جدار حماية PIX لترجمة المضيف الوارد على نفق شبكة بعيدة متصلة عبر مثال تكوين L2L IPsec

المحتويات

المقدمة

يصف هذا المستند الخطوات المستخدمة لترجمة IP المصدر لمضيف يأتي عبر نفق IP من شبكة LAN إلى شبكة LAN بين جدرتي حماية PIX المؤمنتين من Cisco. يحتوي كل جدار حماية PIX على شبكة خاصة محمية خلفه. ينطبق هذا المفهوم أيضا عند ترجمة الشبكات الفرعية بدلا من البيئات المضيفة الفردية.

ملاحظة: أستخدم هذه الخطوات لتكوين السيناريو نفسه في PIX/ASA 7.x:

- من أجل تكوين نفق VPN من موقع إلى موقع ل PIX/ASA 7.x، ارجع إلى PIX/ASA 7.x: مثال تكوين نفق PIX-to-PIX VPN البسيط.
- **الأمر static** المستخدم للاتصالات الواردة مماثل لكل من x.6 و x.7 كما هو موضح في هذا المستند.
- أوامر **show** و**clear** و**debug** المستخدمة في هذا المستند متشابهة في PIX 6.x و x.7.

المتطلبات الأساسية

المتطلبات

تأكد من تكوين جدار حماية PIX باستخدام عناوين IP على الواجهات وأن لديك اتصال أساسي قبل المتابعة بمثال التكوين هذا.

المكونات المستخدمة

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

- جدار حماية Cisco PIX 506e
- برنامج Cisco Secure PIX Firewall، الإصدار 6.3(3)

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

الاصطلاحات

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

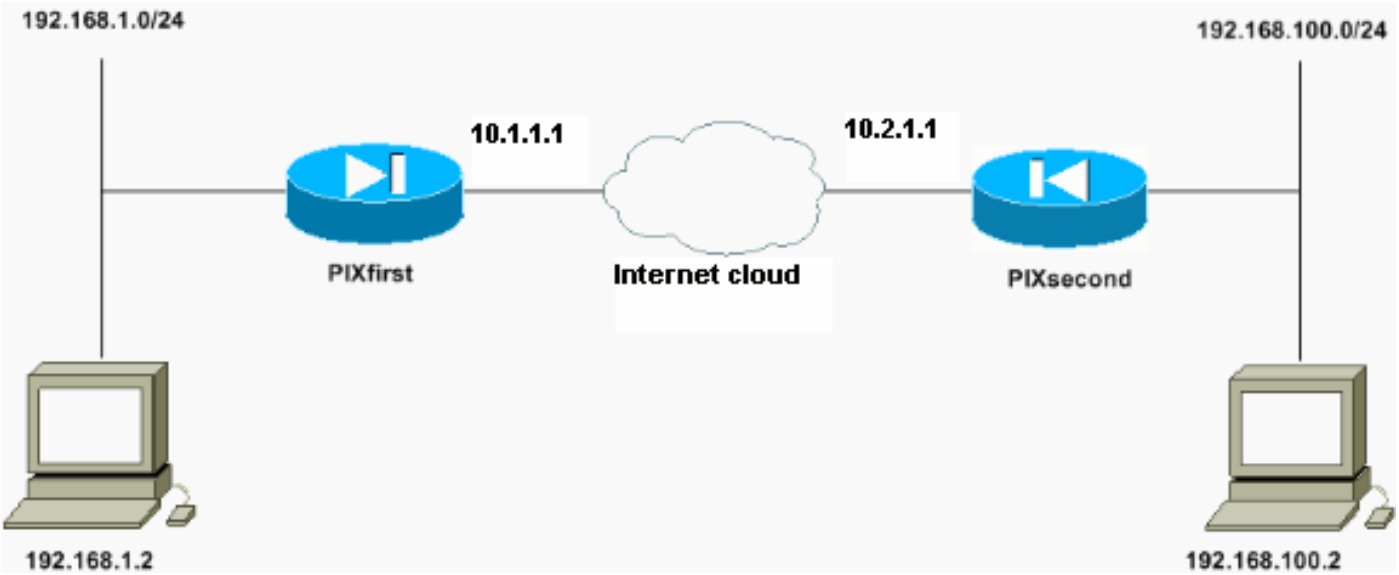
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تتم ترجمة المضيف صاحب عنوان IP 192.168.100.2 إلى 192.168.50.2 على جدار حماية PIX باستخدام اسم المضيف ل PIXfirst. هذه الترجمة شفافة للمضيف ووجهته.

ملاحظة: لا تتم ترجمة أي عناوين IP مضمنة بشكل افتراضي ما لم يتم تمكين إصلاح لذلك التطبيق. عنوان IP المضمن هو عنوان يضمنه التطبيق ضمن جزء حمولة البيانات من حزمة IP. تعدل ترجمة عنوان الشبكة (NAT) رأس IP الخارجي فقط لحزمة IP. لا تقوم بتعديل حمولة البيانات للحزمة الأصلية التي يمكن من خلالها تضمين IPs بواسطة تطبيقات معينة. يتسبب ذلك أحيانا في عدم عمل هذه التطبيقات بشكل صحيح.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين PIXfirst
- تكوين PIXii

تكوين PIXfirst

```
PIXfirst(config)#write terminal

...Building configuration

Saved :

:

(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXfirst
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
Define encryption domain (interesting traffic) !--- ---!
    for the IPsec tunnel. access-list 110 permit ip host
192.168.1.2 host 192.168.100.2

    Accept the private network traffic from the NAT ---!
process. access-list 120 permit ip host 192.168.1.2 host
192.168.50.2
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 10.1.1.1 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400

  Bypass translation for traffic that goes over the ---!
IPsec tunnel. nat (inside) 0 access-list 120

    Inbound translation for the host located on the ---!
    remote network. static (outside,inside) 192.168.50.2
192.168.100.2 netmask 255.255.255.255 0 0
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
```

```
                                        timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                        0:10:00 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


    Accept traffic that comes over the IPsec tunnel ---!
from !--- Adaptive Security Algorithm (ASA) rules and !-
-- access control lists (ACLs) configured on the outside
                interface. sysopt connection permit-ipsec

          Create the Phase 2 policy for actual data ---!
 encryption. crypto ipsec transform-set chevelle esp-des
                                                esp-md5-hmac
                          crypto map transam 1 ipsec-isakmp
                    crypto map transam 1 match address 110
                    crypto map transam 1 set peer 10.2.1.1
              crypto map transam 1 set transform-set chevelle
                          crypto map transam interface outside
                                       isakmp enable outside

      Pre-shared key for the IPsec peer. isakmp key ---!
       ******** address 10.2.1.1 netmask 255.255.255.255

 Create the Phase 1 policy. isakmp identity address ---!
                    isakmp policy 1 authentication pre-share
                              isakmp policy 1 encryption des
                                    isakmp policy 1 hash md5
                                   isakmp policy 1 group 1
                                isakmp policy 1 lifetime 1000
                                               telnet timeout 5
                                                  ssh timeout 5
                                             console timeout 0
                                             terminal width 80
        Cryptochecksum:778f934d42c037a978b8b5236a93b5f4

                                                        end :


                                                        [OK]

                                                #(PIXfirst(config
```

تكوين PIXii

```
                                PIXsecond(config)#write terminal

                                        ...Building configuration

                                                        Saved :

                                                              :
```

```
(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXsecond
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

   Accept the private network traffic from the NAT ---!
process. access-list nonat permit ip host 192.168.100.2
host 192.168.1.2

Define encryption domain (interesting traffic) for ---!
the IPsec tunnel. access-list 110 permit ip host
192.168.100.2 host 192.168.1.2
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 10.2.1.1 255.255.255.0
ip address inside 192.168.100.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400

Bypass translation for traffic that goes over the ---!
IPsec tunnel. nat (inside) 0 access-list nonat
route outside 0.0.0.0 0.0.0.0 10.2.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 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

   Accept traffic that comes over the IPsec tunnel ---!
from ASA rules and !--- ACLs configured on the outside
interface. sysopt connection permit-ipsec

Create the Phase 2 policy for actual data ---!
encryption. crypto ipsec transform-set chevelle esp-des
```

```
esp-md5-hmac
crypto map transam 1 ipsec-isakmp
crypto map transam 1 match address 110
crypto map transam 1 set peer 10.1.1.1
crypto map transam 1 set transform-set chevelle
crypto map transam interface outside
isakmp enable outside

Pre-shared key for the IPsec peer. isakmp key ---!
******** address 10.1.1.1 netmask 255.255.255.255

Create the Phase 1 policy. isakmp identity address ---!
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:a686f71a023d1cd7078728a38acf529e

end :

[OK]

#(PIXsecond(config
```

إذا قمت بإنشاء أكثر من إدخال خريطة تشفير لواجهة معينة، فأنت بحاجة إلى إستخدام الرقم التسلسلي لكل إدخال لترتيبه. كلما قل رقم التسلسل، كلما إرتفعت الأولوية. في الواجهة التي تحتوي على مجموعة خريطة التشفير، يقيم جهاز الأمان حركة مرور البيانات مقابل إدخالات خرائط الأولوية الأعلى أولا.

