Пример конфигурации "Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling"

Содержание

Введение

В этом документе приведены пошаговые инструкции, как разрешить клиентам VPN доступ в Интернет в то время, как их трафик туннелируется в маршрутизатор Cisco IOS®. Эта конфигурация необходима, чтобы разрешить клиентам VPN безопасный доступ к корпоративным ресурсам через IPsec и в то же время разрешить небезопасный доступ в Интернет. Эта конфигурация называется раздельным туннелированием.

Примечание. Раздельное туннелирование может представлять угрозу безопасности. Поскольку клиенты VPN получают небезопасный доступ в Интернет, они могут подвергаться атакам. И в случае успешной атаки злоумышленник сможет получить доступ к корпоративной сети через туннель IPsec. В качестве компромисса между полным и раздельным туннелированием можно разрешить клиентам VPN только доступ к локальной сети. Дополнительные сведения см. в разделе PIX/ASA 7.x: Пример конфигурации, разрешающей клиентам VPN доступ к локальной сети.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

Маршрутизатор Cisco Router 3640 с ПО Cisco IOS версии 12.4

Cisco VPN Client 4.8

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

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 данном примере устройством центрального узла является маршрутизатор Cisco IOS, в котором используются динамические криптокарты.

При включении раздельного туннелирования для VPN-соединений требуется настроить список контроля доступа (ACL) на маршрутизаторе. В этом примере команда **access-list 101** связана с группой для раздельного туннелирования, а в сети 10.10.10.x/24 формируется туннель. Незашифрованный трафик (например Интернет), поступающий на устройства, исключается из сетей, настроенных в ACL 101.

```
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Применение списка управления доступом к свойствам группы.

```
crypto isakmp client configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl 101
```

В этом примере конфигурации туннель IPsec настроен со следующими элементами:

Криптокарты, применяемые к внешним интерфейсам PIX.

Расширенная аутентификация (Xauth) клиентов VPN вместо локальной аутентификации

Динамическое назначение частного IP-адреса из пула для клиентов VPN

Функциональность команды **nat 0 access-list** позволяет узлам локальной сети использовать частные IP-адреса для удаленных пользователей и при этом получить NAT-адрес от PIX для доступа к ненадежным сетям.

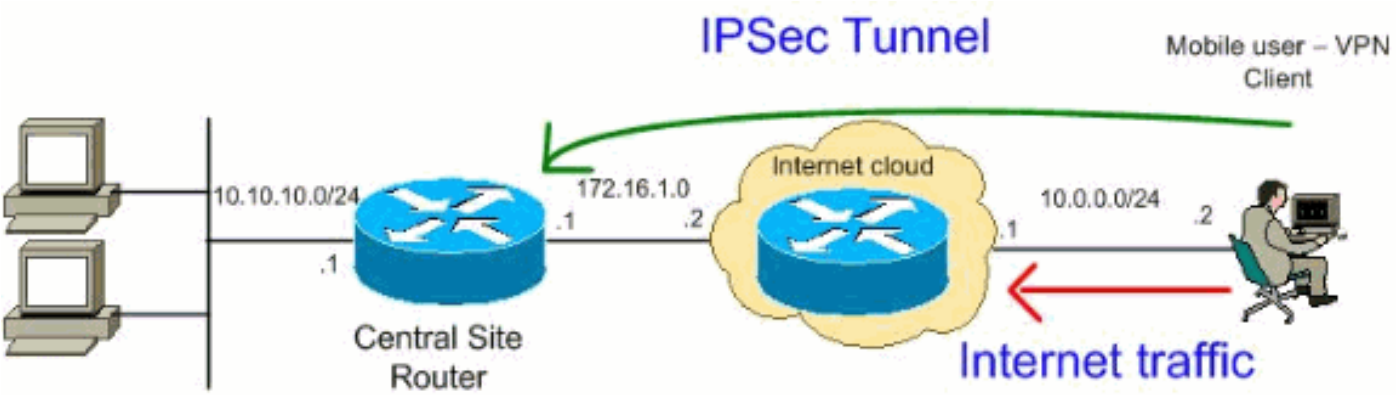
Настройка

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

Примечание. Для поиска дополнительной информации о командах, приведенных в данном документе, используйте инструмент Средство поиска команд (только для зарегистрированных пользователей).

Схема сети

В настоящем документе используется следующая схема сети:



Примечание. Схемы IP-адресации, используемые в этой конфигурации, нельзя использовать для маршрутизации в Интернете. Это адреса RFC 1918 , которые использовались в лабораторной среде.

Варианты конфигурации

В этом документе используются следующие конфигурации:

- Маршрутизатор
- Cisco VPN Client

Маршрутизатор

```
VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
```

```
!
boot-start-marker
boot-end-marker
!
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.


aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!--- For local authentication of the IPsec user, !---
create the user with a password. username user password
0 cisco
!
!
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2

!--- Create a group that is used to specify the !---
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. Use
ACL 101 used for !--- the Split tunneling in the VPN
Clinet end. crypto isakmp client configuration group
vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl 101
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
 set transform-set myset
 reverse-route
!

!--- Create the actual crypto map, !--- and apply the
```

```
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside

!--- Apply the crypto map on the outbound interface.
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map clientmap
!
interface Serial2/0
 no ip address
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ! ip local pool ippool 192.168.1.1
192.168.1.2
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 111
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 111 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic !-
-- is to be translated for the outside Internet.
access-list 111 deny ip 10.10.10.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 111 permit ip any any


!--- Configure the interesting traffic to be encrypted
from the VPN Client !--- to the central site router
(access list 101). !--- Apply this ACL in the ISAKMP
configuration. access-list 101 permit ip 10.10.10.0
0.0.0.255 192.168.1.0 0.0.0.255
```

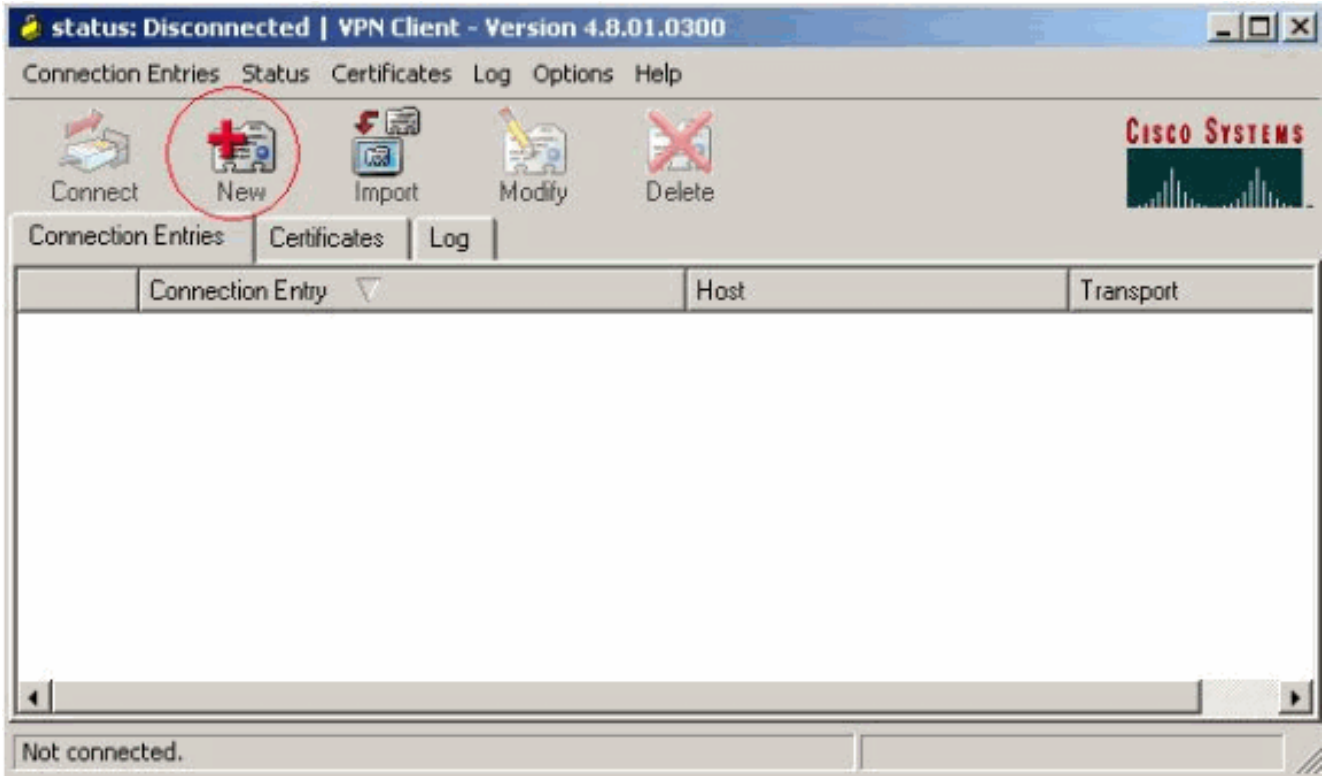
```
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

Настройка VPN Client 4.8

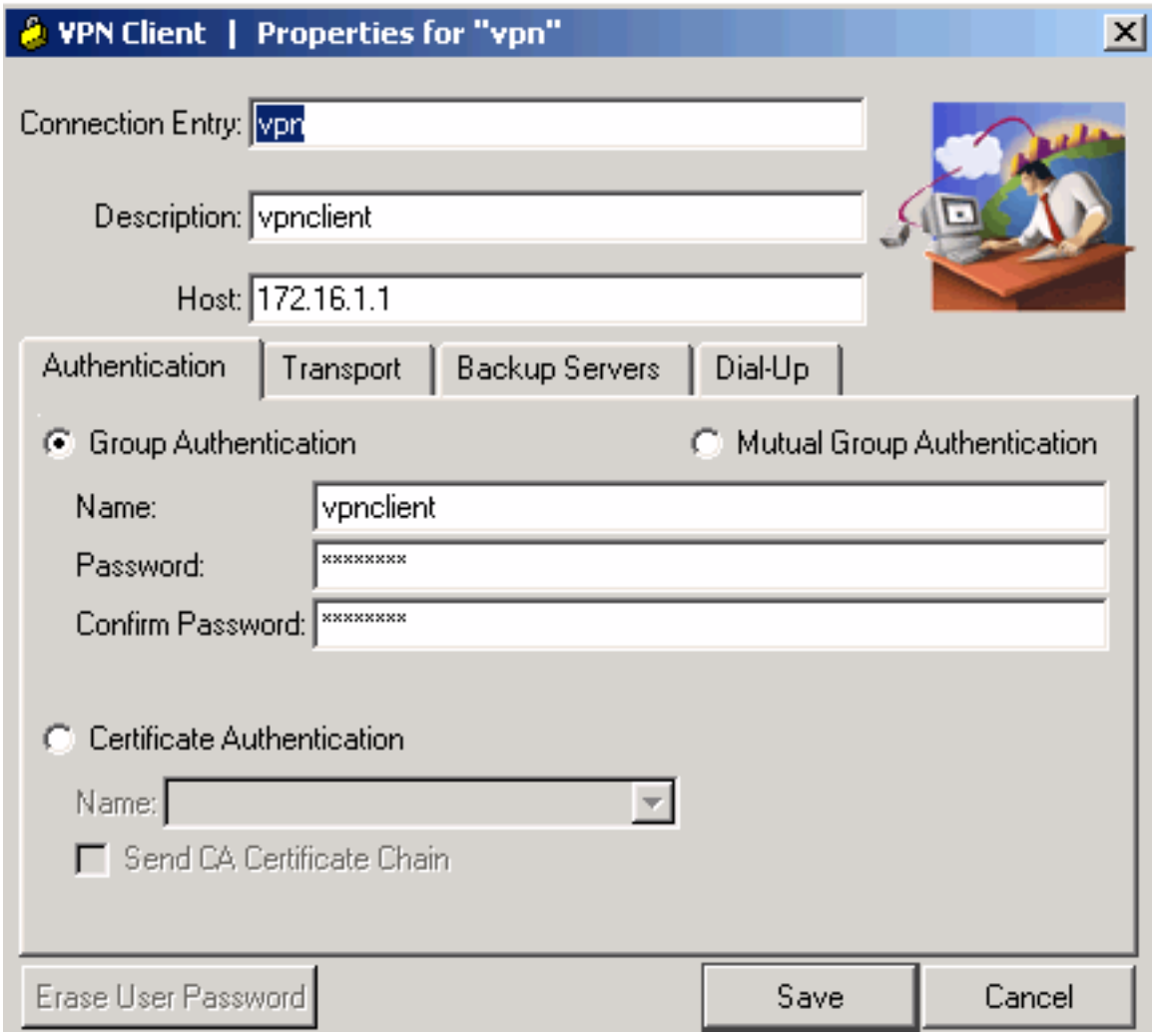
Чтобы настроить VPN Client 4.8, выполните следующие действия.

Выберите **Пуск > Программы > Cisco Systems VPN Client > VPN Client**.

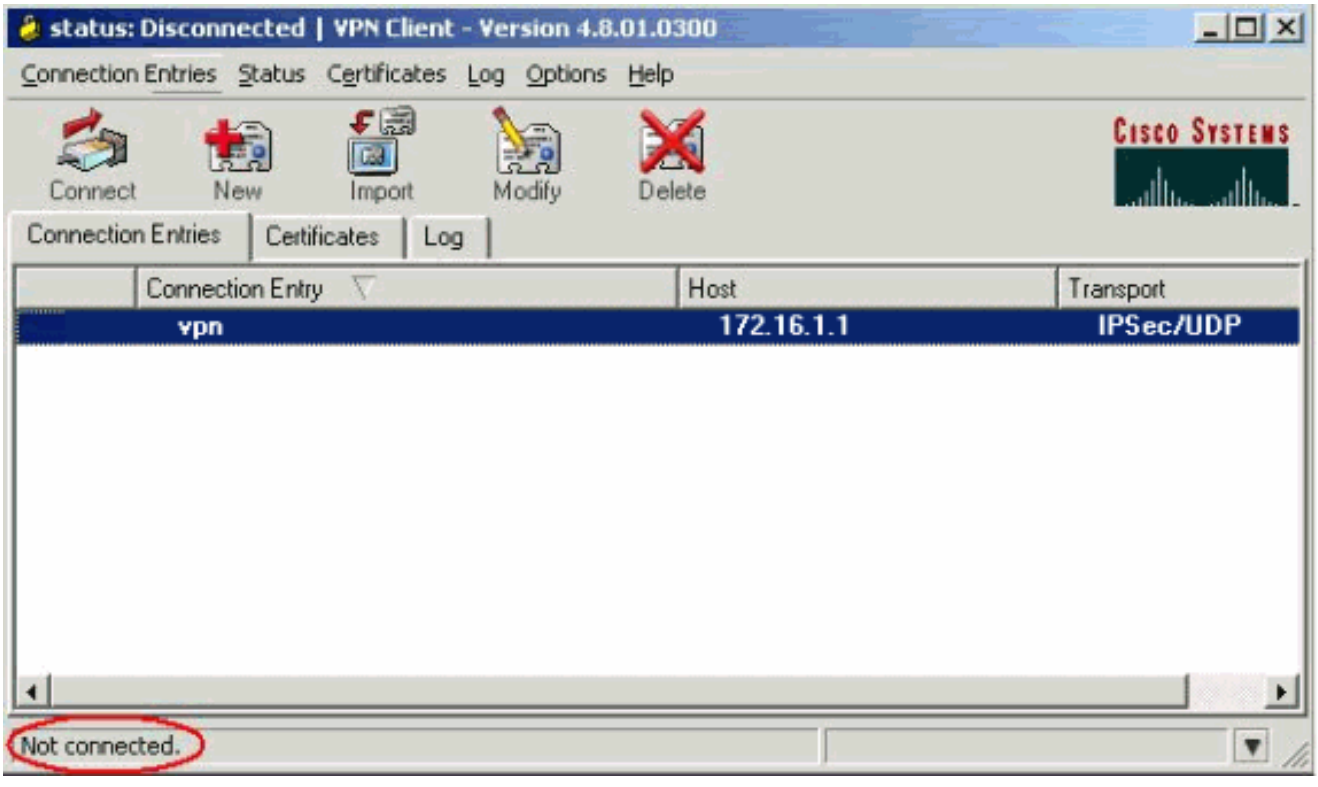
Нажмите **New**, чтобы открыть окно "Create New VPN Connection Entry" (Создание новой записи VPN-соединения).



Введите имя записи подключения и его описание, а также внешний IP-адрес маршрутизатора в поле "Host" и имя и пароль группы VPN. Нажмите **Save**.

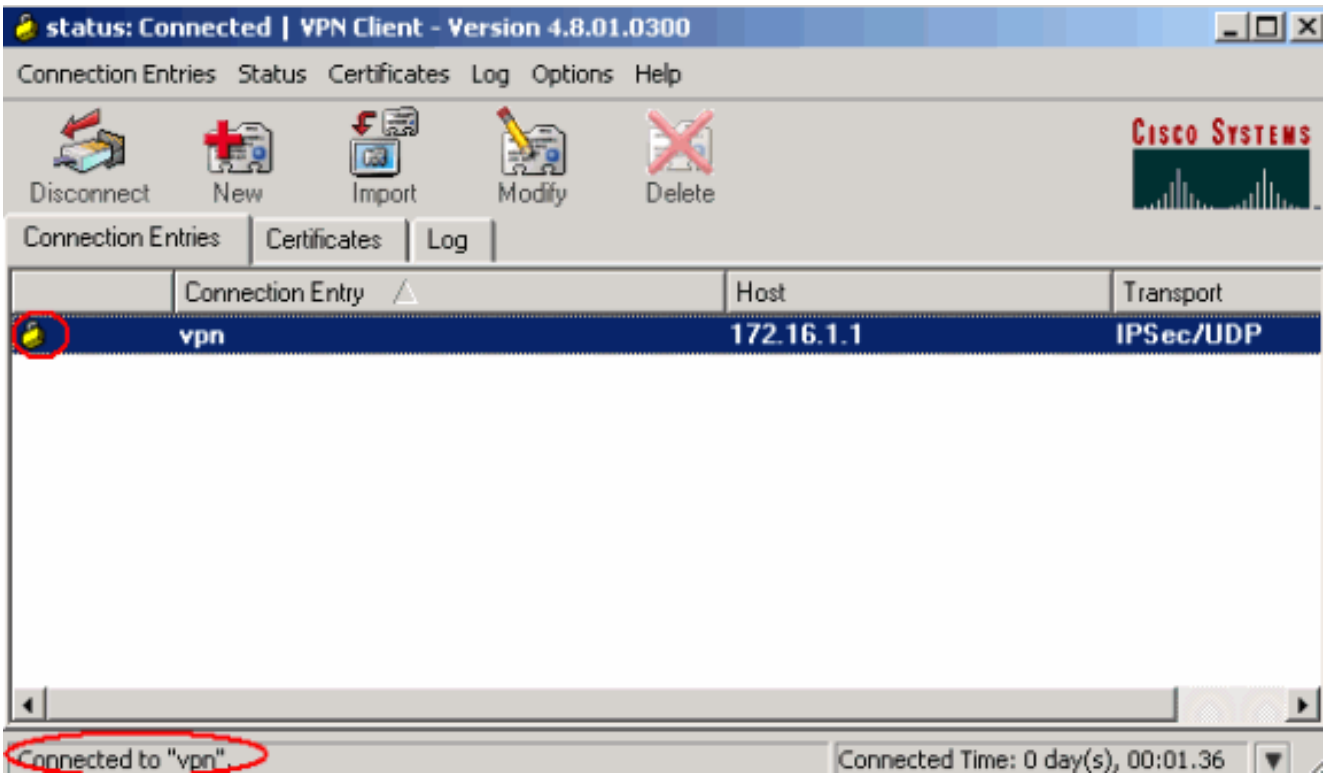


Выберите подключение, которое необходимо использовать, и нажмите **Connect** в главном окне VPN Client.

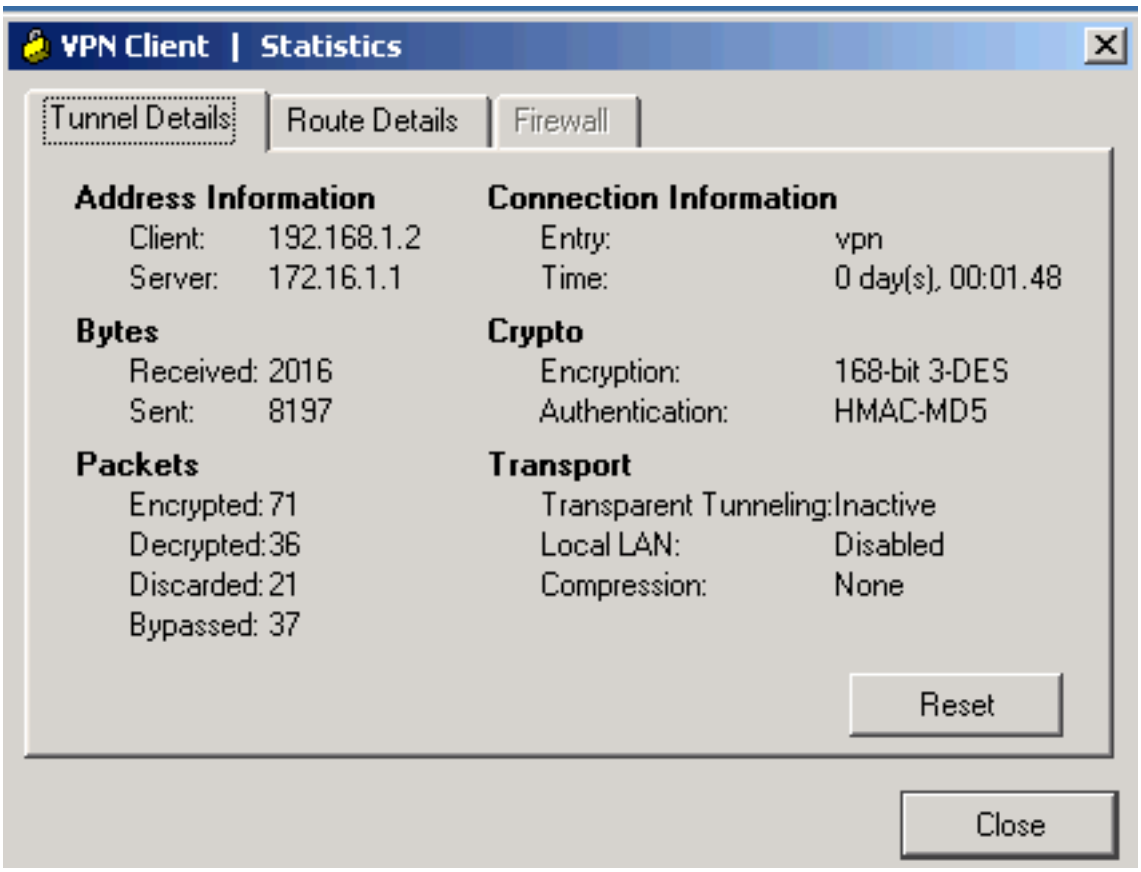


При появлении соответствующего запроса введите имя пользователя и пароль для аутентификации Xauth и нажмите **OK** для подключения к удаленной сети.

ПО VPN Client соединится с маршрутизатором на центральном узле.

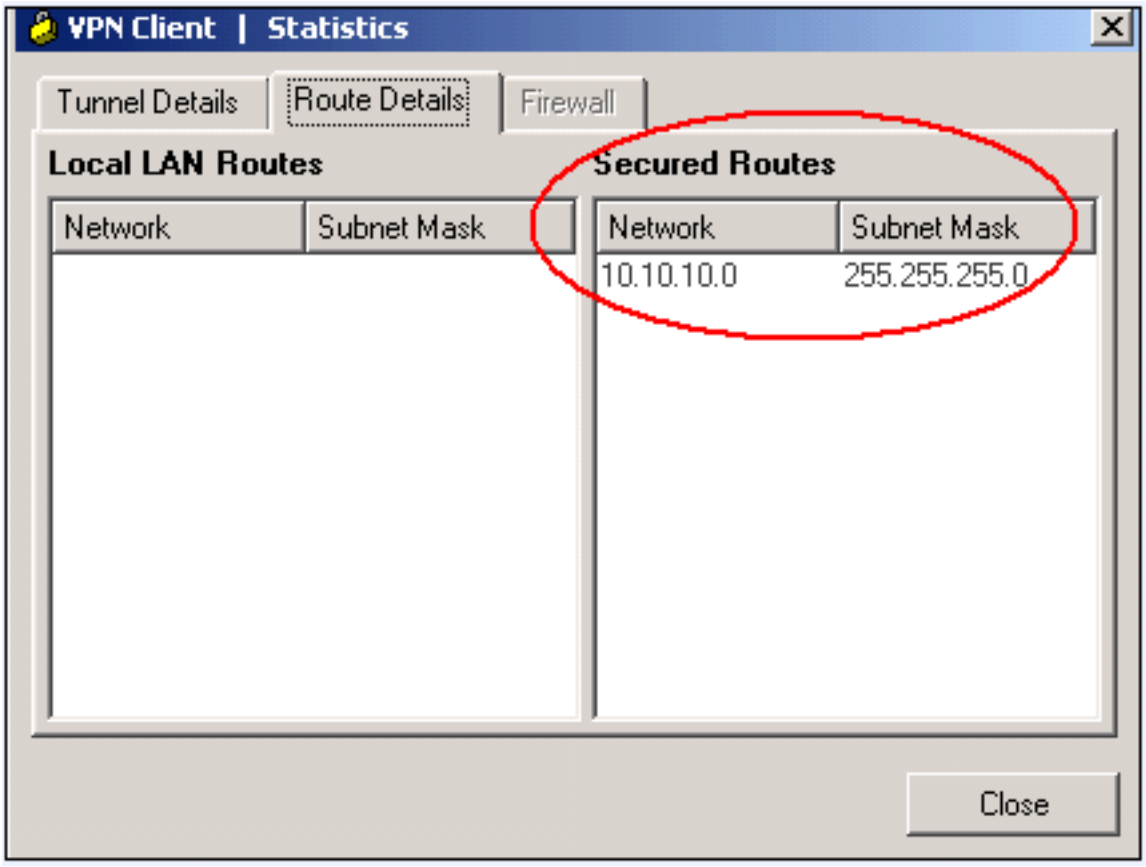


Выберите **Status > Statistics**, чтобы проверить статистику туннеля для VPN Client.



Перейдите на вкладку "Route Details" (Сведения о маршруте), чтобы увидеть маршруты маршрутизатору, защищенные клиентом VPN.

В этом примере клиент VPN защищает доступ к сети 10.10.10.0/24, а весь остальной трафик не шифруется и не отправляется по туннелю. Защищенная сеть загружается из ACL 101, который настроен на маршрутизаторе центрального узла.



Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Интерпретатор выходных данных – OIT (только для зарегистрированных пользователей) поддерживает ряд команд **show**. Посредством OIT можно анализировать выходные данные команд **show**.

show crypto isakmp sa—отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле.

```
VPN#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: clientmap, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={}
    #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
    #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0xEF7C20EA(4017889514)

inbound esp sas:
 spi: 0x17E0CBEC(400608236)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2001, flow_id: SW:1, crypto map: clientmap
   sa timing: remaining key lifetime (k/sec): (4530341/3288)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xEF7C20EA(4017889514)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2002, flow_id: SW:2, crypto map: clientmap
   sa timing: remaining key lifetime (k/sec): (4530354/3287)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

show crypto ipsec sa—отображает параметры, используемые текущими SA.

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE              15    0 ACTIVE
```

Устранение неполадок

Команды для устранения неполадок

Интерпретатор выходных данных – OIT (только для зарегистрированных пользователей) поддерживает ряд команд **show**. Посредством OIT можно анализировать выходные данные команд **show**.

Примечание. Перед использованием команд **debug** обратитесь к документу Важные сведения о командах отладки.

debug crypto ipsec—отображает согласования протокола IPsec на 2-м этапе.

debug crypto isakmp—отображает согласования ISAKMP на 1-м этапе.

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Клиент Cisco VPN – Поддержка продукта
- Маршрутизатор Cisco — Поддержка продукта
- Cisco Systems – техническая поддержка и документация