Устранение неполадок PIX при передаче трафика по установленному туннелю IPSec

Содержание

Введение

В этом документе рассматривается проблема невозможности передачи данных по успешно установленному туннелю IPSec с Cisco VPN Client к PIX и предлагается решение.

Когда вы не можете пропинговать или Telnet от Клиента VPN ни к каким хостам на LAN позади PIX, с неспособностью передать данные установке туннеля IPSec между Клиентом VPN и PIX часто встречаются. Другими словами, Клиент VPN и PIX не могут передать зашифрованные данные между ними. Это происходит, потому что PIX имеет Туннель IPSec между локальными сетями к маршрутизатору и также Клиенту VPN. Неспособность передать данные является результатом конфигурации с тем же списком контроля доступа (ACL) и для nat 0 и для статической криптокарты для узла IPsec LAN-LAN.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Межсетевой экран Cisco Secure PIX 6.0.1
- Маршрутизатор Cisco 1720, который выполняет релиз 12.2 программного обеспечения Cisco IOS (6)

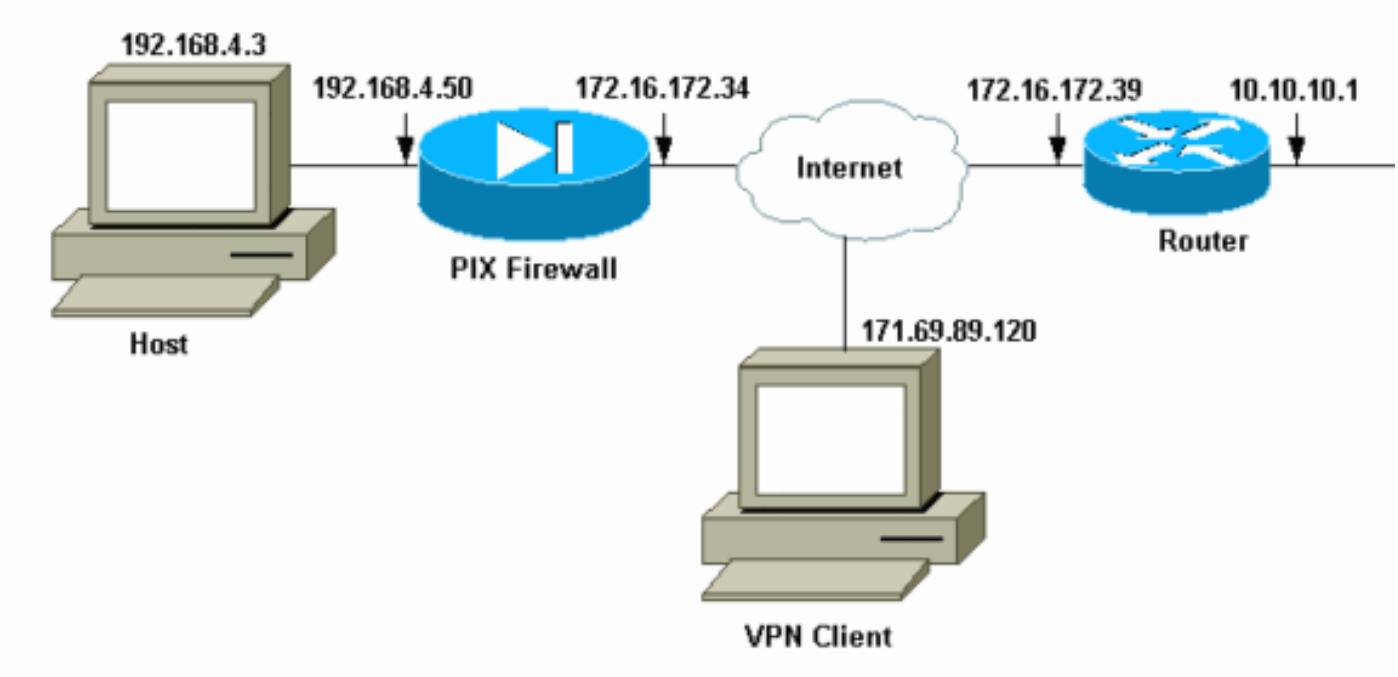
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Поиск и устранение неполадок PIX

Схема сети



Проблематичный пример конфигурации

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
255.255.255.0no 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 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
```

В конфигурации с проблемами представляющий интерес трафик или трафик, который будет зашифрован для туннеля между локальными сетями (LAN-to-LAN), определен ACL 140.

Конфигурация использует тот же ACL в качестве ACL nat 0.

Поймите общую последовательность событий

Когда пакет IP поступает во внутренний интерфейс PIX, Технология NAT проверена. После этого ACL для криптокарт проверены.

- **Как используется nat 0.**ACL nat 0 определяет то, что не должно быть включено в NAT. ACL в **команде nat 0** определяет адрес источника и назначения, для которого отключены правила NAT о PIX. Поэтому пакет IP, который имеет адрес источника и назначения, который совпадает с ACL, определенным в **команде nat 0**, обходит все правила NAT о PIX.Для реализации туннелей между локальными сетями (LAN-to-LAN) между PIX и другим устройством VPN с помощью частных адресов, используйте **команду nat 0** для обхода NAT. Правила о межсетевом экране PIX препятствуют тому, чтобы частные адреса были включены в NAT, в то время как эти правила переходят к удаленной LAN по Туннелю IPSec.
- **Как используется крипто-ACL.**После проверок NAT PIX проверяет источник и назначение каждого пакета IP, который поступает в его внутренний интерфейс для соответствия с ACL, определенными в статических и динамических криптокартах. Если PIX находит соответствие с ACL, PIX делает любой из этих шагов:Если нет никакого текущего IPsec Security Association (SA), уже созданного с одноранговым устройством IPSec для трафика, PIX инициирует согласования IPsec. Как только SA созданы, это шифрует пакет и передает его по Туннелю IPSec к узлу IPsec.Если уже существует контекст безопасности IPSec, созданный с узлом, PIX шифрует пакет IP и передает зашифрованный пакет к одноранговому устройству IPSec.
- **Динамический ACL.**Как только Клиент VPN соединяется с PIX с помощью IPsec, PIX создает динамический ACL, который задает адрес источника и назначения для использования для определения представляющего интерес трафика для этого IP - безопасного соединения.

Поймите неразрешенную последовательность событий на PIX

Ошибка обычной конфигурации состоит в том, чтобы использовать тот же ACL для nat 0 и статических криптокарт. Эти разделы обсуждают, почему это приводит к ошибке и как исправить проблему.

Конфигурация PIX показывает, что nat 0 ACL 140 обходит NAT, когда пакеты IP идут от сети 192.168.4.0/24 к сетям 10.10.10.0/24 и 10.1.2.0/24 (сетевой адрес, определенный в IP local pool ipool). Кроме того, ACL 140 определяет представляющий интерес трафик для статической криптокарты для узла 172.16.172.39.

Когда пакет IP прибывает во внутренний интерфейс PIX, проверка NAT завершает, и затем PIX проверяет ACL в криптокартах. PIX запускается с криптокарты с самым низким номером экземпляра. Это вызвано тем, что статическая криптокарта в предыдущем примере имеет самый низкий номер экземпляра, ACL 140 проверен. Затем, динамический ACL для динамической криптокарты проверен. В этой конфигурации ACL 140 определен для шифрования трафика, который идет от сети 192.168.4.0 / 24 к сетям 10.10.10.0/24 0 и 10.1.2.0 / 24. Однако для туннеля между локальными сетями (LAN-to-LAN), вы только хотите зашифровать трафик между сетями 192.168.4.0 / 24 и 10.10.10.0 / 24. Это - то, как Одноранговый маршрутизатор IPSec определяет свой крипто-ACL.

Поймите неразрешенную последовательность событий на PIX

Когда клиент устанавливает IP - безопасное соединение к PIX, этому назначают IP-адрес от IP local pool. В этом случае клиенту назначают 10.1.2.1. PIX также генерирует динамический ACL, поскольку эти выходные данные **команды show crypto map** показывают:

```
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)#
```

Команда show crypto map также показывает статическую криптокарту:

```
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,}
```

Как только Туннель IPSec установлен между клиентом и PIX, клиент инициирует эхо-запрос к хосту 192.168.4.3. Когда это получает запрос эха, ответы хоста 192.168.4.3 с эхо-ответом, поскольку эти выходные данные команды **debug icmp trace** показывают.

```
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
```

Однако эхо - ответ не достигает Клиента VPN (хост 10.1.2.1) и сбои эхо-запроса. Вы видите это с помощью **команды show crypto ipsec sa** на PIX. Эти выходные данные показывают, что PIX дешифрует 120 пакетов, которые прибывают от Клиента VPN, но это не шифрует пакетов или передает зашифрованные пакеты клиенту. Поэтому количество инкапсулировавших пакетов является нулем.

```
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:
```

Примечание: Когда ответы хоста 192.168.4.3 на запрос эха, пакет IP прибывает во внутренний интерфейс PIX.

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

Как только пакет IP поступает во внутренний интерфейс, PIX проверяет nat 0 ACL 140 и решает, что адреса источника и назначения пакета IP совпадают с ACL. Поэтому этот пакет IP обходит все правила NAT о PIX. Затем, Crypto ACLS проверен. Так как статическая криптокарта имеет самый низкий номер экземпляра, его ACL проверен сначала. Так как данный пример использует ACL 140 для статической криптокарты, PIX проверяет этот ACL. Теперь, пакет IP имеет адрес источника 192.168.4.3 и назначение 10.1.2.1. Так как это совпадает с ACL 140, PIX думает, что этот пакет IP предназначен для Туннеля IPSec между локальными сетями с узлом 172.16.172.39 (вопреки нашим целям). Поэтому это проверяет базу данных SA, чтобы видеть, существует ли уже текущий SA с узлом 172.16.72.39 для этого трафика. Поскольку выходные данные **команды show crypto ipsec sa** показывают, никакой SA не существует для этого трафика. PIX не шифрует или передает пакет Клиенту VPN. Вместо этого это инициирует другое согласование IPsec с узлом 172.16.172.39 как показано в выходных данных ниже:

```
crypto_isakmp_process_block: src 172.16.172.39, dest 172.16.172.34return 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= 0x4004702303: 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=
0x4004ISAKMP (0): sending NOTIFY message 36137 protocol 1return status is
IKMP_NO_ERR_NO_TRANSIPSEC(key_engine): request timerfired: 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)
```

Согласование IPsec отказывает по этим причинам:

- Узел 172.16.172.39 определяет только сети 10.10.10.0/24 и 192.168.4.0/24, поскольку представляющий интерес трафик в его ACL для криптокарты взаимодействует 172.16.172.34.
- Идентичность прокси не совпадает во время согласования IPsec между двумя узлами.
- Если узел инициирует согласование, и локальная конфигурация задает абсолютную секретность переадресации (PFS), узел должен выполнить обмен безопасной пересылки (PFS) или сбои согласования. Если локальная конфигурация не задает группу, по умолчанию group1 принят, и предложение или group1 или group2 принято. Если локальная конфигурация задает group2, та группа должна быть частью предложения узла или сбоев согласования. Если локальная конфигурация не задает безопасную пересылку (PFS), она принимает любое предложение безопасной пересылки (PFS) от узла. 1024-разрядный Диффи-Хеллман главная группа модуля, group2, предоставляет больше безопасности, чем group1, но требует большего количества времени обработки, чем group1.**Примечание: Криптокарта заставила** IPsec наборов команд **pfs** просить безопасную пересылку (PFS), когда это запрашивает новые SA на этот элемент криптокарты. Используйте **команду no crypto map set pfs**, чтобы указать, что IPsec не запрашивает безопасную пересылку (PFS). Эта команда только доступна для элементов криптокарты ISAKMP Ipsec и записей динамической

криптокарты. По умолчанию PFS не запрашивается. С безопасной пересылкой (PFS), каждый раз, когда о новом SA выполняют согласование, происходит новый Обмен Диффи-Хеллмана. Это требует дополнительного времени обработки. Безопасная пересылка (PFS) добавляет другой уровень безопасности, потому что, если один ключ когда-либо взламывается атакующим, только данные, передаваемые с тем ключом, поставились под угрозу. Во время согласования эта команда заставляет IPsec запрашивать безопасную пересылку (PFS), когда это запрашивает новые SA на элемент криптокарты. Если **оператор set pfs** не задает группу, по умолчанию (group1) передается.**Примечание:** Ike согласование с удаленным узлом могут "зависнуть", когда межсетевой экран PIX имеет многочисленные туннели, которые происходят из межсетевого экрана PIX и оконечный на одиночном удаленном узле. Эта проблема происходит, когда безопасная пересылка (PFS) не включена, и локальный партнер запрашивает, чтобы многие одновременные повторно ввели запросы. Если эта проблема происходит, IKE SA не восстанавливается, пока это не испытывает таймаут или пока вы вручную не очищаете его с **командой clear [crypto] isakmp sa**. Модули межсетевого экрана PIX настроили со многими туннелями ко многим узлам или многим клиентам, которые совместно используют тот же туннель, не влияются этой проблемой. Если на вашу конфигурацию влияют, включите безопасную пересылку (PFS) с **командой crypto map mapname seqnum set pfs**.

Пакеты IP на PIX в конечном счете отброшены.

Поймите решение

Корректный метод для исправления этой ошибки должен определить два отдельных ACL для nat 0 и статических криптокарт. Чтобы сделать это, пример определяет ACL 190 для **команды nat 0** и использует модифицированный ACL 140 для статической криптокарты, как показано в выходных данных ниже.

PIX 520-1

