

PIX Firewall for Inbound Host Translation on a Remote Network Connected over L2L IPsec Tunnel Configuration Example

Document ID: 51843

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Clear Security Associations (SAs)

Verify

- Verify PIXfirst
- Verify PIXsecond

Troubleshoot

- Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes the steps used to translate the source IP of a host that comes over a LAN-to-LAN IPsec tunnel between two Cisco Secure PIX Firewalls. Each PIX Firewall has a private protected network behind it. This concept also applies when you translate subnets instead of individual hosts.

Note: Use these steps in order to configure the same scenario in PIX/ASA 7.x:

- In order to configure a site-to-site VPN tunnel for PIX/ASA 7.x, refer to PIX/ASA 7.x: Simple PIX-to-PIX VPN Tunnel Configuration Example.
- The **static** command used for inbound communication is similar for both 6.x and 7.x as described in this document.
- The **show**, **clear**, and **debug** commands used in this document are similar in PIX 6.x and 7.x.

Prerequisites

Requirements

Ensure that you have configured the PIX Firewall with IP addresses on the interfaces and have basic connectivity before you proceed with this configuration example.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco PIX 506E Firewall

- Cisco Secure PIX Firewall Software Version 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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

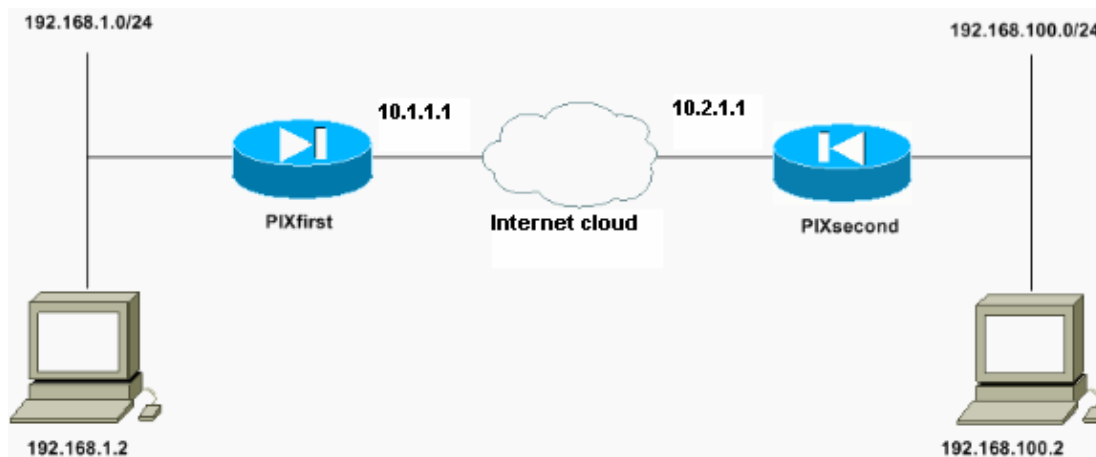
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



The host with the IP address of 192.168.100.2 is translated to 192.168.50.2 on the PIX Firewall with the host name of PIXfirst. This translation is transparent to the host and its destination.

Note: Any embedded IP addresses are not translated by default unless a fixup for that application is enabled. An embedded IP address is one that the application includes within the data payload portion of an IP packet. Network Address Translation (NAT) modifies only the outer IP header of an IP packet. It does not modify the data payload of the original packet within which IPs can be embedded by certain applications. This sometimes causes those applications not to function properly.

Configurations

This document uses these configurations:

- PIXfirst Configuration
- PIXsecond Configuration

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)#
```

PIXsecond Configuration

```
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)#

```

If you create more than one crypto map entry for a given interface, you need to use the sequence number of each entry to rank it. The lower the sequence number, the higher is the priority. At the interface that has the crypto map set, the security appliance evaluates traffic against the entries of higher priority maps first.

Create multiple crypto map entries for a given interface if either different peers handle different data flows or if you want to apply different IPsec security to different types of traffic (to the same or separate peers). For example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case, define the different types of traffic in two separate access lists, and create a separate crypto map entry for each crypto access list.

Clear Security Associations (SAs)

In the privilege mode of the PIX, use these commands:

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword *crypto* is optional.

- **clear [crypto] isakmp sa** Deletes the active IKE SAs. The keyword *crypto* is optional.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa** Shows Phase 1 Security Associations (SAs).
- **show crypto ipsec sa** Shows Phase 2 SAs.
- **ping** Diagnoses basic network connectivity. A ping from one PIX to the other verifies connectivity between the two PIXes. A ping can also be run from the host behind PIXsecond to the host behind PIXfirst to invoke the IPsec tunnel.
- **show local-host <IP_address>** Displays the translation and connection slots for the local host that has had its IP address specified.
- **show xlate detail** Displays the contents of the translation slots. This is used to verify that the host is translated.

Verify PIXfirst

This is the output of the **ping** command.

```
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)#
```

This is the output of the **show crypto isakmp sa** command.

```
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
```

This is the output of the **show crypto ipsec sa** command.

```
!--- 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:

```

This is the output of the **show local-host** command.

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

This is the output of the **show xlate detail** command.

```
!-- 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)#
```

Verify PIXsecond

This is the output of the **ping** command.

```
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)#
```

This is the output of the **show crypto isakmp sa** command.

```
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
```

This is the output of the **show crypto ipsec sa** command.

```
!-- 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

This section provides the information to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays information about IPsec events.
- **debug crypto isakmp** Displays messages about Internet Key Exchange (IKE) events.
- **debug packet if_name [src source_ip [netmask mask]] [dst dest_ip [netmask mask]] [[proto icmp] | [proto tcp [sport src_port] [dport dest_port]] | [proto udp [sport src_port] [dport dest_port]] [rx | tx | both]** Displays the packets that hit the specified interface. This command is useful when you determine the type of traffic on the inside interface of PIXfirst. This command is also used to verify that the translation intended does occur.
- **logging buffered level** Sends syslog messages to an internal buffer that is viewed with the **show logging** command. Use the **clear logging** command to clear the message buffer. New messages append to the end of the buffer. This command is used to view the translation that is built. Logging to the buffer must be turned on when required. Turn off logging to buffer with **no logging buffer level** and/or **no logging on**.
- **debug icmp trace** Shows Internet Control Message Protocol (ICMP) packet information, the source IP address, and the destination address of the packets that arrive at, depart from, and traverse the PIX Firewall. This includes pings to the PIX Firewall unit's own interfaces. Use **no debug icmp trace** to turn off **debug icmp trace**.

This is the output of the **debug crypto isakmp** and **debug crypto ipsec** commands.

```
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)#
```

This is the output of the **debug packet inside src** command.

!--- 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)#

This is the output of the **logging buffer** command.

!--- 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= 0x892deldf(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)#
```

This is the output of the **debug icmp trace** command.

*!--- 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)#
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [PIX 500 Series Security Appliances Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [IPsec Negotiation/IKE Protocols Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 23, 2007

Document ID: 51843
