PIX-firewall voor inkomende hostomzetting in een Remote Network Connected via L2L IPsec Tunnel Configuration-voorbeeld

Inhoud

Inleiding

Dit document beschrijft de stappen die worden gebruikt om de bron IP van een host te vertalen die via een LAN-to-LAN IPsec-tunnel tussen twee Cisco Secure PIX-firewalls komt. Elke PIX-firewall heeft een beveiligd privénetwerk. Dit concept is ook van toepassing wanneer je subnetten vertaalt in plaats van afzonderlijke hosts.

Opmerking: gebruik deze stappen om hetzelfde scenario in PIX/ASA 7.x te configureren:

- Om een site-to-site VPN-tunnel te configureren voor PIX/ASA 7.x, raadpleeg PIX/ASA 7.x: Eenvoudig voorbeeld van PIX-to-PIX VPN-tunnelconfiguratie.
- De **statische** opdracht die voor inkomende communicatie wordt gebruikt, is gelijk voor zowel 6.x als 7.x zoals in dit document beschreven wordt.
- De opdrachten in dit document worden **weergegeven**, **duidelijk** en **debug** gebruikt en zijn vergelijkbaar in PIX 6.x en 7.x.

Voorwaarden

Vereisten

Zorg ervoor dat u de PIX-firewall met IP-adressen op de interfaces hebt ingesteld en een basisconnectiviteit hebt voordat u doorgaat met dit configuratievoorbeeld.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco PIX 506E firewall
- Cisco Secure PIX-firewall versie 6.3(3)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

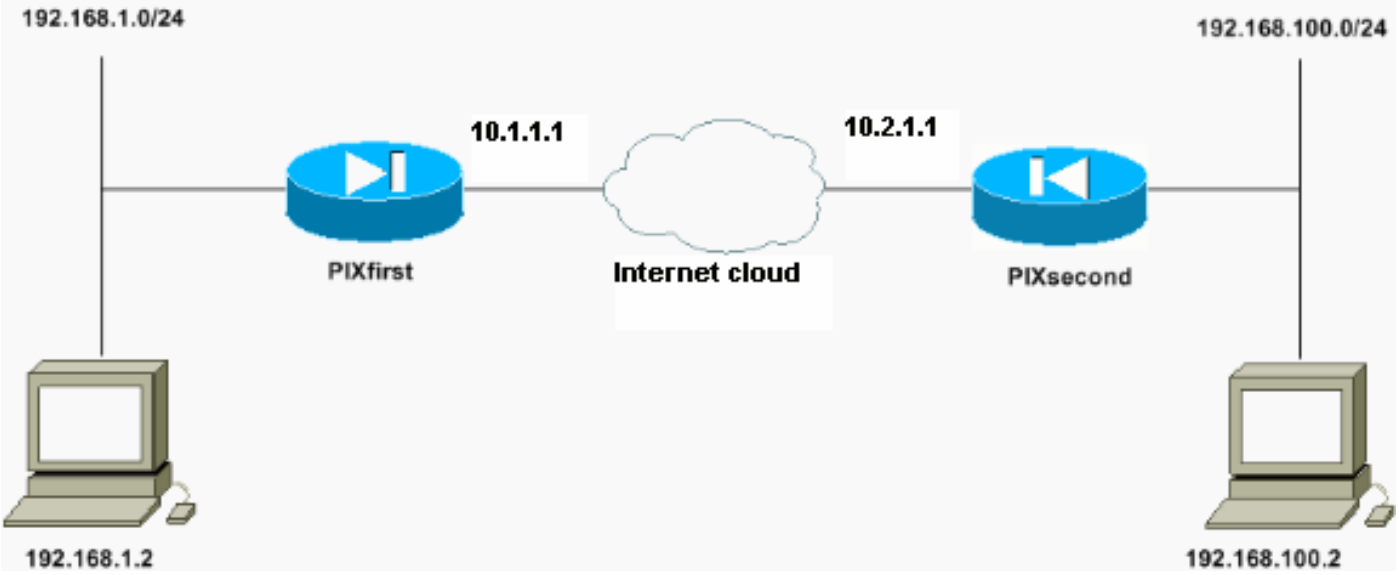
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



De host met het IP-adres van 192.168.100.2 wordt vertaald naar 192.168.50.2 in de PIX-firewall met de gastnaam PIXfirst. Deze vertaling is transparant voor de gastheer en zijn bestemming.

Opmerking: Alle ingesloten IP-adressen worden standaard niet vertaald, tenzij een vaste-up voor

deze toepassing is ingeschakeld. Een ingesloten IP-adres is een adres dat de toepassing binnen het gedeelte voor gegevenslading van een IP-pakket omvat. Network adresomzetting (NAT) wijzigt alleen de IP-header van een IP-pakket. Het wijzigt de gegevenslading van het oorspronkelijke pakket niet waarbinnen IP's door bepaalde toepassingen kunnen worden ingesloten. Hierdoor werken deze toepassingen soms niet goed.

Configuraties

Dit document gebruikt deze configuraties:

- PIXeerste configuratie
- PIXtweede configuratie

PIXeerste configuratie

```
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)#
```

PIXtweede configuratie

```
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)#
```

Als u meer dan één crypto kaartingang voor een bepaalde interface maakt, moet u het sequentienummer van elke ingang gebruiken om het te rangschikken. Hoe lager het sequentienummer, hoe hoger de prioriteit. Op de interface die de crypto map set heeft, evalueert het veiligheidsapparaat eerst het verkeer aan de hand van de hoger prioritaire kaarten.

Maak meerdere crypto plattegronden voor een bepaalde interface als een van de verschillende peers verschillende gegevensstromen verwerkt of als u verschillende IPsec security wilt toepassen op verschillende soorten verkeer (op dezelfde of afzonderlijke peers). Bijvoorbeeld, als u wilt dat het verkeer tussen één reeks subnetten echt wordt verklaard, en verkeer tussen een andere reeks subnetten zowel authentiek als gecodeerd wordt. In dit geval, definieer de verschillende types van verkeer in twee afzonderlijke toegangslijsten, en creëer een afzonderlijke crypto kaartingang voor elke crypto toegangslijst.

Security Associations (SA's) wissen

Gebruik in de bevoorrechte modus van de PIX deze opdrachten:

- **Schakel [crypto] ipsec sa**-Verwijdert de actieve IPsec SAs. Het sleutelwoord *crypto* is optioneel.

- **Schakel [crypto] isakmp sa**—Verwijdert de actieve IKE SA's. Het sleutelwoord *crypto* is optioneel.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon crypto isakmp sa**-Toont fase 1 Security Associations (SAs).
- **toon crypto ipsec sa**-shows Phase 2 SAs.
- **ping**-diagnosticeert basisnetwerkconnectiviteit. Ping van één PIX aan de andere verifieert connectiviteit tussen de twee PIX's. Een ping kan ook van de gastheer achter PIXsecond aan de gastheer achter PIXfirst worden uitgevoerd om de IPsec tunnel aan te roepen.
- **toon lokaal-host <IP_adres>**-Hiermee geeft u de vertaal- en verbindingssleuven weer voor de lokale host waarop het IP-adres is opgegeven.
- **detail tonen** - Hiermee geeft u de inhoud van de vertaalsleuven weer. Dit wordt gebruikt om te verifiëren dat de host wordt vertaald.

Controleer PIXfirst

Dit is de uitvoer van de **ping**-opdracht.

```
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
10.2.1.1 response received -- 0ms
10.2.1.1 response received -- 0ms
PIXfirst(config)#
```

Dit is de output van de **show crypto isakmp sa** opdracht.

```
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
```

Dit is de uitvoer van de **show crypto ipsec als** opdracht.

```
!--- 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:
```

Dit is de uitvoer van het **tonen lokaal-host** bevel.

```
!--- 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):
```

Dit is de uitvoer van de opdracht **detail tonen**.

```
!--- Shows translation for the host on a remote network. PIXfirst(config)#show xlate detail
1 in use, 1 most used
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)#
```

Controleer PIXseconde

Dit is de uitvoer van de **ping**-opdracht.

```
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
10.1.1.1 response received -- 0ms
10.1.1.1 response received -- 0ms
PIXsecond(config)#
```

Dit is de output van de **show crypto isakmp sa** opdracht.

```
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
```

Dit is de uitvoer van de **show crypto ipsec als** opdracht.

```
!--- 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)#
```

Problemen oplossen

Deze sectie verschaft de informatie om uw configuratie problemen op te lossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug van crypto ipsec** - informatie over IPsec gebeurtenissen.
- **debug crypto isakmp**-displays over de gebeurtenissen op de Internet Key Exchange (IKE).
- **debug van pakje if_name [src source_ip [netmask]] [dst dest_ip [netmasker] [[proto icmp] | [haven van tcp [sport src_port] [dport dest_port] | [Proto udp [sport src_port] [dport dest_port] [rx] | belastingen | zowel]** - Hiermee worden de pakketten weergegeven die op de gespecificeerde interface zijn geraakt. Deze opdracht is handig wanneer u het type verkeer op de interne interface van PIXfirst bepaalt. Deze opdracht wordt ook gebruikt om na te gaan of de voorgenomen vertaling wel bestaat.
- **loggen gebufferd niveau**—verzenden syslogberichten naar een interne buffer die wordt bekeken met de opdracht **show logging logging logging logging logging logging**. Gebruik de opdracht **heldere houtkap** om de berichtbuffer los te maken. Nieuwe berichten worden toegevoegd aan het einde van de buffer. Deze opdracht wordt gebruikt om de ingebouwde vertaling te bekijken. De vastlegging aan de buffer moet indien nodig worden ingeschakeld. Schakel de houtkap uit om de **houtkap** te bufferen zonder **houtbufferniveau** en/of **zonder houtkap**.

- **bug** van **ICMP-**overtrekken: toont ICMP-pakketinformatie (Internet Control Message Protocol), het Bron-IP-adres en het doeladres van de pakketten die in de PIX-firewall zijn aangekomen, van de PIX-firewall afwijken en verplaatsen. Dit omvat pings aan de eigen interfaces van de PIX-firewall-unit. Gebruik **geen debug icmp sporen** om het **debug-voetspoor** uit te schakelen.

Dit is de uitvoer van de **debug crypto isakmp** en **debug crypto ipsec** opdrachten.

```
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)#
```

Dit is de uitvoer van het **debug-pakket binnen de** opdracht **src**.

```
!--- 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 --

192.168.50.2 ==> 192.168.1.2

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 --

192.168.50.2 ==> 192.168.1.2

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 --

192.168.50.2 ==> 192.168.1.2


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)#
```

Dit is de output van de opdracht **houtbuffer**.

```
!--- 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

111009: User 'enable_15' executed cmd: show logging
602301: sa created, (sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0xb1274c19(2972142617), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2
```

```
602301: sa created, (sa) sa_dest= 10.2.1.1, sa_prot= 50,
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
305009: Built static translation from outside:192.168.100.2 to inside:192.168.50.2
PIXfirst(config)#
```

Dit is de uitvoer van de opdracht **Picmp-sporen debug**.

```
!--- 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
6: ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2
7: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1280 length=40
8: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2
9: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=1536 length=40
10: ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2
11: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1536 length=40
12: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2
13: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=1792 length=40
14: ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2
15: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1792 length=40
16: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2
17: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=2048 length=40
18: ICMP echo-request: translating outside:192.168.100.2 to inside:192.168.50.2
19: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=2048 length=40
20: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2


PIXfirst(config)#
```

Gerelateerde informatie

- Ondersteuning van PIX 500 Series security applicaties pagina
- PIX-opdrachtreferenties
- Verzoeken om opmerkingen (RFC's)
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems