

Ejemplo de Configuración de Firewall PIX para Traducción de Host Entrante en una Red Remota Conectada sobre Túnel IPsec L2L

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Clear Security Associations \(SA\)](#)

[Verificación](#)

[Verificar PIXfirst](#)

[Verificar PIXsecond](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe los pasos utilizados para traducir la IP de origen de un host que llega a través de un túnel IPsec de LAN a LAN entre dos Cisco Secure PIX Firewalls. Cada firewall PIX tiene una red privada protegida detrás de ella. Este concepto también se aplica cuando se traducen subredes en lugar de hosts individuales.

Nota: Utilice estos pasos para configurar el mismo escenario en PIX/ASA 7.x:

- Para configurar un túnel VPN de sitio a sitio para PIX/ASA 7.x, consulte [PIX/ASA 7.x: Ejemplo de Configuración Simple de Túnel PIX a PIX VPN](#).
- El comando **static** utilizado para la comunicación entrante es similar para 6.x y 7.x, como se describe en este documento.
- Los comandos **show**, **clear** y **debug** utilizados en este documento son similares en PIX 6.x y 7.x.

[Prerequisites](#)

[Requirements](#)

Asegúrese de haber configurado el Firewall PIX con direcciones IP en las interfaces y de tener conectividad básica antes de continuar con este ejemplo de configuración.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

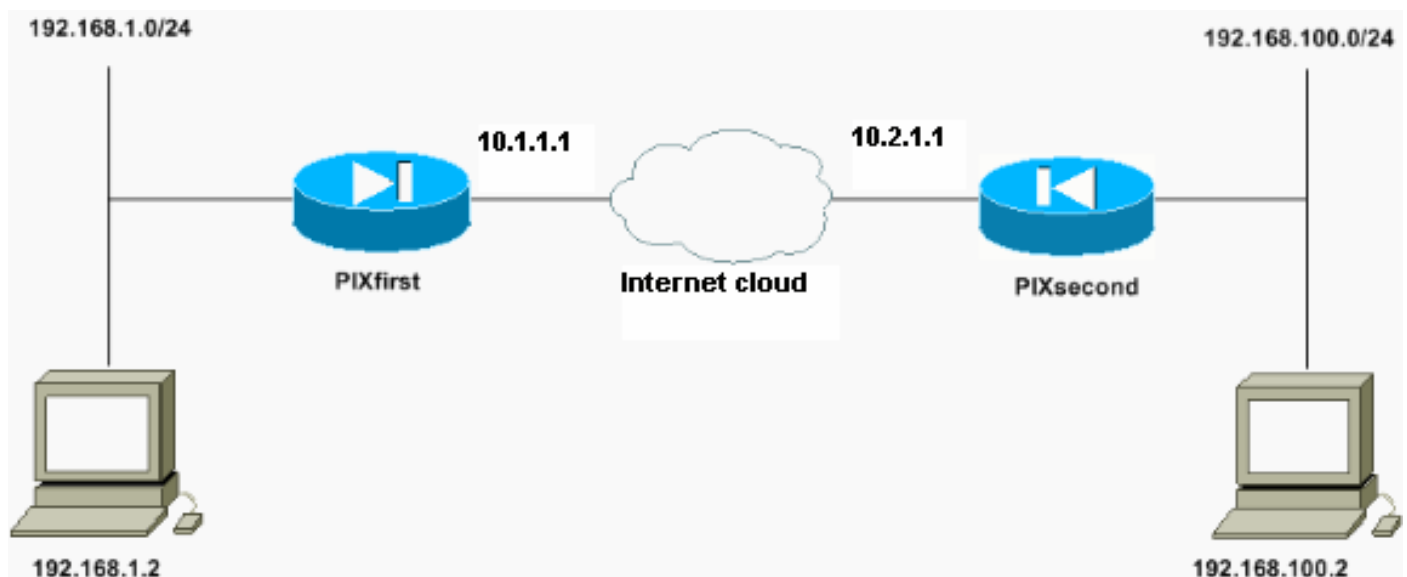
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



El host con la dirección IP de 192.168.100.2 se traduce a 192.168.50.2 en el firewall PIX con el nombre de host de PIXfirst. Esta traducción es transparente para el host y su destino.

Nota: Las direcciones IP incrustadas no se traducen de forma predeterminada a menos que se habilite un arreglo para esa aplicación. Una dirección IP incrustada es aquella que la aplicación incluye dentro de la porción de carga útil de datos de un paquete IP. La traducción de direcciones de red (NAT) sólo modifica el encabezado IP exterior de un paquete IP. No modifica la carga útil de datos del paquete original dentro del cual las IP pueden ser incrustadas por ciertas aplicaciones. Esto a veces hace que esas aplicaciones no funcionen correctamente.

Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración PIXfirst](#)
- [Configuración PIXSecond](#)

Configuración 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)#
```

Configuración 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)#

```

Si crea más de una entrada de mapa criptográfico para una interfaz dada, debe utilizar el número de secuencia de cada entrada para clasificarla. Cuanto más bajo sea el número de secuencia, mayor será la prioridad. En la interfaz que tiene el conjunto de mapa crypto, el dispositivo de seguridad evalúa primero el tráfico con respecto a las entradas de mapas de mayor prioridad.

Cree múltiples entradas de mapa crypto para una interfaz dada si diferentes pares manejan diferentes flujos de datos o si desea aplicar diferentes seguridad IPsec a diferentes tipos de tráfico (a los mismos pares o separados). Por ejemplo, si desea que el tráfico entre un conjunto de subredes se autentique y el tráfico entre otro conjunto de subredes se autentique y se cifre. En este caso, defina los diferentes tipos de tráfico en dos listas de acceso independientes y cree una entrada de mapa criptográfico independiente para cada lista de acceso criptográfico.

[Clear Security Associations \(SA\)](#)

En el modo de privilegio del PIX, utilice estos comandos:

- **clear [crypto] ipsec sa:** elimina las SAs IPsec activas. La palabra clave *crypto* es opcional.
- **clear [crypto] isakmp sa:** elimina las SA IKE activas. La palabra clave *crypto* es opcional.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto isakmp sa:** muestra las asociaciones de seguridad (SA) de la fase 1.
- **show crypto ipsec sa**—Muestra las SA de la Fase 2.
- **ping:** diagnostica conectividad de red básica. Un ping de un PIX al otro verifica la conectividad entre los dos PIX. También se puede ejecutar un ping desde el host detrás de PIXsecond al host detrás de PIXfirst para invocar el túnel IPsec.
- **show local-host <IP_address>**—Muestra las ranuras de traducción y conexión para el host local que ha especificado su dirección IP.
- **show xlate detail**—Muestra el contenido de las ranuras de traducción. Esto se utiliza para verificar que el host esté traducido.

Verificar PIXfirst

Ésta es la salida 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)#
```

Este es el resultado 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
```

Este es el resultado 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:
```

Este es el resultado 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):
```

Este es el resultado 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)#
```

Verificar PIXsecond

Ésta es la salida 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)#
```

Este es el resultado 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
```

Este es el resultado 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)#
```

Troubleshoot

Esta sección proporciona la información para resolver problemas de su configuración.

Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

- **debug crypto ipsec**—Muestra información acerca de eventos de IPSec.
- **debug crypto isakmp** — Muestra mensajes acerca de eventos de intercambio de claves por Internet (IKE).
- **debug packet if_name [src source_ip [netmask]] [dst dest_ip [netmask mask mask]] [[proto icmp] | [proto tcp [sport src_port] [dport dest_port]] | [proto udp [sport src_port] [dport dest_port]] [rx | tx | both]:** muestra los paquetes que llegaron a la interfaz especificada. Este comando es útil cuando determina el tipo de tráfico en la interfaz interna de PIX primero. Este comando también se utiliza para verificar que se produce la traducción deseada.
- **logging buffered level:** envía mensajes de syslog a un buffer interno que se ve con el comando **show logging**. Utilice el comando **clear logging** para borrar el búfer de mensajes. Los nuevos mensajes se añaden al final del búfer. Este comando se utiliza para ver la traducción que se genera. El registro en el búfer debe activarse cuando sea necesario. Desactive el registro en el búfer sin **nivel de búfer de registro** ni **sin inicio de sesión**.
- **debug icmp trace:** muestra la información del paquete del protocolo de mensajes de control de Internet (ICMP), la dirección IP de origen y la dirección de destino de los paquetes que llegan, salen y atraviesan el firewall PIX. Esto incluye pings a las propias interfaces de la unidad PIX Firewall. No utilice **debug icmp trace** para desactivar **debug icmp trace**.

Ésta es la salida de los comandos **debug crypto isakmp** y **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 0 IPSEC(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)#
```

Este es el resultado 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)#

Ésta es la salida del comando **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

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)#

Este es el resultado 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)#
```

[Información Relacionada](#)

- [Página de Soporte de PIX 500 Series Security Appliances](#)
- [Referencias de Comando PIX](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Página de Soporte de IPSec Negotiation/IKE Protocols](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)