確立されたIPSec トンネル上のパスデータトラフィックへのPIX のトラブルシューティング

内容

概要
前提条件
要件
使用するコンポーネント
表記法
PIX のトラブルシューティング
ネットワーク図
問題のある設定例
一般的なイベントの順序の理解
PIX 上の問題となる一連のイベントの理解
PIX 上の問題となる一連のイベントの理解
ソリューションの理解
ルータ設定と showコマンド出力
関連情報

概要

このドキュメントでは、Cisco VPN Client から PIX への正常に確立された IPSec トンネルがデータを渡すことができないという問題に対応し、その解決策について説明します。

VPN クライアントから PIX の背後にある LAN 上のホストに ping または Telnet できない場合は、VPN クライアントと PIX 間で確立された IPSec トンネルでデータを渡せないという現象が頻繁に発生します。つまり、VPN クライアントと PIX は暗号化データをやり取りすることができません。この現象は、PIX に、ルータまでの LAN 間 IPsec トンネルと VPN クライアントが存在するために発生します。nat 0 と、LAN 間 IPSec ピアのスタティック暗号マップの両方のアクセスコントロール リスト（ACL）が同じ設定であると、データを渡すことができなくなります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure PIX Firewall 6.0.1
- Cisco IOS® ソフトウェア リリース 12.2(6) が稼働する Cisco 1720 ルータ

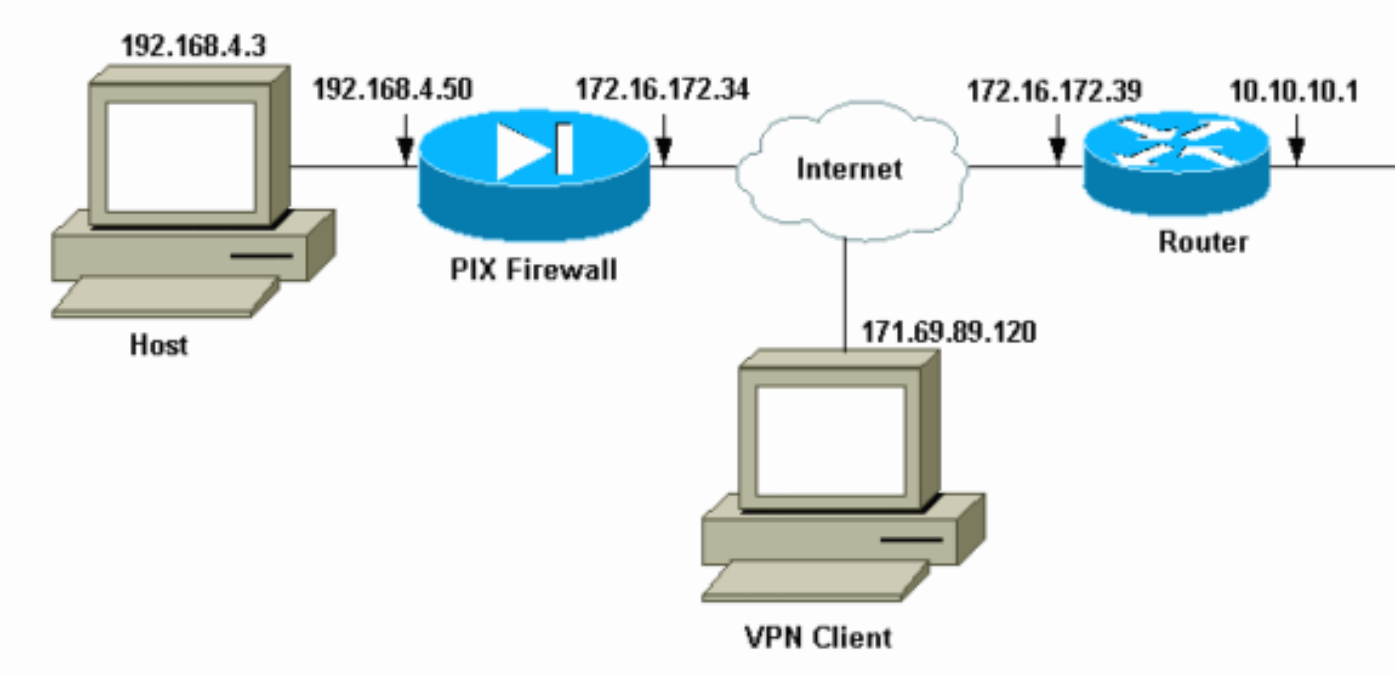
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

PIX のトラブルシューティング

ネットワーク図



問題のある設定例

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
```

問題のある設定では、対象トラフィック、またはLAN-to-LANトンネル用に暗号化されるトラフィックは、ACL 140によって定義されます。設定では、nat 0 ACLと同じACLを使用します。

一般的なイベントの順序の理解

IP パケットが PIX の内部インターフェイスに到着すると、ネットワーク アドレス変換（NAT）が検査されます。その後で、暗号マップの ACL が検査されます。

- **nat 0 の使用方法。**nat 0 ACL は NAT に含めないものを定義します。**nat 0 コマンド内の ACL は、PIX 上の NAT ルールが無効になっている送信元アドレスと宛先アドレスを定義します。**

そのため、送信元アドレスと宛先アドレスが **nat 0 コマンドで定義された ACL と一致する IP パケットは、PIX 上のすべての NAT ルールをバイパスします。**プライベート アドレスを使用して PIX と別の VPN デバイス間に LAN 間トンネルを実装するには、**nat 0 コマンドを使用して NAT をバイパスします。**PIX ファイアウォール上のルールによってプライベート アドレスは NAT に含まれないように排除されますが、このルールが IPsec トンネルを介してリモート LAN に適用されます。

- **暗号 ACL の使用方法。**NAT インスペクション後に、内部インターフェイスに到着した各 IP パケットの送信元と宛先がスタティック暗号マップとダイナミック暗号マップで定義された ACL と一致するかどうかが PIX で検査されます。PIX が ACL との一致を検出すると、PIX は次の手順のいずれかを実行します。トラフィック用のピア IPSec デバイスとの IPSec セキュリティ アソシエーション（SA）がまだ構築されていない場合は、PIX が IPsec ネゴシエーションを開始します。SA が構築されると、PIX がパケットを暗号化して、それを IPSec トンネルを介して IPsec ピアに送信します。すでにピアとの IPSec SA が構築されている場合は、PIX が IP パケットを暗号化して、それをピア IPSec デバイスに送信します。
- **ダイナミック ACL。**VPN クライアントが IPSec を使用して PIX に接続すると、その IPSec 接続の対象トラフィックを定義するために使用する送信元アドレスと宛先アドレスを指定したダイナミック ACL を PIX が作成します。

PIX 上の問題となる一連のイベントの理解

よくある設定の誤りは、nat 0 とスタティック暗号マップに同じ ACL を使用することです。このセクションでは、これがエラーを引き起こす理由と問題の解決方法について説明します。

この PIX 設定は、IP パケットがネットワーク 192.168.4.0/24 からネットワーク 10.10.10.0/24 と 10.1.2.0/24（IP ローカル プール ipool で定義されたネットワーク アドレス）に移動したときに nat 0 ACL 140 が NAT をバイパスすることを示しています。 加えて、ACL 140 はピア 172.16.172.39 のスタティック暗号マップの対象トラフィックを定義します。

IP パケットが PIX 内部インターフェイスに到着すると、NAT 検査が完了してから、PIX が暗号マップ内の ACL を検査します。PIX は、インスタンス番号が最小の暗号マップから始めます。これは、前の例のスタティック暗号マップに最小のインスタンス番号が割り当てられているためであり、ACL 140 が検査されます。次に、ダイナミック暗号マップのダイナミック ACL が検査されます。この設定では、ACL 140は、ネットワーク192.168.4.0 /24からネットワーク10.10.10.0/240および10.1.2.0 /24に送信されるトラフィックを暗号化するように定義されています。ただし、LAN-to-LANトンネルでは、ネットワーク192.168.4.0 /24と10.10.10.0 /24間のトラフィックのみを暗号化します。

PIX 上の問題となる一連のイベントの理解

クライアントが PIX への IPsec 接続を確立すると、IP ローカル プールから IP アドレスが割り当てられます。この例では、クライアントに10.1.2.1が割り当てられています。この**show crypto mapコマンドの出力に示すように、PIXはダイナミックACL**も生成します。

```
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 コマンドでは、スタティック暗号マップも表示されます。

```
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,}
```

クライアントとPIXの間にIPsecトンネルが確立されると、クライアントはホスト192.168.4.3へのpingを開始します。エコー要求を受信すると、ホスト192.168.4.3は**debug icmp traceコマンドの次の出力が示すようにecho-replyで応答します。**

```
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
```

しかし、エコー応答は VPN クライアント (ホスト 10.1.2.1) に到達せずに、ping が失敗します。これは、PIX で **show crypto ipsec sa コマンドを使用して確認できます。**この出力は、PIX が VPN クライアントから送信された 120 個のパケットを復号化するが、パケットを暗号化したり、暗号化されたパケットをクライアントに送信したりしていないことを示しています。そのため、カプセル化されたパケットの数は 0 です。

```
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:
```

注：ホスト192.168.4.3がエコー要求に応答すると、IPパケットはPIXの内部インターフェイスに到達します。

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

IP パケットが内部インターフェイスに到着すると、PIX が nat 0 ACL 140 を検査して、IP パケッ

トの送信元アドレスと宛先アドレスが ACL と一致することを確認します。そのため、この IP パケットは PIX 上のすべての NAT ルールをバイパスします。次に、暗号 ACL が検査されます。スタティック暗号マップには最小のインスタンス番号が割り当てられているため、その ACL が最初に検査されます。この例ではスタティック暗号マップに ACL 140 が使用されているため、PIX はこの ACL を検査します。IPパケットの送信元アドレスは192.168.4.3、宛先は10.1.2.1です。これはACL 140と一致するため、PIXはこのIPパケットがピア172.16.172.39とのLAN-to-LAN IPSecトンネルを目的としていると考えます（これは目的とは異なります）。 そのため、PIX は、SA データベースを検査して、このトラフィック用のピア 172.16.72.39 との SA がすでに存在するかどうかを確認します。**show crypto ipsec sa コマンドの出力が示すように、このトラフィック用の SA は存在しません。**PIX は、パケットを暗号化したり、パケットを VPN クライアントに送信したりしません。代わりに、この出力が示すように、ピア 172.16.172.39 との別の IPsec ネゴシエーションを開始します。

```
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)
```

次の理由で IPsec ネゴシエーションは失敗します。

- ピア 172.16.172.39 は、暗号マップ ピア 172.16.172.34 向けの ACL 内の対象トラフィックとして、ネットワーク 10.10.10.0/24 と 192.168.4.0/24 のみを定義しています。
- 2 つのピア間の IPsec ネゴシエーション中はプロキシ ID が一致しません。
- ピアがネゴシエーションを開始し、ローカル設定で Perfect Forward Secrecy（PFS）を指定する場合は、ピアが PFS 交換を実行する必要があります。実行しなかった場合は、ネゴシエーションが失敗します。ローカル設定でグループが指定されていない場合は、グループ 1 のデフォルトが想定され、グループ 1 またはグループ 2 のオファーが受け入れられます。ローカル設定でグループ 2 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合は、ネゴシエーションが失敗します。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。1024 ビットの Diffie-Hellman プライム モジュラス グループであるグループ 2 はグループ 1 よりも高いセキュリティを提供します。ただし、グループ 1 よりも処理時間が長くなります。**注：crypto map set pfsコマンド**は、このクリプトマップエントリに対して新しいSAを要求する場合に、PFSを要求するようにIPSecを設定します。IPSec から PFS を要求しないように指定するには、**no crypto map set pfs コマンドを使用します。**このコマンドは、IPsec-ISAKMP 暗号マップ エントリとダイナミック暗号マップ エントリにのみ使用できます。デフォルトでは、PFS は要求されません。PFS を使用すると、新しい SA がネゴシエートされるたびに、新しい Diffie-Hellman 交換が行われます。そのため、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけに

なるためです。ネゴシエーション中に、このコマンドを使用すると、暗号マップ エントリ用の新しい SA を要求するときに IPsec が PFS を要求します。**set pfs ステートメントでグループを指定しなかった場合は、デフォルト (グループ 1) が送信されます。注：PIX**ファイアウォールから発信され、単一のリモートピアで終端する多数のトンネルがPIXファイアウォールにある場合、リモートピアとのIKEネゴシエーションがハングする可能性があります。この問題は、PFS が無効になっていて、ローカル ピアが多数の同時キー再生成要求を要求した場合に発生します。この問題が発生した場合は、タイムアウトが発生するか、**clear [crypto] isakmp sa コマンドを使って手動でクリアするまで、IKE SA が回復しません。**多数のピアへの多数のトンネル、または同じトンネルを共有している多数のクライアントを使って設定された PIX ファイアウォール ユニットは、この問題の影響を受けません。設定が影響を受ける場合は、**crypto map mapname seqnum set pfs コマンドを使って PFS を有効にします。**

PIX 上の IP パケットは、最終的には破棄されます。

ソリューションの理解

このエラーを修正する適切な方法は、nat 0 用とスタティック暗号マップ用の 2 つの別個の ACL を定義することです。これを行うには、この出力例が示すように、**nat 0 コマンド用の ACL 190 を定義して、スタティック暗号マップ用に修正された ACL 140 を使用します。**

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
```

変更が完了して、クライアントが PIX との IPSec トンネルを確立したら、**show crypto map コマンドを発行します。**このコマンドによって、スタティック暗号マップでは、ACL 140 によって定義される対象トラフィックが、元々の目標だった 192.168.4.0/24 と 10.10.10.0/24 だけであることが示されます。加えて、ダイナミック アクセス リストは、対象トラフィックがクライアント（10.1.2.1）と PIX（172.16.172.34）として定義されていることを示しています。

```
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 クライアント 10.1.2.1 がホスト 192.168.4.3 に ping を送信すると、エコー応答が PIX の内部インターフェイスに着信します。PIX は、nat 0 ACL 190 を検査して、IP パケットが ACL と一致することを確認します。そのため、パケットは PIX 上の NAT ルールをバイパスします。次に、PIX がスタティック暗号マップ ACL 140 を検査して一致するものを探します。今回は、IPパケットの送信元と宛先がACL 140と一致しないため、PIXはダイナミックACLをチェックして一致するものを見つけます。その後で、PIX は SA データベースを検査して IPsec SA がクライアントと

すでに確立されているかどうかを確認します。クライアントはすでに PIX との IPSec 接続を確立しているため、IPsec SA が存在します。その後で、PIX はパケットを暗号化して、それを VPN クライアントに送信します。PIX からの **show crypto ipsec sa コマンドの出力を使用して、パケットが暗号化され、復号化されたことを確認します。**このケースでは、PIX が 16 個のパケットを暗号化して、それらをクライアントに送信しています。また、VPN クライアントから暗号化されたパケットを受信して、16 個のパケットを復号化しました。

```
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
```

ルータ設定と showコマンド出力

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
```

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Requests for Comments (RFCs)
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems