تكوين IPSec بين الموزع و PIXs البعيد باستخدام عميل VPN والمصادقة الموسعة

المحتويات

المقدمة

يوضح هذا المستند تكوين IPsec الذي يتضمن كل من العبارة إلى البوابة ووظائف المستخدم البعيد. باستخدام المصادقة الموسعة (Xauth)، تتم مصادقة الجهاز من خلال المفتاح المشترك مسبقا ويصادق المستخدم من خلال اعتراض اسم المستخدم/كلمة المرور.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- PIX Firewall، الإصدار 6.3(3)
- عميل Cisco VPN، الإصدار 3.5
- Cisco Secure ACS ل Windows، الإصدار 2.6

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي

أمر.

الاصطلاحات

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

معلومات أساسية

في هذا المثال، هناك نفق IPsec من العبارة إلى البوابة من PIX البعيد إلى PIX صرة. يقوم هذا النفق بتشفير حركة المرور من الشبكة x.10.48.67 خلف PIX البعيد إلى الشبكة x.10.48.66 خلف PIX للمحور. يمكن أن يشكل الكمبيوتر الشخصي الموجود على الإنترنت نفق IPsec من خلال PIX الموزع إلى الشبكة x.10.48.66.

لاستخدام ميزة Xauth، يجب عليك أولا إعداد خادم المصادقة والتفويض والمحاسبة (AAA) الأساسي لديك. أستخدم الأمر **crypto map client authentication** لمصادقة جدار حماية PIX لاستخدام تحدي Xauth (اسم مستخدم وكلمة مرور RADIUS/TACACS+) أثناء المرحلة 1 من IKE (Internet Key Exchange) لمصادقة IKE. في حالة فشل Xauth، لا يتم إنشاء رابطة أمان IKE. حدد اسم خادم AAA نفسه داخل بيان أمر **مصادقة عميل خريطة التشفير** الذي يتم تحديده في بيان أوامر **aaa-server**. يجب على المستخدم البعيد تشغيل الإصدار x.3 من عميل Cisco VPN أو إصدار أحدث.

ملاحظة: توصي Cisco باستخدام عميل Cisco VPN 3.5.x أو إصدار أحدث. لا يعمل عميل VPN 1.1 مع هذا التكوين وهو خارج نطاق هذا المستند.

ملاحظة: لا يدعم عميل Cisco VPN الإصدار 3.6 والإصدارات الأحدث مجموعة التحويل من DES/SHA.

إذا كنت بحاجة إلى إستعادة التكوين دون Xauth، فاستخدم الأمر **no crypto map client authentication**. لا يتم تمكين ميزة Xauth بشكل افتراضي.

ملاحظة: تخضع تكنولوجيا التشفير لضوابط التصدير. من مسؤوليتك معرفة القانون المتعلق بتصدير تقنية التشفير. راجع الصفحة الرئيسية لمكتب إدارة التصدير للحصول على مزيد من المعلومات. إرسال بريد إلكتروني إلى export@cisco.com إذا كانت لديك أية أسئلة متعلقة بالتحكم في التصدير.

ملاحظة: في الإصدار 5.3 من جدار حماية PIX والإصدارات الأحدث، تم تقديم منافذ RADIUS القابلة للتكوين. تستخدم بعض خوادم RADIUS منافذ RADIUS بخلاف 1646/1645 (عادة 1813/1812). في PIX 5.3 والإصدارات الأحدث، يمكن تغيير منافذ مصادقة RADIUS ومحاسبته إلى أخرى غير منافذ 1646/1645 الافتراضية باستخدام هذه الأوامر:

```
# aaa-server radius-authport
# aaa-server radius-acctport
```

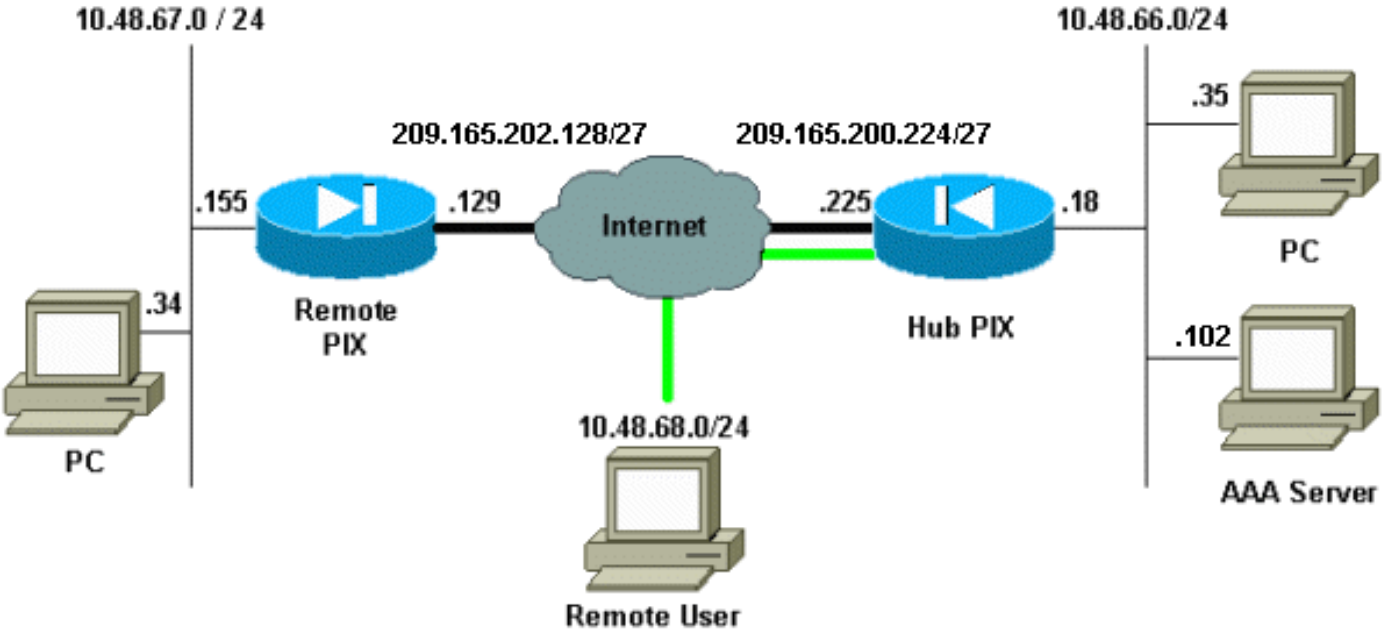
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المخطط خطوطا عريضة خضراء وأسود للإشارة إلى أنفاق الشبكات الخاصة الظاهرية (VPN).



التكوينات

يستخدم هذا المستند هذه التكوينات.

- Hub PIX
- Remote PIX

ملاحظة: على سبيل المثال في هذا المستند، يكون عنوان IP الخاص بخادم VPN هو 209.165.200.225، واسم المجموعة هو "VPN3000"، وكلمة مرور المجموعة هي Cisco.

تكوين Hub PIX

```
(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname hubfixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
Include traffic in the encryption process. access- ---!
list 101 permit ip 10.48.66.0 255.255.255.0 10.48.67.0
255.255.255.0
Accept traffic from the Network Address Translation ---!
(NAT) process
access-list nonat permit ip 10.48.66.0 255.255.255.0
10.48.67.0 255.255.255.0
```

```
access-list nonat permit ip 10.48.66.0 255.255.255.0
                                    10.48.68.0 255.255.255.0
                                             pager lines 24
                                           mtu outside 1500
                                            mtu inside 1500
      ip address outside 209.165.200.225 255.255.255.224
             ip address inside 10.48.66.18 255.255.255.0
                                 ip audit info action alarm
                               ip audit attack action alarm
           ip local pool mypool 10.48.68.1-10.48.68.254
                                                 no failover
                                  failover timeout 0:00:00
                                          failover poll 15
                              no failover ip address outside
                               no failover ip address inside
                                        pdm history enable
                                         arp timeout 14400
global (outside) 1 209.16.200.230-209.16.200.240 netmask
                                          255.255.255.224
                        global (outside) 1 209.16.200.241
Except traffic from the NAT process. nat (inside) 0 ---!
                                          access-list nonat
             nat (inside) 1 10.48.66.0 255.255.255.0 0 0
        route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
                                       timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                        0:10:00 h225 1:00:00
 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
                                                 0:02:00
                          timeout uauth 0:05:00 absolute
                      +aaa-server TACACS+ protocol tacacs
                        aaa-server RADIUS protocol radius
                          aaa-server LOCAL protocol local
                  +aaa-server mytacacs protocol tacacs
   aaa-server mytacacs (inside) host 10.48.66.102 cisco
                                                timeout 5
                                    no snmp-server location
                                     no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                        floodguard enable
                             sysopt connection permit-ipsec
  crypto ipsec transform-set myset esp-des esp-md5-hmac
    crypto dynamic-map dynmap 10 set transform-set myset
 Use the crypto-map sequence 10 command for PIX to ---!
                                                      .PIX


                        crypto map mymap 10 ipsec-isakmp
                    crypto map mymap 10 match address 101
               crypto map mymap 10 set peer 209.165.202.129
                crypto map mymap 10 set transform-set myset
 Use the crypto-map sequence 20 command for PIX to ---!
                                                  .VPN Client


          crypto map mymap 20 ipsec-isakmp dynamic dynmap
          crypto map mymap client authentication mytacacs
                    crypto map mymap interface outside
                                    isakmp enable outside
    isakmp key ******** address 209.165.202.129 netmask
                                              255.255.255.255
                                    isakmp identity address
                isakmp policy 10 authentication pre-share
                          isakmp policy 10 encryption des
                             isakmp policy 10 hash md5
```

```
ISAKMP policy for VPN Client that runs 3.x code ---!
needs to be DH group 2. isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
IPsec group configuration for VPN Client. vpngroup ---!
vpn3000 address-pool mypool
vpngroup vpn3000 dns-server 10.48.66.129
vpngroup vpn3000 wins-server 10.48.66.129
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
******** vpngroup vpn3000 password
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:7293dd9fc7c58ff5d65f042dd6ddbe13
end :
```

تكوين PIX عن بعد

```
(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 100basetx
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname remote
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit ip 10.48.67.0 255.255.255.0
10.48.66.0 255.255.255.0
Accept traffic from the NAT process. access-list ---!
nonat permit ip 10.48.67.0 255.255.255.0 10.48.66.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 209.165.202.129 255.255.255.224
ip address inside 10.48.67.155 255.255.255.0
no ip address intf2
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
```

```
pdm history enable
arp timeout 14400
global (outside) 1 209.16.202.135-209.16.202.145 netmask
255.255.255.224
global (outside) 1 209.16.202.146
Except traffic from the NAT process. nat (inside) 0 ---!
access-list nonat
nat (inside) 1 10.48.0.0 255.255.255.0 0 0
nat (inside) 1 10.48.67.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.202.130 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map mymap 10 ipsec-isakmp
Include traffic in the encryption process. crypto ---!
map mymap 10 match address 101
crypto map mymap 10 set peer 209.165.200.225
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 209.165.200.225 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:13ef4d29384c65c2cd968b5d9396f6e8
end :
```

ارجع إلى قسم "التكوينات" في تكوين PIX إلى PIX و VPN Client 3.x للحصول على معلومات تفصيلية حول كيفية إعداد عميل VPN. ارجع أيضا إلى كيفية إضافة مصادقة (AAA (Xauth إلى PIX IPsec 5.2 والإصدارات الأحدث للحصول على معلومات إضافية حول تكوين مصادقة AAA إلى PIX IPsec.

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** .

- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1.

- **show crypto ipSec sa**—يعرض اقترانات أمان المرحلة 2.

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**.

يجب تشغيل عمليات تصحيح الأخطاء هذه على كل من موجهات IPsec (الأقران). يجب مسح اقترانات الأمان على كلا النظرين.

- **debug crypto isakmp**—يعرض الأخطاء أثناء المرحلة 1.
- **debug crypto ipSec**—يعرض الأخطاء أثناء المرحلة 2.
- **debug crypto engine**—يعرض معلومات من محرك التشفير.
- **مسح التشفير isakmp sa**—يعمل على مسح اقترانات أمان المرحلة الأولى.
- **مسح تشفير IPsec**—يعمل على مسح اقترانات أمان المرحلة 2.
- **debug radius [جلسة | الكل | اسم مستخدم]**—متوفر في PIX 6.2، يقوم هذا الأمر بتسجيل معلومات جلسة RADIUS وسمات حزم RADIUS المرسلة والمستلمة.
- **debug tacacs [session|user <user_name>]**— **متوفر** في PIX 6.3، يقوم هذا الأمر بتسجيل معلومات TACACS.
- **debug aaa [المصادقة|الاعتماد|المحاسبة|internal]**— **متوفر** في PIX 6.3، يعرض معلومات نظام AAA الفرعي.

تصحيح الأخطاء من Hub PIX

ملاحظة: كن على علم بأنه في بعض الأحيان عندما تكون مفاوضات IPsec ناجحة، لا يتم عرض جميع تصحيح الأخطاء على PIX بسبب معرف تصحيح الأخطاء من CSCdu84168 Cisco (العملاء المسجلون فقط) وهو تكرار لمعرف تصحيح الأخطاء الداخلي من CSCdt31745 Cisco (العملاء المسجلون فقط). لم يتم حل هذا بعد بدءا من كتابة هذا المستند.

ملاحظة: في بعض الأحيان قد لا ينتهي IPSec VPN من عملاء VPN على PIX. لحل هذه المشكلة، تأكد من أن كمبيوتر العميل لا يحتوي على أي جدران حماية. إذا كانت جدران الحماية موجودة، فتحقق من تعطيل منفذ UDP 500 و 4500. إذا كانت هذه هي الحالة، فقم بتمكين IPSec عبر TCP أو إلغاء حظر منافذ UDP.

تصحيح أخطاء نفق IPsec ديناميكي بين الموزع و PIXs البعيد

```
,crypto_isakmp_process_block:src:209.165.202.129
                dest:209.165.200.225 spt:500 dpt:500
                                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 2
```

```
                                                    ISAKMP:      auth pre-share
                                                ISAKMP:      life type in seconds
                                ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
                                    ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
                                                    return status is IKMP_NO_ERROR
          crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
                                                                spt:500 dpt:500
                                                                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): received xauth v6 vendor id

                                            ISAKMP (0): processing vendor id payload

                                ISAKMP (0): remote peer supports dead peer detection

                                            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:209.165.202.129, dest:209.165.200.225
                                                                spt:500 dpt:500
                                                                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: Created a peer struct for 209.165.202.129, peer port 62465
                                                              ISAKMP (0): ID payload
                                                                next-payload : 8
                                                                type         : 1
                                                               protocol     : 17
                                                              port         : 500
                                                                length       : 8
                                                    ISAKMP (0): Total payload length: 12
                                                    return status is IKMP_NO_ERROR
                                            ISAKMP (0): sending INITIAL_CONTACT notify
                                ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:209.165.202.129/500 Total VPN Peers:1
    VPN Peer: ISAKMP: Peer ip:209.165.202.129/500 Ref cnt incremented to:1
                                                                Total VPN Peers:1
          crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
                                                                spt:500 dpt:500
                                ISAKMP (0): processing NOTIFY payload 24578 protocol 1
                                            spi 0, message ID = 863921625
                  :(ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine
                                                              ...got a queue event
                    IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
  IPSEC(key_engine_delete_sas): delete all SAs shared with 209.165.202.129

                                            return status is IKMP_NO_ERR_NO_TRANS
          crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
                                                                spt:500 dpt:500
                                                                OAK_QM exchange
                                                          :oakley_process_quick_mode
                                                                OAK_QM_IDLE
```

ISAKMP (0): processing SA payload. message ID = 2542705093

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= 209.165.200.225, src= 209.165.202.129)
,(dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4
,(src_proxy= 10.48.67.0/255.255.255.0/0/0 (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 = 2542705093

ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.48.67.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.48.66.0/255.255.255.0 prot 0 port 0
...IPSEC(key_engine): got a queue event
IPSEC(spi_response): getting spi 0x858c841a(2240578586) for SA
from 209.165.202.129 to 209.165.200.225 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
:oakley_process_quick_mode
OAK_QM_AUTH_AWAIT
ISAKMP (0): **Creating IPSec SAs**
inbound SA from 209.165.202.129 to 209.165.200.225
(proxy 10.48.67.0 to 10.48.66.0)
has spi 2240578586 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 209.165.200.225 to 209.165.202.129
(proxy 10.48.66.0 to 10.48.67.0)
has spi 681010504 and conn_id 4 and flags 4
lifetime of 28800 seconds
...lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event
, :(IPSEC(initialize_sas
,key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129)
,(dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4
,(src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 28800s and 4608000kb
spi= 0x858c841a(2240578586), conn_id= 3, keysize= 0, flags= 0x4
, :(IPSEC(initialize_sas
,key eng. msg.) src= 209.165.200.225, dest= 209.165.202.129)
,(src_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 28800s and 4608000kb
spi= 0x28976548(681010504), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:209.165.202.129/500
Ref cnt incremented to:2 Total VPN Peers:1

```
VPN Peer: IPSEC: Peer ip:209.165.202.129/500
  Ref cnt incremented to:3 Total VPN Peers:1
                 return status is IKMP_NO_ERROR
```

تصحيح الأخطاء عند توصيل عميل VPN بموزع PIX

```
                    ,crypto_isakmp_process_block:src:10.48.68.2
               dest:209.165.200.225 spt:500 dpt:500OAK_AG exchange
                 ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash SHA
                                          ISAKMP:      default group 2
                                (ISAKMP:      extended auth pre-share (init
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 256
           ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash MD5
                                          ISAKMP:      default group 2
                                (ISAKMP:      extended auth pre-share (init
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 256
           ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash SHA
                                          ISAKMP:      default group 2
                                           ISAKMP:      auth pre-share
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 256
           ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash MD5
                                          ISAKMP:      default group 2
                                           ISAKMP:      auth pre-share
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 256
           ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash SHA
                                          ISAKMP:      default group 2
                                (ISAKMP:      extended auth pre-share (init
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 128
           ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
                                ISAKMP:      encryption AES-CBC
                                        ISAKMP:      hash MD5
                                          ISAKMP:      default group 2
                                (ISAKMP:      extended auth pre-share (init
                                        ISAKMP:      life type in seconds
          ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                          ISAKMP:      keylength of 128
           ISAKMP (0): atts are not acceptable. Next payload is 3
```

```
                    ISAKMP (0): Checking ISAKMP transform 7 against priority 10 policy
                                                ISAKMP:      encryption AES-CBC
                                                          ISAKMP:      hash SHA
                                                       ISAKMP:      default group 2
                                                        ISAKMP:      auth pre-share
                                                    ISAKMP:      life type in seconds
                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                      ISAKMP:      keylength of 128
                                 ISAKMP (0): atts are not acceptable. Next payload is 3
                    ISAKMP (0): Checking ISAKMP transform 8 against priority 10 policy
                                                ISAKMP:      encryption AES-CBC
                                                          ISAKMP:      hash MD5
                                                       ISAKMP:      default group 2
                                                        ISAKMP:      auth pre-share
                                                    ISAKMP:      life type in seconds
                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                      ISAKMP:      keylength of 128
                                 ISAKMP (0): atts are not acceptable. Next payload is 3
                    ISAKMP (0): Checking ISAKMP transform 9 against priority 10 policy
                                                 ISAKMP:      encryption 3DES-CBC
                                                          ISAKMP:      hash SHA
                                                       ISAKMP:      default group 2
                                           (ISAKMP:      extended auth pre-share (init
                                                    ISAKMP:      life type in seconds
                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                 .ISAKMP (0): atts are not acceptable
      crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
      crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                                       ISAKMP_TRANSACTION exchange
    ISAKMP (0:0): processing transaction payload from 10.48.68.2.message ID = 17138612
                 ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS
        (ISAKMP (0:0): initiating peer config to 10.48.68.2. ID = 134858975 (0x809c8df
      crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                                       ISAKMP_TRANSACTION exchange
    ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
                                                        ISAKMP: Config payload CFG_ACK
                                                        return status is IKMP_NO_ERROR
      crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                                       ISAKMP_TRANSACTION exchange
    ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
                                                  ISAKMP: Config payload CFG_REQUEST
                                                     :ISAKMP (0:0): checking request
                                                (ISAKMP: attribute    IP4_ADDRESS (1
                                                (ISAKMP: attribute    IP4_NETMASK (2
                                                    (ISAKMP: attribute    IP4_DNS (3
                                                   (ISAKMP: attribute    IP4_NBNS (4
                                              (ISAKMP: attribute    ADDRESS_EXPIRY (5
                                                         Unsupported Attr: 5
                                                (ISAKMP: attribute    UNKNOWN (28672
                                                     Unsupported Attr: 28672
                                                (ISAKMP: attribute    UNKNOWN (28673
                                                     Unsupported Attr: 28673
                                           (ISAKMP: attribute    ALT_DEF_DOMAIN (28674
                                         (ISAKMP: attribute    ALT_SPLIT_INCLUDE (28676
                                         (ISAKMP: attribute    ALT_SPLITDNS_NAME (28675
                                                (ISAKMP: attribute    ALT_PFS (28679
                                       (ISAKMP: attribute    ALT_BACKUP_SERVERS (28681
                                          (ISAKMP: attribute    APPLICATION_VERSION (7
                                                (ISAKMP: attribute    UNKNOWN (28680
                                                     Unsupported Attr: 28680
                                                (ISAKMP: attribute    UNKNOWN (28682
                                                     Unsupported Attr: 28682
                                                (ISAKMP: attribute    UNKNOWN (28677
                                                     Unsupported Attr: 28677
```

```
ISAKMP (0:0): responding to peer config from 10.48.68.2. ID = 1128513895
                                                  return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                                                OAK_QM exchange
                                                      :oakley_process_quick_mode
                                                                   OAK_QM_IDLE
                                  ISAKMP (0): processing SA payload. message ID = 3681346539
                                                  ISAKMP : Checking IPSec proposal 1
                                                        ISAKMP: transform 1, ESP_AES
                                                    :ISAKMP:   attributes in transform
                                                ISAKMP:      authenticator is HMAC-MD5
                                                       ISAKMP:      key length is 256
                                                             ISAKMP:      encaps is 1
                                                   ISAKMP:      SA life type in seconds
                                ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not supported
                                       ISAKMP (0): atts not acceptable. Next payload is 0
                                             (ISAKMP (0): skipping next ANDed proposal (1
                                                  ISAKMP : Checking IPSec proposal 2
                                                        ISAKMP: transform 1, ESP_AES
                                                    :ISAKMP:   attributes in transform
                                                ISAKMP:      authenticator is HMAC-SHA
                                                       ISAKMP:      key length is 256
                                                             ISAKMP:      encaps is 1
                                                   ISAKMP:      SA life type in seconds
                                ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not supported
                                       ISAKMP (0): atts not acceptable. Next payload is 0
                                             (ISAKMP (0): skipping next ANDed proposal (2
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                                                        #(hub(config
                                                                        #(hub(config
                                                                        #(hub(config
                                                                        #(hub(config
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
                                    ISAKMP (0): processing NOTIFY payload 36136 protocol 1
                                                  spi 0, message ID = 3784834735
                                  ISAMKP (0): received DPD_R_U_THERE from peer 10.48.68.2
                                      ISAKMP (0): sending NOTIFY message 36137 protocol 1
                                                  return status is IKMP_NO_ERR_NO_TRANS
```

معلومات ذات صلة

- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- مرجع أوامر PIX
- صفحة دعم PIX
- TACACS+ في وثائق IOS
- صفحة دعم TACACS+
- 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).