설정된 IPSec 터널에서 데이터 트래픽을 전달하기 위한 PIX 트러블슈팅

목차

소개

이 문서는 Cisco VPN 클라이언트에서 PIX로 성공적으로 설정된 IPsec 터널이 데이터를 전달할 수 없는 이유에 대한 해결책을 제공하고 있습니다.

VPN 클라이언트에서 PIX 뒤의 LAN에 있는 호스트로 ping 또는 텔넷을 할 수 없는 경우 VPN 클라이언트와 PIX 간에 설정된 IPsec 터널에서 데이터를 전달할 수 없는 경우가 자주 발생합니다. 즉, VPN 클라이언트와 PIX는 암호화된 데이터를 서로 전달할 수 없습니다. 이는 PIX에 라우터와 VPN 클라이언트에 대한 LAN-to-LAN IPsec 터널이 있기 때문입니다. 데이터를 전달할 수 없는 것은 nat 0 및 LAN-to-LAN IPsec 피어에 대한 고정 암호화 맵이 모두 동일한 ACL(Access Control List)을 사용하는 컨피그레이션의 결과입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure PIX Firewall 6.0.1
- Cisco IOS® 소프트웨어 릴리스 12.2(6)를 실행하는 Cisco 1720 Router

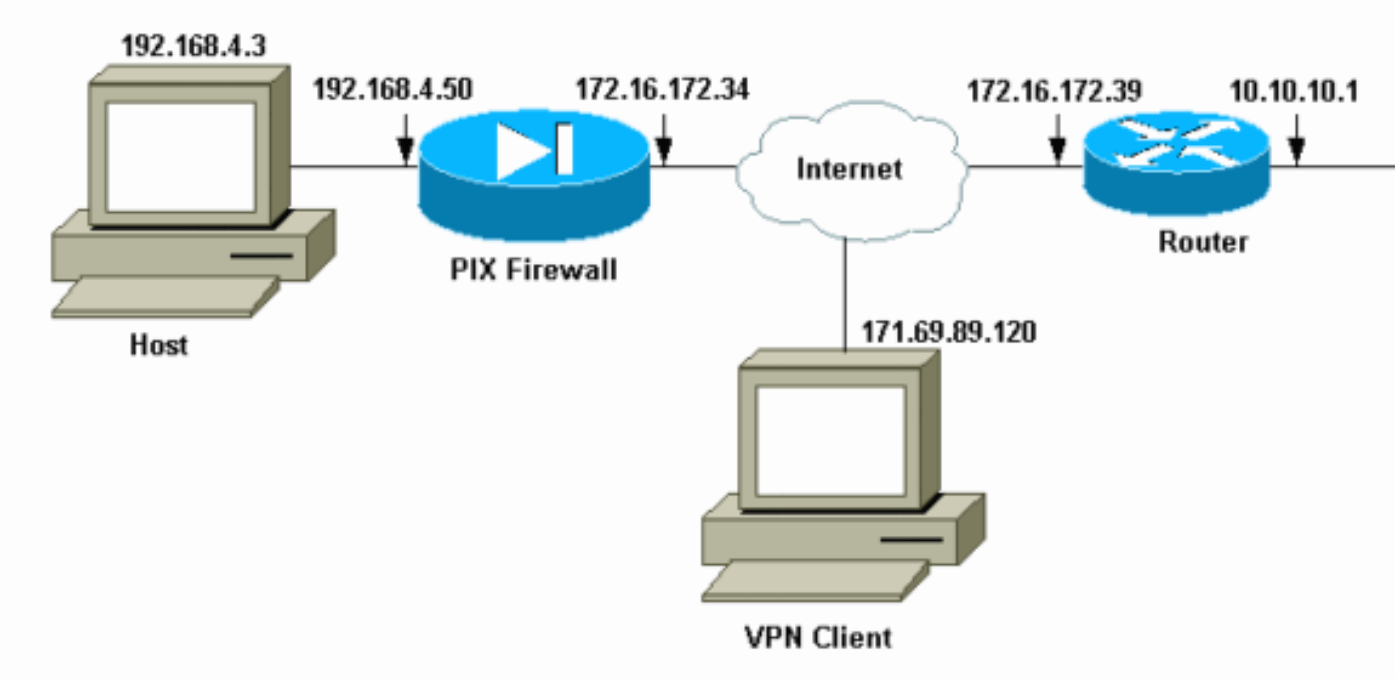
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

PIX 문제 해결

네트워크 다이어그램



문제가 있는 샘플 컨피그레이션

PIX 520

```
pix520-1#write terminal
Building configuration...
: Saved
:
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix520-1
domain-name vpn.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
```

```
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- 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 10.10.10.0 255.255.255.0
access-list 140 permit ip 192.168.4.0 255.255.255.0
10.1.2.0 255.255.255.0
no pager
logging on
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
logging history debugging
logging host outside 192.168.2.6
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
!--- IP addresses on the outside and inside interfaces.
ip address outside 172.16.172.34 255.255.255.240
ip address inside 192.168.4.50 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
global (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 140
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.172.33 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
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 mytest protocol tacacs+
AAA-server nasir protocol radius
snmp-server host outside 192.168.2.6
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
!--- The sysopt command bypasses conduits or ACLs that
check to be applied !--- on the inbound VPN packets
after decryption.

sysopt connection permit-ipsec
no sysopt route dnat
```

```
!--- The crypto ipsec command defines IPsec encryption
and authen algo.

crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto 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-isakmp
crypto map mymap 5 match address 140
crypto map mymap 5 set peer 172.16.172.39
crypto map mymap 5 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp 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-xauth
no-config-mode
isakmp identity address
!--- The isakmp policy defines the Phase 1 SA
parameters.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption Des
isakmp policy 20 hash sha
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
vpngroup vpn3000 address-pool ippool
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet 192.168.4.0 255.255.255.0 inside
telnet 171.69.89.82 255.255.255.255 inside
telnet timeout 5
ssh 172.0.0.0 255.0.0.0 outside
ssh 171.0.0.0 255.255.255.0 outside
ssh 171.0.0.0 255.0.0.0 outside
ssh timeout 60
terminal width 80
Cryptochecksum:55948dc706cc700e9c10e1d24a8b125c
```

문제가 있는 컨피그레이션에서 흥미로운 트래픽 또는 LAN-to-LAN 터널을 위해 암호화할 트래픽은 ACL 140에 의해 정의됩니다. 컨피그레이션에서는 nat 0 ACL과 동일한 ACL을 사용합니다.

이벤트의 일반적인 순서 이해

IP 패킷이 PIX의 내부 인터페이스에 도착하면 NAT(Network Address Translation)가 선택됩니다. 그런 다음 암호화 맵의 ACL을 확인합니다.

- **nat 0의 사용 방법.**nat 0 ACL은 NAT에 포함해서는 안 되는 항목을 정의합니다. nat 0 명령의 ACL은 PIX의 NAT 규칙이 비활성화된 소스 및 대상 주소를 정의합니다. 따라서 nat 0 명령에 정의된 ACL과 일치하는 소스 및 목적지 주소가 있는 IP 패킷은 PIX의 모든 NAT 규칙을 건너뜁니다.사설 주소의 도움말과 함께 PIX와 다른 VPN 디바이스 간에 LAN-to-LAN 터널을 구현하려면

nat 0 명령을 사용하여 NAT를 우회합니다. PIX 방화벽의 규칙은 IPsec 터널을 통해 원격 LAN으로 이동하는 동안 사설 주소가 NAT에 포함되지 않도록 합니다.

- **암호화 ACL의 사용 방법.**NAT 검사 후 PIX는 내부 인터페이스에 도착하는 각 IP 패킷의 소스 및 대상을 고정 및 동적 암호화 맵에 정의된 ACL과 일치하는지 확인합니다. PIX가 ACL과 일치하는 항목을 찾으면 PIX는 다음 단계를 수행합니다.트래픽에 대해 피어 IPsec 디바이스로 이미 구축된 현재 IPsec SA(Security Association)가 없는 경우 PIX는 IPsec 협상을 시작합니다. SA가 구축되면 패킷을 암호화하고 IPsec 터널을 통해 IPsec 피어로 전송합니다.피어로 작성된 IPsec SA가 이미 있는 경우 PIX는 IP 패킷을 암호화하고 암호화된 패킷을 피어 IPsec 디바이스로 전송합니다.
- **동적 ACL.**VPN 클라이언트가 IPsec의 도움을 받아 PIX에 연결되면 PIX는 이 IPsec 연결에 대한 흥미로운 트래픽을 정의하기 위해 사용할 소스 및 목적지 주소를 지정하는 동적 ACL을 생성합니다.

PIX에서 문제가 있는 일련의 이벤트 이해

일반적인 컨피그레이션 오류는 nat 0 및 고정 암호화 맵에 동일한 ACL을 사용하는 것입니다. 이 섹션에서는 이러한 오류가 발생하는 이유와 문제를 해결하는 방법에 대해 설명합니다.

PIX 컨피그레이션은 IP 패킷이 네트워크 192.168.4.0/24에서 네트워크 10.10.10.0/24 및 10.1.2.0/24(IP 로컬 풀 풀에 정의된 네트워크 주소)으로 이동할 때 nat 0 ACL 140이 NAT를 우회함을 보여줍니다. 또한 ACL 140은 피어 172.16.172.39에 대한 고정 암호화 맵의 흥미로운 트래픽을 정의합니다.

IP 패킷이 PIX 내부 인터페이스에 도달하면 NAT 검사가 완료된 다음 PIX가 암호화 맵에서 ACL을 확인합니다. PIX는 인스턴스 번호가 가장 낮은 암호화 맵으로 시작합니다. 이전 예의 정적 암호화 맵에 인스턴스 번호가 가장 낮은 ACL 140이 선택되어 있기 때문입니다. 그런 다음 동적 암호화 맵에 대한 동적 ACL을 선택합니다. 이 구성에서 ACL 140은 네트워크 192.168.4.0/24에서 네트워크 10.10.10.0/24 0 및 10.1.2.0/24로 이동하는 트래픽을 암호화하도록 정의됩니다. 그러나 LAN-to-LAN 터널의 경우 네트워크 192.168.4.0/24와 10.10.10.0/24 사이의 트래픽만 암호화하려고 합니다. IPsec 피어 라우터가 암호화 ACL을 정의하는 방법입니다.

PIX에서 문제가 있는 일련의 이벤트 이해

클라이언트가 PIX에 대한 IPsec 연결을 설정하면 IP 로컬 풀에서 IP 주소가 할당됩니다. 이 경우 클라이언트가 10.1.2.1에 할당됩니다. PIX는 다음과 같이 **show crypto map** 명령 출력에 표시된 대로 동적 ACL도 생성합니다.

```
Crypto Map "mymap" 20 ipsec-isakmp
Peer = 171.69.89.120
access-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: 171.69.89.120
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset, }
Crypto Map "mymap" 30 ipsec-isakmp
Peer = 171.69.89.120
access-list dynacl3 permit ip any host 10.1.2.1 (hitcnt=0)
dynamic (created from dynamic map dynmap/10)
Current peer: 171.69.89.120
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
```

```
Transform sets={ myset, }
pix520-1(config)#
```

show crypto **map** 명령에는 고정 암호화 맵도 표시됩니다.

```
Crypto Map: "mymap" interfaces: { outside }
Crypto Map "mymap" 5 ipsec-isakmp
Peer = 172.16.172.39
access-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: 172.16.172.39
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset,}
```

클라이언트와 PIX 간에 IPsec 터널이 설정되면 클라이언트는 호스트 192.168.4.3에 대한 ping을 시작합니다. 에코 요청을 수신하면 호스트 192.168.4.3은 **debug icmp trace** 명령의 이 출력에 표시된 echo-reply로 응답합니다.

```
27: Inbound ICMP echo request (len 32 id 2 seq 7680)
   10.1.2.1 > 192.168.4.3> 192.168.4.3
28: Outbound ICMP echo reply (Len 32 id 2 seq 7680)
   192.168.4.3 >192.168.4.3 > 10.1.2.1
29: Inbound ICMP echo request (Len 32 id 2 seq 7936)
   10.1.2.1 > 192.168.4.3> 192.168.4.3
30: Outbound ICMP echo reply (Len 32 id 2 seq 7936)
   192.168.4.3 >192.168.4.3 > 10.1.2.1
```

그러나 에코 응답은 VPN 클라이언트(호스트 10.1.2.1)에 도달하지 않으며 ping에 실패합니다. PIX에서 **show crypto ipsec sa** 명령의 도움을 받아 볼 수 있습니다. 이 출력은 PIX가 VPN 클라이언트에서 오는 120개의 패킷을 해독하지만 패킷을 암호화하지 않거나 암호화된 패킷을 클라이언트로 전송하지는 않음을 보여줍니다. 따라서 캡슐화된 패킷 수는 0입니다.

```
pix520-1(config)#show crypto ipsec sa
interface: outside
Crypto map tag: mymap, local addr. 172.16.172.34
local 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: 171.69.89.120
dynamic allocated peer ip: 10.1.2.1
PERMIT, 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 0
local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 33a45029
inbound esp sas:
spi: 0x279fc5e9(664782313)
transform: ESP-Des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 5, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607985/27809)
```

```
IV size: 8 bytes
replay detection support: Y
inbound 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: mymap
sa timing: remaining key lifetime (k/sec): (4608000/27809)
IV size: 8 bytes
replay detection support: Y
outbound 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: 172.16.172.39
PERMIT, 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 0
local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: f264e92c
inbound ESP sas:
spi: 0x2772b869(661829737)
transform: ESP-Des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607997/2420)
IV size: 8 bytes
replay detection support: Y
inbound 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: mymap
sa timing: remaining key lifetime (k/sec): (4607999/2420)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound PCP sas:
```

참고: 호스트192.168.4.3 에코 요청에 응답하면 IP 패킷이 PIX의 내부 인터페이스로 전달됩니다.

```
38: Outbound ICMP echo reply (Len 32 id 2 seq 8960)
   192.168.4.3 >192.168.4.3 > 10.1.2.1
```

IP 패킷이 내부 인터페이스에 도착하면 PIX는 nat 0 ACL 140을 확인하고 IP 패킷의 소스 및 목적지 주소가 ACL과 일치하는지 확인합니다. 따라서 이 IP 패킷은 PIX의 모든 NAT 규칙을 우회합니다. 다음으로 암호화 ACL을 확인합니다. 고정 암호화 맵은 인스턴스 번호가 가장 낮으므로 먼저 해당 ACL을 확인합니다. 이 예에서는 고정 암호화 맵에 ACL 140을 사용하므로 PIX는 이 ACL을 확인합니다. 이제 IP 패킷에는 소스 주소가 192.168.4.3이고 대상이 10.1.2.1입니다. 이 주소가 ACL 140과 일치하므로 PIX는 이 IP 패킷이 피어 172.16.172.39을 사용하는 LAN-to-LAN IPsec 터널을 위한 것이라고 생각합니다(목표에 반대됨). 따라서 SA 데이터베이스에서 이 트래픽에 대해 피어 172.16.72.39이 있는 현재 SA가 이미 있는지 확인합니다. show crypto ipsec sa 명령의 출력에 따르면 이 트래픽에 대한 SA가 없습니다. PIX는 패킷을 암호화하거나 VPN 클라이언트로 전송하지 않습니다. 대신 다음 출력에 표시된 대로 피어 172.16.172.39과 다른 IPsec 협상을 시작합니다.

```
crypto_isakmp_process_block: src 172.16.172.39, dest 172.16.172.34
return status is IKMP_NO_ERR_NO_TRANS02303: sa_request, (key eng. msg.)
src= 172.16.172.34, dest= 172.16.172.39,
src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform=
ESP-Des esp-md5-hmac , lifedur= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
702303: sa_request, (key Eng. msg.) src= 172.16.172.34, dest=
172.16.172.39, src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform=
ESP-Des esp-md5-hmac , lifedur= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANSIPSEC(key_engine): request timer
fired: count = 2,
(identity) local= 172.16.172.34, remote= 172.16.172.39,
local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4)
```

다음과 같은 이유로 IPsec 협상이 실패합니다.

- 피어 172.16.172.39은 네트워크 10.10.10.0/24 및 192.168.4.0/24만 암호화 맵 피어 172.16.172.34에 대한 ACL의 흥미로운 트래픽으로 정의합니다.
- 두 피어 간의 IPsec 협상 중에 프록시 ID가 일치하지 않습니다.
- 피어가 협상을 시작하고 로컬 컨피그레이션에서 PFS(Perfect Forward Secrecy)를 지정하는 경우 피어가 PFS 교환을 수행해야 합니다. 그렇지 않으면 협상이 실패합니다. 로컬 컨피그레이션에서 그룹을 지정하지 않으면 group1의 기본값이 가정되고 group1 또는 group2의 제안이 수락됩니다. 로컬 컨피그레이션에서 group2를 지정하는 경우 해당 그룹은 피어의 제안에 속해야 합니다. 그렇지 않으면 협상이 실패합니다. 로컬 컨피그레이션에서 PFS를 지정하지 않으면 피어에서 PFS의 모든 제안을 수락합니다. 1024비트 Diffie-Hellman prime modulus group2는 group1보다 더 많은 보안을 제공하지만 group1보다 더 많은 처리 시간이 필요합니다.**참고:** **crypto map set pfs** 명령은 이 암호화 맵 엔트리에 대해 새 SA를 요청할 때 PFS를 요청하도록 IPsec을 설정합니다. no crypto map **set pfs** 명령을 사용하여 IPsec이 PFS를 요청하지 않도록 지정합니다. 이 명령은 IPsec-ISAKMP 암호화 맵 항목 및 동적 암호화 맵 항목에 대해서만 사용할 수 있습니다. 기본적으로 PFS는 요청되지 않습니다. PFS를 사용하면 새 SA가 협상될 때마다 새로운 Diffie-Hellman 교환이 이루어집니다. 이를 위해서는 추가 처리 시간이 필요합니다. PFS는 또 다른 보안 수준을 추가합니다. 한 키가 공격자에 의해 깨지면 해당 키로 전송된 데이터만 손상되기 때문입니다. 협상 중에 이 명령은 암호화 맵 엔트리에 대해 새 SA를 요청할 때 IPsec에서 PFS를 요청합니다. **set pfs** 문이 그룹을 지정하지 않으면 기본값(group1)이 전송됩니다.**참고:** PIX 방화벽에 PIX 방화벽에서 시작되어 단일 원격 피어에서 종료되는 여러 터널이 있는 경우 원격 피어와의 IKE 협상이 중단될 수 있습니다. 이 문제는 PFS가 활성화되지 않고 로컬 피어가 여러 개의 동시 키 재설정 요청을 요청할 때 발생합니다. 이 문제가 발생하면 IKE SA는 시간이 초과되거나 **clear [crypto] isakmp sa** 명령을 사용하여 수동으로 지울 때까지 복구되지 않습니다. 많은 피어로 구성된 PIX 방화벽 유닛 또는 동일한 터널을 공유하는 여러 클라이언트에 구성된 PIX 방화벽 유닛은 이 문제의 영향을 받지 않습니다. 컨피그레이션이 영향을 받는 경우 crypto map mapname seqnum set pfs 명령으로 PFS를 활성화합니다.

PIX의 IP 패킷은 궁극적으로 삭제됩니다.

솔루션 이해

이 오류를 수정하는 올바른 방법은 nat 0에 대해 두 개의 개별 ACL과 고정 암호화 맵을 정의하는 것입니다. 이를 위해 이 예에서는 nat **0** 명령에 대해 ACL 190을 정의하고 고정 암호화 맵에 대해 수정

된 ACL 140을 사용합니다(이 출력에 표시됨).

PIX 520-1

```
pix520-1(config)#
pix520-1(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix520-1
domain-name vpn.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- 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
10.10.10.0255.255.255.0
access-list 190 permit ip 192.168.4.0 255.255.255.0
10.1.2.0 255.255.255.0
no pager
logging on
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging

logging history debugging
logging host outside 192.168.2.6
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.16.172.34 255.255.255.240
ip address inside 192.168.4.50 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
global (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 190
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.172.33 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
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 mytest protocol tacacs+
AAA-server nasir protocol radius
snmp-server host outside 192.168.2.6
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset ESP-Des esp-md5-hmac
crypto 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-isakmp
crypto map mymap 5 match address 140
crypto map mymap 5 set peer 172.16.172.39
crypto map mymap 5 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 172.16.172.39 netmask
255.255.255.255 no-xauth
no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption Des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption Des
isakmp policy 20 hash sha
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
vpngroup vpn3000 address-pool ippool
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet 192.168.4.0 255.255.255.0 inside
telnet 171.69.89.82 255.255.255.255 inside
telnet timeout 5
ssh 172.0.0.0 255.0.0.0 outside
ssh 171.0.0.0 255.255.255.0 outside
ssh 171.0.0.0 255.0.0.0 outside
ssh timeout 60
terminal width 80
Cryptochecksum:e2cb98b30d3899597b3af484fae4f9ae
: end
[OK]
pix520-1(config)# pix520-1(config)#show crypto map
```

변경 사항을 적용하고 클라이언트가 PIX를 사용하여 IPsec 터널을 설정한 후 show crypto **map** 명

령을 실행합니다. 이 명령은 고정 암호화 맵의 경우 ACL 140에 의해 정의된 흥미로운 트래픽은 원래 목표였던 192.168.4.0/24 및 10.10.10.0/24뿐입니다. 또한 동적 액세스 목록에는 클라이언트(10.1.2.1) 및 PIX(172.16.172.34)으로 정의된 흥미로운 트래픽이 표시됩니다.

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

VPN 클라이언트 10.1.2.1이 호스트 192.168.4.3에 ping을 전송하면 에코 응답이 PIX의 내부 인터페이스로 전송됩니다. PIX는 nat 0 ACL 190을 확인하고 IP 패킷이 ACL과 일치하는지 확인합니다. 따라서 패킷은 PIX에서 NAT 규칙을 우회합니다. 다음으로, PIX는 일치하는 항목을 찾기 위해 고정 암호화 맵 ACL 140을 확인합니다. 이번에는 IP 패킷의 소스와 대상이 ACL 140과 일치하지 않습니다. 따라서 PIX는 동적 ACL을 확인하고 일치하는 항목을 찾습니다. 그런 다음 PIX는 SA 데이터베이스를 검사하여 IPsec SA가 클라이언트에 이미 설정되어 있는지 확인합니다. 클라이언트가 PIX와 IPsec 연결을 이미 설정했으므로 IPsec SA가 있습니다. 그런 다음 PIX는 패킷을 암호화하여 VPN 클라이언트로 전송합니다. PIX의 **show crypto ipsec sa** 명령 출력을 사용하여 패킷이 암호화되어 해독되었는지 확인합니다. 이 경우 PIX는 16개의 패킷을 암호화하여 클라이언트로 전송합니다. 또한 PIX는 VPN 클라이언트에서 암호화된 패킷을 수신하고 16개의 패킷을 해독했습니다.

```
pix520-1(config)#show crypto ipsec sa
interface: outside
Crypto map tag: mymap, local addr. 172.16.172.34
local 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: 171.69.89.120
dynamic allocated peer ip: 10.1.2.1
PERMIT, 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 0
local crypto endpt.: 172.16.172.34, remote crypto endpt.: 171.69.89.120
path mtu 1500, ipsec overhead 56, media mtu 1500
```

```
current outbound spi: 613d083d
inbound ESP sas:
spi: 0x6adf97df(1793038303)
transform: ESP-Des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607998/27420)
IV size: 8 bytes
replay detection support: Y
inbound 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: mymap
sa timing: remaining key lifetime (k/sec): (4607999/27420)
IV size: 8 bytes
replay detection support: Y
outbound 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: 172.16.172.39
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 1, #recv errors 0
local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.39
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 58009c01
inbound ESP sas:
spi: 0x2d408709(759203593)
transform: ESP-Des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607998/3319)
IV size: 8 bytes
replay detection support: Y
inbound 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: mymap
sa timing: remaining key lifetime (k/sec): (4607999/3319)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound PCP sas:
pix520-1(config)# sh cr isa sa
Total : 2
Embryonic : 0
dst src state pending created
172.16.172.39 172.16.172.34 QM_IDLE 0 1
172.16.172.34 171.69.89.120 QM_IDLE 0 2
pix520-1(config)# sh cr ipsec sa
```

라우터 컨피그레이션 및 show 명령 출력

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 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-1
!
no logging buffered
enable secret 5 $1$6jAs$tNxI1a/2DYFAtPLyCDXjo/
enable password ww
!
username cisco password 0 cisco
memory-size iomem 15
clock timezone PST -8
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!--- The crypto isakmp policy command defines the Phase
1 SA parameters.

crypto isakmp policy 15
authentication pre-share
crypto 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-isakmp
set peer 172.16.172.34
set transform-set myset
match address 150
!
!
!
!
!
interface FastEthernet0
ip address 172.16.172.39 255.255.255.240
speed auto
!--- The crypto map applied to the outbound interface.
```

```
crypto map vpn
interface Ethernet0
ip address 10.10.10.1 255.255.255.240
speed auto
no ip route-cache
no ip mroute-cache
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.33
no ip http server
ip 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 0
line aux 0
line vty 0 4
exec-timeout 0 0
password cisco
no login
line vty 5 15
login
!
no scheduler allocate
end
1720-1#
```

```
1720-1#show crypto isa sa
DST src state conn-id slot
172.16.172.39 172.16.172.34 QM_IDLE 132 0
1720-1#show crypto ipsec sa
interface: FastEthernet0
Crypto 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.: 172.16.172.34
path mtu 1500, media mtu 1500
current outbound spi: 2D408709
inbound 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 bytes
replay detection support: Y
inbound 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 bytes
replay detection support: Y
outbound ah sas:
outbound PCP sas:
1720-1#

1720-1#show crypto map
Interfaces using crypto map mymap:
Crypto Map "vpn" 10 ipsec-isakmp
Peer = 172.16.172.34
Extended IP access list 150
access-list 150 permit ip 10.10.10.0 0.0.0.255 192.168.4.0 0.0.0.255
Current peer: 172.16.172.34
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ myset, }
Interfaces using crypto map vpn: FastEthernet0
```

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems