Пример настройки маршрутизатора и клиента VPN для общедоступной сети Интернет "on a Stick"

Содержание

Введение

В этом документе приводятся инструкции по настройке центрального маршрутизатора для обработки мобильного трафика IPsec. Эта установка применяется в особой ситуации, в которой маршрутизатор (без раздельного туннелирования) и мобильные пользователи (Cisco VPN Client) могут получать доступ в Интернет через центральный маршрутизатор. Чтобы достичь этого, настройте карту политик маршрутизатора на пересылку всего трафика VPN (Cisco VPN Client) в интерфейс возвратной петли. Это позволяет выполнять преобразование адресов портов (PAT) Интернет-трафика во внешние сети.

См. сведения об аналогичной конфигурации брандмауэра PIX на центральном узле в документе Пример конфигурации PIX/ASA 7.x и Cisco VPN Client для организации мобильного доступа в общедоступный Интернет.

Примечание: Во избежание наложения IP-адресов в сети назначьте совершенно другой пул IP-адресов Клиенту VPN (например, 10. x. x. x, 172.16. x. x, 192.168. x. x. Эта схема IP-адресации помогает вам устранять неполадки своей 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 3640 с выпуском 12.4 программного обеспечения Cisco IOS
- Cisco VPN Client 4.8

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.

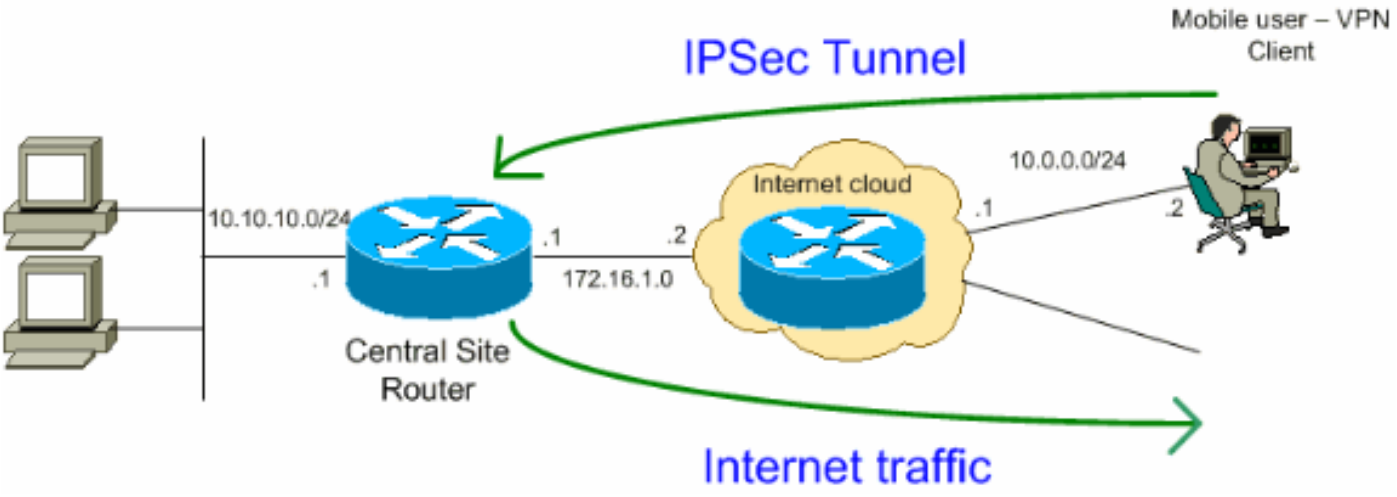
Настройка

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:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Конфигурации

Эти конфигурации используются в данном документе:

- Маршрутизатор
- Cisco VPN Client

Маршрутизатор

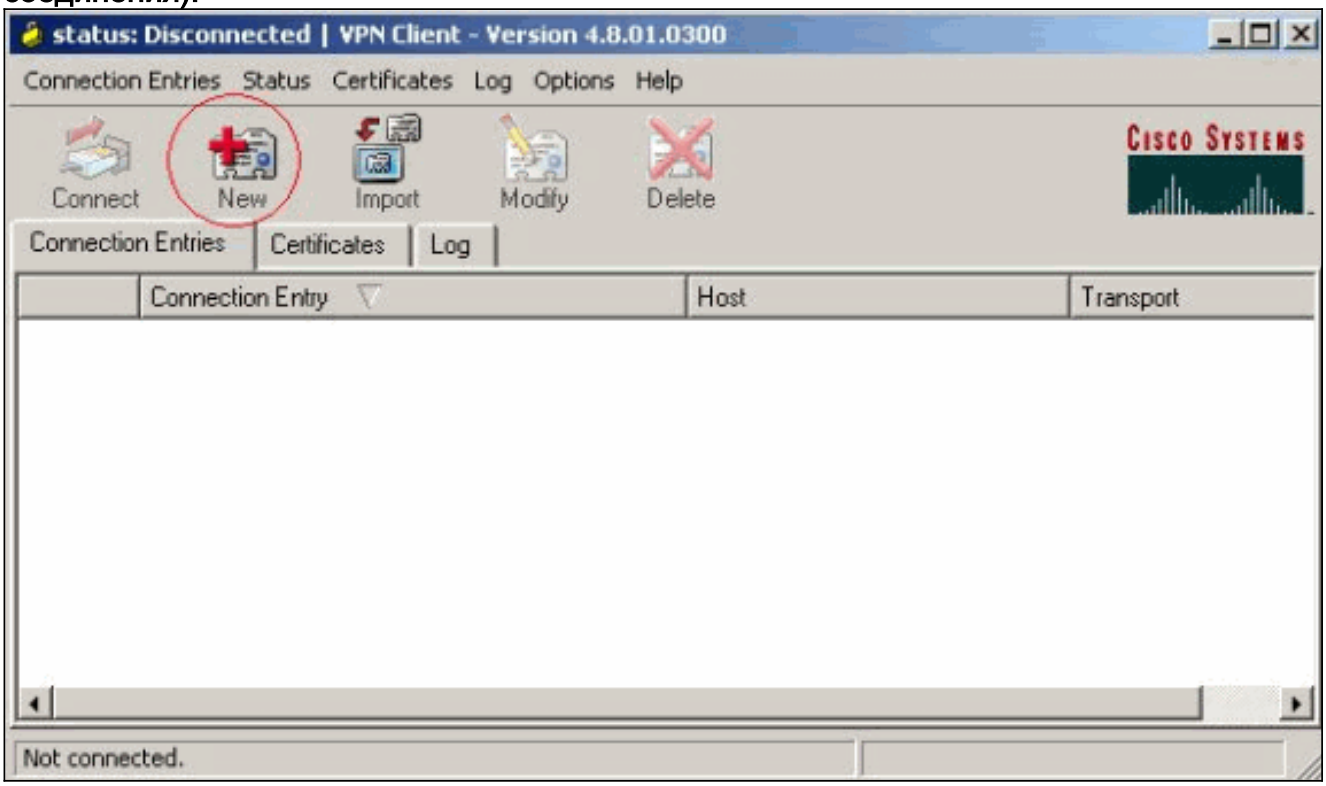
```
VPN#show run Building configuration... Current configuration : 2170 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname VPN ! boot-start-marker boot-end-marker ! ! !--- Enable authentication, authorization and 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. crypto isakmp client configuration group vpnclient key cisco123 dns 10.10.10.10 wins 10.10.10.20 domain cisco.com pool ippool ! !--- 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 ! ! ! ! !--- Create the loopback interface for the VPN user traffic . interface Loopback0 ip address 10.11.0.1 255.255.255.0 ip nat inside ip virtual-reassembly ! interface Ethernet0/0 ip address 10.10.10.1 255.255.255.0 half-duplex ip nat inside !--- Apply the crypto map on the interface. interface FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip nat outside ip virtual-reassembly ip policy route-map VPN-Client 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 10.0.0.0 255.255.255.0 172.16.1.2 !--- Enables Network Address Translation (NAT) !--- of the inside source address that matches access list 101 !--- and gets PATed with the FastEthernet IP address. ip nat inside source list 101
```

```
interface FastEthernet1/0 overload ! !--- The access
list is used to specify which traffic is to be
translated for the !--- outside Internet. access-list
101 permit ip any any !--- Interesting traffic used for
policy route. access-list 144 permit ip 192.168.1.0
0.0.0.255 any !--- Configures the route map to match the
interesting traffic (access list 144) !--- and routes
the traffic to next hop address 10.11.0.2. ! route-map
VPN-Client permit 10 match ip address 144 set ip next-
hop 10.11.0.2 ! ! control-plane ! line con 0 line aux 0
line vty 0 4 ! end
```

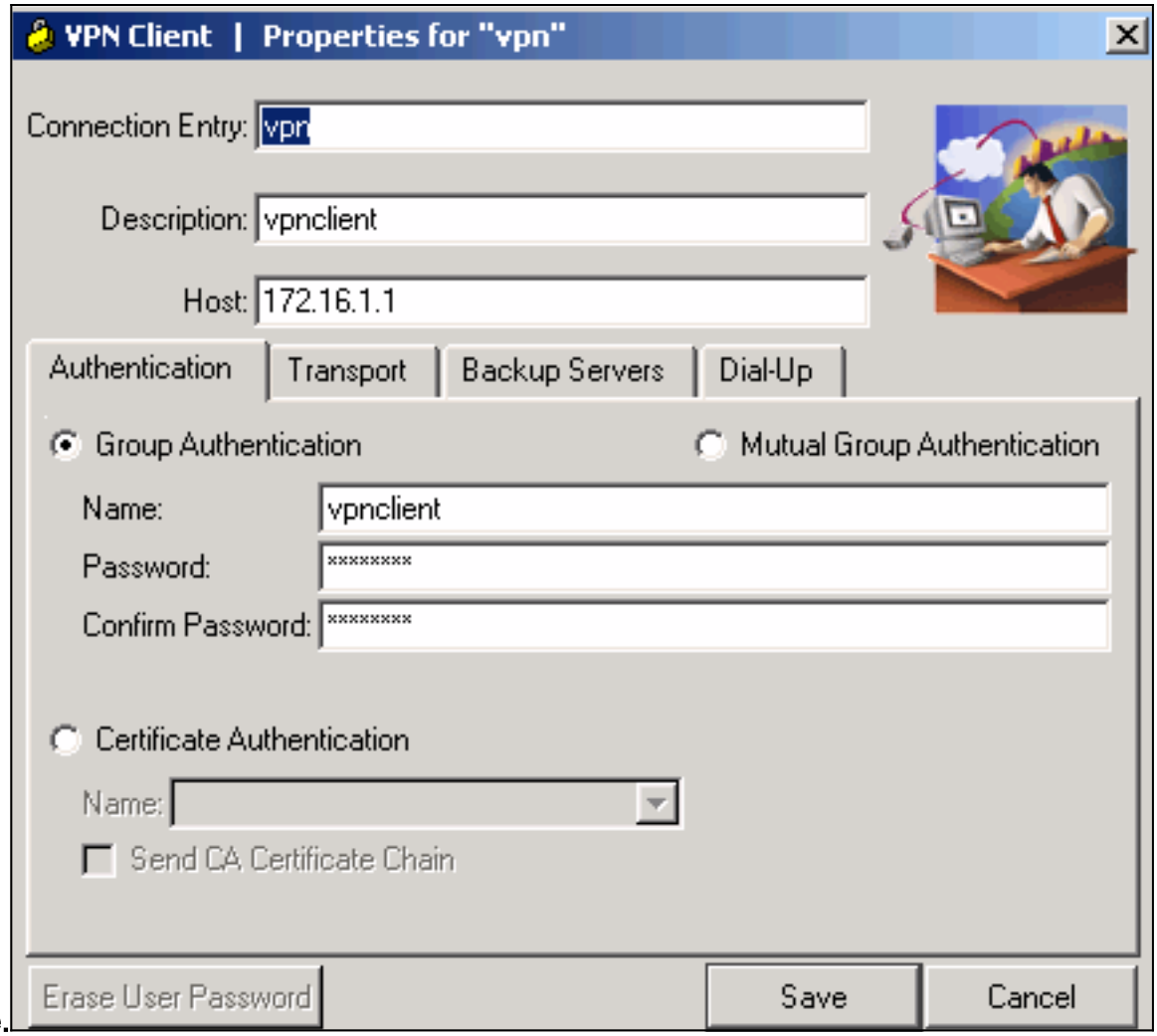
Настройка VPN Client 4.8

Чтобы настроить VPN Client 4.8, выполните следующие действия.

1. **Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client.**
2. **Нажмите New, чтобы открыть окно "Create New VPN Connection Entry" (Создание новой записи VPN-соединения).**

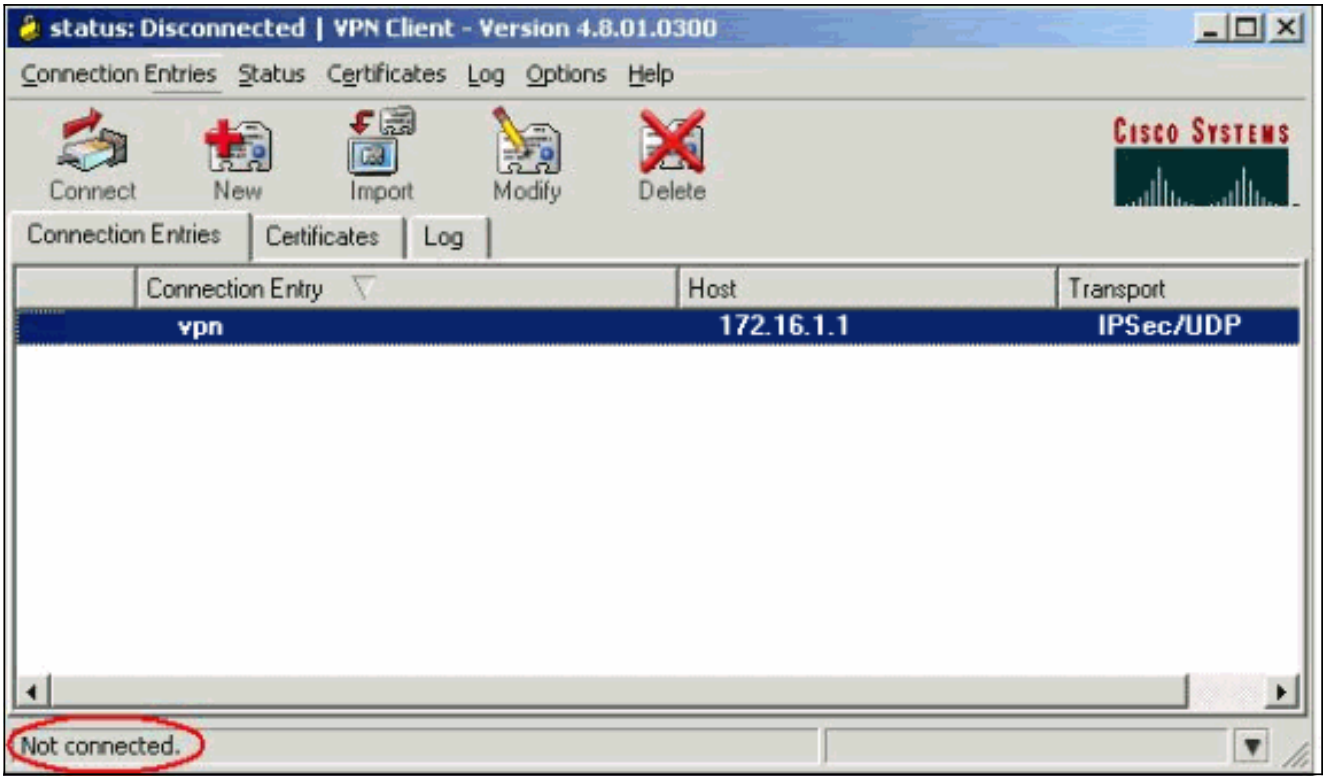


3. Введите имя записи подключения и его описание, а также внешний IP-адрес маршрутизатора в поле "Host" и имя и пароль группы VPN. **Нажмите**



Save.

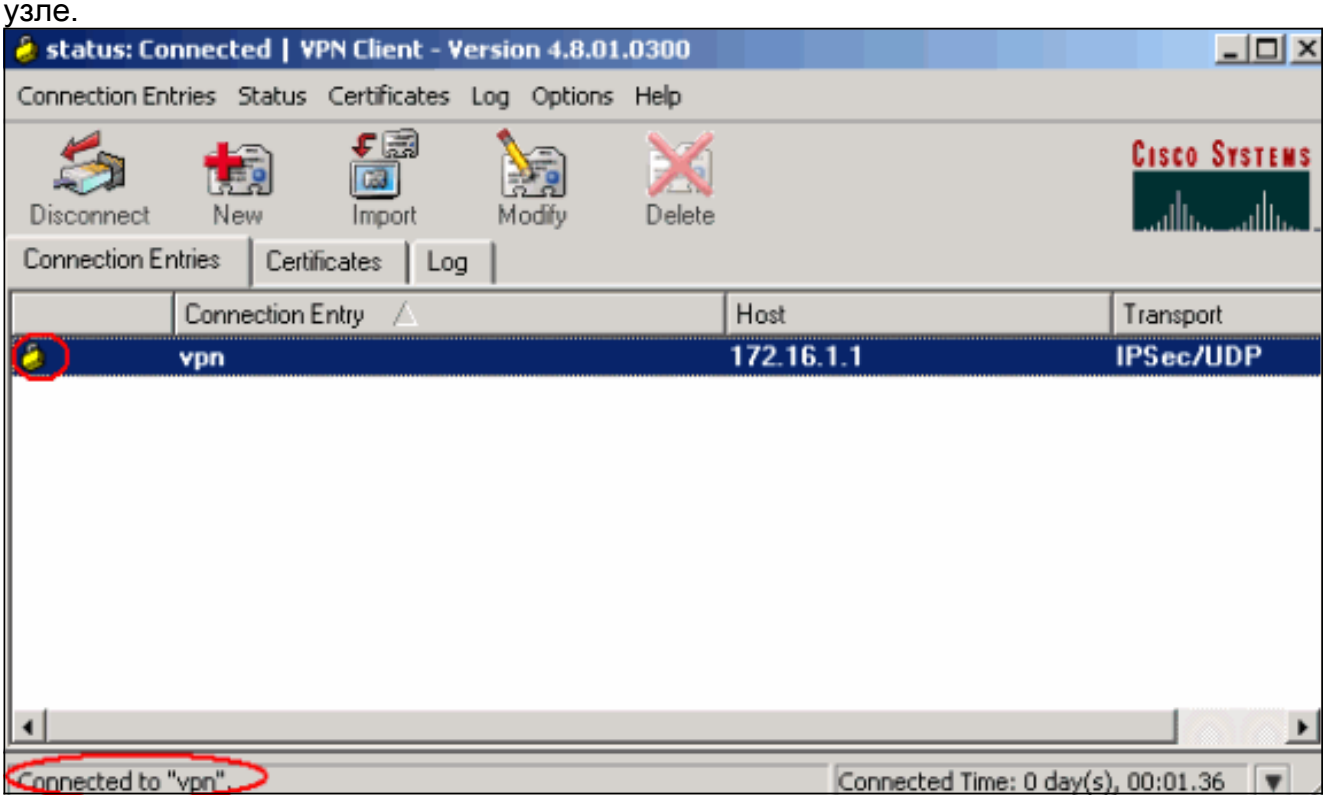
4. Выберите подключение, которое необходимо использовать, и нажмите Connect в главном окне VPN Client.



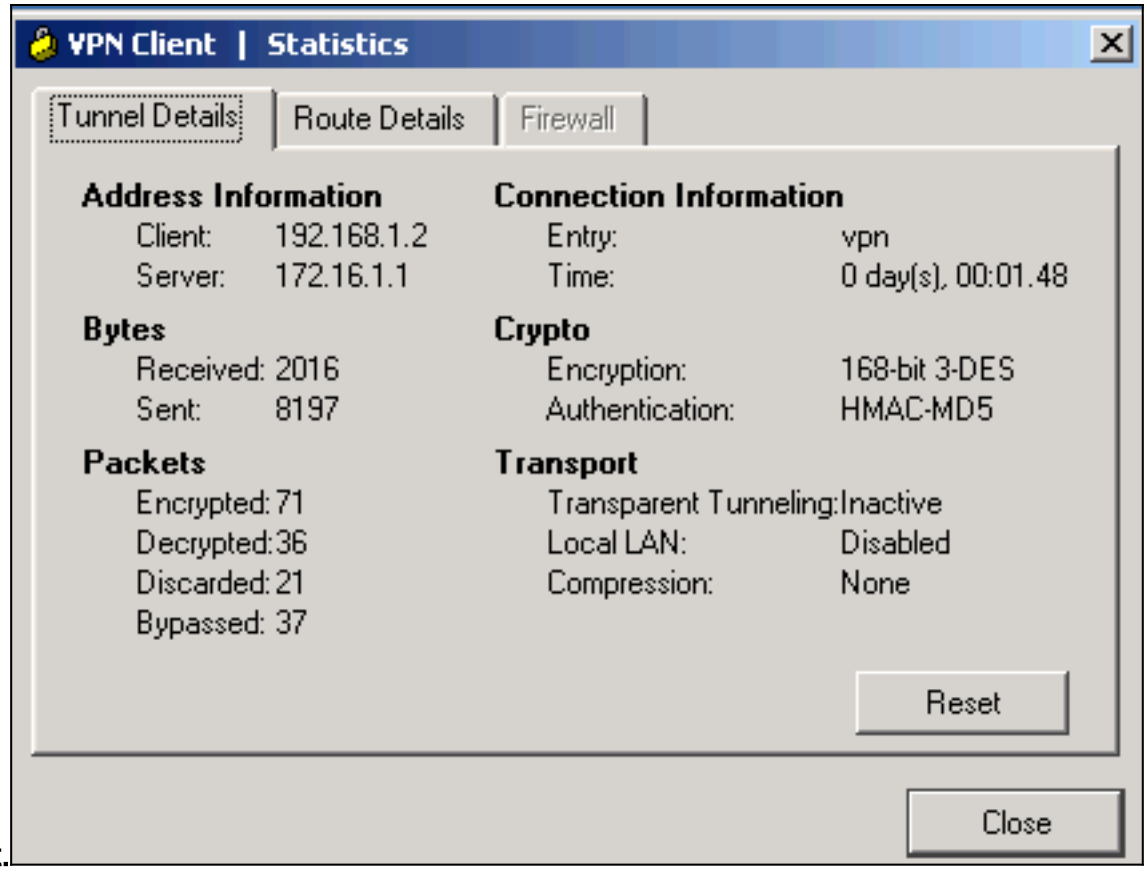
5. При появлении соответствующего запроса введите имя пользователя и пароль для аутентификации Xauth и нажмите OK для подключения к удаленной

сети.

6. ПО VPN Client соединится с маршрутизатором на центральном узле.



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



Client.

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

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

- show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.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

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

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- debug crypto ipsec – отображает согласования IPSec на Этапе 2.
- 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