قم بإنشاء إدخالات خريطة تشفير متعددة لواجهة معينة إذا كان أي من الأقران المختلفين يعالج تدفقات بيانات مختلفة أو إذا كنت تريد تطبيق أمان IPsec مختلف على أنواع مختلفة من حركة المرور (على الأقران المتشابهين أو المنفصلين). على سبيل المثال، إذا كنت تريد مصادقة حركة مرور البيانات بين مجموعة واحدة من الشبكات الفرعية، وحركة مرور البيانات بين مجموعة أخرى من الشبكات الفرعية أن تكون مصدق عليها ومشفرة على حد سواء. في هذه الحالة، حدد الأنواع المختلفة لحركة المرور في قائمتي وصول منفصلتين، وقم بإنشاء إدخال خريطة تشفير منفصل لكل قائمة وصول تشفير.

مسح اقترانات الأمان (SAs)

في وضع الامتيازات ل PIX، أستخدم الأوامر التالية:

- **مسح [crypto] ipSec sa**—يحذف شبكات IPsec النشطة. كلمة *التشفير* الرئيسية إختيارية.
- **مسح [crypto] isakmp sa**— يحذف شبكات IKE النشطة. كلمة *التشفير* الرئيسية إختيارية.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

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

- **show crypto ipSec sa**—يعرض المرحلة 2 SAs.
- **ping**—تشخيص الاتصال الأساسي بالشبكة. يتحقق إختبار الاتصال من PIX إلى الآخر من الاتصال بين محركي PIX. كما يمكن تشغيل إختبار الاتصال من المضيف خلف PIXsecond إلى المضيف خلف PIXfirst لاستدعاء نفق IPsec.
- **show local-host <ip_address>**—يعرض فتحات الترجمة والاتصال للمضيف المحلي الذي تم تحديد عنوان IP له.
- **إظهار تفاصيل xlate**—يعرض محتويات فتحات الترجمة. يتم إستخدام هذا للتحقق من ترجمة المضيف.

التحقق من PIXfirst

هذا هو مخرج الأمر **ping**.

```
PIXfirst(config)#ping 10.2.1.1

PIX pings the outside interface of the peer. !--- This implies that connectivity between ---!
peers is available. 10.2.1.1 response received -- 0ms
response received -- 0ms 10.2.1.1
response received -- 0ms 10.2.1.1
#(PIXfirst(config
```

هذا هو مخرج الأمر **show crypto isakmp sa**.

```
PIXfirst(config)#show crypto isakmp sa
Total : 1
Embryonic : 0

Phase 1 SA is authenticated and established. dst src state pending created 10.1.1.1 ---!
10.2.1.1     QM_IDLE   0           1
```

هذا هو مخرج الأمر **show crypto ipSec sa**.

```
Shows Phase 2 SAs. PIXfirst(config)#show crypto ipsec sa ---!

interface: outside
Crypto map tag: transam, local addr. 10.1.1.1
Shows addresses of hosts that !--- communicate over this tunnel. local ident ---!
((addr/mask/prot/port): (192.168.1.2/255.255.255.255/0/0
(remote ident (addr/mask/prot/port): (192.168.100.2/255.255.255.255/0/0
current_peer: 10.2.1.1:500

{,PERMIT, flags={origin_is_acl
Shows if traffic passes over the tunnel or not. !--- Encapsulated packets translate to ---!
packets that are sent. !--- Decapsulated packets translate to packets that are received. #pkts
encaps: 21, #pkts encrypt: 21, #pkts digest 21
pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21#
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.: 10.1.1.1, remote crypto endpt.: 10.2.1.1
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 6ef53756

If an inbound Encapsulating Security Payload (ESP) !--- SA and outbound ESP SA exists with ---!
a !--- security parameter index (SPI) !--- number, it implies that the Phase 2 SAs !--- are
established successfully. inbound esp sas:
```

```
(spi: 0x1cf45b9f(485776287

, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2, crypto map: transam
(sa timing: remaining key lifetime (k/sec): (4607998/28756
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas


:outbound esp sas

(spi: 0x6ef53756(1861564246

, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 1, crypto map: transam
(sa timing: remaining key lifetime (k/sec): (4607998/28756
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas
```

هذا هو مخرج الأمر **show local-host**.

```
Shows translation for the host on a remote network. PIXfirst(config)#show local-host ---!
192.168.100.2

Interface outside: 1 active, 1 maximum active, 0 denied
,<local host: <192.168.100.2
TCP connection count/limit = 0/unlimited
TCP embryonic count = 0
TCP intercept watermark = unlimited
UDP connection count/limit = 0/unlimited
:AAA
:(Xlate(s
Global 192.168.50.2 Local 192.168.100.2
:(Conn(s
```

هذا هو مخرج الأمر **show xlate detail**.

```
Shows translation for the host on a remote network. PIXfirst(config)#show xlate detail ---!
in use, 1 most used 1
,Flags: D - DNS, d - dump, I - identity, i - inside, n - no random
o - outside, r - portmap, s - static
NAT from outside:192.168.100.2 to inside:192.168.50.2 flags s
#(PIXfirst(config
```

التحقق من PIXii

هذا هو مخرج الأمر **ping**.

```
PIXsecond(config)#ping 10.1.1.1

PIX can ping the outside interface of the peer. !--- This implies that connectivity between ---!
peers is available. 10.1.1.1 response received -- 0ms
response received -- 0ms 10.1.1.1
response received -- 0ms 10.1.1.1
#(PIXsecond(config
```

هذا هو مخرج الأمر **show crypto isakmp sa**.

```
PIXsecond(config)#show crypto isakmp sa

Total : 1
Embryonic : 0
Phase 1 SA is authenticated and established. dst src state pending created 10.1.1.1 ---!
10.2.1.1    QM_IDLE      0            1
```

هذا هو مخرج الأمر **show crypto ipSec sa**.

```
Shows Phase 2 SAs. PIXsecond(config)#show crypto ipsec sa ---!

interface: outside
Crypto map tag: transam, local addr. 10.2.1.1
Shows addresses of hosts that communicate !--- over this tunnel. local ident ---!
((addr/mask/prot/port): (192.168.100.2/255.255.255.255/0/0
(remote ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/0/0
current_peer: 10.1.1.1:500

{,PERMIT, flags={origin_is_acl
Shows if traffic passes over the tunnel or not. !--- Encapsulated packets translate to ---!
packets that are sent. !--- Decapsulated packets translate to packets that are received. #pkts
encaps: 21, #pkts encrypt: 21, #pkts digest 21
pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21#
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.: 10.2.1.1, remote crypto endpt.: 10.1.1.1
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 1cf45b9f

If an inbound ESP SA and outbound ESP SA exists with an SPI !--- number, it implies that ---!
:the Phase 2 SAs are established successfully. inbound esp sas

(spi: 0x6ef53756(1861564246

, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2, crypto map: transam
(sa timing: remaining key lifetime (k/sec): (4607990/28646
IV size: 8 bytes
replay detection support: Y
:inbound ah sas

:inbound pcp sas

:outbound esp sas

(spi: 0x1cf45b9f(485776287
```

```
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 1, crypto map: transam
(sa timing: remaining key lifetime (k/sec): (4607993/28645
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas

#(PIXsecond(config
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات أستكشاف 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**—يعرض معلومات حول أحداث IPsec.
- **debug crypto isakmp**—يعرض رسائل حول أحداث IKE (Internet Key Exchange).
- **debug packet if_name [src source_ip [netmask]] [dst dest_ip [netmask]] [[proto icmp] | [proto tcp [sport src_port] [dport dest_port] | [proto udp [sport src_port] [dport dest_port] [rx | tx كلا]**— يعرض الحزم التي تصل إلى الواجهة المحددة. يكون هذا الأمر مفيدا عندما تحدد نوع حركة مرور البيانات على الواجهة الداخلية ل PIXfirst. كما يتم إستخدام هذا الأمر للتحقق من حدوث الترجمة المقصودة.
- **logging buffered level**—يرسل رسائل syslog إلى مخزن مؤقت داخلي يتم عرضه باستخدام الأمر **show logging**. أستخدم الأمر **clear logging** لمسح المخزن المؤقت للرسالة. يتم إلحاق الرسائل الجديدة بنهاية المخزن المؤقت. استعملت هذا أمر أن يشاهد الترجمة أن يكون بنيت. يجب تشغيل التسجيل إلى المخزن المؤقت عند الحاجة. قم بإيقاف تشغيل التسجيل إلى المخزن المؤقت بدون **مستوى المخزن المؤقت للتسجيل** و/أو **بدون تسجيل الدخول**.
- **debug icmp trace**—يعرض معلومات حزمة بروتوكول رسائل التحكم في الإنترنت (ICMP) وعنوان IP المصدر وعنوان الوجهة للحزم التي تصل إلى جدار حماية PIX وتغادر منه وتجتاز به. ويتضمن ذلك إختبار الاتصال للواجهات الخاصة بوحدة جدار حماية PIX. أستخدم **لا تصحيح أخطاء تتبع ICMP** لإيقاف تشغيل **تتبع ICMP**.

هذا هو مخرج الأمر **debug crypto isakmp** و**debug crypto ipSec**.

```
PIXfirst(config)#debug crypto isakmp
PIXfirst(config)#debug crypto ipsec
PIXfirst(config)#debug crypto engine
PIXfirst(config)#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
#(PIXfirst(config

#(PIXfirst(config

crypto_isakmp_process_block:src:10.2.1.1, dest:10.1.1.1 spt:500 dpt:500
OAK_QM exchange
```

:oakley_process_quick_mode
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 137660894

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

:(*Phase 1 policy accepted.* ISAKMP (0): **atts are acceptable.** IPSEC(validate_proposal_request *---!*
,proposal part #1
,key eng. msg.) dest= 10.1.1.1, src= 10.2.1.1)
Encryption domain (interesting traffic) that invokes the tunnel. **dest_proxy=** *---!*
,(192.168.1.2/255.255.255.255/0/0 (type=1
,(src_proxy= 192.168.100.2/255.255.255.255/0/0 (type=1
, 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 = 137660894
ISAKMP (0): processing ID payload. message ID = 137660894
ISAKMP (0): ID_IPV4_ADDR src 192.168.100.2 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 137660894
:(ISAKMP (0): ID_IPV4_ADDR dst 192.168.1.2 prot 0 port 0IPSEC(key_engine
...got a queue event
IPSEC(spi_response): getting spi 0x15ee92d9(367956697) for SA
from 10.2.1.1 to 10.1.1.1 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.2.1.1, dest:10.1.1.1 spt:500 dpt:500
OAK_QM exchange
:oakley_process_quick_mode
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 2
map_alloc_entry: allocating entry 1

ISAKMP (0): Creating IPSec SAs
(inbound SA from 10.2.1.1 to 10.1.1.1 (proxy 192.168.100.2 to 192.168.1.2
has spi 367956697 and conn_id 2 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
(outbound SA from 10.1.1.1 to 10.2.1.1 (proxy 192.168.1.2 to 192.168.100.2
has spi 1056204195 and conn_id 1 and flags 4
lifetime of 28800 seconds
...lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event
, :(IPSEC(initialize_sas
,key eng. msg.) dest= 10.1.1.1, src= 10.2.1.1)
,(dest_proxy= 192.168.1.2/0.0.0.0/0/0 (type=1
,(src_proxy= 192.168.100.2/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 28800s and 4608000kb
spi= 0x15ee92d9(367956697), conn_id= 2, keysize= 0, flags= 0x4
, :(IPSEC(initialize_sas
,key eng. msg.) src= 10.1.1.1, dest= 10.2.1.1)
,(src_proxy= 192.168.1.2/0.0.0.0/0/0 (type=1
,(dest_proxy= 192.168.100.2/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 28800s and 4608000kb
spi= 0x3ef465a3(1056204195), conn_id= 1, keysize= 0, flags= 0x4

```
VPN Peer: IPSEC: Peer ip:10.2.1.1/500 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:10.2.1.1/500 Ref cnt incremented to:3 Total VPN Peers:1
                                                    return status is IKMP_NO_ERROR

                                                                #(PIXfirst(config
```

هذا هو مخرج **حزمة** تصحيح **الأخطاء داخل src** أمر.

```
Shows that the remote host packet is translated. PIXfirst(config)#debug packet inside src ---!
                                                    192.168.50.2 dst 192.168.1.2
                                                     PIXfirst(config)# show debug
                                  debug packet inside src 192.168.50.2 dst 192.168.1.2 both

                                                         --------- PACKET ---------

                                                                      -- IP --

                    Source IP is translated to 192.168.50.2. 192.168.50.2 ==> 192.168.1.2 ---!

                                                    ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c

                                                      id = 0x82 flags = 0x0 frag off=0x0

                                                    ttl = 0x80 proto=0x1 chksum = 0x85ea

                                  -- ICMP echo packet, as expected. -- ICMP ---!

                                                    type = 0x8 code = 0x0 checksum=0x425c

                                                      identifier = 0x200 seq = 0x900

                                                                      -- DATA --

0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop

0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi

                                                    . | 0000003c: 01

                                                         --------- END OF PACKET ---------

                                                         --------- PACKET ---------

                                                                      -- IP --

                                                    192.168.1.2 <== 192.168.50.2

                                                    ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c

                                                      id = 0x83 flags = 0x0 frag off=0x0

                                                    ttl = 0x80 proto=0x1 chksum = 0x85e9

                                                                      -- ICMP --
```

```
                                        type = 0x8 code = 0x0 checksum=0x415c
                                               identifier = 0x200 seq = 0xa00
                                                                    -- DATA --
0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop
0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi
                                                          . | 0000003c: 01

                                           --------- END OF PACKET ---------

                                                  --------- PACKET ---------

                                                                       -- IP --
                                                192.168.1.2 <== 192.168.50.2

                                      ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c
                                                id = 0x84 flags = 0x0 frag off=0x0
                                               ttl = 0x80 proto=0x1 chksum = 0x85e8

                                                                    -- ICMP --
                                        type = 0x8 code = 0x0 checksum=0x405c
                                               identifier = 0x200 seq = 0xb00
                                                                    -- DATA --
0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop
0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi
                                                          . | 0000003c: 01

                                           --------- END OF PACKET ---------

                                                  --------- PACKET ---------

                                                                       -- IP --
                                                192.168.1.2 <== 192.168.50.2

                                      ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c
                                                id = 0x85 flags = 0x0 frag off=0x0
                                               ttl = 0x80 proto=0x1 chksum = 0x85e7
```

```
                                                        -- ICMP --

                                              type = 0x8 code = 0x0 checksum=0x3f5c

                                                    identifier = 0x200 seq = 0xc00

                                                        -- DATA --

     0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop

     0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi

                                                    . | 0000003c: 01


                                                --------- END OF PACKET ---------

                                                                        #(PIXfirst(config
```

هذا هو مخرج الأمر **logging buffer**.

```
                    Logs show translation is built. PIXfirst(config)#logging buffer 7 ---!
                                                        PIXfirst(config)#logging on
                                                      PIXfirst(config)#show logging

                                                            Syslog logging: enabled
                                                                    Facility: 20
                                                          Timestamp logging: disabled
                                                            Standby logging: disabled
                                                            Console logging: disabled
                                                            Monitor logging: disabled
                                                Buffer logging: level debugging, 53 messages logged
                                                               Trap logging: disabled
                                                            History logging: disabled
                                                                  Device ID: disabled

                                                  User 'enable_15' executed cmd: show logging :111009
                                               ,sa created, (sa) sa_dest= 10.1.1.1, sa_prot= 50 :602301
          sa_spi= 0xb1274c19(2972142617), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2
                                               ,sa created, (sa) sa_dest= 10.2.1.1, sa_prot= 50 :602301
          sa_spi= 0x892de1df(2301485535), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 1
               Translation is built. 609001: Built local-host outside:192.168.100.2 ---!
     Built static translation from outside:192.168.100.2 to inside:192.168.50.2 :305009
                                                                        #(PIXfirst(config
```

هذا هو مخرج أمر **debug icmp trace**.

```
                Shows ICMP echo and echo-reply with translations !--- that take place. ---!
                                                      PIXfirst(config)#debug icmp trace

                                                                  ICMP trace on

                                                  Warning: this may cause problems on busy networks


          PIXfirst(config)# 5: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2
                                                                  ID=1024 seq=1280 length=40
             ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2 :6
     ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1280 length=40 :7
```

```
                ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2 :8
 ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=1536 length=40 :9
           ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2 :10
    ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1536 length=40 :11
           ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2 :12
ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=1792 length=40 :13
           ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2 :14
    ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1792 length=40 :15
           ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2 :16
ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=2048 length=40 :17
           ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2 :18
    ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=2048 length=40 :19
           ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2 :20


#(PIXfirst(config
```

معلومات ذات صلة

- صفحة دعم أجهزة الأمان PIX 500 Series Security Appliances
- مراجع أوامر PIX
- طلبات التعليقات (RFCs)
- صفحة دعم 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).