

# PIX с PIX 6.x: Пример конфигурации Easy VPN (NEM)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Команды show для сервера PIX EasyVPN и пример выходных данных](#)

[Команды show для вынесенного аппаратного клиента PIX EasyVPN и пример выходных данных](#)

[Устранение неполадок](#)

[Команды сервера EasyVPN](#)

[Команды для вынесенного аппаратного клиента EasyVPN](#)

[Дополнительные сведения](#)

## Введение

Этот документ предоставляет пример конфигурации для IPsec между Удаленным аппаратным клиентом Easy VPN PIX и Сервером Pix Easy VPN. Функция удаленной стороны Easy VPN Remote для PIX впервые представлена в PIX версии 6.2 и для нее также используются названия «аппаратный клиент» и EzVPN Client. Сервер Cisco Easy VPN поддерживается в Версии ПО PIX 6.0 и позже.

См. [PIX/ASA 7.x Легкая VPN с ASA 5500 как Сервер и PIX 506E как Клиент \(NEM\) Пример конфигурации](#) для узнавания больше о том же сценарии, куда устройство безопасности выполняется с версией программного обеспечения 7. x.

[Описание аналогичного сценария, в котором маршрутизатор Cisco 871 играет роль удаленной стороны Easy VPN, см. в документе Пример настройки Easy VPN с PIX/ASA 7.x с ASA 5500 в качестве сервера и Cisco 871 в качестве удаленной стороны Easy VPN.](#)

[Описание аналогичного сценария, в котором концентратор Cisco VPN 3000 служит в качестве сервера Easy VPN, см. в документе Пример настройки аппаратного клиента VPN на модуле защиты PIX серии 501/506 с концентратором VPN 3000.](#)

См. [PIX 501/506 Easy VPN Remote к Маршрутизатору IOS в Режиме расширения сети с](#)

[Примером конфигурации Расширенной проверки подлинности](#) для получения дополнительной информации о подобном сценарии, где маршрутизатор Cisco IOS® действует как Сервер Easy VPN.

## Предварительные условия

### Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Гарантируйте, что вашим Удаленным аппаратным клиентом Easy VPN PIX является PIX 501 или PIX 506/506E, который выполняет Версию ПО PIX 6.2 или позже.
- Гарантируйте, что вашим Сервером Easy VPN является Межсетевой экран PIX, который выполняет Версию ПО PIX 6.0 или позже.

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Удаленным аппаратным клиентом Easy VPN PIX является PIX 501, который выполняет Версию ПО PIX 6.3 (1).
- Сервером Easy VPN является PIX 515, который выполняет Версию ПО PIX 6.3 (1).

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.](#)

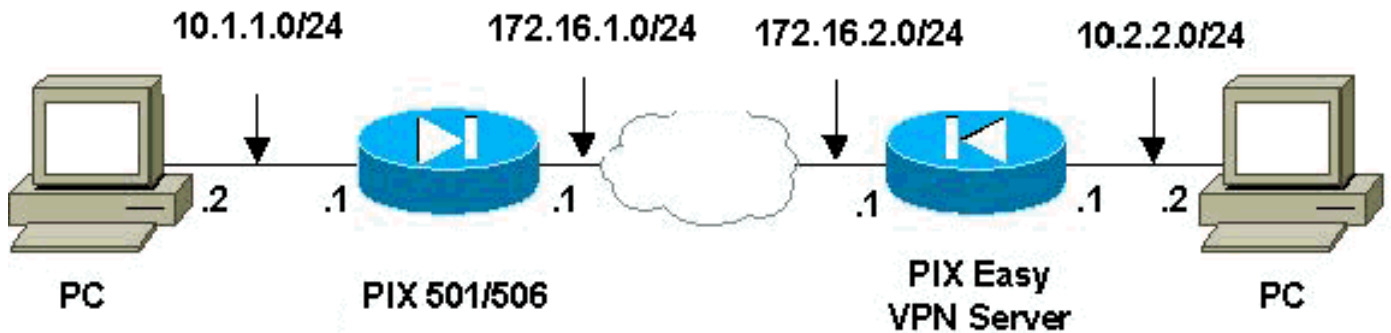
## Настройка

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

**Примечание:** [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\)](#) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

### Схема сети

В настоящем документе используется следующая схема сети:



## Конфигурации

Эти конфигурации используются в данном документе:

- [Сервер Pix Easy VPN](#)
- [Удаленный аппаратный клиент Easy VPN PIX](#)

### Сервер Pix Easy VPN

```

pix515#write terminal Building configuration... : Saved
: PIX Version 6.3(1) !--- Specify speed and duplex
settings. interface ethernet0 auto interface ethernet1
auto interface ethernet2 auto shutdown interface
ethernet3 auto shutdown interface ethernet4 auto
shutdown interface ethernet5 auto shutdown nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 nameif ethernet2 intf2 security4 nameif
ethernet3 intf3 security6 nameif ethernet4 intf4
security8 nameif ethernet5 intf5 security10 enable
password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted hostname pix515 fixup
protocol ftp 21 fixup protocol h323 h225 1720 fixup
protocol h323 ras 1718-1719 fixup protocol http 80 fixup
protocol ils 389 fixup protocol rsh 514 fixup protocol
rtsp 554 fixup protocol sip 5060 fixup protocol sip udp
5060 fixup protocol skinny 2000 fixup protocol smtp 25
fixup protocol sqlnet 1521 names !--- Specify split
tunnelling access list and "nonat" access list. access-
list 101 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 mtu intf2 1500 mtu intf3 1500 mtu intf4 1500 mtu
intf5 1500 !--- Define IP address for the PIX's inside
and outside interfaces. ip address outside 172.16.2.1
255.255.255.0 ip address inside 10.2.2.1 255.255.255.0
no ip address intf2 no ip address intf3 no ip address
intf4 no ip address intf5 ip audit info action alarm ip
audit attack action alarm ip local pool ippool 10.3.3.1-
10.3.3.254 no failover failover timeout 0:00:00 failover
poll 15 no failover ip address outside no failover ip
address inside no failover ip address intf2 no failover
ip address intf3 no failover ip address intf4 no
failover ip address intf5 pdm history enable arp timeout
14400 !--- Configure Network Address Translation (NAT)/
!--- Port Address Translation (PAT) for regular traffic,
!--- as well as NAT for IPsec traffic. global (outside)
1 interface nat (inside) 0 access-list 101 nat (inside)
1 0.0.0.0 0.0.0.0 0 0 !--- Define the outside router as
the default gateway. !--- Typically this is the IP
address of your !--- Internet service provider's (ISP)
router. route outside 0.0.0.0 0.0.0.0 172.16.2.2 1

```

```

timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout
h323 0:05:00 mgcp 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 LOCAL protocol local no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable sysopt
connection permit-ipsec !--- Configure IPsec transform
set and dynamic crypto map. crypto ipsec transform-set
myset esp-aes esp-md5-hmac crypto dynamic-map dynmap 10
set transform-set myset crypto map mymap 10 ipsec-isakmp
dynamic dynmap !--- Apply crypto map to the outside
interface. crypto map mymap interface outside !---
Configure Phase 1 Internet Security Association !-- and
Key Management Protocol (ISAKMP) parameters. isakmp
enable outside isakmp identity address isakmp policy 10
authentication pre-share isakmp policy 10 encryption aes
isakmp policy 10 hash md5 isakmp policy 10 group 2
isakmp policy 10 lifetime 86400 !--- Configure VPNGroup
parameters, to be sent down to the client. vpngroup
mygroup address-pool ippool vpngroup mygroup dns-server
10.2.2.2 vpngroup mygroup wins-server 10.2.2.2 vpngroup
mygroup default-domain cisco.com vpngroup mygroup split-
tunnel 101 vpngroup mygroup idle-time 1800 vpngroup
mygroup password ***** vpngroup idle-time idle-time
1800 telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:67106d7a5a3aa3da0caaeaa93b9fc8d6 : end
[OK] pix515#

```

## Удаленный аппаратный клиент Easy VPN PIX

```

pix501#write terminal Building configuration... : Saved
: PIX Version 6.3(1) !--- Specify speed and duplex
settings. interface ethernet0 auto interface ethernet1
100full nameif ethernet0 outside security0 nameif
ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix501 fixup protocol ftp 21 fixup
protocol h323 h225 1720 fixup protocol h323 ras 1718-
1719 fixup protocol http 80 fixup protocol ils 389 fixup
protocol rsh 514 fixup protocol rtsp 554 fixup protocol
sip 5060 fixup protocol sip udp 5060 fixup protocol
skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet
1521 names pager lines 24 mtu outside 1500 mtu inside
1500 !--- Define IP address for the PIX's inside and
outside interfaces. ip address outside 172.16.1.1
255.255.255.0 ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm ip audit attack action alarm
pdm history enable arp timeout 14400 !--- Configure NAT
for traffic that is not encrypted. global (outside) 1
interface nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Define
the outside router as the default gateway. !--
Typically this is the IP address of your ISP's router.
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 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 LOCAL
protocol local no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable telnet timeout 5 ssh
timeout 5 console timeout 0 !--- Define Easy VPN Remote

```

```
parameters. vpnclient server 172.16.2.1 vpnclient mode
network-extension-mode vpnclient vpngroup mygroup
password ***** !--- Enable the VPN Client. !--- (This
automatically initiates the IPSec tunnel to the server.)
vpnclient enable terminal width 80
Cryptochecksum:b8242b410ad8e3b372018cd1cff77f91 : end
[OK]
```

## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

## Команды show для сервера PIX EasyVPN и пример выходных данных

- команда `show crypto isakmp sa` выводит все текущие сопоставления безопасности (security associations, SA) протокола IKE (Internet Key Exchange, обмен ключами в Интернете) на одноранговом узле.  
`pix515#show crypto isakmp sa Total : 1 Embryonic : 0 dst src state pending created 172.16.2.1 172.16.1.1 QM_IDLE 0 2 pix515#`

- `show crypto ipsec sa` - Отображает сопоставление IPSec SA, построенное между узлами.  
`pix515#show crypto ipsec sa !--- This command was issued after a ping !--- was attempted from the PC behind the !--- Easy VPN Client to the PC !--- behind the server.`  
interface: outside Crypto map tag: mymap, local addr. 172.16.2.1 local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) current\_peer: 172.16.1.1:500 dynamic allocated peer ip: 0.0.0.0 PERMIT, flags={ } #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 0, #recv errors 0 !--- Ping packets !--- were successfully exchanged between the !--- Easy VPN Remote Hardware Client !--- and the Easy VPN Server. local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: 3a5a28e4 inbound esp sas: spi: 0x505c96c6(1348245190) transform: esp-aes esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 2, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607999/28471) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x3a5a28e4(978987236) transform: esp-aes esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 1, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607999/28471) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/0/0) current\_peer: 172.16.1.1:500 dynamic allocated peer ip: 0.0.0.0 PERMIT, flags={ } #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #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.: 172.16.2.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: 27f378f9 inbound esp sas: spi: 0xf2bb4f00(4072361728) transform: esp-aes esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 3, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4608000/27796) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x27f378f9(670267641) transform: esp-aes esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 4, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4608000/27787) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas: pix515#

## Команды show для вынесенного аппаратного клиента PIX EasyVPN и пример

## ВЫХОДНЫХ ДАННЫХ

- команда `vpnclient enable` включает удаленное подключение Easy VPN. В режиме расширения сети (Network Extension Mode, NEM) туннель остается включенным, даже если нет значимого трафика для обмена с сервером головного узла

`EasyVPN.)pix501(config)#vpnclient enable`

- команда `show crypto isakmp policy` выводит параметры для каждой политики

**IKE.**`pix501#show crypto isakmp policy` Default protection suite encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume limit

**Выходные данные от команды show crypto isakmp policy после аппаратного клиента включены, показан здесь.**`pix501(config)#show crypto isakmp policy`

Protection suite of priority 65001 encryption algorithm: AES - Advanced Encryption Standard (256 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65002 encryption algorithm: AES - Advanced Encryption Standard (256 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65003 encryption algorithm: AES - Advanced Encryption Standard (192 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65004 encryption algorithm: AES - Advanced Encryption Standard (192 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65005 encryption algorithm: AES - Advanced Encryption Standard (128 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65006 encryption algorithm: AES - Advanced Encryption Standard (128 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65007 encryption algorithm: Three key triple DES hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65008 encryption algorithm: Three key triple DES hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65009 encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key with XAUTH Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65010 encryption algorithm: AES - Advanced Encryption Standard (256 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65011 encryption algorithm: AES - Advanced Encryption Standard (256 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65012 encryption algorithm: AES - Advanced Encryption Standard (192 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65013 encryption algorithm: AES - Advanced Encryption Standard (192 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65014 encryption algorithm: AES - Advanced Encryption Standard (128 bit keys). hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65015 encryption algorithm: AES - Advanced Encryption Standard (128 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65016 encryption algorithm: Three key triple DES hash algorithm: Secure Hash Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit  
Protection suite of priority 65017 encryption algorithm: Three key triple DES hash algorithm: Message Digest 5 authentication



method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit Protection suite of priority 65018 encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 86400 seconds, no volume limit

- **show crypto isakmp sa — отображает все текущие IKE SA на одноранговом**

**уэле.**pix501(config)#**show crypto isakmp sa** Total : 1 Embryonic : 0 dst src state pending created 172.16.2.1 172.16.1.1 QM\_IDLE 0 1

- **show crypto ipsec sa - Отображает сопоставление IPsec SA, построенное между**

**узлами.**pix501(config)#**show crypto ipsec sa** *!--- This command was issued after a ping !--- was attempted from the PC behind the !--- Easy VPN client to the PC !--- behind the server.*  
interface: outside Crypto map tag: \_vpnc\_cm, local addr. 172.16.1.1 local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) current\_peer: 172.16.2.1:500 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, #rcv errors 0 *!--- Ping packets !--- were successfully exchanged between !--- the Easy VPN Remote Hardware Client !--- and the Easy VPN Server.* local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: 505c96c6 inbound esp sas: spi: 0x3a5a28e4(978987236) transform: esp-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: \_vpnc\_cm sa timing: remaining key lifetime (k/sec): (4607999/28745) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x505c96c6(1348245190) transform: esp-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: \_vpnc\_cm sa timing: remaining key lifetime (k/sec): (4607999/28745) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) current\_peer: 172.16.2.1:500 PERMIT, flags={origin\_is\_acl,} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #rcv errors 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: f2bb4f00 inbound esp sas: spi: 0x27f378f9(670267641) transform: esp-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: \_vpnc\_cm sa timing: remaining key lifetime (k/sec): (4608000/28125) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xf2bb4f00(4072361728) transform: esp-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: \_vpnc\_cm sa timing: remaining key lifetime (k/sec): (4608000/28125) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas: pix501(config)#

- **команда show vpnclient служит для отображения данных конфигурации для клиента VPN или удаленного устройства Easy VPN.**

pix501(config)#**show vpnclient** LOCAL CONFIGURATION  
vpnclient server 172.16.2.1 vpnclient mode network-extension-mode vpnclient vpngroup mygroup password \*\*\*\*\* vpnclient enable DOWNLOADED DYNAMIC POLICY Current Server : 172.16.2.1 Primary DNS : 10.2.2.2 Primary WINS : 10.2.2.2 Default Domain : cisco.com PFS Enabled : No Secure Unit Authentication Enabled : No User Authentication Enabled : No Split Networks : 10.2.2.0/255.255.255.0 Backup Servers : None pix501(config)#

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Если вы установили Удаленного аппаратного клиента Easy VPN и Сервер Easy VPN, как описано в этом документе и все еще испытываете проблемы, собираете выходные данные отладки из каждого PIX и выходные данные от команд показа для анализа Центром технической поддержки Cisco (TAC). [Дополнительные сведения см. в документах Устранение проблем блока PIX для передачи трафика данных на установленном туннеле IPsec или Устранение проблем протокола IP Security — общие сведения и использование команд debug.](#) Разрешить отладку протокола IPsec на блоке расширения параллельного

интерфейса (PIX).

Команды отладки PIX и пример выходных данных показывают здесь.

- [Команды сервера EasyVPN](#)
- [Команды для вынесенного аппаратного клиента EasyVPN](#)

**Примечание:** [Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки"](#).

## Команды сервера EasyVPN

- **debug crypto ipsec** – отображает согласования IPSec на Этапе 2.
- **debug crypto isakmp** – отображает согласования ISAKMP на 1-м этапе.

Вот пример выходных данных.

```
pix515(config)#
!--- As soon as the vpnclient enable command !--- is issued on the remote client PIX, !--- the
server receives an IKE negotiation request. crypto_isakmp_process_block:src:172.16.1.1,
dest:172.16.2.1 spt:500 dpt:500 OAK_AG exchange ISAKMP (0): processing SA payload. message ID =
0 ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption AES-CBC
ISAKMP: keylength of 256 ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-
share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 2
against priority 10 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 256 ISAKMP: hash MD5
ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next
payload is 3 ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy ISAKMP:
encryption AES-CBC ISAKMP: keylength of 192 ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP:
extended auth pre-share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0
0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP
transform 4 against priority 10 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 192
ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP: life
type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not
acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash SHA ISAKMP: default group 2
ISAKMP: extended auth pre-share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI)
of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking
ISAKMP transform 6 against priority 10 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of
128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP: life
type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not
acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 7 against priority 10 policy
ISAKMP: encryption 3DES-CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-
share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 8
against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash MD5 ISAKMP: default group 2
ISAKMP: extended auth pre-share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI)
of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking
ISAKMP transform 9 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5
ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next
payload is 3 ISAKMP (0): Checking ISAKMP transform 10 against priority 10 policy
crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1 spt:500 dpt:500 OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578
protocol 1 spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event... IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.1.1 ISAKMP (0): processing
vendor id payload ISAKMP (0): received xauth v6 vendor id ISAKMP (0): processing vendor id
payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id
payload ISAKMP (0): speaking to another IOS box! ISAKMP (0): processing vendor id payload
```



```

crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1 spt:500 dpt:500 ISAKMP_TRANSACTION
exchange crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1 spt:500 dpt:500 OAK_QM
exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID =
4788683 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_AES ISAKMP: attributes in
transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic)
of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA ISAKMP: key length is 256IPSEC(validate_proposal): transform
proposal (prot 3, trans 12, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next
payload is 0 ISAKMP : Checking IPsec proposal 2 ISAKMP: transform 1, ESP_AES ISAKMP: attributes
in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration
(basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46
0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP: key length is 256IPSEC(validate_proposal):
transform proposal (prot 3, trans 12, hmac_alg 1) not supported ISAKMP (0): atts not acceptable.
Next payload is 0 ISAKMP : Checking IPsec proposal 3 ISAKMP: transform 1, ESP_AES ISAKMP:
attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life
duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP: key length is
192IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not supported
ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 4 ISAKMP:
transform 1, ESP_AES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type
in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP:
SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP: key length
is 192IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP:
transform 1, ESP_AES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type
in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP:
SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP: key length
is 128IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not supported
ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 6 ISAKMP:
transform 1, ESP_AES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type
in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP:
SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP: key length
is 128 ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1, (key
eng. msg.) dest= 172.16.2.1, src= 172.16.1.1, dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-
hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x4 !--- Both PIXes
accept the policy for IPsec. ISAKMP (0): processing NONCE payload. message ID = 4788683 ISAKMP
(0): processing ID payload. message ID = 4788683 ISAKMP (0): ID_IPV4_ADDR src 172.16.1.1 prot 0
port 0 ISAKMP (0): processing ID payload. message ID = 4788683 ISAKMP (0): ID_IPV4_ADDR_SUBNET
dst 10.2.2.0/255.255.255.0 prot 0 port 0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf5720496(4117890198) for SA from 172.16.1.1 to 172.16.2.1 for
prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block:src:172.16.1.1,
dest:172.16.2.1 spt:500 dpt:500 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs inbound SA from 172.16.1.1 to 172.16.2.1 (proxy 172.16.1.1 to
10.2.2.0) has spi 4117890198 and conn_id 3 and flags 4 lifetime of 28800 seconds
crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1 spt:500 dpt:500 ISAKMP (0):
processing NOTIFY payload 36136 protocol 1 spi 0, message ID = 843197376 ISAMKP (0): received
DPD_R_U_THERE from peer 172.16.1.1 ISAKMP (0): sending NOTIFY message 36137 protocol 1 return
status is IKMP_NO_ERR_NO_TRANS crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1
spt:500 dpt:500 ISAKMP (0): processing NOTIFY payload 36136 protocol 1 spi 0, message ID =
1985282089 ISAMKP (0): received DPD_R_U_THERE from peer 172.16.1.1 ISAKMP (0): sending NOTIFY
message 36137 protocol 1 return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.16.1.1, dest:172.16.2.1 spt:500 dpt:500 ISAKMP (0):
processing NOTIFY payload 36136 protocol 1 spi 0, message ID = 1510977390 ISAMKP (0): received
DPD_R_U_THERE from peer 172.16.1.1 ISAKMP (0): sending NOTIFY message 36137 protocol 1 return
status is IKMP_NO_ERR_NO_TRANS

```

## [Команды для вынесенного аппаратного клиента EasyVPN](#)

- **debug crypto ipsec** – отображает согласования IPsec на Этапе 2.
- **debug crypto isakmp** – отображает согласования ISAKMP на 1-м этапе.

```

pix501(config)#vpnclient enable (cIoSnAfKigM)P# (0): ID payload next-payload : 13 type : 11

```

protocol : 17 port : 0 length : 11 ISAKMP (0): Total payload length: 15 ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3 ISAKMP (0): beginning Aggressive Mode exchange  
crypto\_isakmp\_process\_block:src:172.16.2.1, dest:172.16.1.1 spt:500 dpt:500 OAK\_AG exchange  
ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 65001 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65002 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65003 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65004 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65005 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65006 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65007 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65008 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are not acceptable. Next payload is 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 65009 policy ISAKMP: encryption AES-CBC ISAKMP: keylength of 128 ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP : attributes being requested  
crypto\_isakmp\_process\_block:src:172.16.2.1, dest:172.16.1.1 spt:500 dpt:500 ISAKMP (0): beginning Quick Mode exchange, M-ID of 1112046058:424879eaIPSEC(key\_engine): got a queue event... IPSEC(spi\_response): getting spi 0x274d3063(659370083) for SA from 172.16.2.1 to 172.16.1.1 for prot 3 crypto\_isakmp\_process\_block:src:172.16.2.1, dest:172.16.1.1 spt:500 dpt:500 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_IDLE ISAKMP (0): processing SA payload. message ID = 1112046058 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP\_AES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP: key length is 128 ISAKMP (0): atts are acceptable.IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) dest= 172.16.2.1, src= 172.16.1.1, dest\_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4), src\_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 128, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 1112046058 ISAKMP (0): processing ID payload. message ID = 1112046058 ISAKMP (0): processing ID payload. message ID = 1112046058 ISAKMP (0): Creating IPsec SAs inbound SA from 172.16.2.1 to 172.16.1.1 (proxy 10.2.2.0 to 172.16.1.1) has spi 659370083 and conn\_id 2 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from 172.16.1.1 to 172.16.2.1 (proxy 172.16.1.1 to 10.2.2.0) has spi 264316759 and conn\_id 1 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key\_engine): got a queue event... IPSEC(initialize\_sas): , (key eng. msg.) dest= 172.16.1.1, src= 172.16.2.1, dest\_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1), src\_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x274d3063(659370083), conn\_id= 2, keysize= 128, flags= 0x4 IPSEC(initialize\_sas): , (key eng. msg.) src= 172.16.1.1, dest= 172.16.2.1, src\_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1), dest\_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0xfc12757(264316759), conn\_id= 1, keysize= 128, flags= 0x4  
VPN Peer: IPSEC: Peer ip:172.16.2.1/500 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:172.16.2.1/500 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP\_NO\_ERROR pix501(config)# pix501(config)# ISAKMP (0): sending NOTIFY message 36136 protocol 1 crypto\_isakmp\_process\_block:src:172.16.2.1, dest:172.16.1.1 spt:500 dpt:500 ISAKMP (0):

processing NOTIFY payload 36137 protocol 1 spi 0, message ID = 136860646n ISAKMP (0): received DPD\_R\_U\_THERE\_ACK from peer 172.16.2.1

- **отладка vpnclient** — Отображает согласования, определенные для Клиента VPN.

```
pix501(config)#vpnclient enable pix501(config)# 505: VPNC CFG: transform set unconfig attempt
done 506: VPNC CLI: no isakmp keepalive 10 507: VPNC CLI: no isakmp nat-traversal 20 508: VPNC
CFG: IKE unconfig successful 509: VPNC CLI: no crypto map _vpnc_cm 510: VPNC CFG: crypto map
deletion attempt done 511: VPNC CFG: crypto unconfig successful 512: VPNC CLI: no global
(outside) 65001 513: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl 514: VPNC CFG: nat
unconfig attempt failed 515: VPNC CLI: no http 10.1.1.1 255.255.255.0 inside 516: VPNC CLI: no
http server enable 517: VPNC CLI: no access-list _vpnc_acl 518: VPNC CFG: ACL deletion attempt
failed 519: VPNC CLI: no crypto map _vpnc_cm interface outside 520: VPNC CFG: crypto map
de/attach failed 521: VPNC CLI: no sysopt connection permit-ipsec 522: VPNC CLI: sysopt
connection permit-ipsec 523: VPNC CFG: transform sets configured 524: VPNC CFG: crypto config
successful 525: VPNC CLI: isakmp keepalive 10 526: VPNC CLI: isakmp nat-traversal 20 527: VPNC
CFG: IKE config successful 528: VPNC CLI: http 10.1.1.1 255.255.255.0 inside 529: VPNC CLI: http
server enable 530: VPNC CLI: no access-list _vpnc_acl 531: VPNC CFG: ACL deletion attempt failed
532: VPNC CLI: access-list _vpnc_acl permit ip host 172.16.1.1 host 172.16.2.1 533: VPNC CLI:
crypto map _vpnc_cm 10 match address _vpnc_acl 534: VPNC CFG: crypto map acl update successful
535: VPNC CLI: no crypto map _vpnc_cm interface outside 536: VPNC CLI: crypto map _vpnc_cm
interface outside 537: VPNC INF: IKE trigger request done 538: VPNC INF: Constructing policy
download req 539: VPNC INF: Packing attributes for policy request 540: VPNC INF: Attributes
being requested 541: VPNC ATT: ALT_DEF_DOMAIN: cisco.com 542: VPNC ATT: INTERNAL_IP4_NBNS:
10.2.2.2 543: VPNC ATT: INTERNAL_IP4_DNS: 10.2.2.2 544: VPNC ATT: ALT_SPLIT_INCLUDE 545: VPNC
INF: 10.2.2.0/255.255.255.0 546: VPNC ATT: ALT_PFS: 0 547: VPNC ATT: ALT_CFG_SEC_UNIT: 0 548:
VPNC ATT: ALT_CFG_USER_AUTH: 0 549: VPNC CLI: no access-list _vpnc_acl 550: VPNC CLI: access-
list _vpnc_acl permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 551: VPNC CLI: access-
list _vpnc_acl permit ip host 172.16.1.1 10.2.2.0 255.255.255.0 552: VPNC CFG: _vpnc_acl ST
define done 553: VPNC CFG: Split DNS config attempt done 554: VPNC CLI: crypto map _vpnc_cm 10
match address _vpnc_acl 555: VPNC CFG: crypto map acl update successful 556: VPNC CLI: no crypto
map _vpnc_cm interface outside 557: VPNC CLI: crypto map _vpnc_cm interface outside 558: VPNC
CLI: no global (outside) 65001 559: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl 560: VPNC
CFG: nat unconfig attempt failed 561: VPNC CLI: nat (inside) 0 access-list _vpnc_acl 562: VPNC
INF: IKE trigger request done
```

## [Дополнительные сведения](#)

- [Страница поддержки PIX](#)
- [Справочник по командам PIX](#)
- [Страница технической поддержки Протоколов Согласований/IKE IPsec](#)
- [Запросы комментариев \(RFC\)](#)
- [Техническая поддержка - Cisco Systems](#)