أستكشاف أخطاء PIX وإصلاحها لتمرير حركة مرور البيانات على نفق IPSec المنشأ

المحتويات

المقدمة

يتناول هذا المستند ويوفر حلا لمشكلة عدم قدرة نفق IPsec الذي تم إنشاؤه بنجاح من عميل Cisco VPN إلى PIX على تمرير البيانات.

غالبا ما تتم مواجهة عدم القدرة على تمرير البيانات على نفق IPsec تم إنشاؤه بين عميل VPN و PIX عندما لا يمكنك إختبار الاتصال أو Telnet من عميل VPN إلى أي مضيف على الشبكة المحلية (LAN) خلف PIX. بمعنى آخر، لا يمكن لعميل الشبكة الخاصة الظاهرية (VPN) و PIX تمرير البيانات المشفرة بينهما. وهذا يحدث لأن PIX يحتوي على نفق IPsec من شبكة LAN إلى شبكة LAN إلى موجه وأيضا عميل شبكة VPN. عدم القدرة على تمرير البيانات هو نتيجة تكوين بنفس قائمة التحكم في الوصول (ACL) لكل من NAT 0 ومخطط التشفير الثابت لنظير IPsec من شبكة LAN إلى شبكة LAN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- جدار حماية Cisco Secure PIX 6.0.1
- الموجه 1720 من Cisco الذي يشغل برنامج Cisco IOS® الإصدار 12.2(6)

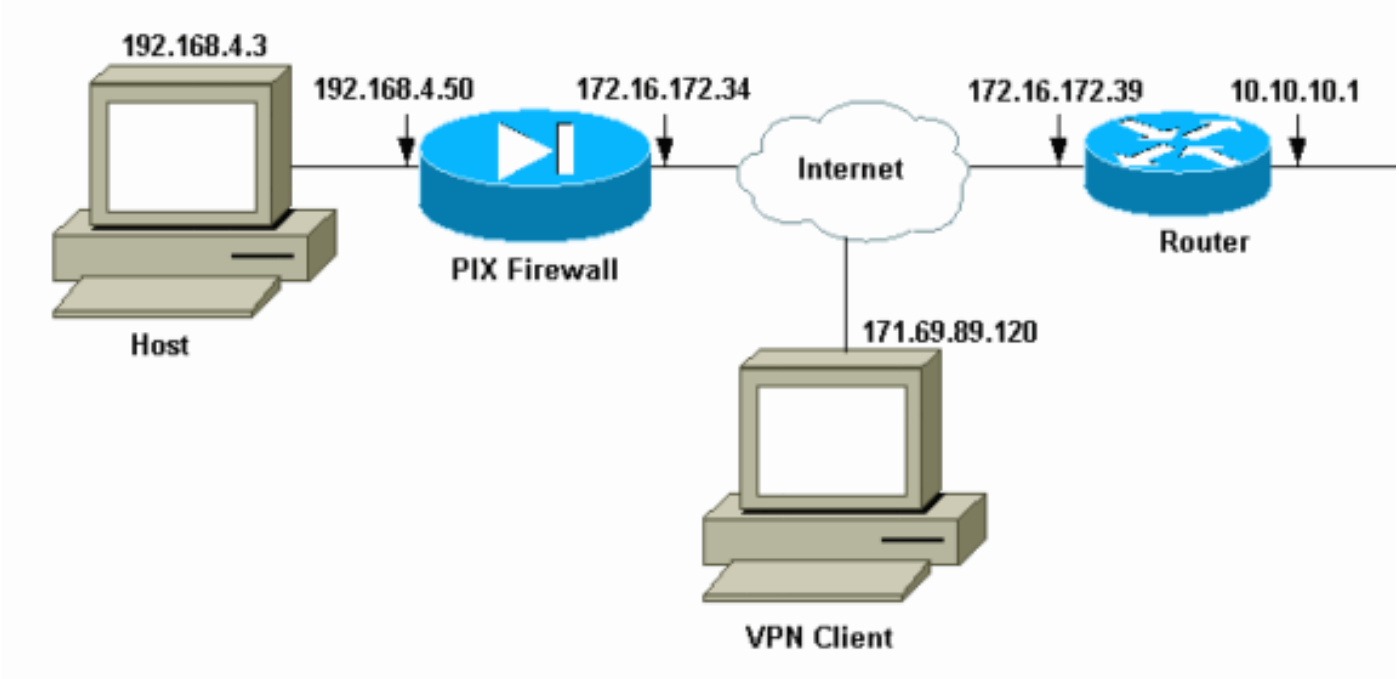
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

أستكشاف أخطاء PIX وإصلاحها

الرسم التخطيطي للشبكة



إشكالية عينة تشكيل

PIX 520
pix520-1#**write terminal** ...Building configuration Saved : : (PIX Version 6.0(1 nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix520-1 domain-name vpn.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
Access-List "140" defines interesting traffic to ---!
bypass NAT for VPN !--- and defines VPN interesting
traffic. This is incorrect. access-list 140 permit ip
192.168.4.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list 140 permit ip 192.168.4.0 255.255.255.0
10.1.2.0 255.255.255.0
no pager
logging on
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
logging history debugging
logging host outside 192.168.2.6
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
IP addresses on the outside and inside interfaces. ---!
ip address outside 172.16.172.34 255.255.255.240
ip address inside 192.168.4.50 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
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
pdm history enable
arp timeout 14400
global (outside) 1 172.16.172.57 netmask 255.255.255.255
The nat 0 command bypasses NAT for the packets ---!
.destined over the IPsec tunnel

Nat (inside) 0 access-list 140
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.172.33 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 0:05:00
sip_media 0:02:00 0:30:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
AAA-server RADIUS protocol radius
+AAA-server mytest protocol tacacs
AAA-server nasir protocol radius
snmp-server host outside 192.168.2.6
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
The sysopt command bypasses conduits or ACLs that ---!
check to be applied !--- on the inbound VPN packets
.after decryption

sysopt connection permit-ipsec
no sysopt route dnat
```

```
The crypto ipsec command defines IPsec encryption ---!
.and authen algo

crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
The crypto map commands define the IPsec !--- ---!
.Security Assocation (SA) (Phase II SA) parameters

crypto map mymap 5 ipsec-isakmp
crypto map mymap 5 match address 140
crypto map mymap 5 set peer 172.16.172.39
crypto map mymap 5 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
The isakmp key command defines the pre-shared key ---!
.for the peer address

isakmp key ******** address 172.16.172.39 netmask
255.255.255.255 no-xauth
no-config-mode
isakmp identity address
The isakmp policy defines the Phase 1 SA ---!
.parameters

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption Des
isakmp policy 20 hash sha
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
vpngroup vpn3000 address-pool ippool
vpngroup vpn3000 idle-time 1800
******** vpngroup vpn3000 password
telnet 192.168.4.0 255.255.255.0 inside
telnet 171.69.89.82 255.255.255.255 inside
telnet timeout 5
ssh 172.0.0.0 255.0.0.0 outside
ssh 171.0.0.0 255.255.255.0 outside
ssh 171.0.0.0 255.0.0.0 outside
ssh timeout 60
terminal width 80
Cryptochecksum:55948dc706cc700e9c10e1d24a8b125c
```

في التكوين المشر للمشاكل يتم تحديد حركة المرور المثيرة للاهتمام، أو حركة المرور التي سيتم تشفيرها لنفق شبكة LAN إلى شبكة LAN، بواسطة قائمة التحكم في الوصول (ACL) رقم 140. يستخدم التكوين قائمة التحكم في الوصول (ACL) نفسها الخاصة بقوائم التحكم في الوصول (ACL) ل NAT 0.

فهم التسلسل العام للأحداث

عندما تصل حزمة IP إلى الواجهة الداخلية ل PIX، يتم التحقق من ترجمة عنوان الشبكة (NAT). بعد ذلك، يتم التحقق من قوائم التحكم في الوصول لخرائط التشفير.

- **كيف يتم إستخدام nat 0.**تحدد قائمة التحكم في الوصول (ACL) ل NAT 0 ما يجب عدم تضمينه في NAT. تحدد قائمة التحكم في الوصول (ACL) في الأمر **nat 0** عنوان المصدر والوجهة الذي يتم تعطيل قواعد NAT على PIX من أجله. لذلك، فإن حزمة IP التي تحتوي على عنوان مصدر ووجهة يطابق قائمة التحكم في الوصول

(ACL) المعرفة في الأمر **nat 0** تتجاوز جميع قواعد NAT على PIX.من أجل تنفيذ أنفاق من شبكة LAN إلى شبكة LAN بين PIX وجهاز VPN آخر بمساعدة العناوين الخاصة، أستخدم الأمر **nat 0** لتخطي NAT. تمنع القواعد الموجودة على جدار حماية PIX تضمين العناوين الخاصة في NAT بينما تتنقل هذه القواعد إلى شبكة LAN البعيدة عبر نفق IPsec.

- **كيفية إستخدام قائمة التحكم في الوصول (ACL) للتشفير.**بعد عمليات فحص NAT، يتحقق PIX من مصدر ووجهة كل حزمة IP تصل إلى الواجهة الداخلية الخاصة بها لمطابقة قوائم التحكم في الوصول (ACL) المحددة في خرائط التشفير الثابتة والحيوية. إذا عثر PIX على تطابق مع قائمة التحكم في الوصول (ACL)، فإن PIX يتخذ أي من الخطوات التالية:في حالة عدم وجود اقتران أمان IPsec (SA) حالي تم إنشاؤه بالفعل باستخدام جهاز IPsec النظير لحركة المرور، يقوم PIX ببدء مفاوضات IPsec. بمجرد إنشاء شبكات SA، فإنها تقوم بتشفير الحزمة وإرسالها عبر نفق IPsec إلى نظير IPsec.إذا تم بالفعل إنشاء IPsec SA مع النظير، يقوم PIX بتشفير حزمة IP وإرسال الحزمة المشفرة إلى جهاز IPsec النظير.
- **قائمة تحكم في الوصول (ACL) ديناميكية.**بمجرد اتصال عميل شبكة VPN ب PIX باستخدام تعليمات IPsec، يقوم PIX بإنشاء قائمة تحكم في الوصول (ACL) ديناميكية تحدد عنوان المصدر والوجهة المراد إستخدامه لتحديد حركة المرور المثيرة للاهتمام لاتصال IPsec هذا.

تعرف على سلسلة الأحداث الإشكالية على PIX

خطأ تكوين شائع هو إستخدام قائمة التحكم في الوصول (ACL) نفسها ل NAT 0 وخرائط التشفير الثابتة. وتناقش هذه الأقسام سبب حدوث خطأ ما وكيفية تصحيح المشكلة.

يوضح تكوين PIX أن قائمة التحكم في الوصول (ACL) ل NAT 0 تتجاوز NAT عندما تتنقل حزم IP من الشبكة 24/192.168.4.0 إلى الشبكات 24/10.10.10.0 و 24/10.1.2.0 (عنوان الشبكة المحدد في تجمع IP المحلي). وبالإضافة إلى ذلك، تحدد قائمة التحكم في الوصول (140 (ACL حركة المرور المثيرة للاهتمام لخريطة التشفير الثابتة للنظير 172.16.172.39.

عندما تأتي حزمة IP إلى واجهة PIX الداخلية، يتم التحقق من NAT ثم يتحقق PIX من قوائم التحكم في الوصول (ACL) في خرائط التشفير. يبدأ PIX بخريطة التشفير بأقل رقم مثيل. وذلك لأن خريطة التشفير الثابتة في المثال السابق تحتوي على أقل رقم مثيل، يتم التحقق من قائمة التحكم في الوصول (140 (ACL. بعد ذلك، يتم تحديد قائمة التحكم في الوصول (ACL) الديناميكية لخريطة التشفير الديناميكية. في هذا التكوين، يتم تحديد قائمة التحكم في الوصول (140 (ACL لتشفير حركة المرور التي تتنقل من الشبكة 192.168.4.0 /24 إلى الشبكات 24/10.10.10.0 و 10.1.2.0 /24. ومع ذلك، بالنسبة لنفق شبكة LAN إلى شبكة LAN، تريد فقط تشفير حركة مرور البيانات بين الشبكات 192.168.4.0 /24 و 10.10.10.0 /24. هذه هي الطريقة التي يحدد بها موجه نظير IPsec قائمة التحكم في الوصول (ACL) المشفرة الخاصة به.

تعرف على سلسلة الأحداث الإشكالية على PIX

عندما يقوم العميل بإنشاء اتصال IPsec ب PIX، يتم تعيين عنوان IP له من تجمع IP المحلي. في هذه الحالة، يتم تعيين العميل إلى 10.1.2.1. كما يقوم PIX بإنشاء قائمة تحكم في الوصول (ACL) ديناميكية، كما يوضح إخراج الأمر **show crypto map**:

```
Crypto Map "mymap" 20 ipsec-isakmp
                                Peer = 171.69.89.120
(access-list dynacl2 permit ip host 172.16.172.34 host 10.1.2.1 (hitcnt=0
                        (dynamic (created from dynamic map dynmap/10
                                Current peer: 171.69.89.120
        Security association lifetime: 4608000 kilobytes/28800 seconds
                                PFS (Y/N): N
                        { ,Transform sets={ myset
Crypto Map "mymap" 30 ipsec-isakmp
                                Peer = 171.69.89.120
(access-list dynacl3 permit ip any host 10.1.2.1 (hitcnt=0
```

```
(dynamic (created from dynamic map dynmap/10
                                        Current peer: 171.69.89.120
                Security association lifetime: 4608000 kilobytes/28800 seconds
                                                PFS (Y/N): N
                                  { ,Transform sets={ myset
                                          #(pix520-1(config
```

يعرض الأمر **show crypto map** أيضا خريطة التشفير الثابتة:

```
                                  { Crypto Map: "mymap" interfaces: { outside
                                        Crypto Map "mymap" 5 ipsec-isakmp
                                                Peer = 172.16.172.39
access-list 140 permit ip 192.168.4.0 255.255.255.0 10.10.10.0255.255.255.0
                                                        (hitcnt=45)
 access-list 140 permit ip 192.168.4.0 255.255.255.0 10.1.2.0 255.255.255.0
                                                        (hitcnt=84)
                                        Current peer: 172.16.172.39
                Security association lifetime: 4608000 kilobytes/28800 seconds
                                                PFS (Y/N): N
                                  {,Transform sets={ myset
```

بمجرد إنشاء نفق IPsec بين العميل و PIX، يقوم العميل بتهيئة إختبار اتصال للمضيف 192.168.4.3. عندما يستلم طلب echo، يرد المضيف 192.168.4.3 مع رد echo كما يظهر هذا الإخراج من أمر **debug icmp trace**.

```
(Inbound ICMP echo request (len 32 id 2 seq 7680 :27
                192.168.4.3 <192.168.4.3 < 10.1.2.1
 (Outbound ICMP echo reply (Len 32 id 2 seq 7680 :28
                10.1.2.1 < 192.168.4.3< 192.168.4.3
(Inbound ICMP echo request (Len 32 id 2 seq 7936 :29
                192.168.4.3 <192.168.4.3 < 10.1.2.1
 (Outbound ICMP echo reply (Len 32 id 2 seq 7936 :30
                10.1.2.1 < 192.168.4.3< 192.168.4.3
```

مهما، لا يبلغ الرد صدى أن ال VPN زبون (مضيف 10.1.2.1)، وال ping يفشل. يمكنك رؤية ذلك باستخدام الأمر **show crypto ipSec** على PIX. يوضح هذا الإخراج أن PIX يقوم بفك تشفير الحزم 120 التي تأتي من عميل VPN، ولكنه لا يقوم بتشفير أي حزم أو إرسال الحزم المشفرة إلى العميل. لذلك، فإن عدد الحزم التي يتم تغليفها هو صفر.

```
                                pix520-1(config)#show crypto ipsec sa
                                                interface: outside
                                Crypto map tag: mymap, local addr. 172.16.172.34
                        (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
                (remote ident (addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0
                                                current_peer: 171.69.89.120
                                        dynamic allocated peer ip: 10.1.2.1
                                                        {}=PERMIT, flags
                                pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
No packets encrypted and sent to client. #pkts decaps: 120, #pkts decrypt: 120, #pkts ---!
                                                                verify 120
packets received from client. #pkts compressed: 0, #pkts decompressed: 0 120 ---!
                pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                                                send errors 0, #recv errors 0#
                local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120
                                path mtu 1500, ipsec overhead 56, media mtu 1500
                                        current outbound spi: 33a45029
                                                :inbound esp sas
                                                (spi: 0x279fc5e9(664782313
                                , transform: ESP-Des esp-md5-hmac
                                                { ,in use settings ={Tunnel
                                slot: 0, conn id: 5, crypto map: mymap
```

```
(sa timing: remaining key lifetime (k/sec): (4607985/27809
                                                IV size: 8 bytes
                                    replay detection support: Y
                                                 :inbound ah sas
                                                :inbound pcp sas
                                               :outbound ESP sas
                                        (spi: 0x33a45029(866406441
                                    , transform: ESP-Des esp-md5-hmac
                                         { ,in use settings ={Tunnel
                                    slot: 0, conn id: 6, crypto map: mymap
                    (sa timing: remaining key lifetime (k/sec): (4608000/27809
                                                IV size: 8 bytes
                                    replay detection support: Y
                                                :outbound ah sas
                                               :outbound PCP sas
    (local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0
    (remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                                        current_peer: 172.16.172.39
                                      {,PERMIT, flags={origin_is_acl
                      pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10#
                      pkts decaps: 23, #pkts decrypt: 23, #pkts verify 23#
                                  pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#
                                      send errors 0, #recv errors 0#
    local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39
                    path mtu 1500, ipsec overhead 56, media mtu 1500
                                    current outbound spi: f264e92c
                                                :inbound ESP sas
                                         (spi: 0x2772b869(661829737
                                    , transform: ESP-Des esp-md5-hmac
                                         { ,in use settings ={Tunnel
                                    slot: 0, conn id: 1, crypto map: mymap
                    (sa timing: remaining key lifetime (k/sec): (4607997/2420
                                                IV size: 8 bytes
                                    replay detection support: Y
                                                 :inbound ah sas
                                                :inbound PCP sas
                                               :outbound ESP sas
                                        (spi: 0xf264e92c(4066699564
                                    , transform: ESP-Des esp-md5-hmac
                                         { ,in use settings ={Tunnel
                                    slot: 0, conn id: 2, crypto map: mymap
                    (sa timing: remaining key lifetime (k/sec): (4607999/2420
                                                IV size: 8 bytes
                                    replay detection support: Y
                                                :outbound ah sas
                                               :outbound PCP sas
```

ملاحظة: عندما يرد المضيف 192.168.4.3 على طلب echo، تأتي حزمة IP إلى الواجهة الداخلية ل PIX.

```
(Outbound ICMP echo reply (Len 32 id 2 seq 8960 :38
                    10.1.2.1 < 192.168.4.3< 192.168.4.3
```

بمجرد وصول حزمة IP إلى الواجهة الداخلية، يتحقق PIX من قائمة التحكم في الوصول (ACL) إلى 140 0 NAT ويحدد أن عناوين المصدر والوجهة لحزمة IP تطابق قائمة التحكم في الوصول (ACL). لذلك، تتجاوز حزمة IP هذه جميع قواعد NAT على PIX. بعد ذلك، يتم التحقق من قوائم التحكم في الوصول (ACL) للتشفير. نظرا لأن خريطة التشفير الثابتة تحتوي على أقل رقم مثيل، يتم التحقق من قائمة التحكم في الوصول (ACL) الخاصة بها أولا. بما أن هذا المثال يستخدم قائمة التحكم في الوصول (140 (ACL لخريطة التشفير الثابتة، فإن PIX يتحقق من قائمة التحكم في الوصول (ACL) هذه. تحتوي حزمة IP الآن على عنوان مصدر بقيمة 192.168.4.3 ووجهة بقيمة 10.1.2.1. بما أن هذا يطابق قائمة التحكم في الوصول (140 (ACL، فإن PIX يعتقد أن حزمة IP هذه مخصصة لنفق IPsec من الشبكة المحلية إلى الشبكة المحلية مع النظير 172.16.172.39 (بخلاف أهدافنا). لذلك، يتحقق من قاعدة بيانات SA أن يرى إن هناك بالفعل SA حالي مع نظير 172.16.72.39 ل هذا حركة مرور. كما يظهر إخراج الأمر **show crypto**

ipSec sa، لا توجد SA لحركة المرور هذه. لا يقوم PIX بتشفير الحزمة أو إرسالها إلى عميل VPN. بدلا من ذلك، يقوم ببدء تفاوض IPsec آخر مع النظير 172.16.172.39 كما يوضح هذا الإخراج:

```
crypto_isakmp_process_block: src 172.16.172.39, dest 172.16.172.34
(.return status is IKMP_NO_ERR_NO_TRANS02303: sa_request, (key eng. msg
,src= 172.16.172.34, dest= 172.16.172.39
,(src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
=dest_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform
,ESP-Des esp-md5-hmac , lifedur= 28800s and 4608000kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
=sa_request, (key Eng. msg.) src= 172.16.172.34, dest :702303
,(src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4 ,172.16.172.39
=dest_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform
,ESP-Des esp-md5-hmac , lifedur= 28800s and 4608000kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANSIPSEC(key_engine): request timer
,fired: count = 2
,identity) local= 172.16.172.34, remote= 172.16.172.39)
,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
(remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4
```

يفشل تفاوض IPsec لهذه الأسباب:

- يحدد النظير 172.16.172.39 الشبكات 24/10.10.10.0 و 24/192.168.4.0 فقط كحركة مرور مثيرة للاهتمام في قائمة التحكم في الوصول (ACL) الخاصة به لنظير خريطة التشفير 172.16.172.34.
- لا تتطابق هويات الوكيل أثناء تفاوض IPsec بين النظامين.
- إذا قام النظير بتهيئة التفاوض وقام التكوين المحلي بتحديد سرية إعادة التوجيه (PFS) المثالية، فيجب على النظير تنفيذ تبادل PFS أو فشل التفاوض. إذا لم يحدد التكوين المحلي مجموعة، يتم افتراض وجود مجموعة افتراضية من المجموعة 1، ويتم قبول عرض من إما المجموعة 1 أو المجموعة 2. إذا كان التكوين المحلي يحدد المجموعة 2، فيجب أن تكون تلك المجموعة جزءا من عرض النظير أو فشل التفاوض. إذا لم يحدد التكوين المحلي PFS، فإنه يقبل أي عرض من PFS من النظير. توفر مجموعة وحدات Diffie-Hellman الأساسية بنظام 1024 بت، المجموعة 2، أمانا أكثر من المجموعة 1، ولكنها تتطلب وقتا معالجة أكبر من المجموعة 1.**ملاحظة:** يقوم الأمر **crypto map set pfs** بتعيين IPsec لطلب PFS عندما يطلب SAs جديدة لإدخال خريطة التشفير هذا. أستخدم الأمر **no crypto map set pfs** لتحديد أن IPsec لا يطلب PFS. يتوفر هذا الأمر فقط لإدخالات خريطة التشفير و IPsec-ISAKMP وإدخالات خريطة التشفير الديناميكية. بشكل افتراضي، لا يتم طلب ملفات PFS. مع PFS، في كل مرة يتم التفاوض على مساعدة مالية جديدة، يحدث تبادل جديد ل Diffie-Hellman. وهذا يتطلب وقتا إضافيا للمعالجة. يضيف PFS مستوى آخر من التأمين لأنه إذا تم تصدع مفتاح واحد من قبل المهاجم، فإن البيانات المرسلة مع ذلك المفتاح يتم إختراقها. أثناء التفاوض، يتسبب هذا الأمر في قيام IPsec بطلب PFS عندما يطلب SAs جديدة لإدخال خريطة التشفير. يتم إرسال الافتراضي (المجموعة 1) إذا كانت جملة **مجموعة ملفات PFS** لا تحدد مجموعة.**ملاحظة:** يمكن تعليق مفاوضات IKE مع نظير بعيد عندما يحتوي جدار حماية PIX على أنفاق عديدة تنشأ من جدار حماية PIX وتنتهي على نظير واحد بعيد. تحدث هذه المشكلة عندما يكون PFS غير ممكن، ويطلب النظير المحلي العديد من طلبات rekey المتزامنة. إذا حدثت هذه المشكلة، فإن IKE SA لا يسترد حتى يبلغ نهايته أو حتى تقوم بمسحه يدويا باستخدام الأمر **clear [crypto] isakmp sa**. لا تتأثر وحدات جدار حماية PIX التي تم تكوينها باستخدام أنفاق عديدة للعديد من الأقران أو العديد من العملاء الذين يتقاسمون نفس النفق بهذه المشكلة. إذا تأثر التكوين الخاص بك، قم بتمكين PFS باستخدام الأمر **crypto map map seqnum set pfs**.

يتم إسقاط حزم IP على PIX في نهاية المطاف.

تعرف على الحل

الطريقة الصحيحة لتصحيح هذا الخطأ هي تحديد قوائم التحكم في الوصول (ACL) منفصلة ل NAT 0 وخرائط التشفير الثابتة. للقيام بهذا الإجراء، يحدد المثال قائمة التحكم في الوصول (ACL) رقم 190 للأمر **nat 0** ويستخدم

قائمة التحكم في الوصول (ACL) المعدلة رقم 140 لخريطة التشفير الثابتة، كما يظهر هذا الإخراج.

PIX 520-1

```
#(pix520-1(config
pix520-1(config)#write terminal
...Building configuration
Saved :
:
(PIX Version 6.0(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix520-1
domain-name vpn.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
Access list 140 defines interesting traffic in ---!
order to bypass NAT for VPN. access-list 140 permit ip
192.168.4.0 255.255.255.0 10.10.10.0255.255.255.0
Defines VPN interesting traffic. access-list 190 ---!
permit ip 192.168.4.0 255.255.255.0
10.10.10.0255.255.255.0
access-list 190 permit ip 192.168.4.0 255.255.255.0
10.1.2.0 255.255.255.0
no pager
logging on
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging

logging history debugging
logging host outside 192.168.2.6
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.16.172.34 255.255.255.240
ip address inside 192.168.4.50 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
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
pdm history enable
arp timeout 14400
global (outside) 1 172.16.172.57 netmask 255.255.255.255
The nat 0 command bypasses NAT for the packets ---!
..destined over the IPsec tunnel
```

```
                                Nat (inside) 0 access-list 190
                                    Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
                                route outside 0.0.0.0 0.0.0.0 172.16.172.33 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
                                  +AAA-server mytest protocol tacacs
                                     AAA-server nasir protocol radius
                                 snmp-server host outside 192.168.2.6
                                              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
    crypto dynamic-map dynmap 10 set transform-set myset
 The crypto map commands define the IPsec SA (Phase ---!
                                                .II SA) parameters

                                    crypto map mymap 5 ipsec-isakmp
                                  crypto map mymap 5 match address 140
                                crypto map mymap 5 set peer 172.16.172.39
                               crypto map mymap 5 set transform-set myset
                            crypto map mymap 10 ipsec-isakmp dynamic dynmap
                                    crypto map mymap interface outside
                                                isakmp enable outside
          isakmp key ******** address 172.16.172.39 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 sha
                                         isakmp policy 10 group 2
                                    isakmp policy 10 lifetime 86400
                                isakmp policy 20 authentication pre-share
                                        isakmp policy 20 encryption Des
                                          isakmp policy 20 hash sha
                                         isakmp policy 20 group 1
                                    isakmp policy 20 lifetime 86400
                                vpngroup vpn3000 address-pool ippool
                                    vpngroup vpn3000 idle-time 1800
                                ******** vpngroup vpn3000 password
                              telnet 192.168.4.0 255.255.255.0 inside
                            telnet 171.69.89.82 255.255.255.255 inside
                                                telnet timeout 5
                                    ssh 172.0.0.0 255.0.0.0 outside
                                ssh 171.0.0.0 255.255.255.0 outside
                                    ssh 171.0.0.0 255.0.0.0 outside
                                                ssh timeout 60
                                               terminal width 80
          Cryptochecksum:e2cb98b30d3899597b3af484fae4f9ae
                                                            end :
                                                           [OK]
      pix520-1(config)# pix520-1(config)#show crypto map
```

بعد إجراء التغييرات وإنشاء العميل نفق IPsec باستخدام PIX، قم بإصدار الأمر **show crypto map**. يوضح هذا

الأمر أنه بالنسبة لخريطة التشفير الثابتة، فإن حركة المرور المفيدة المعرفة بواسطة ACL 140 هي فقط 24/192.168.4.0 و 24/10.10.10.0، والتي كانت الهدف الأصلي. بالإضافة إلى ذلك، توضح قائمة الوصول الديناميكية حركة المرور المهمة المعرفة باسم العميل (10.1.2.1) و 172.16.172.34) PIX).

```
pix520-1(config)#show crypto map
{ Crypto Map: "mymap" interfaces: { outside
Crypto Map "mymap" 5 ipsec-isakmp
Peer = 172.16.172.39
access-list 140 permit ip 192.168.4.0 255.255.255.0 10.10.10.0255.255.255.0
(hitcnt=57)
Current peer: 172.16.172.39
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
{ ,Transform sets={ myset
Crypto Map "mymap" 10 ipsec-isakmp
Dynamic map template tag: dynmap
Crypto Map "mymap" 20 ipsec-isakmp
Peer = 171.69.89.120
(access-list dynacl4 permit ip host 172.16.172.34 host 10.1.2.1 (hitcnt=0
(dynamic (created from dynamic map dynmap/10
Current peer: 171.69.89.120
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
{ ,Transform sets={ myset
Crypto Map "mymap" 30 ipsec-isakmp
Peer = 171.69.89.120
(access-list dynacl5 permit ip any host 10.1.2.1 (hitcnt=13
(dynamic (created from dynamic map dynmap/10
Current peer: 171.69.89.120
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
{ ,Transform sets={ myset
```

عندما يرسل عميل 10.1.2.1 VPN إختبار اتصال إلى المضيف 192.168.4.3، يأتي رد الصدى إلى الواجهة الداخلية ل PIX. يتحقق PIX من قائمة التحكم في الوصول إلى 190 ACL 0 NAT ويحدد أن حزمة IP تطابق قائمة التحكم في الوصول (ACL). لذلك، تتجاوز الحزمة قواعد NAT على PIX. بعد ذلك، يتحقق PIX من قائمة التحكم في الوصول (ACL) الخاصة بخريطة التشفير الثابتة للعثور على تطابق. هذه المرة، لا يطابق مصدر حزمة IP ووجهتها قائمة التحكم في الوصول (140 (ACL. لذلك، يتحقق PIX من قائمة التحكم في الوصول (ACL) الديناميكية ويجد تطابق. بعد ذلك يقوم PIX بفحص قاعدة بيانات SA الخاصة به لمعرفة ما إذا كان قد تم إنشاء IPsec SA بالفعل مع العميل أم لا. نظرا لأن العميل قام بالفعل بإنشاء اتصال IPsec مع PIX، يوجد IPsec SA. وبعد ذلك يقوم PIX بتشفير الحزم وإرسالها إلى عميل VPN. أستخدم إخراج الأمر **show crypto ipSec sa** من PIX لرؤية تشفير الحزم وفك تشفيرها. في هذه الحالة، يقوم PIX بتشفير ست عشرة حزمة وإرسالها إلى العميل. تلقى PIX أيضا حزم مشفرة من عميل VPN وفك تشفير ست عشرة حزمة.

```
pix520-1(config)#show crypto ipsec sa
interface: outside
Crypto map tag: mymap, local addr. 172.16.172.34
(local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0
current_peer: 171.69.89.120
dynamic allocated peer ip: 10.1.2.1
{}=PERMIT, flags
pkts encaps: 16, #pkts encrypt: 16,#pkts digest 16#
pkts decaps: 16, #pkts decrypt: 16, #pkts verify 16#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#
send errors 0, #recv errors 0#
local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120
path mtu 1500, ipsec overhead 56, media mtu 1500
```

```
                                                current outbound spi: 613d083d
                                                              :inbound ESP sas
                                                   (spi: 0x6adf97df(1793038303
                                          , transform: ESP-Des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                        slot: 0, conn id: 4, crypto map: mymap
                                (sa timing: remaining key lifetime (k/sec): (4607998/27420
                                                              IV size: 8 bytes
                                                 replay detection support: Y
                                                               :inbound ah sas
                                                              :inbound PCP sas
                                                             :outbound ESP sas
                                                   (spi: 0x613d083d(1631389757
                                          , transform: ESP-Des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                        slot: 0, conn id: 3, crypto map: mymap
                                (sa timing: remaining key lifetime (k/sec): (4607999/27420
                                                              IV size: 8 bytes
                                                 replay detection support: Y
                                                              :outbound ah sas
                                                             :outbound PCP sas
                        (local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0
                        (remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                                                    current_peer: 172.16.172.39
                                                    {,PERMIT, flags={origin_is_acl
                                      pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9#
                                      pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9#
                                                pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#
                                                send errors 1, #recv errors 0#
    local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39
                                        path mtu 1500, ipsec overhead 56, media mtu 1500
                                                current outbound spi: 58009c01
                                                              :inbound ESP sas
                                                    (spi: 0x2d408709(759203593
                                          , transform: ESP-Des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                        slot: 0, conn id: 2, crypto map: mymap
                                (sa timing: remaining key lifetime (k/sec): (4607998/3319
                                                              IV size: 8 bytes
                                                 replay detection support: Y
                                                               :inbound ah sas
                                             :inbound PCP sas: outbound ESP sas
                                                   (spi: 0x58009c01(1476434945
                                          , transform: ESP-Des esp-md5-hmac
                                                   { ,in use settings ={Tunnel
                                        slot: 0, conn id: 1, crypto map: mymap
                                (sa timing: remaining key lifetime (k/sec): (4607999/3319
                                                              IV size: 8 bytes
                                                 replay detection support: Y
                                                              :outbound ah sas
                                                             :outbound PCP sas
                                                pix520-1(config)# sh cr isa sa
                                                                    Total : 2
                                                                Embryonic : 0
                                                 dst src state pending created
                                            QM_IDLE 0 1 172.16.172.34 172.16.172.39
                                            QM_IDLE 0 2 171.69.89.120 172.16.172.34
                                                   pix520-1(config)# sh cr ipsec sa
```

تكوين الموجه وإظهار الأمر output

Cisco 1720-1

