Пример конфигурации IPSec между брандмауэром PIX и концентратором Cisco VPN 3000 с накладывающимися частными сетями

Содержание

Введение

Этот документ описывает, как настроить межсетевой экран Cisco Secure PIX в VPN защищенного взаимодействия между сетями Site-to-Site IPsec с адресами наложения частной сети позади Шлюзов VPN. Расширенная трансляция сетевых адресов (NAT) функция, представленная в PIX 6.2, используется в данном примере для перевода наложений сети на каждой стороне VPN-туннеля IPSec к неадресным пространствам с перекрытием.

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 506 с версией программного обеспечения 6.3 (3)
- Концентратор VPN 3030 с версией программного обеспечения 4.1 (5)

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

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

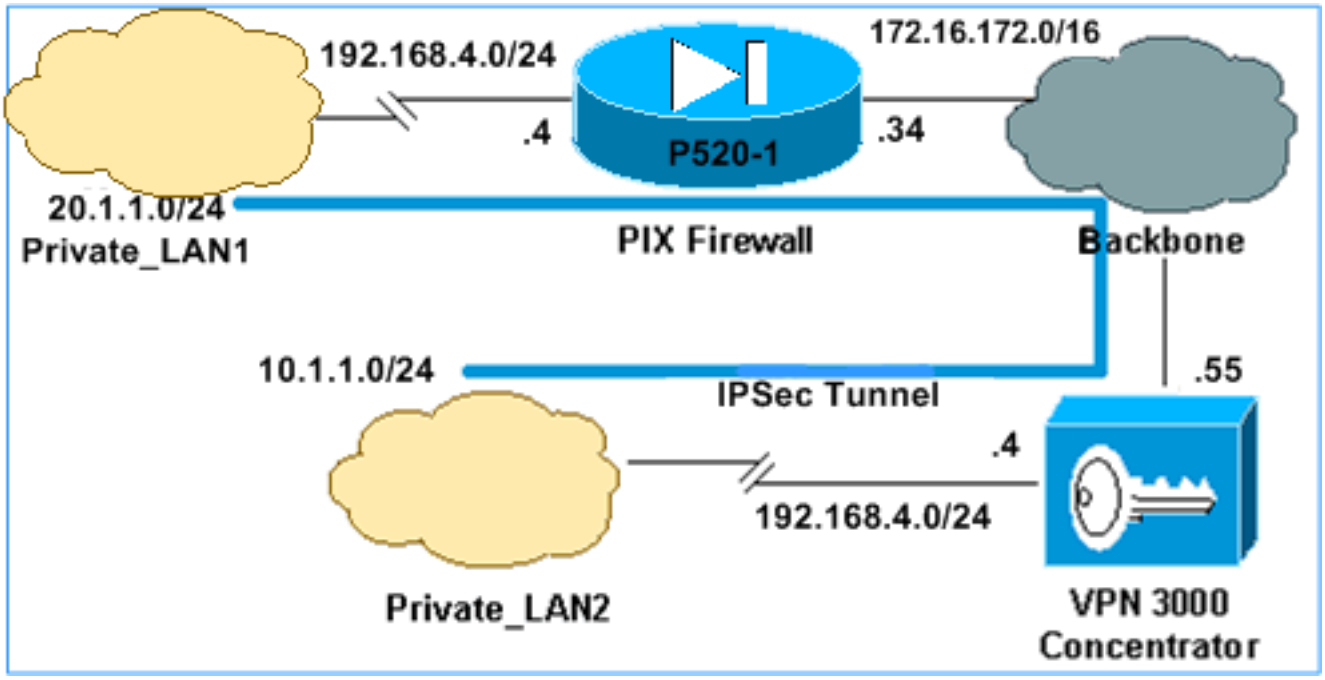
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



И Private_LAN1 и Private_LAN2 имеют IP-подсеть 192.168.4.0/24. Это моделирует адресное пространство с перекрытием позади каждой стороны Туннеля IPSec. VPN 3000 Concentrator используется здесь в качестве одного примера концентратора, который не имеет функциональности трафика NAT over VPN.

В данном примере PIX выполняет двунаправленную трансляцию так, чтобы эти две частных

локальных сети (LAN) могли связаться по Туннелю IPSec. Трансляция означает, что Private_LAN1 "рассматривает" Private_LAN2 как 10.1.1.0/24 через Туннель IPSec, и Private_LAN2 "рассматривает" Private_LAN1 как 20.1.1.0/24 через Туннель IPSec.

Конфигурации

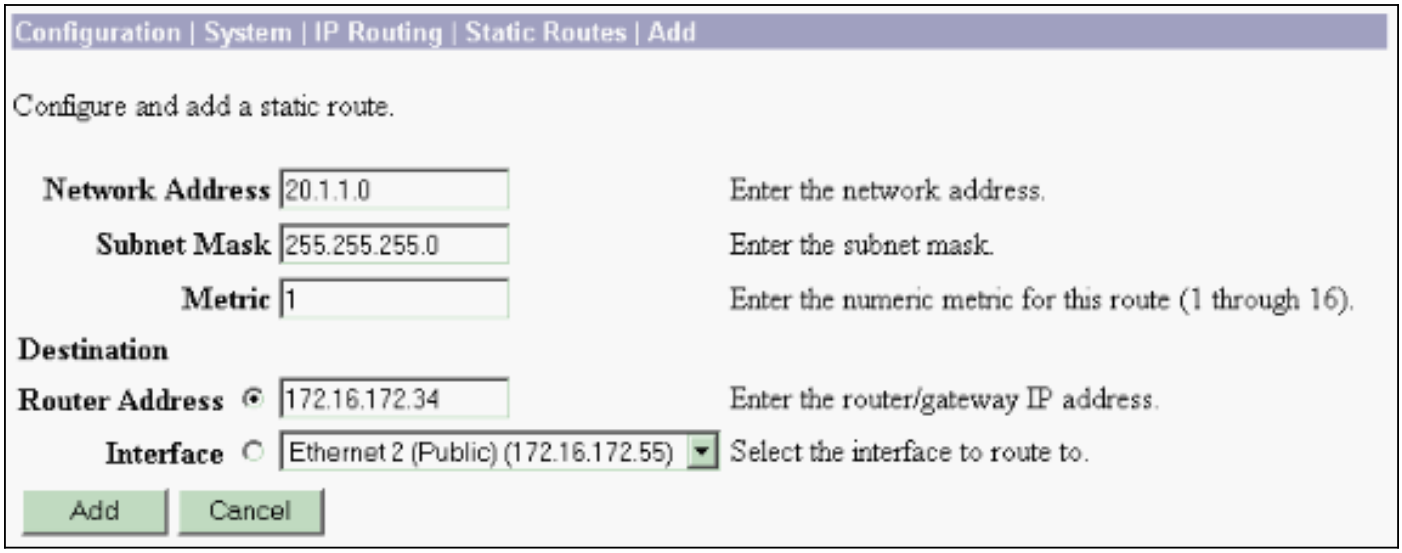
PIX

```
P520-1(config)#show run: Saved:PIX Version
6.3(3)interface ethernet0 autointerface ethernet1
autonameif ethernet0 outside security0nameif ethernet1
inside security100enable password 8Ry2YjIyt7RRXU24
encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname P520-
1domain-name bru-ch.comfixup protocol dns maximum-length
512fixup protocol ftp 21fixup protocol h323 h225
1720fixup protocol h323 ras 1718-1719fixup protocol http
80fixup protocol rsh 514fixup protocol rtsp 554fixup
protocol sip 5060fixup protocol sip udp 5060fixup
protocol skinny 2000fixup protocol smtp 25fixup protocol
sqlnet 1521fixup protocol tftp 69names !--- Defines
IPSec interesting traffic. !--- Note that the host
behind PIX communicates !--- to Private_LAN1 using
10.1.1.0/24. !--- When the packets arrive at the PIX,
they are first !--- translated to 192.168.4.0/24 and
then encrypted by IPSec.access-list 101 permit ip
20.1.1.0 255.255.255.0 192.168.4.0 255.255.255.0 pager
lines 24mtu outside 1500mtu inside 1500ip address
outside 172.16.172.34 255.255.255.0ip address inside
192.168.4.4 255.255.255.0ip audit info action alarmip
audit attack action alarmpdm history enablearp timeout
14400!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.4.0/24 to
10.1.1.0/24.static (outside,inside) 10.1.1.0 192.168.4.0
netmask 255.255.255.0 0 0!--- Static translation defined
to translate Private_LAN1 !--- from 192.168.4.0/24 to
20.1.1.0/24. !--- Note that this translation is used for
both !--- VPN and Internet traffic from Private_LAN1. !-
-- A routable global IP address range, or an extra NAT
!--- at the ISP router (in front of PIX), is !---
required if Private_LAN1 also needs internal
access.static (inside,outside) 20.1.1.0 192.168.4.0
netmask 255.255.255.0 0 0route outside 0.0.0.0 0.0.0.0
172.16.172.55 1timeout xlate 3:00:00timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server locationno snmp-server contactsnmp-server
community publicno snmp-server enable trapsfloodguard
enablesysopt connection permit-ipsec!--- Defines IPSec
encryption and authentication algorithms.crypto ipsec
transform-set myset esp-des esp-md5-hmac !--- Defines
crypto map.crypto map vpn 10 ipsec-isakmpcrypto map vpn
10 match address 101crypto map vpn 10 set peer
172.16.172.55crypto map vpn 10 set transform-set myset!-
-- Apply crypto map on the outside interface.crypto map
vpn interface outsideisakmp enable outside!--- Defines
pre-shared secret (cisco123) used for IKE
authentication.isakmp key ******** address 172.16.172.55
netmask 255.255.255.255 isakmp identity address!---
Defines ISAKMP policy.isakmp policy 1 authentication
```

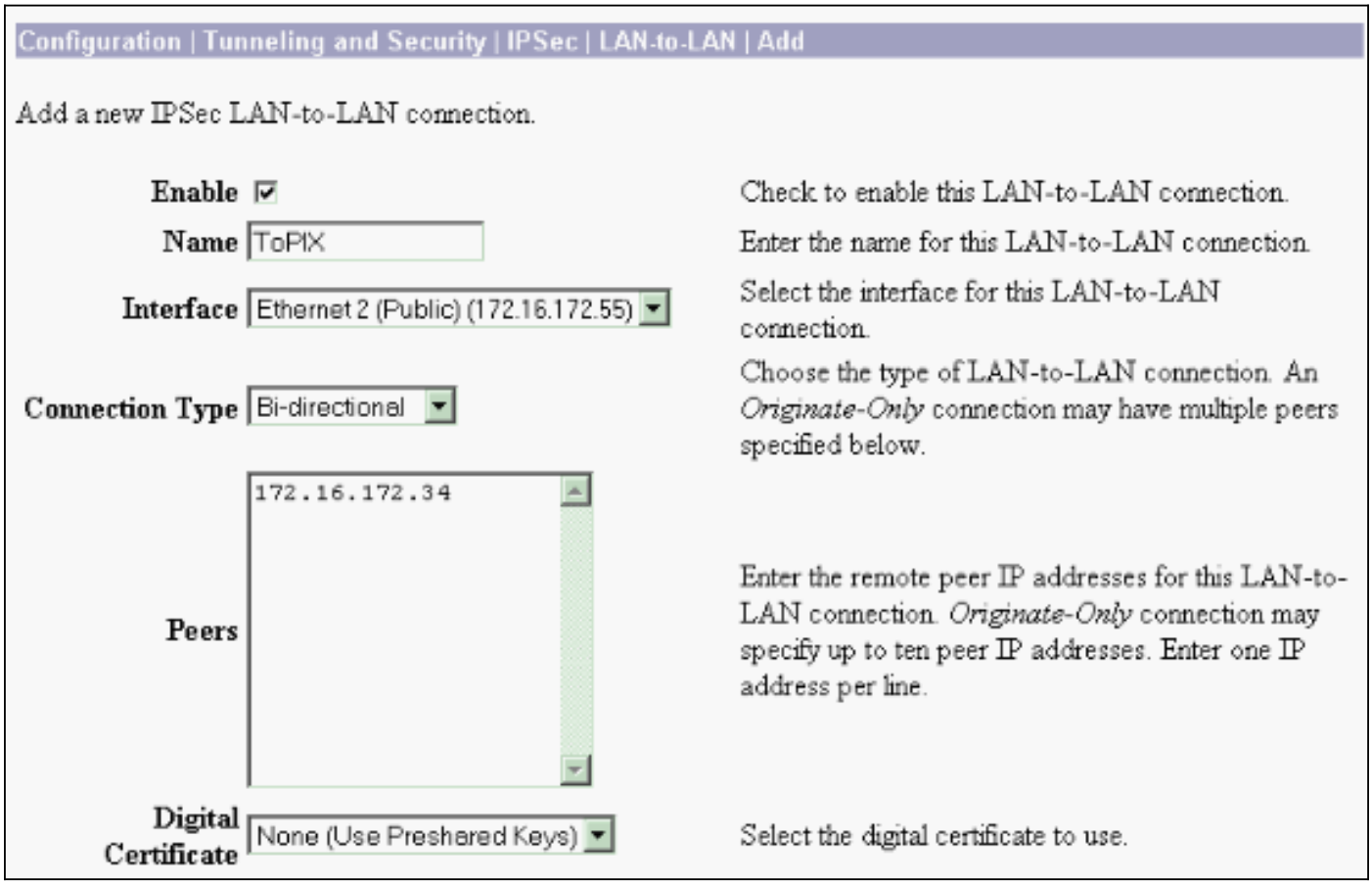
```
pre-shareisakmp policy 1 encryption desisakmp policy 1
hash md5isakmp policy 1 group 1isakmp policy 1 lifetime
86400telnet timeout 5ssh timeout 5console timeout
0terminal width
80Cryptochecksum:6cc25fc2fea20958dfe74c1fca45ada2: end
```

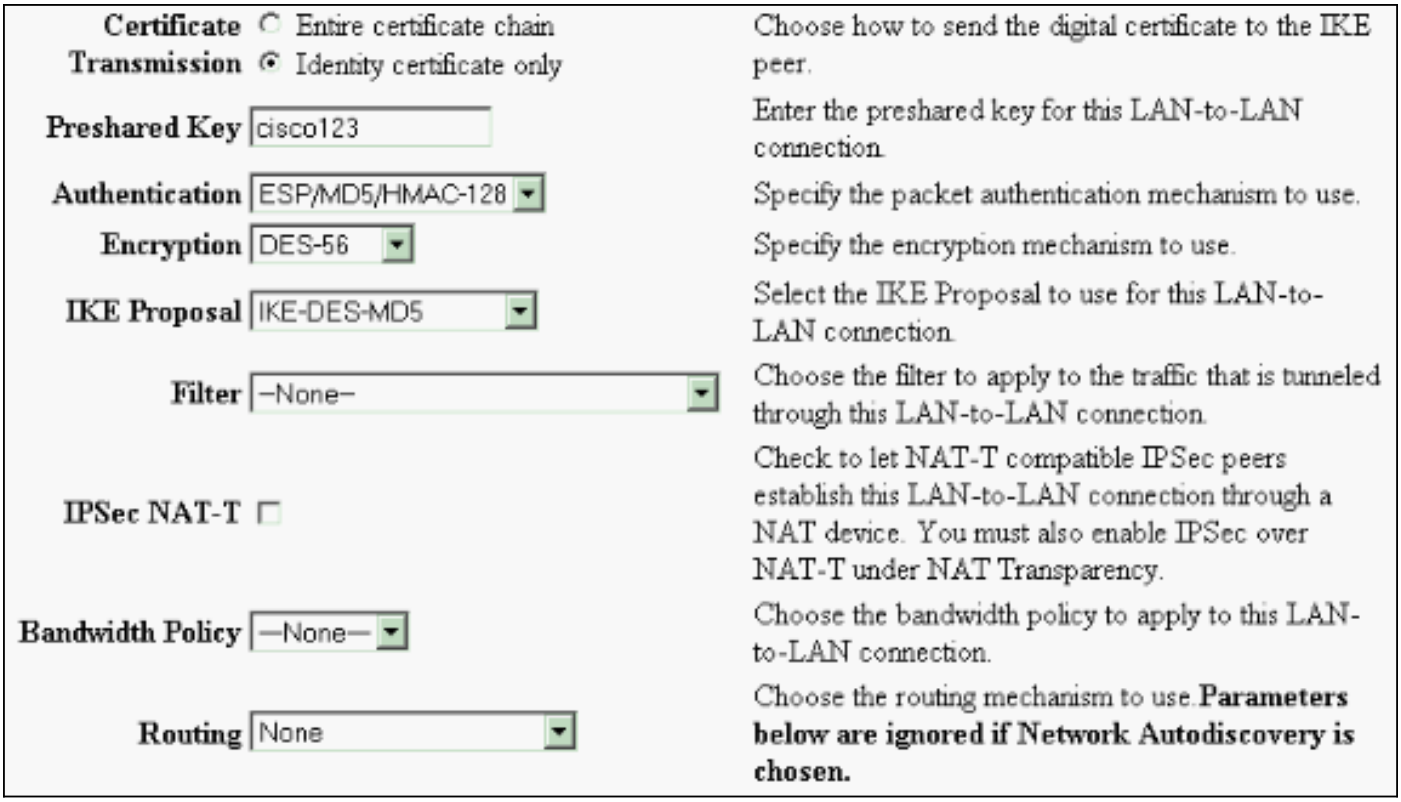
Конфигурация туннеля между локальными сетями VPN 3000 Concentrator

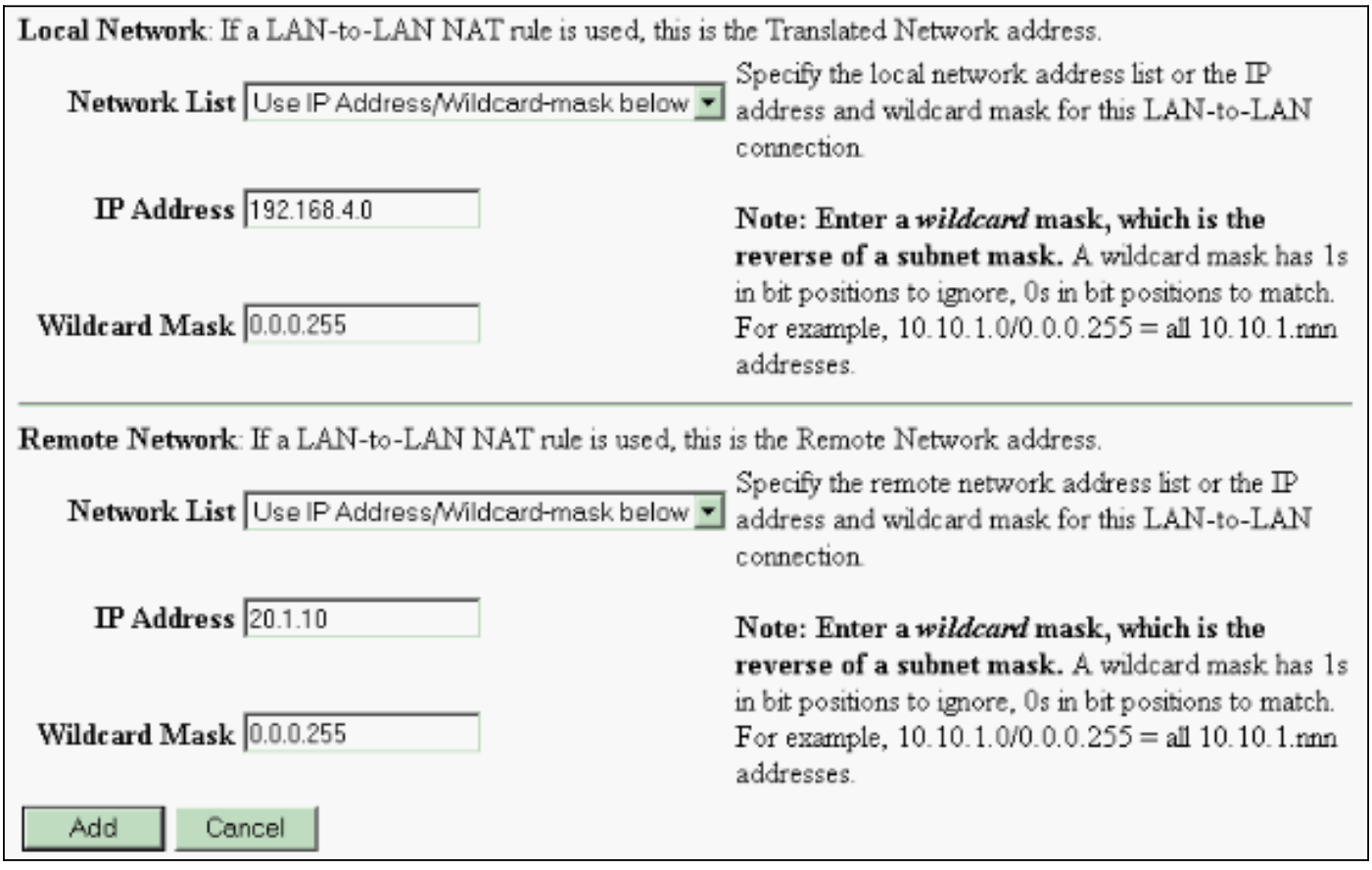
Для адреса назначения (DA) 20.1.1.0 / 24 (Private_LAN1) у вас должен быть статический маршрут на VPN 3000. Чтобы сделать, выберите **Configuration> System> IP Routing> Static Routes** и выберите **Add**. Как только вы убраны, заполнив поля, **нажмите Add**.



Используйте параметры настройки в этих образах для настройки VPN 3000 Concentrator.







Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику

выходных данных команды show.

- **show crypto isakmp sa-** Отобразите все текущие сопоставления безопасности Протокола IKE (SA) в узле.
- **show crypto isakmp sa detail** - Отобразите подробные данные всех текущих SA IKE в узле.
- **show crypto ipsec sa — отображает настройки, используемые текущими SA.**
- **show xlate detail** - Информация о слоте преобразования Показов.

PIX

```
P520-1(config)# P520-1(config)#show crypto isakmp saTotal : 1Embryonic : 0 dst src state pending
created 172.16.172.55 172.16.172.34 QM_IDLE 0 1P520-1(config)#show crypto isakmp sa detailTotal
: 1Embryonic : 0 Local Remote Encr Hash Auth State Lifetime 172.16.172.34:500 172.16.172.55:500
des md5 psk QM_IDLE 86211P520-1(config)# P520-1(config)#show crypto ipsec sainterface: outside
Crypto map tag: vpn, local addr. 172.16.172.34 local ident (addr/mask/prot/port):
(20.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer: 172.16.172.55:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt:
4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4 #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.:
172.16.172.55 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 734575cb
inbound esp sas: spi: 0xe028850d(3760751885) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 1, crypto map: vpn sa timing: remaining key lifetime (k/sec):
(4607999/28751) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0x734575cb(1933931979) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 2, crypto map: vpn sa timing: remaining key lifetime (k/sec):
(4607999/28751) IV size: 8 bytes replay detection support: Y outbound ah sas:P520-1(config)#show
xlate detail2 in use, 2 most usedFlags: D - DNS, d - dump, I - identity, i - inside, n - no
random, o - outside, r - portmap, s - staticNAT from inside:192.168.4.1 to outside:20.1.1.1
flags sNAT from outside:192.168.4.1 to inside:10.1.1.1 flags s
```

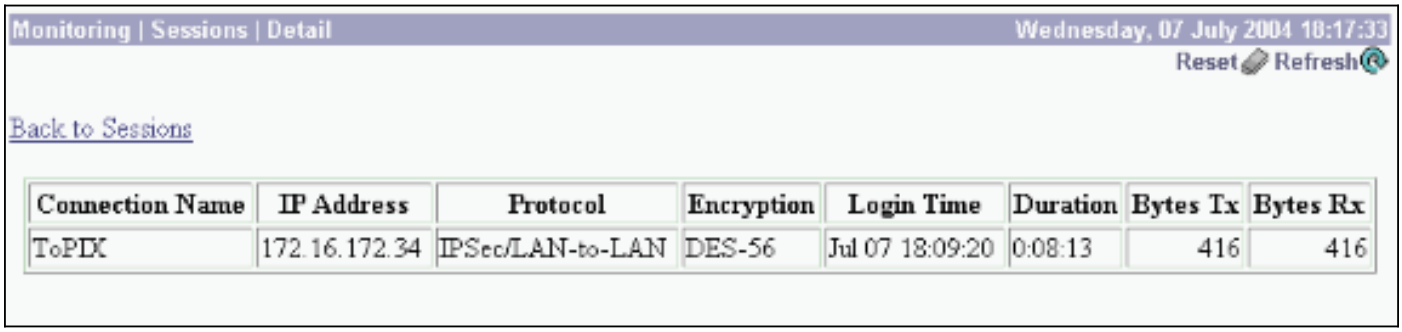
Используйте трафик эхо-тестирования для проверки туннеля. Эти выходные данные **debug icmp trace**, собранные на PIX, иллюстрируют, как пакеты преобразованы NAT.

```
P520-1(config)# debug icmp traceICMP trace onWarning: this may cause problems on busy
networksP520-1(config)# 1: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3060
seq=4391 length=802: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.13:
ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.14: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3060 seq=4391 length=805: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.16: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.17: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3061 seq=4391
length=808: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.19: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.110: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3061 seq=4391 length=8011: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.112: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.113: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3062 seq=4391
length=8014: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.115: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.116: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3062 seq=4391 length=8017: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.118: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.119: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3063 seq=4391
length=8020: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.121: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.122: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3063 seq=4391 length=8023: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.124: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.125: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3064 seq=4391
length=8026: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.127: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.128: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3064 seq=4391 length=8029: ICMP echo-reply: translating
```

```
outside:192.168.4.1 to inside:10.1.1.130: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.1P520-1(config)#
```

VPN-концентратор

Выберите **Monitoring> Sessions> Detail** для проверки конфигурации VPN 3000 Concentrator.

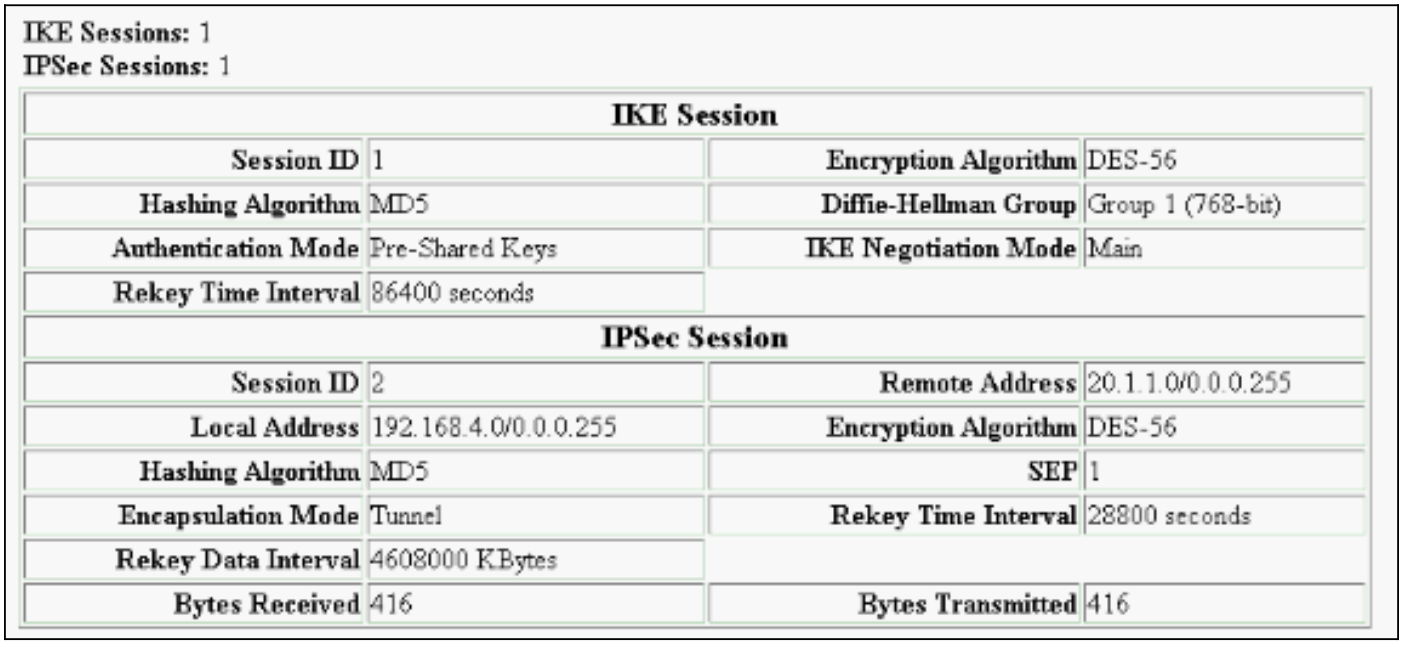


Monitoring | Sessions | Detail — Wednesday, 07 July 2004 18:17:33

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
ToPIX	172.16.172.34	IPSec/LAN-to-LAN	DES-56	Jul 07 18:09:20	0:08:13	416	416



IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	Remote Address	20.1.1.0/0.0.0.255
Local Address	192.168.4.0/0.0.0.255	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Rekey Data Interval	4608000 KBytes		
Bytes Received	416	Bytes Transmitted	416

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации. Дополнительные сведения об устранении проблем могут быть найдены в следующих документах:

- Устранение неполадок соединений в концентраторе VPN 3000
- Устранение проблем IPSec — общие сведения и использование команд debug
- Устранение неполадок PIX при передаче трафика по установленному туннелю IPSec

Команды для устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Эти выходные данные демонстрируют рабочую отладку Ike согласование. Показанный здесь выходные данные **команд debug crypto isakmp и debug crypto ipsec**.

```
P520-1(config)#show debugdebug crypto ipsec 1debug crypto isakmp 1P520-1(config)# ISAKMP (0):
beginning Main Mode exchangecrypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34
spt:500 dpt:500OAK_MM exchangeISAKMP (0): processing SA payload. message ID = 0ISAKMP (0):
Checking ISAKMP transform 1 against priority 1 policyISAKMP: encryption DES-CBCISAKMP: hash
MD5ISAKMP: default group 1ISAKMP: auth pre-shareISAKMP: life type in secondsISAKMP: life
duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are acceptable. Next payload is 0ISAKMP
(0): processing vendor id payloadISAKMP (0): SA is doing pre-shared key authentication using id
type ID_IPV4_ADDRreturn status is IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.16.172.55,
dest:172.16.172.34 spt:500 dpt:500OAK_MM exchangeISAKMP (0): processing KE payload. message ID =
0ISAKMP (0): processing NONCE payload. message ID = 0ISAKMP (0): processing vendor id
payloadISAKMP (0): processing vendor id payloadISAKMP (0): received xauth v6 vendor idISAKMP
(0): processing vendor id payloadISAKMP (0): speaking to another IOS box!ISAKMP (0): processing
vendor id payloadISAKMP (0): speaking to a VPN3000 concentratorISAKMP (0): ID payload next-
payload : 8 type : 1 protocol : 17 port : 500 length : 8ISAKMP (0): Total payload length:
12return status is IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.16.172.55,
dest:172.16.172.34 spt:500 dpt:500OAK_MM exchangeISAKMP (0): processing ID payload. message ID =
0ISAKMP (0): processing HASH payload. message ID = 0ISAKMP (0): processing vendor id
payloadISAKMP (0): remote peer supports dead peer detectionISAKMP (0): SA has been
authenticatedISAKMP (0): beginning Quick Mode exchange, M-ID of -
995061605:c4b0909bIPSEC(key_engine): got a queue event...IPSEC(spi_response): getting spi
0xe028850d(3760751885) for SA from 172.16.172.55 to 172.16.172.34 for prot 3return status is
IKMP_NO_ERRORISAKMP (0): sending INITIAL_CONTACT notifyISAKMP (0): sending NOTIFY message 24578
protocol 1VPN Peer: ISAKMP: Added new peer: ip:172.16.172.55/500 Total VPN Peers:1VPN Peer:
ISAKMP: Peer ip:172.16.172.55/500 Ref cnt incremented to:1 Total VPN
Peers:1crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500OAK_QM
exchangeoakley_process_quick_mode:OAK_QM_IDLEISAKMP (0): processing SA payload. message ID =
3299905691ISAKMP : Checking IPSec proposal 1ISAKMP: transform 1, ESP_DESISAKMP: attributes in
transform:ISAKMP: SA life type in secondsISAKMP: SA life duration (basic) of 28800ISAKMP: SA
life type in kilobytesISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: encaps is
1ISAKMP: authenticator is HMAC-MD5ISAKMP (0): atts are
acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=
172.16.172.55, src= 172.16.172.34, dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4ISAKMP (0): processing NONCE
payload. message ID = 3299905691ISAKMP (0): processing ID payload. message ID = 3299905691ISAKMP
(0): processing ID payload. message ID = 3299905691ISAKMP (0): Creating IPSec SAs inbound SA
from 172.16.172.55 to 172.16.172.34 (proxy 192.168.4.0 to 20.1.1.0) has spi 3760751885 and
conn_id 1 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from
172.16.172.34 to 172.16.172.55 (proxy 20.1.1.0 to 192.168.4.0) has spi 1933931979 and conn_id 2
and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event...IPSEC(initialize_sas): , (key eng. msg.) dest= 172.16.172.34, src= 172.16.172.55,
dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.4.0/255.255.255.0/0/0
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi=
0xe028850d(3760751885), conn_id= 1, keysize= 0, flags= 0x4IPSEC(initialize_sas): , (key eng.
msg.) src= 172.16.172.34, dest= 172.16.172.55, src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-
hmac , lifedur= 28800s and 4608000kb, spi= 0x734575cb(1933931979), conn_id= 2, keysize= 0,
flags= 0x4VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:2 Total VPN
Peers:1VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:3 Total VPN
Peers:1return status is IKMP_NO_ERRORP520-1(config)# P520-1(config)#
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500ISAKMP (0):
processing NOTIFY payload 36136 protocol 1 spi 0, message ID = 1690390088ISAMKP (0): received
DPD_R_U_THERE from peer 172.16.172.55ISAKMP (0): sending NOTIFY message 36137 protocol 1return
status is IKMP_NO_ERR_NO_TRANSP520-1(config)#
```

Дополнительные сведения

- Страницы технической поддержки продукта безопасности и VPN
- Страницы поддержки технологии безопасности и VPN

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems