0
                                 nameif ethernet1 inside security100
                        enable password 8Ry2YjIyt7RRXU24 encrypted
                                  passwd 2KFQnbNIdI.2KYOU encrypted
                                                  hostname pix_2
                                               fixup protocol ftp 21
                                              fixup protocol http 80
                                            fixup protocol h323 1720
                                              fixup protocol rsh 514
                                              fixup protocol smtp 25
                                           fixup protocol sqlnet 1521
                                             fixup protocol sip 5060
                                                             names
      Traffic to PIX 1: access-list 110 permit ip ---!
         10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
      Traffic to PIX 3: access-list 130 permit ip ---!
         10.2.2.0 255.255.255.0 10.3.3.0 255.255.255.0
      Do not perform NAT for traffic to other PIX ---!
         Firewalls: access-list 100 permit ip 10.2.2.0
                    255.255.255.0 10.1.1.0 255.255.255.0
      access-list 100 permit ip 10.2.2.0 255.255.255.0
                                    10.3.3.0 255.255.255.0
                                                pager lines 24
                                                    logging on
                                          no logging timestamp
                                            no logging standby
                                            no logging console
                                            no logging monitor
                                          no logging buffered
```

```
                                        no logging trap
                                     no logging history
                                   logging facility 20
                                     logging queue 512
                                 interface ethernet0 auto
                                 interface ethernet1 auto
                                        mtu outside 1500
                                        mtu inside 1500
          ip address outside 172.18.124.154 255.255.255.0
                 ip address inside 10.2.2.1 255.255.255.0
                               ip audit info action alarm
                            ip audit attack action alarm
                                             no failover
                                failover timeout 0:00:00
                                        failover poll 15
                      failover ip address outside 0.0.0.0
                       failover ip address inside 0.0.0.0
                                     arp timeout 14400
        Do not perform NAT for traffic to other PIX ---!
               Firewalls: nat (inside) 0 access-list 100
             route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
                                   timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                                0:10:00 h323
                 sip 0:30:00 sip_media 0:02:00 0:05:00
                           timeout uauth 0:05:00 absolute
                      +aaa-server TACACS+ protocol tacacs
                        aaa-server RADIUS protocol radius
                                    no snmp-server location
                                     no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                        floodguard enable
                            sysopt connection permit-ipsec
                                    no sysopt route dnat
    crypto ipsec transform-set myset esp-des esp-md5-hmac
IPsec configuration for tunnel to PIX 1: crypto map ---!
                                    newmap 10 ipsec-isakmp
                        crypto map newmap 10 match address 110
                    crypto map newmap 10 set peer 172.18.124.153
                    crypto map newmap 10 set transform-set myset
IPsec configuration for tunnel to PIX 3: crypto map ---!
                                    newmap 30 ipsec-isakmp
                        crypto map newmap 30 match address 130
                    crypto map newmap 30 set peer 172.18.124.157
                    crypto map newmap 30 set transform-set myset
                          crypto map newmap interface outside
                                    isakmp enable outside
      isakmp key ******** address 172.18.124.153 netmask
                                                255.255.255.255
                                    no-xauth no-config-mode
      isakmp key ******** address 172.18.124.157 netmask
                                                255.255.255.255
                                    no-xauth no-config-mode
                                       isakmp identity address
                    isakmp policy 10 authentication pre-share
                              isakmp policy 10 encryption des
                                    isakmp policy 10 hash md5
                                   isakmp policy 10 group 1
                                isakmp policy 10 lifetime 1000
                                        telnet timeout 5
                                           ssh timeout 5
                                      terminal width 80
          Cryptochecksum:aef12453a0ea29b592dd0d395de881f5
```

```
end :
```

تكوين PIX 3

```
(PIX Version 6.1(2
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
IPsec configuration for tunnel to PIX 1: access- ---!
list 110 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0
IPsec configuration for tunnel to PIX 2: access- ---!
list 120 permit ip 10.3.3.0 255.255.255.0 10.2.2.0
255.255.255.0
Do not perform NAT for traffic to other PIX ---!
Firewalls: access-list 100 permit ip 10.3.3.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.3.3.0 255.255.255.0
10.1.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.3.3.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
Do not perform NAT for traffic to other PIX ---!
Firewalls: nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
sip 0:30:00 sip_media 0:02:00 0:05:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
```

```
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
IPsec configuration for tunnel to PIX 1: crypto map ---!
newmap 10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
IPsec configuration for tunnel to PIX 2: crypto map ---!
newmap 20 ipsec-isakmp
crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ******** address 172.18.124.153 netmask
255.255.255.255
no-xauth no-config-mode
isakmp key ******** address 172.18.124.154 netmask
255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:e6ad75852dff21efdb2d24cc95ffbe1c
end :
[OK]
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. راجع أستكشاف أخطاء PIX وإصلاحها لتمرير حركة مرور البيانات على نفق IPsec تم إنشاؤه للحصول على مزيد من المعلومات.

أوامر استكشاف الأخطاء وإصلاحها

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

أوامر debug

أستخدم هذه الأوامر على PIX، مع تشغيل أوامر تصحيح أخطاء **مراقبة التسجيل** أو **تصحيح أخطاء وحدة التحكم في التسجيل**.

- **debug crypto ipSec**—معالجة IPsec للتصحيح.
- **debug crypto isakmp**—debugs إنترنت security association and key management protocol processing (ISAKMP).
- **debug crypto engine**—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.

أوامر مسح

لمسح اقترانات الأمان (SAs)، أستخدم هذه الأوامر في وضع التكوين ل PIX.

- **مسح [crypto] ipSec sa**—يحذف شبكات IPsec النشطة. تشفير الكلمة الأساسية إختياري.
- **مسح [crypto] isakmp sa**— يحذف شبكات SA لتبادل مفتاح الإنترنت النشط (IKE). تشفير الكلمة الأساسية إختياري.

ملاحظة: لكي يعمل IPsec، يجب أن يكون لديك اتصال من نقطة نهاية النفق إلى نقطة نهاية النفق قبل بدء هذا التكوين.

معلومات ذات صلة

- أستكشاف أخطاء PIX وإصلاحها لتمرير حركة مرور البيانات على نفق IPSec المنشأ
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- مراجع أوامر PIX
- مفاوضات IPsec/بروتوكولات IKE
- طلبات التعليقات (RFCs)
- 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).