```
1720-1#show run
...Building configuration
Current configuration : 1592 bytes
!
Last configuration change at 21:08:49 PST Mon Jan 7 !
2002
NVRAM config last updated at 18:18:17 PST Mon Jan 7 !
2002
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-1
!
no logging buffered
/enable secret 5 $1$6jAs$tNxI1a/2DYFAtPLyCDXjo
enable password ww
!
username cisco password 0 cisco
memory-size iomem 15
clock timezone PST -8
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
The crypto isakmp policy command defines the Phase ---!
.1 SA parameters

crypto isakmp policy 15
authentication pre-share
crypto isakmp key cisco123 address 172.16.172.34
!
!
The crypto ipsec transform-set command defines ---!
.IPsec encryption !--- and authentication algorithims

crypto ipsec transform-set myset ESP-Des esp-md5-hmac
!
!
The crypto map command defines the IPsec SA (Phase ---!
..II SA) parameters

crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.34
set transform-set myset
match address 150
!
!
!
!
!
interface FastEthernet0
ip address 172.16.172.39 255.255.255.240
speed auto
The crypto map applied to the outbound interface. ---!
```

```
                                                    crypto map vpn
                                                interface Ethernet0
                                    ip address 10.10.10.1 255.255.255.240
                                                     speed auto
                                                no ip route-cache
                                               no ip mroute-cache
                                                          !
                                                          !
                                                   ip classless
                                    ip route 0.0.0.0 0.0.0.0 172.16.172.33
                                                no ip http server
                                              ip pim bidir-enable
                                                          !
                                    Access-list defines interesting VPN traffic. ---!
                                       access-list 150 permit ip 10.10.10.0 0.0.0.255
                                                    192.168.4.0 0.0.0.255
                                                          !
                                                     line con 0
                                                     line aux 0
                                                   line vty 0 4
                                                exec-timeout 0 0
                                                  password cisco
                                                       no login
                                                  line vty 5 15
                                                         login
                                                          !
                                                no scheduler allocate
                                                         end
                                                      1720-1#
```

```
                                                1720-1#show crypto isa sa
                                                DST src state conn-id slot
                                    QM_IDLE 132 0 172.16.172.34 172.16.172.39
                                                1720-1#show crypto ipsec sa
                                                  interface: FastEthernet0
                                        Crypto map tag: vpn, local addr. 172.16.172.39
                          (local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                         (remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0
                                                    current_peer: 172.16.172.34
                                                {,PERMIT, flags={origin_is_acl
                                      pkts encaps: 9 #pkts encrypt: 9 #pkts digest 9#
                                     pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9#
                                          pkts compressed: 0, #pkts decompressed: 0#
                    pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#
                                                send errors 7, #recv errors 0#
                        local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.34
                                                    path mtu 1500, media mtu 1500
                                                current outbound spi: 2D408709
                                                     :inbound ESP sas
                                                  (spi: 0x58009C01(1476434945
                                        , transform: ESP-Des esp-md5-hmac
                                                { ,in use settings ={Tunnel
.IPsec SA 200 as seen in the show crypto engine connection active command ---!

                                    slot: 0, conn id: 200, flow_id: 1, crypto map: vpn
                                  (sa timing: remaining key lifetime (k/sec): (4607998/3144
                                                     IV size: 8 bytes
                                               replay detection support: Y
                                                     :inbound ah sas
                                                    :inbound PCP sas
                                                   :outbound ESP sas
                                                  (spi: 0x2D408709(759203593
                                        , transform: ESP-Des esp-md5-hmac
```

```
{ ,in use settings ={Tunnel
.IPsec SA 201 as seen in the show crypto engine connection active command ---!

slot: 0, conn id: 201, flow_id: 2, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4607998/3144
IV size: 8 bytes
replay detection support: Y
:outbound ah sas
:outbound PCP sas
1720-1#

1720-1#show crypto map
:Interfaces using crypto map mymap
Crypto Map "vpn" 10 ipsec-isakmp
Peer = 172.16.172.34
Extended IP access list 150
access-list 150 permit ip 10.10.10.0 0.0.0.255 192.168.4.0 0.0.0.255
Current peer: 172.16.172.34
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
{ ,Transform sets={ myset
Interfaces using crypto map vpn: FastEthernet0
```

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- مفاوضة IPSec/بروتوكولات IKE
- 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).