Esempio di configurazione del firewall PIX per la conversione host in ingresso su una rete remota connessa su un tunnel IPsec L2L

Sommario

Introduzione

In questo documento viene descritta la procedura utilizzata per tradurre l'IP di origine di un host che passa attraverso un tunnel IPsec da LAN a LAN tra due Cisco Secure PIX Firewall. Ogni PIX Firewall ha una rete privata protetta dietro di esso. Questo concetto è valido anche quando si convertono subnet anziché singoli host.

Nota: per configurare lo stesso scenario in PIX/ASA 7.x, attenersi alla seguente procedura:

- Per configurare un tunnel VPN da sito a sito per PIX/ASA 7.x, fare riferimento a PIX/ASA 7.x: Esempio di configurazione semplice del tunnel VPN da PIX a PIX.
- Il comando **static** utilizzato per le comunicazioni in entrata è simile sia per 6.x che per 7.x, come descritto in questo documento.
- I comandi **show**, **clear** e **debug** usati in questo documento sono simili in PIX 6.x e 7.x.

Prerequisiti

Requisiti

Prima di procedere con questo esempio di configurazione, accertarsi di aver configurato il firewall PIX con gli indirizzi IP sulle interfacce e di avere la connettività di base.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco PIX 506E Firewall
- Software Cisco Secure PIX Firewall versione 6.3(3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

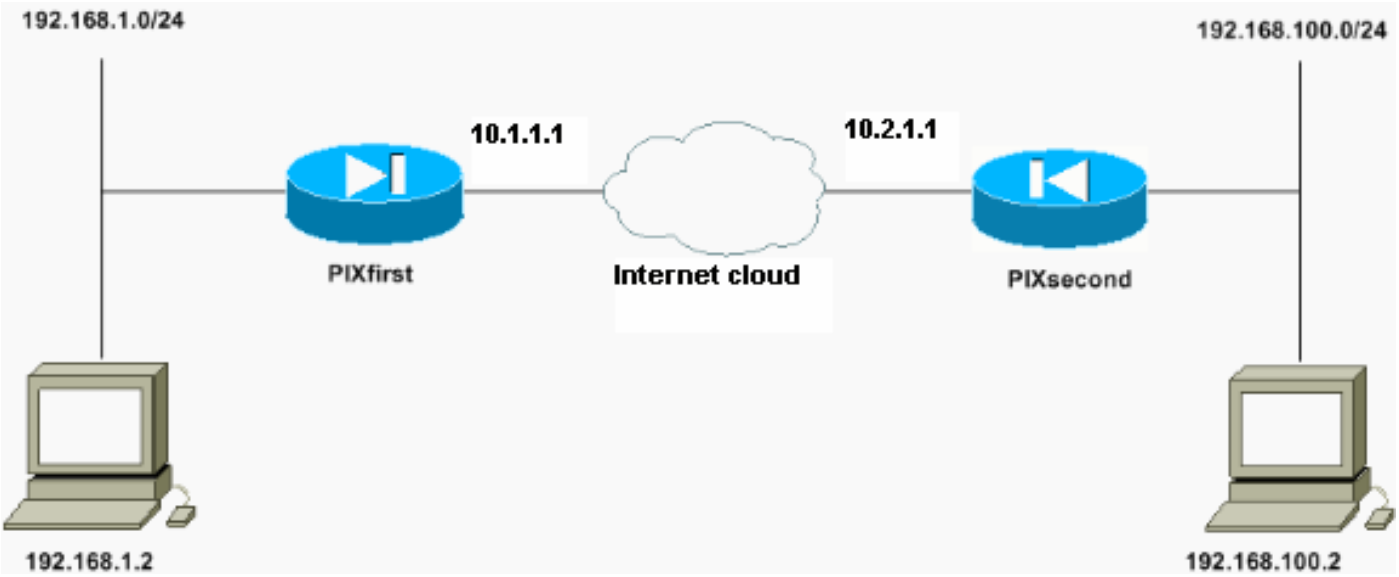
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



L'host con indirizzo IP 192.168.100.2 viene convertito in 192.168.50.2 sul PIX Firewall con il nome host PIXfirst. Questa traduzione è trasparente per l'host e la sua destinazione.

Nota: gli indirizzi IP incorporati non vengono convertiti per impostazione predefinita a meno che non sia abilitata una correzione per l'applicazione. Un indirizzo IP incorporato è un indirizzo che l'applicazione include nella parte del payload dei dati di un pacchetto IP. Network Address Translation (NAT) modifica solo l'intestazione IP esterna di un pacchetto IP. Non modifica il payload di dati del pacchetto originale nel quale gli IP possono essere incorporati da alcune applicazioni. A volte questo può causare il malfunzionamento di tali applicazioni.

Configurazioni

Nel documento vengono usate queste configurazioni:

- PIXfirst Configuration
- Configurazione PIXsecond

PIXfirst Configuration

```
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)#
```

Configurazione PIXsecond

```
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)#
```

Se si creano più voci per una determinata interfaccia, è necessario utilizzare il numero di sequenza di ciascuna voce per classificarla. Più basso è il numero di sequenza, maggiore è la priorità. Sull'interfaccia per la quale è impostata la mappa crittografica, l'appliance di sicurezza valuta prima il traffico rispetto alle voci delle mappe con priorità più alta.

Creare più voci della mappa crittografica per una determinata interfaccia se peer diversi gestiscono flussi di dati diversi o se si desidera applicare una protezione IPsec diversa a tipi di traffico diversi (allo stesso peer o a peer diversi). Ad esempio, se si desidera che il traffico tra un set di subnet venga autenticato e il traffico tra un altro set di subnet venga sia autenticato che crittografato. In questo caso, definire i diversi tipi di traffico in due elenchi degli accessi distinti e creare una voce distinta della mappa crittografica per ciascun elenco degli accessi crittografici.

Cancella associazioni di sicurezza

In modalità di privilegio di PIX, utilizzare i seguenti comandi:

- **clear [crypto] ipsec sa**: elimina le SA IPsec attive. la parola chiave *crypto* è facoltativa.
- **clear [crypto] isakmp sa**: elimina le SA IKE attive. la parola chiave *crypto* è facoltativa.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show crypto isakmp sa**: visualizza le associazioni di sicurezza (SA) della fase 1.
- **show crypto ipsec sa**: visualizza le associazioni di protezione in fase 2.
- **ping** - Esegue la diagnosi della connettività di rete di base. Il ping tra un PIX e l'altro verifica la connettività tra i due PIX. È possibile anche eseguire il ping tra l'host dietro PIXsecond e l'host dietro PIXfirst per richiamare il tunnel IPsec.
- **show local-host <indirizzo_IP>**: visualizza gli slot di conversione e connessione per l'host locale per il quale è stato specificato l'indirizzo IP.
- **show xlate detail** - Visualizza il contenuto degli slot di traslazione. Questa opzione viene utilizzata per verificare che l'host sia stato tradotto.

Verifica PIXfirst

Questo è l'output del comando **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
10.2.1.1 response received -- 0ms
10.2.1.1 response received -- 0ms
PIXfirst(config)#
```

Di seguito viene riportato l'output del comando **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
```

Questo è l'output del comando **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:
```

Questo è l'output del comando **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):
```

Questo è l'output del comando **show xlate detail**.

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

Verifica PIXsecond

Questo è l'output del comando **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
10.1.1.1 response received -- 0ms
10.1.1.1 response received -- 0ms
PIXsecond(config)#
```

Di seguito viene riportato l'output del comando **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
```

Questo è l'output del comando **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)#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec**: visualizza le informazioni sugli eventi IPsec.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi 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 | both]**: visualizza i pacchetti che hanno raggiunto l'interfaccia specificata. Questo comando è utile quando si determina il tipo di traffico sull'interfaccia interna di PIXfirst. Questo comando viene inoltre utilizzato per verificare che la traduzione venga effettivamente eseguita.
- **logging buffered level**: invia messaggi syslog a un buffer interno visualizzato con il comando **show logging**. Utilizzare il comando **clear logging** per cancellare il buffer dei messaggi. I nuovi messaggi vengono aggiunti alla fine del buffer. Questo comando viene utilizzato per visualizzare la traduzione generata. La registrazione nel buffer deve essere attivata quando necessario. Disattivare la registrazione nel buffer **senza livello di registrazione** e/o **senza effettuare l'accesso**.
- **debug icmp trace**: visualizza le informazioni sui pacchetti ICMP (Internet Control Message Protocol), l'indirizzo IP di origine e l'indirizzo di destinazione dei pacchetti che arrivano, partono e attraversano il firewall PIX. Ciò include ping alle interfacce proprie dell'unità PIX

Firewall. Non utilizzare **debug icmp trace** per disattivare **debug icmp trace**. Questo è l'output dei comandi **debug crypto isakmp** e **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)#
```

Questo è l'output del comando **debug packet inside 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)#
```

Questo è l'output del comando **log 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

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)#
```

Questo è l'output del comando **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
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)#
```

Informazioni correlate

- Pagina di supporto per le appliance di sicurezza PIX serie 500
- Riferimenti per i comandi PIX
- RFC (Requests for Comments)
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems