入站主机转换的PIX防火墙在连接到L2L IPSec隧道的远程网络的配置示例

目录

简介

本文档介绍在两个Cisco安全PIX防火墙之间通过LAN到LAN IPsec隧道转换主机的源IP的步骤。每个PIX防火墙后面都有一个受保护的专用网络。当您转换子网而不是单个主机时，此概念也适用。

注意：请使用以下步骤在PIX/ASA 7.x中配置相同方案：

- 要为PIX/ASA 7.x配置站点到站点VPN隧道，请参阅PIX/ASA 7.x:简单的PIX间的VPN隧道配置示例.
- 用于入站通信的**static** 命令在6.x和7.x中都类似，如本文档所述。
- 本文档中**show**、**clear**和**debug**命令在PIX 6.x和7.x中类似。

先决条件

要求

在继续执行此配置示例之前，请确保已在接口上使用IP地址配置了PIX防火墙并具有基本连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科PIX 506E防火墙
- 思科安全PIX防火墙软件版本6.3(3)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

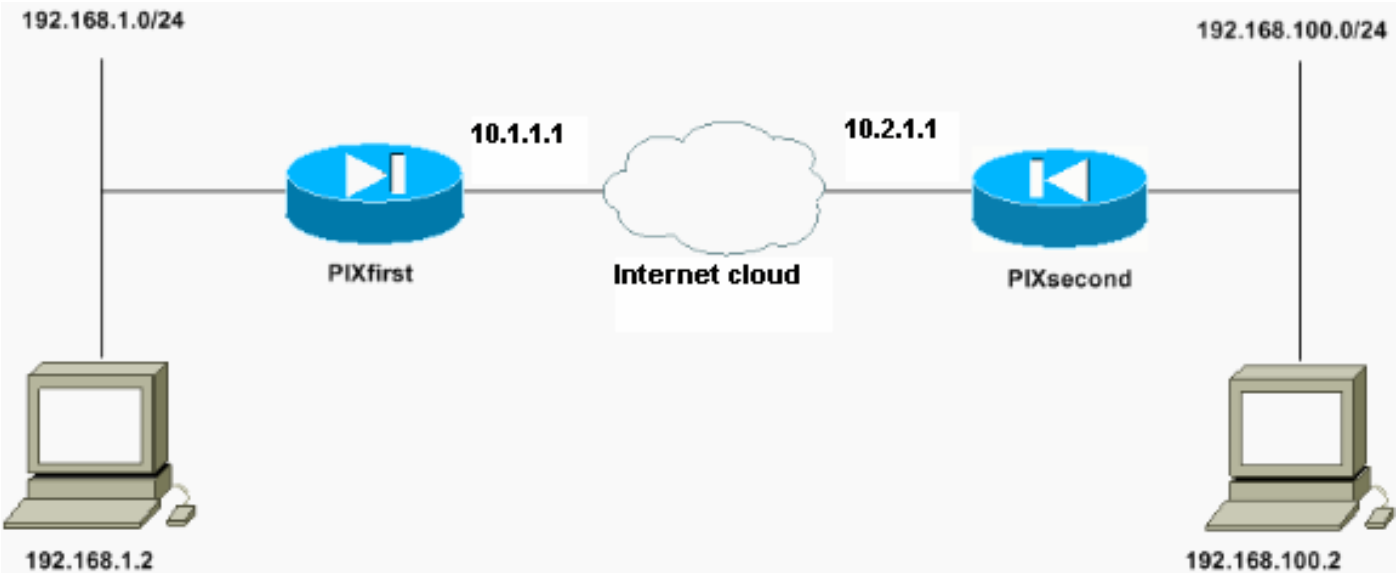
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



IP地址为192.168.100.2的主机在PIX防火墙上转换为192.168.50.2，主机名为PIXfirst。此转换对主机及其目标是透明的。

注意：默认情况下，除非为该应用程序启用修正，否则不会转换任何嵌入式IP地址。嵌入式IP地址是应用在IP数据包的数据负载部分中包括的地址。网络地址转换(NAT)仅修改IP数据包的外部IP报头。它不会修改原始数据包的数据负载，在原始数据包中，IP可由某些应用程序嵌入。这有时会导致这些应用程序无法正常运行。

配置

本文档使用以下配置：

- PIXfirst配置

- PIXsecond配置

PIXfirst配置

```
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配置

```
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)#
```

如果为给定接口创建多个加密映射条目，则需要使用每个条目的序列号对其进行排序。序列号越低，优先级越高。在设置了加密映射的接口上，安全设备首先根据优先级较高的映射条目评估流量。

如果不同的对等体处理不同的数据流，或者您想对不同类型的流量（对同一或单独的对等体）应用不同的IPsec安全，请为给定接口创建多个加密映射条目。 例如，如果希望对一组子网之间的流量进行身份验证，而对另一组子网之间的流量进行身份验证和加密。在这种情况下，在两个单独的访问列表中定义不同类型的流量，并为每个加密访问列表创建一个单独的加密映射条目。

清除安全关联 (SA)

在PIX的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa - 删除活动 IPsec SA。**关键字 **crypto 是可选的。**
- **clear [crypto] isakmp sa - 删除活动 IKE SA。**关键字 **crypto 是可选的。**

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto isakmp sa** — 显示第1阶段安全关联(SA)。
- **show crypto ipsec sa** — 显示第2阶段SA。
- **ping - 诊断基本网络连接。**从一个PIX到另一个PIX的ping检验两个PIX之间的连接。也可以从PIXsecd后的主机向PIXfirst后的主机运行ping以调用IPsec隧道。
- **show local-host <IP_address>** — 显示已指定其IP地址的本地主机的转换和连接插槽。
- **show xlate detail** — 显示转换槽的内容。这用于检验主机是否已转换。

验证PIXfirst

这是ping命令的输出。

```
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)#
```

这是show crypto isakmp sa命令的输出。

```
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
```

以下是 show crypto ipsec sa 命令的输出。

```
!--- 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:
```

这是show local-host**命令的输**出。

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

这是show xlate detail命令**的输**出。

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

验证PIXsecond

这是ping命令的输出。

```
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)#
```

这是show crypto isakmp sa命令**的输**出。

```
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
```

以下是 show crypto ipsec sa 命令的输出。

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

故障排除

此部分提供信息故障排除您的配置。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

- **debug crypto ipsec - 显示有关 IPsec 事件的信息。**
- **debug crypto isakmp — 显示有关 Internet 密钥交换 (IKE) 事件的消息。**
- **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]** — 显示命中指定接口的数据包。当您确定PIXfirst内部接口上的流量类型时，此命令非常有用。此命令还用于检验预期转换是否确实发生。
- **logging buffered level** — 将系统日志消息发送到使用show logging命令查看**的内部**缓冲区。使用**clear logging**命令清除消息缓冲区。新消息会附加到缓冲区的末尾。此命令用于查看所构建的转换。必须在需要时打开对缓冲区的日志记录。关闭日志记录到缓冲区，**而无日志记录缓**冲区级别和**/或未登录**。
- **debug icmp trace** — 显示Internet控制消息协议(ICMP)数据包信息、源IP地址和到达、离开和穿过PIX防火墙的数据包的目的地址。这包括对PIX防火墙单元自己的接口执行ping操作。使用**no debug icmp trace**关闭debug **icmp跟踪**。

这是debug crypto isakmp和debug crypto ipsec**命令的输出**结果。

```
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)#
```

这是debug packet inside src命令的输出。

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

这是logging buffer命令的输出。

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

这是debug icmp trace命令的输出。

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

相关信息

- PIX 500 系列安全设备支持页
- PIX 命令参考
- 请求注解 (RFC)
- IPsec 协商/IKE 协议支持页
- 技术支持和文档 - Cisco Systems