```
pix520-1(config)#pix520-1(config)#write terminalBuilding
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
```

После того, как изменения внесены, и клиент устанавливает Туннель IPSec с PIX, выполните **команду show crypto map**. Эта команда показывает, что для статической криптокарты, представляющий интерес трафик, определенный ACL 140, только 192.168.4.0/24 и 10.10.10.0/24, который был исходной целью. Кроме того, динамический список доступа показывает представляющий интерес трафик, определенный как клиент (10.1.2.1) и 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, }
```

Когда Клиент VPN 10.1.2.1 передает эхо-запрос к хосту 192.168.4.3, эхо - ответ прибывает

во внутренний интерфейс PIX. PIX Проверяет nat 0 ACL 190 и решает, что пакет IP совпадает с ACL. Поэтому пакет обходит правила NAT о PIX. Затем, PIX проверяет статическую криптокарту ACL 140 для обнаружения соответствия. На этот раз источник и назначение пакета IP не совпадают с ACL 140. Поэтому PIX проверяет динамический ACL и находит соответствие. PIX тогда проверяет свою базу данных SA, чтобы видеть, установлен ли контекст безопасности IPSec уже с клиентом. Так как клиент уже установил IP - безопасное соединение с PIX, контекст безопасности IPSec существует. PIX тогда шифрует пакеты и передает его Клиенту VPN. Используйте выходные данные **команды show crypto ipsec sa** от PIX, чтобы видеть, что пакеты и зашифрованы и дешифрованы. В этом случае PIX зашифровал шестнадцать пакетов и передал их клиенту. PIX также получил зашифрованные пакеты от Клиента VPN и дешифровал шестнадцать пакетов.

```
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
```

Конфигурация маршрутизатора и выходные данные по команде "show"

Cisco 1720-1

```
1720-1#show runBuilding 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 mysetmatch address 150!!!!!interface
FastEthernet0ip address 172.16.172.39
255.255.255.240speed auto!--- The crypto map applied to
the outbound interface.crypto map vpninterface
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 saDST src state conn-id slot172.16.172.39 172.16.172.34 QM_IDLE 132
01720-1#show crypto ipsec sainterface: FastEthernet0Crypto map tag: vpn, local addr.
172.16.172.39local 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: 172.16.172.34PERMIT,
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 0local 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: vpnsa 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: vpnsa 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
```

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация