Exemple de configuration d'un pare-feu PIX pour la traduction d'hôte entrante sur un réseau distant connecté sur un tunnel IPsec LAN à LAN

Contenu

Introduction

Ce document décrit les étapes utilisées pour traduire le source ip d'un hôte qui est livré plus d'un tunnel d'IPsec d'entre réseaux locaux entre deux pare-feu Cisco Secure PIX. Chaque Pare-feu PIX a un réseau protégé privé derrière lui. Ce concept s'applique également quand vous traduisez des sous-réseaux au lieu de différents hôtes.

Remarque: Employez ces étapes afin de configurer le même scénario dans PIX/ASA 7.x :

- Afin de configurer un tunnel VPN de site à site pour PIX/ASA 7.x, référez-vous à PIX/ASA 7.x : Simple PIX--PIX à l'exemple de configuration de tunnel VPN.
- La commande **statique** utilisée pour la transmission d'arrivée est semblable pour 6.x et 7.x comme décrit dans ce document.
- **L'exposition**, l'**espace libre**, et les commandes de **débogage** utilisées dans ce document sont semblables dans PIX 6.x et 7.x.

Conditions préalables

Conditions requises

Assurez-vous que vous avez configuré le Pare-feu PIX avec des adresses IP sur les interfaces et ayez la Connectivité de base avant que vous poursuiviez cet exemple de configuration.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu de Cisco PIX 506E
- Version de logiciel de pare-feu Cisco Secure PIX 6.3(3)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

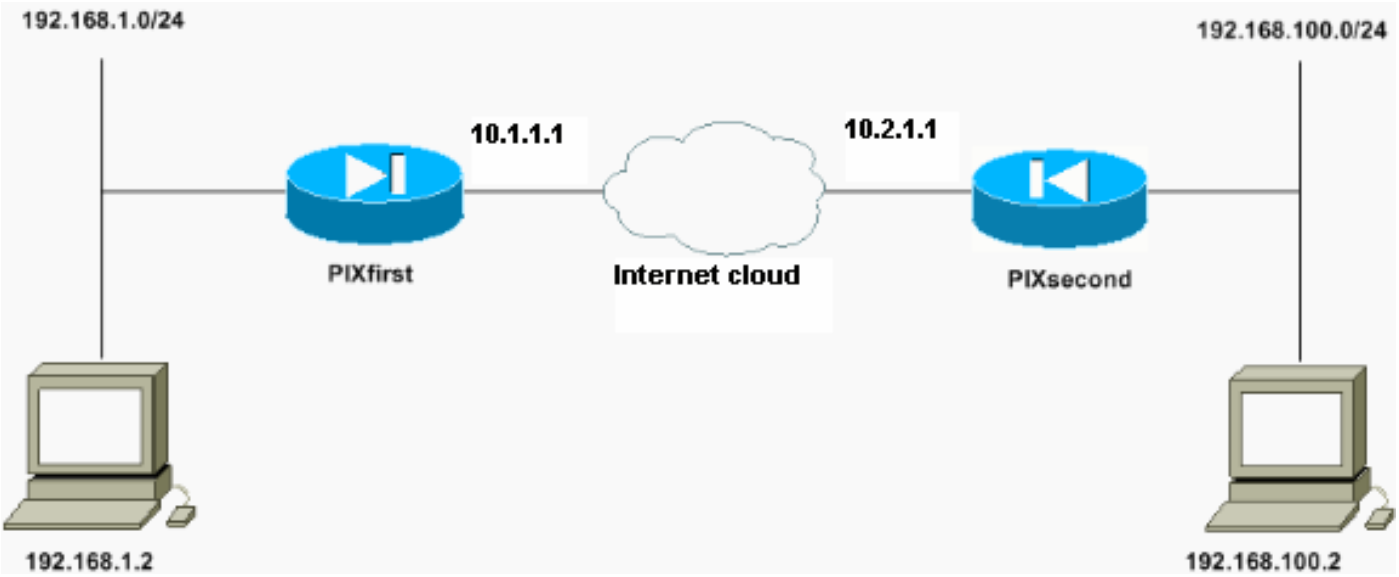
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



L'hôte avec l'adresse IP de 192.168.100.2 est traduit à 192.168.50.2 sur le Pare-feu PIX avec le nom d'hôte de PIXfirst. Cette traduction est transparente à l'hôte et à sa destination.

Remarque: Aucune adresse IP incluse n'est traduite par défaut à moins qu'un fixup pour cette application soit activé. Une adresse IP incluse est une que l'application inclut dans la partie de charge utile de données d'un paquet IP. Le Traduction d'adresses de réseau (NAT) modifie seulement l'en-tête IP externe d'un paquet IP. Il ne modifie pas la charge utile de données du paquet d'origine dans lequel l'IPS peut être inclus par certaines applications. Ceci fait parfois ne pas fonctionner ces applications correctement.

Configurations

Ce document utilise les configurations suivantes :

- Configuration de PIXfirst
- Configuration de PIXsecond

Configuration de 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)#
```

Configuration de 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 vous créez plus d'une entrée de crypto map pour une interface donnée, vous devez utiliser le numéro de séquence de chaque entrée pour le ranger. Plus le numéro de séquence est inférieur, plus est la priorité élevée. À l'interface qui a le crypto map réglé, les dispositifs de sécurité évaluent le trafic contre les entrées des cartes de haute priorité d'abord.

Créez les plusieurs entrées de crypto map pour une interface donnée si ou les différents pairs manipulent différents flux de données ou si vous voulez s'appliquer la Sécurité différente d'IPsec à différents types de trafic (à la même chose ou séparer des pairs). Par exemple, si vous voulez que le trafic entre un ensemble de sous-réseaux soit authentifié, et trafiquez entre un autre ensemble de sous-réseaux pour être authentifié et chiffré. Dans ce cas, définissez les différents types de trafic dans deux Listes d'accès distinctes, et créez une entrée distincte de crypto map pour chaque crypto liste d'accès.

Suppression des associations de sécurité (SA)

Dans le mode privilège du PIX, utilisez ces commandes :

- **clear [crypto] ipsec sa** - Supprime les SA IPSec actives. Le mot clé **crypto** est facultatif.
- **clear [crypto] isakmp sa** — supprime les SA IKE actives. Le mot clé **crypto** est facultatif.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show crypto isakmp sa** — Associations de sécurité de Phase 1 d'expositions (SAS).
- **show crypto ipsec sa** — Phase 2 SAS d'expositions.
- **ping** — Diagnostique la connexion réseau de base. Un ping d'un PIX à l'autre vérifie la Connectivité entre les deux PIXes. Un ping peut également être exécuté de l'hôte derrière PIXsecond à l'hôte derrière PIXfirst pour appeler le tunnel d'IPsec.
- **affichez le <IP_address> d'hôte local** — Affiche les emplacements de traduction et de connexion pour l'hôte local qui a eu son adresse IP spécifiée.
- **détail de show xlate** — Affiche le contenu des emplacements de traduction. Ceci est utilisé pour vérifier que l'hôte est traduit.

Vérifiez PIXfirst

C'est la sortie de la **commande 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)#
```

C'est la sortie de la commande de **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
```

Voici le résultat de la commande **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:

C'est la sortie de la commande d'**hôte local d'exposition**.

!--- 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):

C'est la sortie de la commande de **détail de show xlate**.

!--- 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)#

Vérifiez PIXsecond

C'est la sortie de la **commande 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)#

C'est la sortie de la commande de **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**

Voici le résultat de la commande **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)#
```

Dépannez

Cette section fournit les informations pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** — Affiche des informations au sujet des événements d'IPsec.
- **debug crypto isakmp** — Affiche des messages sur des événements d'Échange de clés Internet (IKE).
- **if_name de debug packet [source_ip de src [masque de netmask]] [dest_ip de dst [masque de netmask]] [[ICMP proto] | [TCP proto [src_port de sport] [dest_port de dport]] | [UDP proto [src_port de sport] [dest_port de dport]] [rx | tx | chacun des deux]** — affiche les paquets qui frappent l'interface spécifiée. Cette commande est utile quand vous déterminez le type de trafic sur l'interface interne de PIXfirst. Cette commande est également utilisée de vérifier que la traduction destinée se produit.
- **logging buffered de niveau** — Envoie des messages de Syslog à une mémoire tampon interne qui est visualisée avec la commande de **show logging**. Utilisez la commande de **clear logging** d'effacer la mémoire tampon de message. Les nouveaux messages s'ajoutent à l'extrémité de la mémoire tampon. Cette commande est utilisée de visualiser la traduction qui est établie. Se connecter à la mémoire tampon doit être activé en cas de besoin. Arrêtez se connecter à mettre en mémoire tampon sans le **niveau de tampon de journalisation** et/ou **pas logging on**.
- **mettez au point le suivi d'ICMP** — Affiche les informations de paquet de Protocole ICMP (Internet Control Message Protocol), l'adresse IP source, et l'adresse de destination des paquets aux lesquels arrivez, partez de, et traversez le Pare-feu PIX. Ceci inclut des pings interfaces de l'unité de Pare-feu PIX à propres. Utilisez l'**aucun mettent au point le suivi d'ICMP** pour arrêter **mettent au point le suivi d'ICMP**.

C'est la sortie des commandes de **debug crypto isakmp** et de **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)#

C'est la sortie du **debug packet à l'intérieur de la** commande de **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)#

C'est la sortie de la commande de **tampon de journalisation**.

!--- 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)#

C'est la sortie de la **commande trace d'ICMP de débogage**.

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

Informations connexes

- Page de support d'appareils de Sécurité de gamme 500 PIX
- Références des commandes du pare-feu PIX
- Demandes de commentaires (RFC)
- Page de support de la négociation IPSec/des protocoles IKE
- Support et documentation techniques - Cisco Systems