Настройка соединения между Cisco VPN Client и PIX с использованием улучшенного стандарта шифрования (AES)

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Общие сведения](#)
[Конфигурации](#)
[Схема сети](#)
[Настройка PIX](#)
[Настройка VPN-клиента](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

В этом примере конфигурации показано, как устанавливать соединение с удаленным доступом VPN между клиентом Cisco VPN и межсетевым экраном PIX при помощи улучшенного стандарта шифрования (AES). В этом примере используется функция Cisco Easy VPN для настройки безопасного канала, а межсетевой экран PIX настроен как сервер Easy VPN.

Начиная с выпуска 6.3 программного обеспечения Cisco Secure PIX Firewall, поддерживается новый международный стандарт шифрования AES для обеспечения безопасности VPN подключений веб-узел-веб-узел и удаленного доступа. Этот стандарт используется наряду с алгоритмами шифрования данных DES и 3DES. Межсетевой экран PIX поддерживает ключи AES длиной 128, 192 и 256 бит.

VPN-клиент поддерживает AES в качестве алгоритма шифрования начиная с версии 3.6.1 программного обеспечения Cisco VPN Client. VPN-клиент поддерживает только ключи длиной 128 и 256 бит.

Предварительные условия

Требования

В этом примере конфигурации предполагается, что PIX полностью функционален и настроен необходимыми командами для обработки трафика в соответствии с политикой безопасности организации.

Используемые компоненты

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

- Программное обеспечение PIX, выпуск 6.3(1)**Примечание:** Эта настройка была протестирована на Релизе программного обеспечения PIX 6.3 (1) и, как ожидают, будет работать на все более поздние версии.
- Cisco VPN Client версии 4.0.3(A)**Примечание:** Эта настройка была протестирована на версии 4.0.3 (A) Клиента VPN, но работает на более ранние релизы назад к 3.6.1 и до текущего релиза.

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.

Общие сведения

VPN адреса удалённого доступа требуются для мобильных сотрудников для безопасного соединения с сетью организации. Мобильные пользователи могут настроить безопасное соединение с помощью программного обеспечения VPN Client, установленного на их ПК. VPN Client инициирует подключение к устройству центрального узла, настроенному для приема таких запросов. В этом примере устройство центрального узла - это межсетевой экран PIX, настроенный как сервер Easy VPN, который использует динамические криптокарты.

Cisco Easy VPN облегчает развертывание VPN, упрощая настройку и управление VPN. Это программное обеспечение состоит из из двух частей: Cisco Easy VPN Server и Cisco Easy VPN Remote. Для Easy VPN Remote требуются минимальные настройки. Easy VPN Remote инициирует соединение. Если аутентификация успешна, Easy VPN Server отправляет конфигурацию VPN на Easy VPN Remote. Дополнительные сведения о настройке сетевого экрана PIX как сервера Easy VPN доступны в разделе Управление удаленным доступом VPN.

Динамические криптокарты используются для конфигурации IPsec, когда некоторые параметры, необходимые для настройки VPN, не могут быть определены заранее, как в случае с мобильными пользователями, которые получают динамические IP-адреса. Динамическая криптокарта служит шаблоном, а отсутствующие параметры определяются при согласовании IPsec. Дополнительные сведения о динамических криптокартах доступны в разделе Динамические криптокарты.

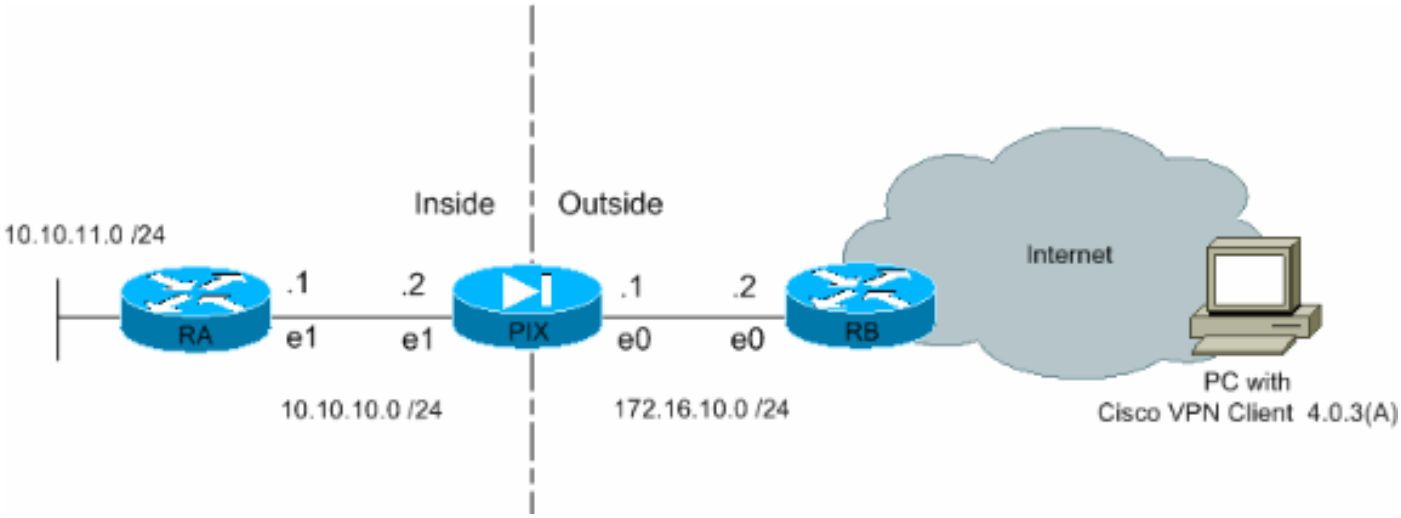
Конфигурации

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:



Настройка PIX

Настройка, необходимая для межсетевого экрана PIX, показана в следующих выходных данных. Эта конфигурация предназначена только для VPN.

PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
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
```

```
!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 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 !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client. isakmp policy 10
authentication pre-share isakmp policy 10 encryption
aes-256 isakmp policy 10 hash sha isakmp policy 10 group
2 isakmp policy 10 lifetime 86400 !--- Create a VPN
group and configure the policy attributes which are !---
downloaded to the Easy VPN Clients. vpngroup
groupmarketing address-pool vpnpool1 vpngroup
groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password ********
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end
```

Примечание: В этой настройке рекомендуется не задать aes 192 при настройке набора преобразований или Политики ISAKMP. VPN-клиенты не поддерживают шифрование aes-192.

Примечание: С более ранними версиями требовались **пул адресов конфигурации клиента isakmp** команд IKE Mode Configuration и **crypto map client configuration address**. Однако с новыми версиями (3.x и более поздние) эти команды больше не нужны. **Множественные пулы адресов теперь можно указать при помощи команды vpngroup address-pool.**

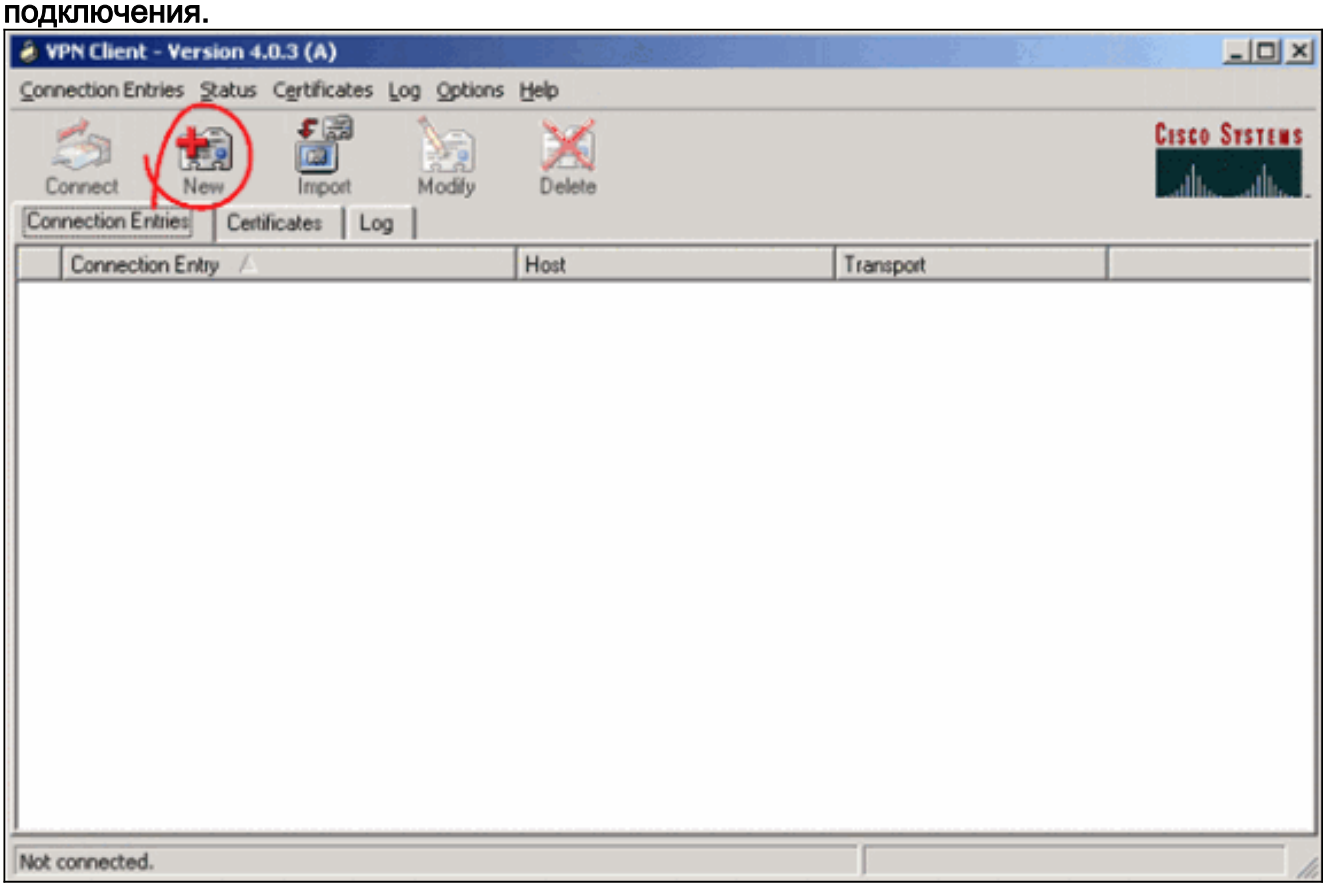
Примечание: Имена групп VPN интерпретируются с учетом регистра символов. Это означает, что аутентификация пользователя не выполнится, если имя группы, указанное в PIX, и имя группы в VPN-клиенте отличаются буквенным регистром (т.е. являются строчными или прописными).

Примечание: Например, при вводе имени группы как **GroupMarketing** в одном устройстве и **groupmarketing** в другом устройстве устройство не работает.

Настройка VPN-клиента

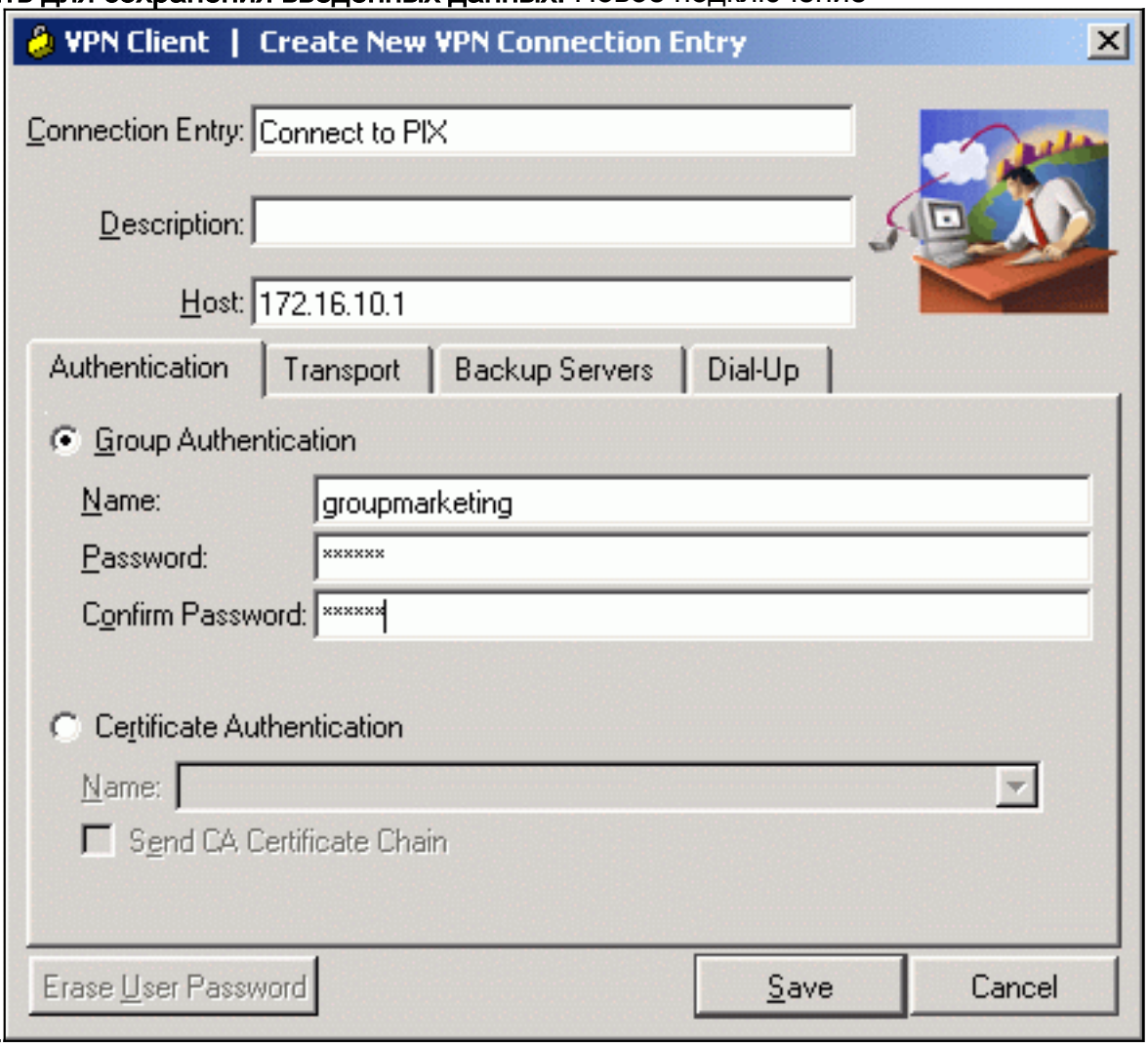
После установки VPN-клиента на ПК создайте новое подключение, как показано ниже:

1. **Запустите приложение VPN Client, а затем нажмите Создать для создания записи нового подключения.**



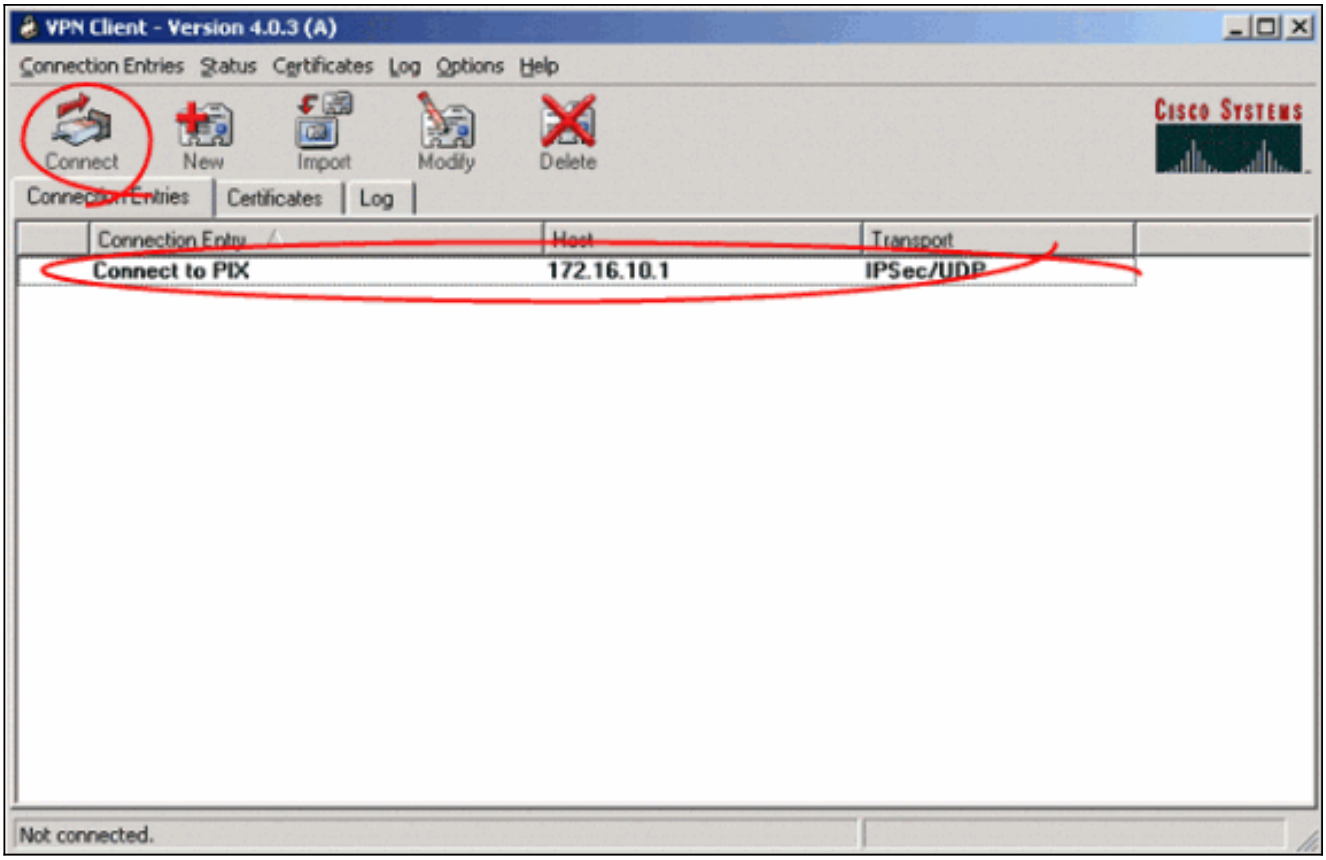
2. Появляется новое диалоговое окно с названием "VPN Client | Create New VPN Connection Entry" (VPN-клиент | Создание записи нового VPN-подключения). Введите сведения о конфигурации нового подключения.В поле "Connection Entry" (Запись подключения) присвойте имя созданной записи.В поле "Host" (Узел) введите IP-адрес общего интерфейса PIX.Откройте вкладку "Authentication" (Аутентификация) и введите

имя группы и пароль (второй раз для подтверждения). **Эти данные должны совпадать с данными, введенными в PIX с помощью команды vpngroup password.Нажмите кнопку Сохранить для сохранения введенных данных.** Новое подключение



создано.

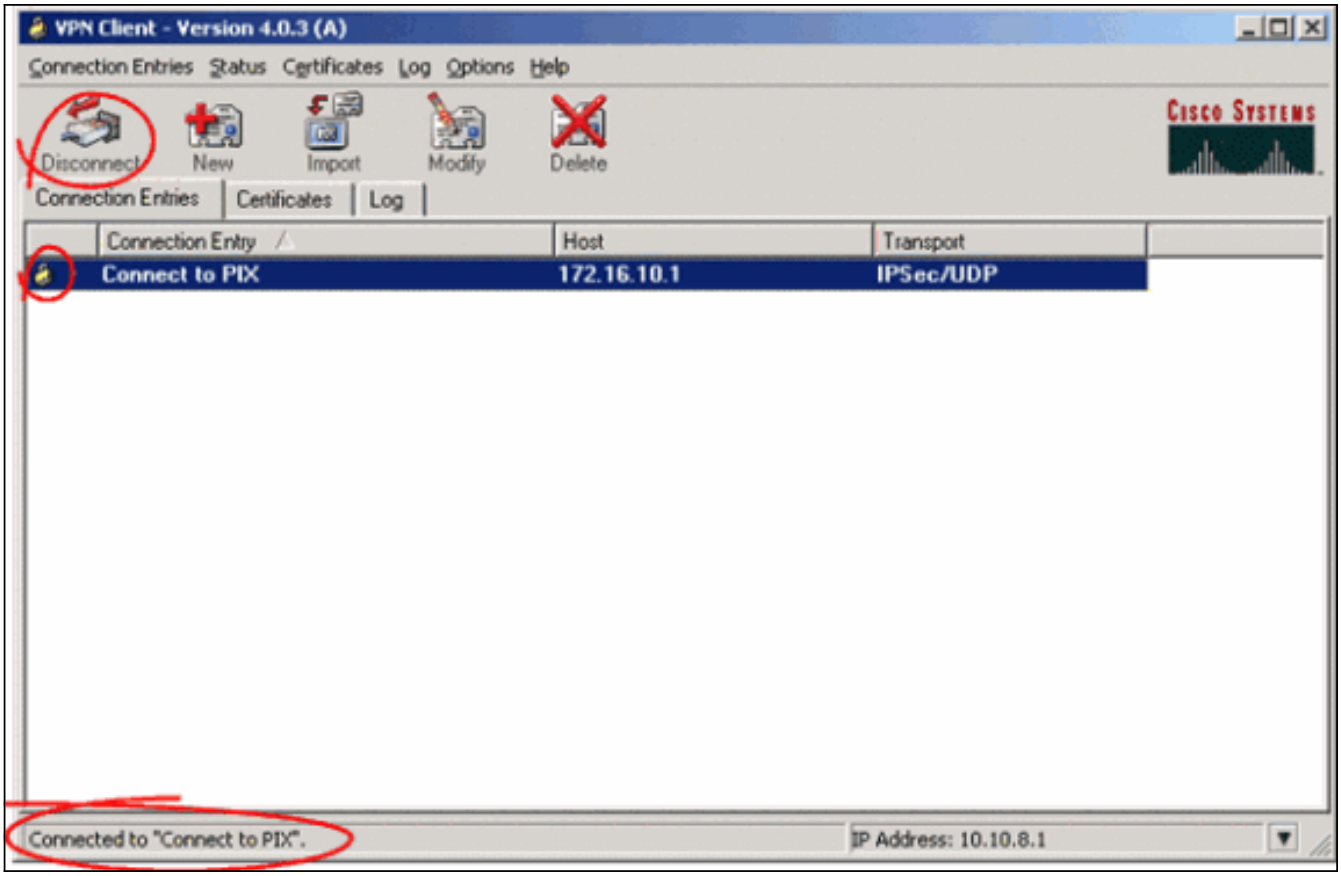
3. **Чтобы подключиться к шлюзу с помощью новой записи подключения, выберите эту запись, щелкнув ее кнопкой мыши, и нажмите на значок Соединение.** Двойной щелчок записи подключения имеет такой же
результат.



Проверка

На VPN-клиенте успешно установленное подключение к удаленному шлюзу указывается следующими элементами:

- Напротив записи об активном соединении появляется желтый значок в виде закрытого замка.
- Значок соединения на панели инструментов (над вкладкой "Connection Entries" (Записи подключений)) меняет состояние на "Disconnect" (Отключить).
- В нижней части окна в строке статуса отображается статус "Connected to" (Подключено) и имя
соединения.



Примечание: По умолчанию после установления соединения VPN Client свертывается в значок закрытого замка в правом нижнем углу панели задач Windows. Чтобы снова сделать окно VPN Client видимым, дважды щелкните значок закрытого замка.

На межсетевом экране PIX команды show могут использоваться для проверки статуса установленных соединений.

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

- **show crypto ipsec sa—Показывает все текущие IPsec SA на PIX.** Кроме того, выходные данные показывают фактический IP-адрес удаленного одноранговового узла, назначенный IP-адрес, локальный IP-адрес и интерфейс, а также применяемую криптокарту.`Pixfirewall#`**`show crypto ipsec sa`** `interface: outside Crypto map tag: map1, local addr. 172.16.10.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0) current_peer: 172.16.12.3:500 dynamic allocated peer ip: 10.10.8.1 PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25 #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.: 172.16.10.1, remote crypto endpt.: 172.16.12.3 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: cbabd0ce inbound esp sas: spi: 0x4d8a971d(1300928285) transform: esp-aes-256 esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: map1 sa timing: remaining key lifetime (k/sec): (4607996/28685) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xcbabd0ce(3417034958) transform: esp-aes-256 esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: map1 sa timing: remaining key lifetime (k/sec): (4608000/28676) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas:`
- **show crypto isakmp sa—Показывает статус ISAKMP SA, установленных между одноранговыми узлами.**`Pixfirewall#`**`show crypto isakmp sa`** `Total : 1 Embryonic : 0 dst src state pending created 172.16.10.1 172.16.12.3 QM_IDLE 0 1`

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды отладки могут помочь в устранении неполадок при настройке VPN.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **debug crypto isakmp—Показывает установленные ISAKMP SA и согласованные атрибуты IPsec.** При согласовании ISAKMP SA PIX может отбросить несколько предложений как "неприемлемые", перед тем как принять одно из них. Как только ISAKMP SA согласовано, согласовываются атрибуты IPSec. **Повторим, несколько предложений могут быть отклонены перед тем как одно из них будет принято, как показано в выходных данных команды debug ниже.**

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 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: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP:
life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP: keylength of
256 !--- Proposal is rejected since extended auth is not configured. 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: hash MD5 ISAKMP: default group 2 ISAKMP:
extended auth pre-share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI) of
0x0 0x20 0xc4 0x9b ISAKMP: keylength of 256 !--- Proposal is rejected since MD5 is not
specified as the hash algorithm. 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: hash SHA ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in
seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP: keylength of 256 !--- This
proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are acceptable.
Next payload is 3 ISAKMP (0): processing KE payload. message ID = 0 !--- Output is
suppressed. OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA
payload. message ID = 3348522173 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1,
ESP_AES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: key
length is 256 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration
(VPI) of 0x0 0x20 0xc4 0x9b !--- This proposal is not accepted since transform-set !---
trmset1 does not use MD5. ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0):
skipping next ANDed proposal (1) ISAKMP : Checking IPSec proposal 2 ISAKMP: transform 1,
ESP_AES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: key
length is 256 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration
(VPI) of 0x0 0x20 0xc4 0x9b !--- This proposal is accepted since it matches !--- transform-
set trmset1. ISAKMP (0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP :
Checking IPSec proposal 3 !--- Output is suppressed.
```

- **debug crypto ipsec—Отображает информацию о согласовании IPsec SA.**

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with     172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
```

```
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
        from     172.16.12.3 to     172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4
```

С конфигурациями, показанными в этом документе, VPN-клиент может успешно подключаться к PIX центрального узла, используя AES. Иногда наблюдается ситуация, когда даже при успешной установке VPN-туннеля пользователи не могут выполнять обычные задачи, например эхо-запросы сетевых ресурсов, вход в домен или просмотр сетевого окружения. Дополнительные сведения по устранению данных проблем доступны в документе "Устранение проблем сетевого окружения Microsoft после установки туннеля VPN с клиентом Cisco VPN".

Дополнительные сведения

- Улучшенный стандарт шифрования (AES)
- Введение в шифрование IPSec
- Устранение проблем IPSec — общие сведения и использование команд debug
- Страница технической поддержки протоколов согласования IPSec и IKE
- Страница поддержки PIX
- Страница поддержки Cisco VPN Client
- Справочник по командам PIX
- Cisco Systems – техническая поддержка и документация