Contenido

Introducción

Este documento aborda y proporciona una solución al problema de por qué un túnel de IPSec establecido correctamente desde un Cisco VPN Client a un PIX no es capaz de pasar datos.

La incapacidad para pasar los datos sobre un túnel de IPSec establecido entre un cliente VPN y un PIX se encuentra con frecuencia cuando usted no puede hacer ping o Telnet de un cliente VPN a ninguna host en el LAN detrás del PIX. Es decir el cliente VPN y el PIX no pueden pasar los datos encriptados entre él. Esto ocurre porque el PIX tiene a túnel ipsec de LAN a LAN a un router y también a un cliente VPN. La incapacidad para pasar los datos es el resultado de una configuración con el mismo Access Control List (ACL) para el 0 nacional y la correspondencia de criptografía estática para el peer IPSec del LAN a LAN.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Secure PIX Firewall 6.0.1
- Cisco 1720 Router que funciona con el Software Release 12.2(6) de Cisco IOS®

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

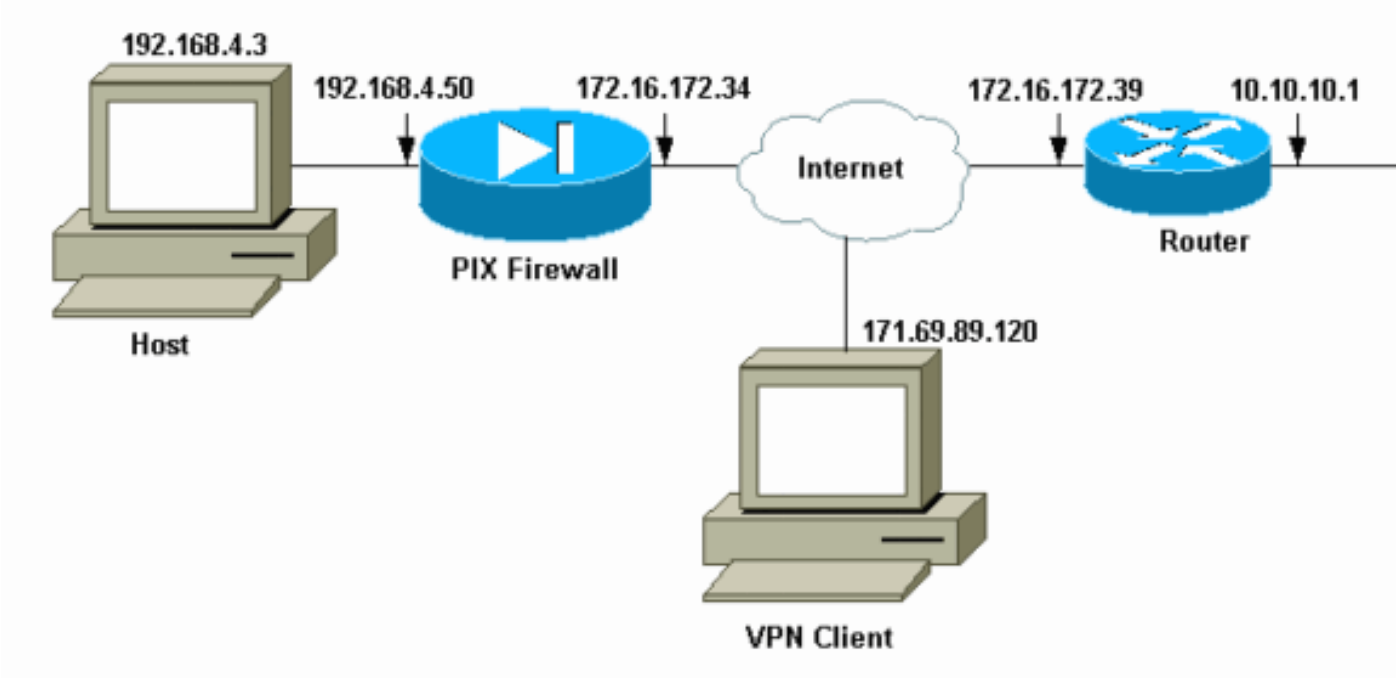
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Resuelva problemas el PIX

Diagrama de la red



Configuración de ejemplo problemático

PIX 520
pix520-1#**write terminal**Building configuration...: Saved:PIX Version 6.0(1)nameif ethernet0 outside security0nameif ethernet1 inside security100enable password 2KFQnbNIdI.2KYOU encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname pix520-1domain-name vpn.comfixup protocol ftp 21fixup protocol http 80fixup protocol h323 1720fixup protocol rsh 514fixup protocol smtp 25fixup protocol sqlnet 1521fixup protocol sip 5060fixup protocol skinny 2000names*!--- Access-List ?140? defines interesting traffic to bypass NAT for VPN !--- and defines VPN interesting traffic. This is incorrect.***access-list 140 permit ip 192.168.4.0 255.255.255.0 10.10.10.0 255.255.255.0access-list 140 permit ip 192.168.4.0 255.255.255.0 10.1.2.0 255.255.255.0**no pagerlogging onlogging console debugginglogging monitor debugginglogging buffered debugginglogging trap debugginglogging history debugginglogging host outside 192.168.2.6interface ethernet0 autointerface ethernet1 automtu outside

```
1500mtu inside 1500!--- IP addresses on the outside and
inside interfaces.ip address outside 172.16.172.34
255.255.255.240ip address inside 192.168.4.50
255.255.255.0ip audit info action alarmip audit attack
action alarmip local pool ippool 10.1.2.1-10.1.2.254no
failoverfailover timeout 0:00:00failover poll 15failover
ip address outside 0.0.0.0failover ip address inside
0.0.0.0pdm history enablearp timeout 14400global
(outside) 1 172.16.172.57 netmask 255.255.255.255!---
The nat 0 command bypasses NAT for the packets destined
over the IPsec tunnel.Nat (inside) 0 access-list 140Nat
(inside) 1 0.0.0.0 0.0.0.0 0 0route outside 0.0.0.0
0.0.0.0 172.16.172.33 1timeout xlate 3:00:00timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h3230:05:00 sip0:30:00 sip_media 0:02:00timeout uauth
0:05:00 absoluteaaa-server TACACS+ protocol tacacs+AAA-
server RADIUS protocol radiusAAA-server mytest protocol
tacacs+AAA-server nasir protocol radiussnmp-server host
outside 192.168.2.6no snmp-server locationno snmp-server
contactsnmp-server community publicsnmp-server enable
trapsfloodguard enable!--- The sysopt command bypasses
conduits or ACLs that check to be applied !--- on the
inbound VPN packets after decryption.sysopt connection
permit-ipsecno sysopt route dnat!--- The crypto ipsec
command defines IPsec encryption and authen algo.crypto
ipsec transform-set myset esp-des esp-md5-hmaccrypto
dynamic-map dynmap 10 set transform-set myset!--- The
crypto map commands define the IPsec !--- Security
Assocation (SA) (Phase II SA) parameters.crypto map
mymap 5 ipsec-isakmpcrypto map mymap 5 match address
140crypto map mymap 5 set peer 172.16.172.39crypto map
mymap 5 set transform-set mysetcrypto map mymap 10
ipsec-isakmp dynamic dynmapcrypto map mymap interface
outsideisakmp enable outside!--- The isakmp key command
defines the pre-shared key for the peer address.isakmp
key ******** address 172.16.172.39 netmask
255.255.255.255 no-xauthno-config-modeisakmp identity
address!--- The isakmp policy defines the Phase 1 SA
parameters.isakmp policy 10 authentication pre-
shareisakmp policy 10 encryption desisakmp policy 10
hash shaisakmp policy 10 group 2isakmp policy 10
lifetime 86400isakmp policy 20 authentication pre-
shareisakmp policy 20 encryption Desisakmp policy 20
hash shaisakmp policy 20 group 1isakmp policy 20
lifetime 86400vpngroup vpn3000 address-pool
ippoolvpngroup vpn3000 idle-time 1800vpngroup vpn3000
password ********telnet 192.168.4.0 255.255.255.0
insidetelnet 171.69.89.82 255.255.255.255 insidetelnet
timeout 5ssh 172.0.0.0 255.0.0.0 outsidessh 171.0.0.0
255.255.255.0 outsidessh 171.0.0.0 255.0.0.0 outsidessh
timeout 60terminal width
80Cryptochecksum:55948dc706cc700e9c10e1d24a8b125c
```

En la configuración problemática el tráfico interesante, o el tráfico que se cifrará para el túnel de LAN a LAN, es definido por ACL 140. La configuración utiliza el mismo ACL que los 0 ACL nacional.

Entienda la secuencia general de evento

Cuando un paquete del IP llega la interfaz interior del PIX, se marca el Network Address Translation (NAT). Después de eso, los ACL para las correspondencias de criptografía se

marcan.

- **Cómo se utiliza 0 nacional.**Los 0 ACL nacional definen qué no se debe incluir en el NAT. El ACL en el **comando nat 0** define a las direcciones de origen y de destino para quien las reglas NAT en el PIX se inhabilitan. Por lo tanto, un paquete del IP que tiene las direcciones de origen y de destino que hacen juego el ACL definido en el **comando nat 0** desvía todas las reglas NAT en el PIX.Para implementar los túneles de LAN a LAN entre un PIX y otro dispositivo VPN con la ayuda de las direcciones privadas, utilice el **comando nat 0** de desviar el NAT. Las reglas en el firewall PIX evitan que incluyan a las direcciones privadas en el NAT mientras que estas reglas van al LAN remoto sobre el túnel IPsec.
- **Cómo se utiliza el ACL crypto.**Después de las inspecciones del NAT, el PIX marca la fuente y el destino de cada paquete del IP que llegue su interfaz interior para hacer juego los ACL definidos en los mapas de criptografía estáticos y dinámicos. Si el PIX encuentra una coincidencia con el ACL, el PIX toma ninguno de estos medidas:Si no hay asociación de seguridad IPSec actual (SA) construida ya con el dispositivo de peer IPSec para el tráfico, el PIX inicia los IPSec Negotiations. Una vez que se construyen los SA, cifra el paquete y lo envía sobre el túnel IPsec al peer IPSec.Si hay ya IPSec SA construido con el par, el PIX cifra el paquete del IP y envía el paquete encriptado al dispositivo de peer IPSec.
- **ACL dinámico.**Una vez que un cliente VPN conecta con el PIX con la ayuda del IPSec, el PIX crea un ACL dinámico que especifique a las direcciones de origen y de destino para utilizar para definir el tráfico interesante para esto conexión IPSec.

Entienda la serie problemática de eventos en el PIX

Un error de la configuración común es utilizar el mismo ACL para 0 nacional y las correspondencias de criptografía estática. Estas secciones discuten porqué ésta lleva a un error y cómo rectificar el problema.

Además, el ACL 140 define el tráfico interesante para la correspondencia de criptografía estática para el par 172.16.172.39.

Cuando un paquete del IP viene a la interfaz interior PIX, el control NAT completa y entonces el PIX marca los ACL en las correspondencias de criptografía. El PIX comienza con la correspondencia de criptografía con el número más bajo del caso. Se marca esto es porque la correspondencia de criptografía estática en el ejemplo anterior tiene el número más bajo del caso, el ACL 140. Después, el ACL dinámico para la correspondencia cifrada dinámica se marca. En esta configuración, el ACL 140 se define para cifrar el tráfico que va de la red 192.168.4.0 /24 a las redes 10.10.10.0/24 0 y 10.1.2.0 /24. Sin embargo, para el túnel de LAN a LAN, usted quiere solamente cifrar el tráfico entre las redes 192.168.4.0 /24 y 10.10.10.0 /24. Éste es cómo el router de peer IPSec define su ACL crypto.

Entienda la serie problemática de eventos en el PIX

Cuando un cliente establece conexión IPSec al PIX, él se asigna una dirección IP de la agrupación local IP. El en este caso, el cliente se asigna 10.1.2.1. El PIX también genera un ACL dinámico, pues esta salida del **comando show crypto map** muestra:

```
Crypto Map "mymap" 20 ipsec-isakmpPeer = 171.69.89.120access-list dynacl2 permit ip host
172.16.172.34 host 10.1.2.1 (hitcnt=0)dynamic (created from dynamic map dynmap/10)Current peer:
171.69.89.120Security association lifetime: 4608000 kilobytes/28800 secondsPFS (Y/N): NTransform
```

```
sets={ myset, }Crypto Map "mymap" 30 ipsec-isakmpPeer = 171.69.89.120access-list dynacl3 permit
ip any host 10.1.2.1 (hitcnt=0)dynamic (created from dynamic map dynmap/10)Current peer:
171.69.89.120Security association lifetime: 4608000 kilobytes/28800 secondsPFS (Y/N): NTransform
sets={ myset, }pix520-1(config)#
```

El comando **show crypto map** también muestra la correspondencia de criptografía estática:

```
Crypto Map: "mymap" interfaces: { outside }Crypto Map "mymap" 5 ipsec-isakmpPeer =
172.16.172.39access-list 140 permit ip 192.168.4.0 255.255.255.0 10.10.10.0255.255.255.0
(hitcnt=45)access-list 140 permit ip 192.168.4.0 255.255.255.0 10.1.2.0 255.255.255.0
(hitcnt=84)Current peer: 172.16.172.39Security association lifetime: 4608000 kilobytes/28800
secondsPFS (Y/N): NTransform sets={ myset,}
```

Una vez que el túnel IPsec se establece entre el cliente y el PIX, el cliente inicia un ping al host 192.168.4.3. Cuando recibe el pedido de eco, el host 192.168.4.3 contesta con una respuesta de eco mientras que esta salida del **comando debug icmp trace** muestra.

```
27: Inbound ICMP echo request (len 32 id 2 seq 7680)    10.1.2.1 > 192.168.4.3> 192.168.4.328:
Outbound ICMP echo reply (Len 32 id 2 seq 7680)    192.168.4.3 >192.168.4.3 > 10.1.2.129:
Inbound ICMP echo request (Len 32 id 2 seq 7936)    10.1.2.1 > 192.168.4.3> 192.168.4.330:
Outbound ICMP echo reply (Len 32 id 2 seq 7936)    192.168.4.3 >192.168.4.3 > 10.1.2.1
```

Sin embargo, la Respuesta de eco no alcanza al cliente VPN (host 10.1.2.1), y el ping falla. Usted puede ver esto con la ayuda del **comando show crypto ipsec sa** en el PIX. Esta salida muestra que el PIX desencripta 120 paquetes que vengan del cliente VPN, pero no cifran ninguna paquetes ni envían los paquetes encriptados al cliente. Por lo tanto, el número de paquetes encapsulado es cero.

```
pix520-1(config)#show crypto ipsec sainterface: outsideCrypto map tag: mymap, local addr.
172.16.172.34local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)remote ident
(addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0)current_peer: 171.69.89.120dynamic
allocated peer ip: 10.1.2.1PERMIT, flags={}#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 !--
- No packets encrypted and sent to client.#pkts decaps: 120, #pkts decrypt: 120, #pkts verify
120 !--- 120 packets received from client.#pkts compressed: 0, #pkts decompressed: 0#pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#send errors 0, #recv errors
0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120path mtu 1500, ipsec
overhead 56, media mtu 1500current outbound spi: 33a45029inbound esp sas:spi:
0x279fc5e9(664782313)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn
id: 5, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607985/27809)IV size: 8
bytesreplay detection support: Yinbound ah sas:inbound pcp sas:outbound ESP sas:spi:
0x33a45029(866406441)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn
id: 6, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4608000/27809)IV size: 8
bytesreplay detection support: Youtbound ah sas:outbound PCP sas:local ident
(addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)remote ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0)current_peer: 172.16.172.39PERMIT, flags={origin_is_acl,}#pkts
encaps: 10, #pkts encrypt: 10, #pkts digest 10#pkts decaps: 23, #pkts decrypt: 23, #pkts verify
23#pkts compressed: 0, #pkts decompressed: 0#pkts not compressed: 0, #pkts compr. Failed: 0,
#pkts decompress failed: 0#send errors 0, #recv errors 0local crypto endpt.: 172.16.172.34,
remote crypto endpt.: 172.16.172.39path mtu 1500, ipsec overhead 56, media mtu 1500current
outbound spi: f264e92cinbound ESP sas:spi: 0x2772b869(661829737)transform: ESP-Des esp-md5-hmac
,in use settings ={Tunnel, }slot: 0, conn id: 1, crypto map: mymapsa timing: remaining key
lifetime (k/sec): (4607997/2420)IV size: 8 bytesreplay detection support: Yinbound ah
sas:inbound PCP sas:outbound ESP sas:spi: 0xf264e92c(4066699564)transform: ESP-Des esp-md5-hmac
,in use settings ={Tunnel, }slot: 0, conn id: 2, crypto map: mymapsa timing: remaining key
lifetime (k/sec): (4607999/2420)IV size: 8 bytesreplay detection support: Youtbound ah
sas:outbound PCP sas:
```

Nota: Cuando el host 192.168.4.3 contesta al pedido de eco, el paquete del IP viene a la interfaz interior del PIX.

```
pix520-1(config)#show crypto ipsec sainterface: outsideCrypto map tag: mymap, local addr.
172.16.172.34local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)remote ident
(addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0)current_peer: 171.69.89.120dynamic
allocated peer ip: 10.1.2.1PERMIT, flags={}#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 !--
```

*- No packets encrypted and sent to client.***#pkts decaps: 120, #pkts decrypt: 120, #pkts verify 120** *!--- 120 packets received from client.***#pkts compressed: 0, #pkts decompressed: 0**#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#send errors 0, #recv errors 0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120path mtu 1500, ipsec overhead 56, media mtu 1500current outbound spi: 33a45029inbound esp sas:spi: 0x279fc5e9(664782313)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 5, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607985/27809)IV size: 8 bytesreplay detection support: Yinbound ah sas:inbound pcp sas:outbound ESP sas:spi: 0x33a45029(866406441)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 6, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4608000/27809)IV size: 8 bytesreplay detection support: Youtbound ah sas:outbound PCP sas:local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)**current_peer: 172.16.172.39PERMIT, flags={origin_is_acl,}#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10#pkts decaps: 23, #pkts decrypt: 23, #pkts verify 23**#pkts compressed: 0, #pkts decompressed: 0#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#send errors 0, #recv errors 0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39path mtu 1500, ipsec overhead 56, media mtu 1500current outbound spi: f264e92cinbound ESP sas:spi: 0x2772b869(661829737)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 1, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607997/2420)IV size: 8 bytesreplay detection support: Yinbound ah sas:inbound PCP sas:outbound ESP sas:spi: 0xf264e92c(4066699564)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 2, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607999/2420)IV size: 8 bytesreplay detection support: Youtbound ah sas:outbound PCP sas:

Una vez que el paquete del IP llega la interfaz interior, el PIX marca los 0 ACL nacional 140 y los determina que las direcciones de origen y de destino del paquete del IP corresponden con el ACL. Por lo tanto, este paquete del IP desvía todas las reglas NAT en el PIX. Después, se marca el ACL de criptografía. Puesto que la correspondencia de criptografía estática tiene el número más bajo del caso, su ACL se marca primero. Puesto que este ejemplo utiliza ACL 140 para la correspondencia de criptografía estática, el PIX marca este ACL. Ahora, el paquete del IP tiene una dirección de origen de 192.168.4.3 y un destino de 10.1.2.1. Puesto que esto hace juego el ACL 140, el PIX piensa que este paquete del IP está pensado para túnel ipsec de LAN a LAN con el par 172.16.172.39 (contrario a nuestros objetivos). Por lo tanto, marca la base de datos SA para ver si hay ya un SA actual con el par 172.16.72.39 para este tráfico. Mientras que la salida del **comando show crypto ipsec sa** muestra, ningún SA existe para este tráfico. El PIX no cifra ni envía el paquete al cliente VPN. En lugar, inicia otro IPSec Negotiation con el par 172.16.172.39 mientras que esta salida muestra:

pix520-1(config)#**show crypto ipsec sa**interface: outsideCrypto map tag: mymap, local addr. 172.16.172.34local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)remote ident (addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0)current_peer: 171.69.89.120dynamic allocated peer ip: 10.1.2.1PERMIT, flags={}**#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0** *!--- No packets encrypted and sent to client.***#pkts decaps: 120, #pkts decrypt: 120, #pkts verify 120** *!--- 120 packets received from client.***#pkts compressed: 0, #pkts decompressed: 0**#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#send errors 0, #recv errors 0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120path mtu 1500, ipsec overhead 56, media mtu 1500current outbound spi: 33a45029inbound esp sas:spi: 0x279fc5e9(664782313)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 5, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607985/27809)IV size: 8 bytesreplay detection support: Yinbound ah sas:inbound pcp sas:outbound ESP sas:spi: 0x33a45029(866406441)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 6, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4608000/27809)IV size: 8 bytesreplay detection support: Youtbound ah sas:outbound PCP sas:local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)**current_peer: 172.16.172.39PERMIT, flags={origin_is_acl,}#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10#pkts decaps: 23, #pkts decrypt: 23, #pkts verify 23**#pkts compressed: 0, #pkts decompressed: 0#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#send errors 0, #recv errors 0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39path mtu 1500, ipsec overhead 56, media mtu 1500current outbound spi: f264e92cinbound ESP sas:spi: 0x2772b869(661829737)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn id: 1, crypto map: mymapsa timing: remaining key

```
lifetime (k/sec): (4607997/2420)IV size: 8 bytesreplay detection support: Yinbound ah
sas:inbound PCP sas:outbound ESP sas:spi: 0xf264e92c(4066699564)transform: ESP-Des esp-md5-hmac
,in use settings ={Tunnel, }slot: 0, conn id: 2, crypto map: mymapsa timing: remaining key
lifetime (k/sec): (4607999/2420)IV size: 8 bytesreplay detection support: Youtbound ah
sas:outbound PCP sas:
```

El IPSec Negotiation falla por estas razones:

- El par 172.16.172.39 define solamente las redes 10.10.10.0/24 y 192.168.4.0/24 como el tráfico interesante en su ACL para el par 172.16.172.34 de la correspondencia de criptografía.
- Las identidades de representación no hacen juego durante el IPSec Negotiation entre los dos pares.
- Si el par inicia la negociación y la configuración local especifica el Confidencialidad directa perfecta (PFS), el par debe realizar un intercambio PFS o la negociación falla. Si la configuración local no especifica a un grupo, un valor por defecto del group1 se asume, y una oferta del group1 o del group2 se valida. Si la configuración local especifica el group2, ese grupo debe ser parte de la oferta del par o la negociación falla. Si la configuración local no especifica el PFS, valida cualquier oferta del PFS del par. El grupo del módulo de la prima 1024-bit Diffie Hellman, group2, proporciona más Seguridad que el group1, pero requiere más tiempo de procesamiento que el group1.**Nota: El comando crypto map set pfs** fija el IPSec para pedir el PFS cuando pide los nuevos SA para esta entrada de correspondencia de criptografía. Utilice el **comando no crypto map set pfs** de especificar que la petición PFS del IPSec no. Este comando está solamente disponible para las entradas de correspondencia de criptografía IPSec-ISAKMP y las entradas de la correspondencia cifrada dinámica. De forma predeterminada, PFS no se solicita. Con el PFS, cada vez que se negocia un nuevo SA, un nuevo intercambio Diffie-Hellman ocurre. Esto requiere el tiempo de procesamiento adicional. El PFS agrega otro nivel de seguridad porque si una clave es quebrada nunca por un atacante, sólo los datos enviados con esa clave se comprometen. Durante la negociación, este comando hace el IPSec pedir el PFS cuando pide los nuevos SA para la entrada de correspondencia de criptografía. Se envía el valor por defecto (group1) si la declaración de los **pfs del conjunto** no especifica a un grupo.**Nota:** Las negociaciones IKE con un peer remoto pueden colgar cuando un firewall PIX tiene túneles numerosos que originen del firewall PIX y terminen en un solo peer remoto. Este problema ocurre cuando el PFS no se habilita, y el peer local pide muchos simultáneos reintroduce las peticiones. Si ocurre este problema, IKE SA no se recupera hasta que mida el tiempo hacia fuera o hasta usted manualmente claro él con el **comando clear [crypto] isakmp sa**. Las unidades del firewall PIX configuradas con muchos túneles a muchos pares o a muchos clientes que compartan el mismo túnel no son afectadas por este problema. Si su configuración es afectada, habilite el PFS con el **comando crypto map mapname seqnum set pfs**.

Los paquetes del IP en el PIX se caen en última instancia.

Entienda la solución

El método correcto para rectificar este error es definir dos ACL separados para 0 nacional y las correspondencias de criptografía estática. Para hacer esto, el ejemplo define ACL 190 para el **comando nat 0** y utiliza el ACL modificado 140 para la correspondencia de criptografía estática, pues esta salida muestra.

PIX 520-1
`pix520-1(config)#pix520-1(config)#`**`write terminal`**`Building`

```
configuration...: Saved:PIX Version 6.0(1)nameif
ethernet0 outside security0nameif ethernet1 inside
security100enable password 2KFQnbNIdI.2KYOU
encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname
pix520-1domain-name vpn.comfixup protocol ftp 21fixup
protocol http 80fixup protocol h323 1720fixup protocol
rsh 514fixup protocol smtp 25fixup protocol sqlnet
1521fixup protocol sip 5060fixup protocol skinny
2000names!--- Access list 140 defines interesting
traffic in order to bypass NAT for VPN.access-list 140
permit ip 192.168.4.0 255.255.255.0
10.10.10.0255.255.255.0!--- Defines VPN interesting
traffic.access-list 190 permit ip 192.168.4.0
255.255.255.0 10.10.10.0255.255.255.0access-list 190
permit ip 192.168.4.0 255.255.255.0 10.1.2.0
255.255.255.0no pagerlogging onlogging console
debugginglogging monitor debugginglogging buffered
debugginglogging trap debugginglogging history
debugginglogging host outside 192.168.2.6interface
ethernet0 autointerface ethernet1 automtu outside
1500mtu inside 1500ip address outside 172.16.172.34
255.255.255.240ip address inside 192.168.4.50
255.255.255.0ip audit info action alarmip audit attack
action alarmip local pool ippool 10.1.2.1-10.1.2.254no
failoverfailover timeout 0:00:00failover poll 15failover
ip address outside 0.0.0.0failover ip address inside
0.0.0.0pdm history enablearp timeout 14400global
(outside) 1 172.16.172.57 netmask 255.255.255.255!---
The nat 0 command bypasses NAT for the packets destined
over the IPsec tunnel..Nat (inside) 0 access-list 190Nat
(inside) 1 0.0.0.0 0.0.0.0 0 0route outside 0.0.0.0
0.0.0.0 172.16.172.33 1timeout xlate 3:00:00timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h3230:05:00 sip 0:30:00 sip_media 0:02:00timeout uauth
0:05:00 absoluteAAA-server TACACS+ protocol tacacs+AAA-
server RADIUS protocol radiusAAA-server mytest protocol
tacacs+AAA-server nasir protocol radiussnmp-server host
outside 192.168.2.6no snmp-server locationno snmp-server
contactsnmp-server community publicsnmp-server enable
trapsfloodguard enablesysopt connection permit-ipsecno
sysopt route dnatcrypto ipsec transform-set myset ESP-
Des esp-md5-hmaccrypto dynamic-map dynmap 10 set
transform-set myset!--- The crypto map commands define
the IPsec SA (Phase II SA) parameters.crypto map mymap 5
ipsec-isakmpcrypto map mymap 5 match address 140crypto
map mymap 5 set peer 172.16.172.39crypto map mymap 5 set
transform-set mysetcrypto map mymap 10 ipsec-isakmp
dynamic dynmapcrypto map mymap interface outsideisakmp
enable outsideisakmp key ******** address 172.16.172.39
netmask 255.255.255.255 no-xauthno-config-modeisakmp
identity addressisakmp policy 10 authentication pre-
shareisakmp policy 10 encryption Desisakmp policy 10
hash shaisakmp policy 10 group 2isakmp policy 10
lifetime 86400isakmp policy 20 authentication pre-
shareisakmp policy 20 encryption Desisakmp policy 20
hash shaisakmp policy 20 group 1isakmp policy 20
lifetime 86400vpngroup vpn3000 address-pool
ippoolvpngroup vpn3000 idle-time 1800vpngroup vpn3000
password ********telnet 192.168.4.0 255.255.255.0
insidetelnet 171.69.89.82 255.255.255.255 insidetelnet
timeout 5ssh 172.0.0.0 255.0.0.0 outsidessh 171.0.0.0
255.255.255.0 outsidessh 171.0.0.0 255.0.0.0 outsidessh
timeout 60terminal width
```

```
80Cryptochecksum:e2cb98b30d3899597b3af484fae4f9ae:
end[OK]pix520-1(config)# pix520-1(config)#show crypto
map
```

Después de que se realicen los cambios y el cliente establece un túnel IPsec con el PIX, publique el comando show crypto map. Este comando muestra que para la correspondencia de criptografía estática, el tráfico interesante definido por el ACL 140 es solamente 192.168.4.0/24 y 10.10.10.0/24, que era el objetivo original. Además, la lista de acceso dinámica muestra el tráfico interesante definido como el cliente (10.1.2.1) y el PIX (172.16.172.34).

```
pix520-1(config)#show crypto mapCrypto Map: "mymap" interfaces: { outside }Crypto Map "mymap" 5
ipsec-isakmpPeer = 172.16.172.39access-list 140 permit ip 192.168.4.0 255.255.255.0
10.10.10.0255.255.255.0    (hitcnt=57)Current peer: 172.16.172.39Security association lifetime:
4608000 kilobytes/28800 secondsPFS (Y/N): NTransform sets={ myset, }Crypto Map "mymap" 10 ipsec-
isakmpDynamic map template tag: dynmapCrypto Map "mymap" 20 ipsec-isakmpPeer =
171.69.89.120access-list dynacl4 permit ip host 172.16.172.34 host 10.1.2.1 (hitcnt=0)dynamic
(created from dynamic map dynmap/10)Current peer: 171.69.89.120Security association lifetime:
4608000 kilobytes/28800 secondsPFS (Y/N): NTransform sets={ myset, }Crypto Map "mymap" 30 ipsec-
isakmpPeer = 171.69.89.120access-list dynacl5 permit ip any host 10.1.2.1 (hitcnt=13)dynamic
(created from dynamic map dynmap/10)Current peer: 171.69.89.120Security association lifetime:
4608000 kilobytes/28800 secondsPFS (Y/N): NTransform sets={ myset, }
```

Cuando el cliente VPN 10.1.2.1 envía un ping para recibir 192.168.4.3, la Respuesta de eco viene a la interfaz interior del PIX. El PIX marca los 0 ACL nacional 190 y los determina que el paquete del IP corresponde con el ACL. Por lo tanto, el paquete desvía las reglas NAT en el PIX. Después, el PIX marca la correspondencia de criptografía estática ACL 140 para encontrar una coincidencia. Esta época, la fuente y el destino del paquete del IP no hace juego el ACL 140. Por lo tanto, el PIX marca el ACL dinámico y encuentra una coincidencia. El PIX entonces marca su base de datos SA para ver independientemente de si IPSec SA está establecido ya con el cliente. Puesto que el cliente ha establecido ya conexión IPSec con el PIX, IPSec SA existe. El PIX después cifra los paquetes y los envía al cliente VPN. Utilice la salida del comando show crypto ipsec sa del PIX para ver que los paquetes están cifrados y desencriptados. En este caso, el PIX cifró dieciséis paquetes y los envió al cliente. El PIX también recibió los paquetes encriptados del cliente VPN y desencriptó dieciséis paquetes.

```
pix520-1(config)#show crypto ipsec sainterface: outsideCrypto map tag: mymap, local addr.
172.16.172.34local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)remote ident
(addr/mask/prot/port): (10.1.2.1/255.255.255.255/0/0)current_peer: 171.69.89.120dynamic
allocated peer ip: 10.1.2.1PERMIT, flags={}#pkts encaps: 16, #pkts encrypt: 16,#pkts digest
16#pkts decaps: 16, #pkts decrypt: 16, #pkts verify 16#pkts compressed: 0, #pkts decompressed:
0#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#send errors 0,
#recv errors 0local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120path mtu
1500, ipsec overhead 56, media mtu 1500current outbound spi: 613d083dinbound ESP sas:spi:
0x6adf97df(1793038303)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn
id: 4, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607998/27420)IV size: 8
bytesreplay detection support: Yinbound ah sas:inbound PCP sas:outbound ESP sas:spi:
0x613d083d(1631389757)transform: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }slot: 0, conn
id: 3, crypto map: mymapsa timing: remaining key lifetime (k/sec): (4607999/27420)IV size: 8
bytesreplay detection support: Youtbound ah sas:outbound PCP sas:local ident
(addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)remote ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0)current_peer: 172.16.172.39PERMIT, flags={origin_is_acl,}#pkts
encaps: 9, #pkts encrypt: 9, #pkts digest 9#pkts decaps: 9, #pkts decrypt: 9, #pkts verify
9#pkts compressed: 0, #pkts decompressed: 0#pkts not compressed: 0, #pkts compr. Failed: 0,
#pkts decompress failed: 0#send errors 1, #recv errors 0local crypto endpt.: 172.16.172.34,
remote crypto endpt.: 172.16.172.39path mtu 1500, ipsec overhead 56, media mtu 1500current
outbound spi: 58009c01inbound ESP sas:spi: 0x2d408709(759203593)transform: ESP-Des esp-md5-hmac
,in use settings ={Tunnel, }slot: 0, conn id: 2, crypto map: mymapsa timing: remaining key
lifetime (k/sec): (4607998/3319)IV size: 8 bytesreplay detection support: Yinbound ah
sas:inbound PCP sas: outbound ESP sas:spi: 0x58009c01(1476434945)transform: ESP-Des esp-md5-hmac
,in use settings ={Tunnel, }slot: 0, conn id: 1, crypto map: mymapsa timing: remaining key
```

lifetime (k/sec): (4607999/3319)IV size: 8 bytesreplay detection support: Youtbound ah sas:outbound PCP sas:pix520-1(config)# sh cr isa saTotal : 2Embryonic : 0dst src state pending created172.16.172.39 172.16.172.34 QM_IDLE 0 1172.16.172.34 171.69.89.120 QM_IDLE 0 2pix520-1(config)# sh cr ipsec sa

Configuración del router y salida del comando show

Cisco 1720-1

1720-1#**show run**Building configuration...Current configuration : 1592 bytes!! Last configuration change at 21:08:49 PST Mon Jan 7 2002! NVRAM config last updated at 18:18:17 PST Mon Jan 7 2002!version 12.2no parser cacheservice timestamps debug uptimeservice timestamps log uptimeno service password-encryption!hostname 1720-1!no logging bufferedenable secret 5 $1$6jAs$tNxI1a/2DYFAtPLyCDXjo/enable password ww!username cisco password 0 ciscomemory-size iomem 15clock timezone PST -8ip subnet-zerono ip domain-lookupip domain-name cisco.com!ip ssh time-out 120ip ssh authentication-retries 3!!*!--- The* **crypto isakmp policy** command defines the Phase 1 SA parameters.crypto isakmp policy 15authentication pre-sharecrypto isakmp key cisco123 address 172.16.172.34!!*!--- The* **crypto ipsec transform-set** command defines IPsec encryption !--- and authentication algorithims.crypto ipsec transform-set myset ESP-Des esp-md5-hmac!!*!--- The* **crypto map** command defines the IPsec SA (Phase II SA) parameters..crypto map vpn 10 ipsec-isakmpset peer 172.16.172.34set transform-set myset**match address 150**!!!!!interface FastEthernet0ip address 172.16.172.39 255.255.255.240speed auto*!--- The crypto map applied to the outbound interface.***crypto map vpn**interface Ethernet0ip address 10.10.10.1 255.255.255.240speed autono ip route-cacheno ip mroute-cache!!ip classlessip route 0.0.0.0 0.0.0.0 172.16.172.33no ip http serverip pim bidir-enable!*!--- Access-list defines interesting VPN traffic.***access-list 150 permit ip 10.10.10.0 0.0.0.255 192.168.4.0 0.0.0.255**!line con 0line aux 0line vty 0 4exec-timeout 0 0password ciscono loginline vty 5 15login!no scheduler allocateend1720-1#

1720-1#**show crypto isa sa**DST src state conn-id slot172.16.172.39 172.16.172.34 **QM_IDLE** 132 01720-1#**show crypto ipsec sa**interface: FastEthernet0Crypto map tag: vpn, local addr. 172.16.172.39**local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)current_peer: 172.16.172.34**PERMIT, flags={origin_is_acl,}#pkts encaps: 9 #pkts encrypt: 9 #pkts digest 9#pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9#pkts compressed: 0, #pkts decompressed: 0#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0#send errors 7, #recv errors 0**local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.34path mtu 1500, media mtu 1500current outbound spi: 2D408709inbound ESP sas:**spi: 0x58009C01(1476434945)**transform**: ESP-Des esp-md5-hmac ,in use settings ={**Tunnel**, }*!--- IPsec SA 200 as seen in the* **show crypto engine connection active** command.slot: 0, **conn id: 200**, flow_id: 1, crypto map: vpn**sa timing**: remaining key lifetime (k/sec): (4607998/**3144**)IV size: 8 bytesreplay detection support: Yinbound ah sas:inbound PCP sas:outbound ESP sas:spi: 0x2D408709(759203593)**transform**: ESP-Des esp-md5-hmac ,in use settings ={Tunnel, }*!--- IPsec SA 201 as seen in the* **show crypto engine connection active** command.slot: 0, **conn id: 201**, flow_id: 2, crypto map: vpn**sa timing**: remaining key lifetime (k/sec): (4607998/**3144**)IV size: 8 bytesreplay detection support: Youtbound ah sas:outbound PCP sas:1720-1#1720-1#show crypto mapInterfaces using crypto map mymap:Crypto Map "**vpn**" 10 ipsec-isakmpPeer = 172.16.172.34Extended IP access list 150access-list 150 permit ip 10.10.10.0 0.0.0.255 192.168.4.0 0.0.0.255Current peer: 172.16.172.34Security association lifetime: 4608000 kilobytes/3600 secondsPFS (Y/N): NTransform sets={ **myset**, }Interfaces using crypto map **vpn**: **FastEthernet0**

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems