PIX Firewall para a Tradução de host de entrada em uma rede remota conectada sobre o exemplo de configuração do túnel de IPsec L2L

Índice

Introdução

Este documento descreve as etapas usadas para traduzir o IP da fonte de um host que venha sobre um túnel IPSec de LAN para LAN entre dois firewall PIX segura Cisco. Cada PIX Firewall tem uma rede protegida privada atrás dela. Este conceito igualmente aplica-se quando você traduz sub-redes em vez dos host individuais.

Nota: Use estas etapas a fim configurar a mesma encenação em PIX/ASA 7.x:

- A fim configurar um túnel do VPN de Site-para-Site para PIX/ASA 7.x, refira PIX/ASA 7.x: Exemplo de configuração do túnel PIX a PIX VPN simples.
- **O comando static** usado para uma comunicação de entrada é similar para 6.x e 7.x como descrito neste documento.
- **A mostra**, o **espaço livre**, e os **comandos debug** usados neste documento são similares em PIX 6.x e 7.x.

Pré-requisitos

Requisitos

Assegure-se de que você configure o PIX Firewall com endereços IP de Um ou Mais Servidores Cisco ICM NT nas relações e tenha-se a conectividade básica antes que você continue com este exemplo de configuração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firewall do Cisco PIX 506E
- Versão de software do firewall PIX segura Cisco 6.3(3)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

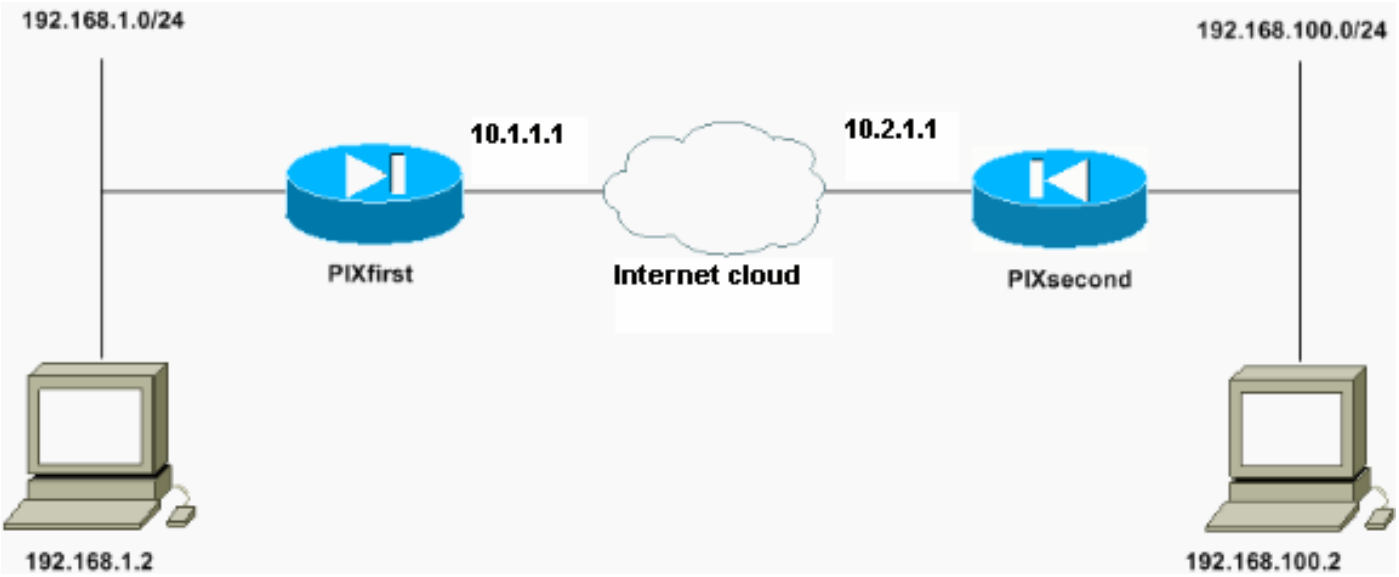
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



O host com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.100.2 é traduzido a 192.168.50.2 no PIX Firewall com o nome de host do PIXfirst. Esta tradução é transparente ao

host e a seu destino.

Nota: Nenhuns endereços IP incorporados não estão traduzidos à revelia a menos que um reparar para esse aplicativo for permitido. Um endereço IP incorporado é um que o aplicativo inclui dentro da parcela do payload de dados de um pacote IP. O Network Address Translation (NAT) altera somente o cabeçalho IP exterior de um pacote IP. Não altera o payload de dados do pacote original dentro de que o IPs pode ser encaixado por determinados aplicativos. Isto causa às vezes aqueles aplicativos não funcionar corretamente.

Configurações

Este documento utiliza as seguintes configurações:

- Primeira configuração de PIX
- Configuração secundária de PIX

Primeira configuração de PIX

```
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)#
```

Configuração secundária de PIX

```
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 você cria mais de uma entrada do crypto map para uma dada interface, você precisa de usar o número de sequência de cada entrada para classificá-lo. Mais baixo o número de sequência, mais alta é a prioridade. Na relação que tem o crypto map ajustado, a ferramenta de segurança avalia o tráfego contra as entradas de mapas da prioridade mais alta primeiramente.

Crie entradas múltiplas do crypto map para uma dada interface se ou os pares diferentes seguram fluxos de dados diferentes ou se você quer aplicar a segurança IPSec diferente aos tipos de tráfego diferentes (ao mesmos ou para separar pares). Por exemplo, se você quer um tráfego entre um grupo de sub-redes ser autenticado, e tráfego entre um outro grupo de sub-redes para ser autenticado e cifrado. Neste caso, defina os tipos de tráfego diferentes em duas Listas de acesso separadas, e crie uma entrada separada do crypto map para cada lista de acessos cripto.

Cancele as associações de segurança (os SA)

No modo do privilégio do PIX, use estes comandos:

- **clear [crypto] ipsec sa** — Suprime do IPSec ativo SA. As palavras-chave crypto são opcionais.
- **clear [crypto] isakmp sa** — Suprime do IKE ativo SA. As palavras-chave crypto são opcionais.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre isakmp cripto sa** — Associações de segurança da fase 1 das mostras (SA).
- **mostre IPsec cripto sa** — Fase 2 SA das mostras.
- **sibilo** — Diagnostica a conectividade de rede básica. Um sibilo de um PIX ao outro verifica a Conectividade entre as duas PIXes. Um sibilo pode igualmente ser executado do host atrás de PIXsecond ao host atrás do PIXfirst para invocar o túnel de IPsec.
- **mostre o <IP_address> do host local** — Indica os entalhes da tradução e da conexão para o host local que teve seu endereço IP de Um ou Mais Servidores Cisco ICM NT especificado.
- **mostre o detalhe do xlate** — Indica os índices dos slots de tradução. Isto é usado para verificar que o host está traduzido.

Verifique o PIXfirst

Esta é a saída do **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)#
```

Esta é a saída do **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
```

Esta é a saída do **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:

Esta é a saída do **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):

Esta é a saída do **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)#

Verifique PIXsecond

Esta é a saída do **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)#

Esta é a saída do **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**

Esta é a saída do **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)#
```

Troubleshooting

Esta seção fornece a informação para pesquisar defeitos sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec do debug crypto** — Indica a informação sobre eventos de IPSec.
- debug crypto isakmp — Exibe mensagens sobre eventos de Intercâmbio de chave de Internet (IKE).
- **debugar o [[proto icmp] do [dst dest_ip [netmask mask] do [src source_ip [netmask mask] do if_name do pacote]] | [dport dest_port] do [proto tcp [sport src_port]] | [dport dest_port]] do [proto udp [sport src_port] [RX | TX | ambos]** — indica os pacotes que batem a interface especificada. Este comando é útil quando você determina o tipo de tráfego na interface interna do PIXfirst. Este comando é usado igualmente verificar que a tradução pretendida ocorre.
- **nível protegido de registro** — Envia mensagens do syslog a um buffer interno que seja visto com o **comando show logging**. Use o **comando clear logging** cancelar o buffer de mensagem. As mensagens novas adicionam à extremidade do buffer. Este comando é usado ver a tradução que é construída. Registrar ao buffer deve ser girado sobre se necessário. Não gire fora o registro a proteger sem o **nível do logging buffer** e/ou a **nenhuma abertura**.
- **debugar o traço ICMP** — Mostra a informação do pacote do Internet Control Message Protocol (ICMP), o endereço IP de origem, e o endereço de destino dos pacotes em que chegue, parta de, e atravesse o PIX Firewall. Isto inclui sibilos a próprias relações da unidade do PIX Firewall. Use o **nenhum debugam o traço ICMP** para desligar **debugam o traço ICMP**.

Esta é a saída dos **comandos 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)#

Esta é a saída do **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)#

Esta é a saída do **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)#

Esta é a saída do **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)#
```

Informações Relacionadas

- Página de suporte das ferramentas de segurança da série PIX 500
- Referências de comando PIX
- Solicitações de Comentários (RFCs)
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems