تكوين PIX إلى PIX Dynamic-to-Static IPSec باستخدام NAT و Cisco VPN Client

المحتويات

المقدمة

في نموذج التكوين هذا، يستقبل بروتوكول PIX عن بعد عنوان IP من خلال بروتوكول التكوين الديناميكي للمضيف (DHCP) ويتصل ببروتوكول PIX المركزي. يتيح هذا التكوين ل PIX المركزي قبول إتصالات IPsec الديناميكية.
يستخدم PIX البعيد ترجمة عنوان الشبكة (NAT) "للانضمام" إلى الأجهزة التي يتم توجيهها بشكل خاص ووراءها إلى الشبكة التي يتم توجيهها بشكل خاص خلف PIX المركزي. يمكن ل PIX البعيد بدء الاتصالات ب PIX المركزي (الذي يعرف نقطة النهاية)، ولكن PIX المركزي لا يمكنه بدء الاتصالات ب PIX البعيد (لا يعرف نقطة النهاية).

في هذا التكوين العينة، Tiger هو PIX البعيد و Lion هو PIX المركزي. لا يعرف ما هو عنوان IP Tiger الذي سيكون، لذلك يجب تكوين Lion لقبول الاتصالات بشكل ديناميكي من أي مكان يعرف البطاقة البرية، المفتاح المشترك مسبقا. يعرف Tiger حركة المرور التي سيتم تشفيرها (لأنها محددة بواسطة قائمة الوصول) ومكان نقطة نهاية الأسد. يتعين على شركة Tiger أن تبدأ الاتصال. يقوم كلا الجانبين ب NAT و 0 NAT بتجاوز NAT لحركة مرور IPsec.

وبالإضافة إلى ذلك، يتصل المستخدم البعيد في هذا التكوين ب PIX المركزي (Lion) باستخدام عميل Cisco VPN الإصدار x.3. يتعذر على المستخدم البعيد الاتصال ب PIX البعيد (Tiger) نظرا لأن كلا الجانبين كانا سيعينان عناوين IP بشكل ديناميكي ولن يعرفا مكان إرسال الطلب.

ارجع إلى PIX/ASA 7.x PIX-to-PIX Dynamic-to-Static IPsec مع مثال تكوين عميل NAT و VPN لمعرفة المزيد حول السيناريو نفسه في PIX/ASA 7.x مع عميل Cisco VPN 4.x.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج جدار حماية Cisco PIX الإصدار 6.0(1) (أو إصدار أكبر ل Cisco VPN Client 3.x)
- برنامج جدار حماية Cisco PIX الإصدار 5.3.1 (PIX عن بعد)
- عميل شبكة VPN من Cisco، الإصدار x.3

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.

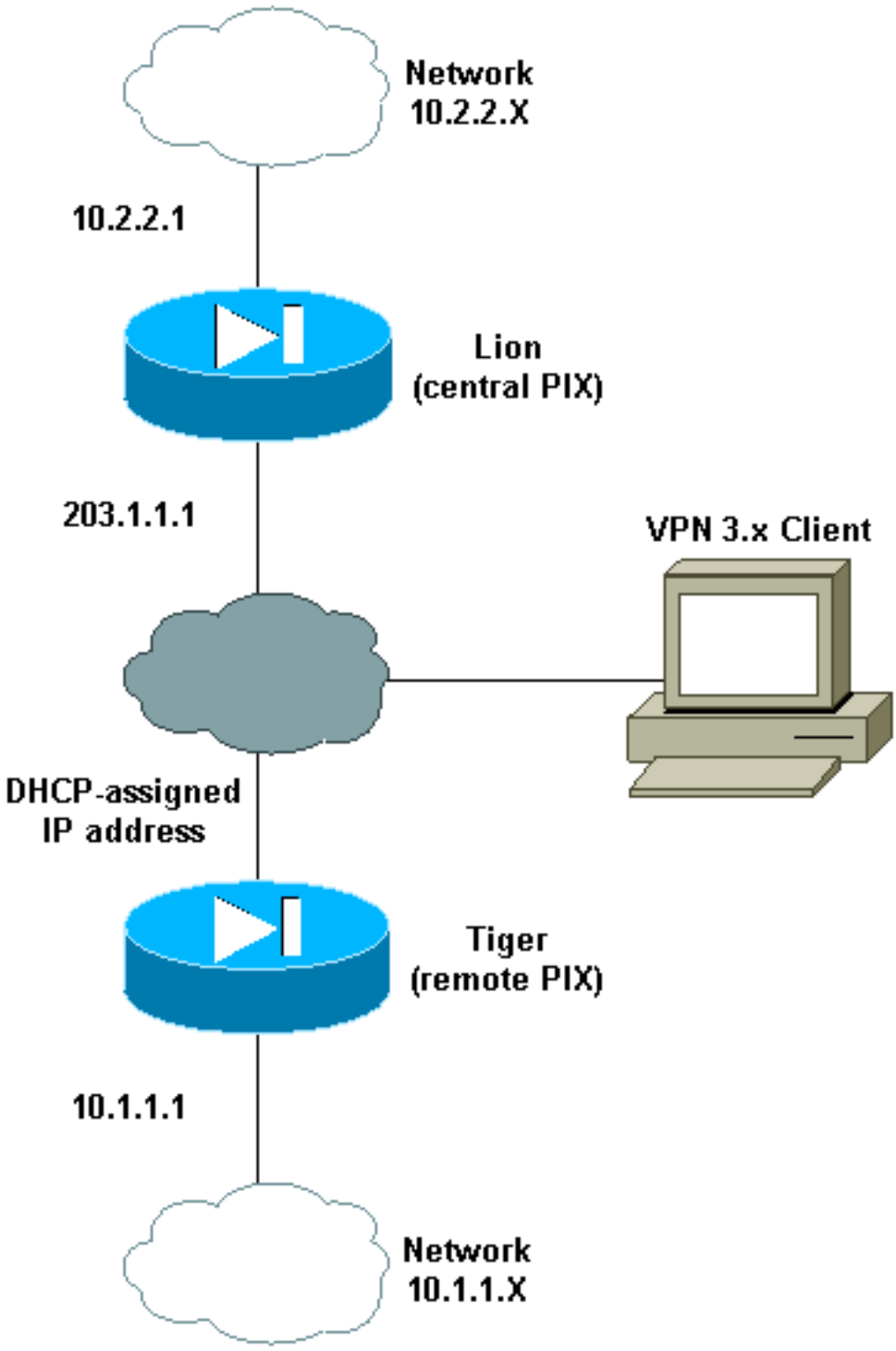
التكوين

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

تشكيل الأسد

```
...Building configuration
                                    Saved :
                                    :
                            (PIX Version 6.0(1
                nameif gb-ethernet0 spare1 security10
                nameif gb-ethernet1 spare2 security15
                   nameif ethernet0 outside security0
                  nameif ethernet1 inside security100
            enable password 8Ry2YjIyt7RRXU24 encrypted
                     passwd 2KFQnbNIdI.2KYOU encrypted
                                    hostname lion
```

```
                                    domain-name cisco.com
                                    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
                                fixup protocol skinny 2000
                                                  names
                                                      !
 ACL to avoid Network Address Translation (NAT) on ---!
  the IPsec packets. 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 buffered debugging
                   interface gb-ethernet0 1000auto shutdown
                   interface gb-ethernet1 1000auto shutdown
                               interface ethernet0 10baset
                               interface ethernet1 10baset
                                           mtu spare1 1500
                                           mtu spare2 1500
                                          mtu outside 1500
                                           mtu inside 1500
              ip address spare1 127.0.0.1 255.255.255.255
              ip address spare2 127.0.0.1 255.255.255.255
                                                      !
 IP addresses on the interfaces ip address outside ---!
                                    203.1.1.1 255.255.255.0
                 ip address inside 10.2.2.1 255.255.255.0
                                                      !
                                 ip audit info action alarm
                               ip audit attack action alarm
              ip local pool clientpool 10.3.3.1-10.3.3.10
                                                no failover
                                  failover timeout 0:00:00
                                          failover poll 15
                        failover ip address spare1 0.0.0.0
                        failover ip address spare2 0.0.0.0
                      failover ip address outside 0.0.0.0
                        failover ip address inside 0.0.0.0
                                       pdm history enable
                                        arp timeout 14400
     global (outside) 1 203.1.1.10-203.1.1.15 !--- ---!
   Change from NAT to PAT on the DHCP interface. global
(outside) 1 interface ! !--- Binding ACL 100 to the NAT
       statement to avoid NAT on the IPsec packets. nat
                                    (inside) 0 access-list 100
                                                      !
                         nat (inside) 1 0.0.0.0 0.0.0.0 0 0
                                conduit permit icmp any any
                                                      !
Default route to the Internet route outside 0.0.0.0 ---!
                                          0.0.0.0 203.1.1.2 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 0:05:00 sip
                                  sip_media 0:02:00 0:30:00
                               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
                                                              !
    The sysopt command avoids conduit on the IPsec ---!
                                                .encrypted traffic

                                  sysopt connection permit-ipsec
                                                              !
                                          no sysopt route dnat
                                                              !
 Phase 2 encryption type crypto ipsec transform-set ---!
                                       myset esp-des esp-md5-hmac
                  crypto dynamic-map cisco 1 set transform-set myset
                    crypto map dyn-map 20 ipsec-isakmp dynamic cisco
                                                              !
   Binds the IPsec engine on the outside interface. ---!
                                 crypto map dyn-map interface outside
                                                              !
 Enables ISAKMP key-exchange. isakmp enable outside ---!
                                                              !
    ISAKMP policy for accepting dynamic connections ---!
from the remote PIX. isakmp key ******** address 0.0.0.0
                                                 netmask 0.0.0.0
      ISAKMP policy for Cisco VPN Client 2.x 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
                                                              !
      ISAKMP policy for Cisco VPN Client 3.x isakmp ---!
                                 policy 20 authentication pre-share
                                    isakmp policy 20 encryption des
                                          isakmp policy 20 hash sha
                                           isakmp policy 20 group 2
                                  isakmp policy 20 lifetime 86400
                                                              !
        IPsec group configuration for either client ---!
                             vpngroup unityclient address-pool clientpool
                                vpngroup unityclient dns-server 10.1.1.3
                              vpngroup unityclient wins-server 10.1.1.3
                        vpngroup unityclient default-domain cisco.com
                                   vpngroup unityclient idle-time 1800
                         ******** vpngroup unityclient password
                                                              !
                                               telnet timeout 5
                                                  ssh timeout 5
                                               terminal width 80
                    Cryptochecksum:d6fe92db883a052c5765be21a74e7c8d
                                                        end :
                                                        [OK]
```

تشكيل النمر

```
                                  ...Building configuration
                                                  Saved :
                                                        :
                                          (PIX Version 5.3(1
                        nameif gb-ethernet0 spare1 security10
```

```
                    nameif gb-ethernet1 spare2 security15
                       nameif ethernet0 outside security0
                     nameif ethernet1 inside security100
              enable password 8Ry2YjIyt7RRXU24 encrypted
                      passwd 2KFQnbNIdI.2KYOU encrypted
                                          hostname tiger
                                   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
                                                     !
 ACL to avoid NAT on the IPsec packets access-list ---!
            101 permit ip 10.1.1.0 255.255.255.0 10.2.2.0
                                           255.255.255.0
                                                     !
                                        pager lines 24
                                            logging on
                                   no logging timestamp
                                     no logging standby
                                     no logging console
                                     no logging monitor
                              logging buffered debugging
                                        no logging trap
                                     no logging history
                                   logging facility 20
                                     logging queue 512
                 interface gb-ethernet0 1000auto shutdown
                 interface gb-ethernet1 1000auto shutdown
                              interface ethernet0 10baset
                              interface ethernet1 10baset
                                          mtu spare1 1500
                                          mtu spare2 1500
                                        mtu outside 1500
                                          mtu inside 1500
              ip address spare1 127.0.0.1 255.255.255.255
              ip address spare2 127.0.0.1 255.255.255.255
                                                     !
                                  ip address outside dhcp
                 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 spare1 0.0.0.0
                      failover ip address spare2 0.0.0.0
                    failover ip address outside 0.0.0.0
                      failover ip address inside 0.0.0.0
                                       arp timeout 14400
                 global (outside) 1 204.1.1.10-204.1.1.15
                                                     !
 Binds ACL 101 to the NAT statement to avoid NAT on ---!
       the IPsec packets. nat (inside) 0 access-list 101
                                                     !
                             nat (inside) 1 0.0.0.0 0.0.0.0 0 0
                                    conduit permit icmp any any
               route outside 0.0.0.0 0.0.0.0 204.1.1.2 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 0:05:00 sip
                                  sip_media 0:02:00 0:30:00
                                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
                                                              !
                    The sysopt command avoids conduit on the IPsec ---!
                                                .encrypted traffic

                                        sysopt connection permit-ipsec
                                                              !
                                               no sysopt route dnat
                                                              !
                Phase 2 encryption type crypto ipsec transform-set ---!
                                          myset esp-des esp-md5-hmac
                                    crypto map newmap 10 ipsec-isakmp
                                crypto map newmap 10 match address 101
                                crypto map newmap 10 set peer 203.1.1.1
                              crypto map newmap 10 set transform-set myset
                                                              !
                  Binds the IPsec engine on the outside interface. ---!
                                    crypto map newmap interface outside
                                                              !
                 Enables ISAKMP key-exchange isakmp enable outside ---!
                                                              !
                  ISAKMP policy for connecting to the central PIX. ---!
                          isakmp key ******** address 203.1.1.1 netmask
                                                    255.255.255.255
                                        isakmp identity hostname
                                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:6743b7bf9476590ecd1a1a8c6d75245b
                                                           end :
                                                          [OK]
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

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

ملاحظة: يجب تنفيذ أوامر **clear** في وضع التكوين.

- **مسح تشفير IPsec**—إعادة ضبط اقترانات IPsec بعد محاولات فاشلة للتفاوض على نفق VPN.
- **مسح التشفير isakmp sa**—إعادة ضبط اقترانات أمان بروتوكول إدارة المفاتيح وارتباط أمان بروتوكول أمان الإنترنت (ISAKMP) بعد محاولات التفاوض الفاشلة على نفق VPN.

- **show crypto engine ipsec**—يعرض الجلسات المشفرة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

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

- **debug crypto ipSec**—يستخدم لمعرفة ما إذا كان العميل يفاوض جزء IPsec من اتصال VPN.
- **debug crypto isakmp connection**— يستخدم لمعرفة ما إذا كان الأقران يتفاوضون على جزء ISAKMP من الشبكة الخاصة الظاهرية (VPN).

إخراج تصحيح الأخطاء "جيد" للعينة

- تصحيح أخطاء PIX المركزي
- تصحيح أخطاء PIX عن بعد
- تصحيح أخطاء العميل

تصحيح أخطاء PIX المركزي

```
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
                                                    OAK_MM exchange
                                ISAKMP (0): processing SA payload. message ID = 0

                ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                                                ISAKMP:      encryption DES-CBC
                                                        ISAKMP:      hash MD5
                                                   ISAKMP:      default group 1
                                                    ISAKMP:      auth pre-share
                                                ISAKMP:      life type in seconds
                                            ISAKMP:      life duration (basic) of 1000
                                    ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_FQDN
                                                  return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
                                                    OAK_MM exchange
                                ISAKMP (0): processing KE payload. message ID = 0

                              ISAKMP (0): processing NONCE payload. message ID = 0

                                           ISAKMP (0): processing vendor id payload

                                           ISAKMP (0): processing vendor id payload

                                           ISAKMP (0): processing vendor id payload

                                           !ISAKMP (0): speaking to another IOS box
```

```
                                                    return status is IKMP_NO_ERROR
                                crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
                                                                  OAK_MM exchange
                                        ISAKMP (0): processing ID payload. message ID = 0
                                      ISAKMP (0): processing HASH payload. message ID = 0
                                                  ISAKMP (0): SA has been authenticated

                                                                    ISAKMP (0): ID payload
                                                                   next-payload : 8
                                                                   type         : 2
                                                                  protocol     : 17
                                                                 port         : 500
                                                                  length       : 10
                                                 ISAKMP (0): Total payload length: 14
                                                       return status is IKMP_NO_ERROR
                                crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
                                                                  OAK_QM exchange
                                                          :oakley_process_quick_mode
                                                                       OAK_QM_IDLE
                                ISAKMP (0): processing SA payload. message ID = 1223411072

                                                     ISAKMP : Checking IPSec proposal 1

                                                            ISAKMP: transform 1, ESP_DES
                                                     :ISAKMP:   attributes in transform
                                                               ISAKMP:      encaps is 1
                                                      ISAKMP:      SA life type in seconds
                                           ISAKMP:      SA life duration (basic) of 28800
                                                    ISAKMP:      SA life type in kilobytes
                             ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
                                                    ISAKMP:      authenticator is HMAC-MD5
,ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1
                                      ,key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1)
                                    ,(dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                                     ,(src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                                    , protocol= ESP, transform= esp-des esp-md5-hmac
                                                    ,lifedur= 0s and 0kb
                                     spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

                                ISAKMP (0): processing NONCE payload. message ID = 1223411072

                                    ISAKMP (0): processing ID payload. message ID = 1223411072
                        ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.2.2.0/255.255.255.0 prot 0 port 0
                                    ISAKMP (0): processing ID payload. message ID = 1223411072
                          ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port
                                                ...0IPSEC(key_engine): got a queue event
              IPSEC(spi_response): getting spi 0xd0e27cb6(3504503990) for SA from 204.1.1.1
                                                    to 203.1.1.1 for prot 3

                                                    return status is IKMP_NO_ERROR
                                crypto_isakmp_process_block: src 204.1.1.1, dest 203.1.1.1
                                                                  OAK_QM exchange
                                                          :oakley_process_quick_mode
                                                                   OAK_QM_AUTH_AWAIT
                                                    ISAKMP (0): Creating IPSec SAs
                   (inbound SA from 204.1.1.1 to 203.1.1.1 proxy 10.2.2.0 to 10.1.1.0
                                        has spi 3504503990 and conn_id 4 and flags 4
                                                    lifetime of 28800 seconds
                                                lifetime of 4608000 kilobytes
                    (outbound SA from 203.1.1.1 to 204.1.1.1(proxy 10.1.1.0 to 10.2.2.0
                                        has spi 2729504033 and conn_id 3 and flags 4
                                                    lifetime of 28800 seconds
                 ...lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event
                                                            , :(IPSEC(initialize_sas
```

```
                                ,key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1)
                              ,(dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                               ,(src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                              , protocol= ESP, transform= esp-des esp-md5-hmac
                                          ,lifedur= 28800s and 4608000kb
          spi= 0xd0e27cb6(3504503990), conn_id= 4, keysize= 0, flags= 0x4
                                                    , :(IPSEC(initialize_sas
                                ,key eng. msg.) src= 203.1.1.1, dest= 204.1.1.1)
                               ,(src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                              ,(dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                              , protocol= ESP, transform= esp-des esp-md5-hmac
                                          ,lifedur= 28800s and 4608000kb
          spi= 0xa2b0ed21(2729504033), conn_id= 3, keysize= 0, flags= 0x4

                                                  return status is IKMP_NO_ERROR
```

تصحيح أخطاء PIX عن بعد

```
                                              ISAKMP (0): beginning Main Mode exchange

                                  crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
                                                                        OAK_MM exchange
                                        ISAKMP (0): processing SA payload. message ID = 0

                         ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                                                      ISAKMP:      encryption DES-CBC
                                                               ISAKMP:      hash MD5
                                                          ISAKMP:      default group 1
                                                           ISAKMP:      auth pre-share
                                                     ISAKMP:      life type in seconds
                                                ISAKMP:      life duration (basic) of 1000
                                     ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_FQDN
                                                  return status is IKMP_NO_ERROR
                                  crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
                                                                        OAK_MM exchange
                                        ISAKMP (0): processing KE payload. message ID = 0

                                     ISAKMP (0): processing NONCE payload. message ID = 0

                                              ISAKMP (0): processing vendor id payload

                                              !ISAKMP (0): speaking to another IOS box

                                                                ISAKMP (0): ID payload
                                                                  next-payload : 8
                                                                  type         : 2
                                                                 protocol     : 17
                                                                port         : 500
                                                                 length       : 18
                                                    ISAKMP (0): Total payload length: 22
                                                  return status is IKMP_NO_ERROR
                                  crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
                                                                        OAK_MM exchange
                                        ISAKMP (0): processing ID payload. message ID = 0
                                     ISAKMP (0): processing HASH payload. message ID = 0
                                                  ISAKMP (0): SA has been authenticated

                                           ISAKMP (0): beginning Quick Mode exchange, M-ID of
                                ...1223411072:48ebc580IPSEC(key_engine):got a queue event
                              IPSEC(spi_response): getting spi 0xa2b0ed21(2729504033) for SA
                                 from       203.1.1.1 to       204.1.1.1 for prot 3
```

```
                                                  return status is IKMP_NO_ERROR
                              crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
                                                                  OAK_QM exchange
                                                 :oakley_process_quick_mode
                                                                  OAK_QM_IDLE
                              ISAKMP (0): processing SA payload. message ID = 1223411072

                                                 ISAKMP : Checking IPSec proposal 1

                                                       ISAKMP: transform 1, ESP_DES
                                                 :ISAKMP:   attributes in transform
                                                           ISAKMP:      encaps is 1
                                                    ISAKMP:      SA life type in seconds
                                          ISAKMP:      SA life duration (basic) of 28800
                                                   ISAKMP:      SA life type in kilobytes
                               ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
                                                   ISAKMP:      authenticator is HMAC-MD5
,ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1
                                        ,key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1)
                                     ,(dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                                      ,(src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                                     , protocol= ESP, transform= esp-des esp-md5-hmac
                                                        ,lifedur= 0s and 0kb
                                      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

                              ISAKMP (0): processing NONCE payload. message ID = 1223411072

                                 ISAKMP (0): processing ID payload. message ID = 1223411072
                                 ISAKMP (0): processing ID payload. message ID = 1223411072
                                                    ISAKMP (0): Creating IPSec SAs
        (inbound SA from 203.1.1.1 to 204.1.1.1 (proxy 10.1.1.0 to 10.2.2.0
                                     has spi 2729504033 and conn_id 4 and flags 4
                                                lifetime of 28800 seconds
                                            lifetime of 4608000 kilobytes
       (outbound SA from 204.1.1.1 to 203.1.1.1 (proxy 10.2.2.0 to 10.1.1.0
                                     has spi 3504503990 and conn_id 3 and flags 4
                                                lifetime of 28800 seconds
       ...lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event
                                                        , :(IPSEC(initialize_sas
                                        ,key eng. msg.) dest= 204.1.1.1, src= 203.1.1.1)
                                     ,(dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                                      ,(src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                                     , protocol= ESP, transform= esp-des esp-md5-hmac
                                                       ,lifedur= 28800s and 4608000kb
              spi= 0xa2b0ed21(2729504033), conn_id= 4, keysize= 0, flags= 0x4
                                                        , :(IPSEC(initialize_sas
                                        ,key eng. msg.) src= 204.1.1.1, dest= 203.1.1.1)
                                      ,(src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4
                                     ,(dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4
                                     , protocol= ESP, transform= esp-des esp-md5-hmac
                                                       ,lifedur= 28800s and 4608000kb
              spi= 0xd0e27cb6(3504503990), conn_id= 3, keysize= 0, flags= 0x4

                                                  return status is IKMP_NO_ERROR
```

تصحيح أخطاء العميل

```
                              Sev=Info/4       CM/0x63100004  06/28/01  16:43:20.402     19
                                        Establish secure connection using Ethernet

                              Sev=Info/4       CM/0x63100025  06/28/01  16:43:20.402     20
                                        "Attempt connection with server "203.1.1.1
```

```
                    Sev=Info/6       IKE/0x6300003B  06/28/01  16:43:20.402     21
                              .Attempting to establish a connection with 203.1.1.1

                    Sev=Info/4       IKE/0x63000013  06/28/01  16:43:20.442     22
            SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 203.1.1.1

                  Sev=Info/4       IPSEC/0x63700014  06/28/01  16:43:20.452     23
                                                                  Deleted all keys

                    Sev=Info/5       IKE/0x6300002F  06/28/01  16:43:20.492     24
                                           Received ISAKMP packet: peer = 203.1.1.1

                    Sev=Info/4       IKE/0x63000014  06/28/01  16:43:20.492     25
  RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH) from 203.1.1.1

                    Sev=Info/5       IKE/0x63000059  06/28/01  16:43:20.492     26
                              Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100


                    Sev=Info/5       IKE/0x63000001  06/28/01  16:43:20.492     27
                                               Peer is a Cisco-Unity compliant peer

                    Sev=Info/5       IKE/0x63000059  06/28/01  16:43:20.492     28
                              Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100


                    Sev=Info/5       IKE/0x63000001  06/28/01  16:43:20.492     29
                                                                Peer supports DPD

                    Sev=Info/5       IKE/0x63000059  06/28/01  16:43:20.492     30
                              Vendor ID payload = A0EB477E6627B406AA10F958254B3517


                    Sev=Info/4       IKE/0x63000013  06/28/01  16:43:20.542     31
      SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 203.1.1.1

                     Sev=Info/4       CM/0x6310000E  06/28/01  16:43:20.542     32
                                Established Phase 1 SA.  1 Phase 1 SA in the system

                    Sev=Info/4       IKE/0x63000013  06/28/01  16:43:21.143     33
                           SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 203.1.1.1

                    Sev=Info/5       IKE/0x6300002F  06/28/01  16:43:24.067     34
                                           Received ISAKMP packet: peer = 203.1.1.1

                    Sev=Info/4       IKE/0x63000014  06/28/01  16:43:24.067     35
                       RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 203.1.1.1

                    Sev=Info/5       IKE/0x63000010  06/28/01  16:43:24.067     36
            MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.3.3.1


                    Sev=Info/5       IKE/0x63000010  06/28/01  16:43:24.067     37
             MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.3


                    Sev=Info/5       IKE/0x63000010  06/28/01  16:43:24.067     38
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.3


                    Sev=Info/5       IKE/0x6300000E  06/28/01  16:43:24.067     39
          MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com
```

```
                                Sev=Info/4       CM/0x63100018  06/28/01  16:43:24.067     40
                                                                    Mode Config data received

                               Sev=Info/5       IKE/0x63000055  06/28/01  16:43:24.668     41
                  Received a key request from Driver for IP address 203.1.1.1, GW IP = 203.1.1.1


                               Sev=Info/4       IKE/0x63000013  06/28/01  16:43:24.668     42
                              SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 203.1.1.1

                               Sev=Info/5       IKE/0x63000055  06/28/01  16:43:24.668     43
                Received a key request from Driver for IP address 10.10.10.255, GW IP = 203.1.1.1

                               Sev=Info/4       IKE/0x63000013  06/28/01  16:43:24.668     44
                              SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 203.1.1.1

                             Sev=Info/4       IPSEC/0x63700014  06/28/01  16:43:24.668     45
                                                                      Deleted all keys

                               Sev=Info/5       IKE/0x6300002F  06/28/01  16:43:25.619     46
                                                    Received ISAKMP packet: peer = 203.1.1.1

                               Sev=Info/4       IKE/0x63000014  06/28/01  16:43:25.619     47
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 203.1.1.1

                               Sev=Info/5       IKE/0x63000044  06/28/01  16:43:25.619     48
                                         RESPONDER-LIFETIME notify has value of 28800 seconds

                               Sev=Info/5       IKE/0x63000045  06/28/01  16:43:25.619     49
                                       RESPONDER-LIFETIME notify has value of 4608000 kb

                               Sev=Info/4       IKE/0x63000013  06/28/01  16:43:25.619     50
                                      SENDING >>> ISAKMP OAK QM *(HASH) to 203.1.1.1

                               Sev=Info/5       IKE/0x63000058  06/28/01  16:43:25.619     51
   (Loading IPsec SA (Message ID = 0x59515364 OUTBOUND SPI = 0xB24CDB55 INBOUND SPI = 0x83AA0042

                               Sev=Info/5       IKE/0x63000025  06/28/01  16:43:25.619     52
                                                    Loaded OUTBOUND ESP SPI: 0xB24CDB55

                               Sev=Info/5       IKE/0x63000026  06/28/01  16:43:25.619     53
                                                     Loaded INBOUND ESP SPI: 0x83AA0042

                                Sev=Info/4       CM/0x63100019  06/28/01  16:43:25.619     54
                                                       One secure connection established

                             Sev=Info/6       DIALER/0x63300003  06/28/01  16:43:25.629     55
                                                                  .Connection established

                             Sev=Info/6       DIALER/0x63300008  06/28/01  16:43:25.669     56
                                         MAPI32 Information - Outlook not default mail client

                               Sev=Info/5       IKE/0x6300002F  06/28/01  16:43:25.960     57
                                                    Received ISAKMP packet: peer = 203.1.1.1

                               Sev=Info/4       IKE/0x63000014  06/28/01  16:43:25.960     58
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 203.1.1.1

                               Sev=Info/5       IKE/0x63000044  06/28/01  16:43:25.960     59
                                         RESPONDER-LIFETIME notify has value of 28800 seconds

                               Sev=Info/5       IKE/0x63000045  06/28/01  16:43:25.960     60
                                       RESPONDER-LIFETIME notify has value of 4608000 kb
```

```
                                Sev=Info/4       IKE/0x63000013  06/28/01  16:43:25.960     61
                                              SENDING >>> ISAKMP OAK QM *(HASH) to 203.1.1.1

                                Sev=Info/5       IKE/0x63000058  06/28/01  16:43:25.960     62
(Loading IPsec SA (Message ID = 0x23A23005 OUTBOUND SPI = 0xAD0599DB INBOUND SPI = 0x2B74D4A4

                                Sev=Info/5       IKE/0x63000025  06/28/01  16:43:25.960     63
                                                        Loaded OUTBOUND ESP SPI: 0xAD0599DB

                                Sev=Info/5       IKE/0x63000026  06/28/01  16:43:25.960     64
                                                        Loaded INBOUND ESP SPI: 0x2B74D4A4

                                 Sev=Info/4       CM/0x63100021  06/28/01  16:43:25.960     65
                                                        .Additional Phase 2 SA established

                             Sev=Info/4       IPSEC/0x63700010  06/28/01  16:43:25.960     66
                                                              Created a new key structure

                             Sev=Info/4       IPSEC/0x6370000F  06/28/01  16:43:25.960     67
                                                  Added key with SPI=0x55db4cb2 into key list

                             Sev=Info/4       IPSEC/0x63700010  06/28/01  16:43:25.960     68
                                                              Created a new key structure

                             Sev=Info/4       IPSEC/0x6370000F  06/28/01  16:43:25.960     69
                                                  Added key with SPI=0x4200aa83 into key list

                             Sev=Info/4       IPSEC/0x63700010  06/28/01  16:43:25.960     70
                                                              Created a new key structure

                             Sev=Info/4       IPSEC/0x6370000F  06/28/01  16:43:25.960     71
                                                  Added key with SPI=0xdb9905ad into key list

                             Sev=Info/4       IPSEC/0x63700010  06/28/01  16:43:25.960     72
                                                              Created a new key structure

                             Sev=Info/4       IPSEC/0x6370000F  06/28/01  16:43:25.960     73
                                                  Added key with SPI=0xa4d4742b into key list

                               Sev=Info/6       IKE/0x6300003D  06/28/01  16:43:35.173     74
                                          Sending DPD request to 203.1.1.1, seq# = 1856135987

                               Sev=Info/4       IKE/0x63000013  06/28/01  16:43:35.173     75
                          SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 203.1.1.1

                               Sev=Info/5       IKE/0x6300002F  06/28/01  16:43:35.173     76
                                                   Received ISAKMP packet: peer = 203.1.1.1

                               Sev=Info/4       IKE/0x63000014  06/28/01  16:43:35.173     77
                          RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK) from 203.1.1.1

                               Sev=Info/5       IKE/0x6300003F  06/28/01  16:43:35.173     78
      Received DPD ACK from 203.1.1.1, seq# received = 1856135987, seq# expected = 1856135987
```

معلومات ذات صلة

- صفحة دعم PIX
- مراجع أوامر PIX
- تكوين أمان شبكة IPSec
- صفحات دعم منتجات أمان IPSec) 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).