ASA/PIX: Пример настройки статической IP-адресация для клиента IPSec VPN с CLI и ASDM

Содержание

Введение

Этот документ описывает, как настроить Устройство адаптивной защиты (ASA) серии 5500 Cisco для обеспечения Статического IP - адреса клиенту VPN с Менеджером устройств адаптивной безопасности (ASDM) (ASDM) или CLI. Программа ASDM предоставляет возможность качественного управления и контроля за безопасностью с помощью интуитивно понятного и простого в использовании web-интерфейса управления. Как только конфигурация Cisco ASA завершена, она может быть проверена с Cisco VPN Client.

См. PIX/ASA 7.x и Cisco VPN Client 4.x с Windows 2003 IAS RADIUS (Против Active Directory) Пример Конфигурации аутентификации для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7. x. Пользователь удаленного клиента VPN аутентифицируется против Active Directory с сервером RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года.

См. PIX/ASA 7.x и Cisco VPN Client 4.x для Примера Конфигурации аутентификации Cisco Secure ACS для устанавливания соединения VPN для удаленного доступа между Cisco VPN

Client (4.x для Windows) и устройством защиты PIX 500 Series 7.x с сервером Cisco Secure Access Control Server (Версия ACS 3.2) для расширенной проверки подлинности (XAUTH).

Предварительные условия

Требования

В этом документе предполагается, что устройство адаптивной защиты полностью исправно и в нем разрешено изменение конфигурации с помощью Cisco ASDM или интерфейса командной строки.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM или PIX/ASA 7. x: Пример настройки SSH на внутреннем и внешнем интерфейсах для удаленной настройки устройства по протоколам ASDM или Secure Shell (SSH).

Используемые компоненты

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

- ПО устройств адаптивной защиты Cisco версии 7.x и более поздних версий
- Менеджер устройств адаптивной безопасности (ASDM) Версайон 5.x и позже
- Cisco VPN Client версии 4.x или выше

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.

Родственные продукты

Эти настройки также могут быть использованы в устройствах защиты Cisco PIX, начиная с версий 7.x.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

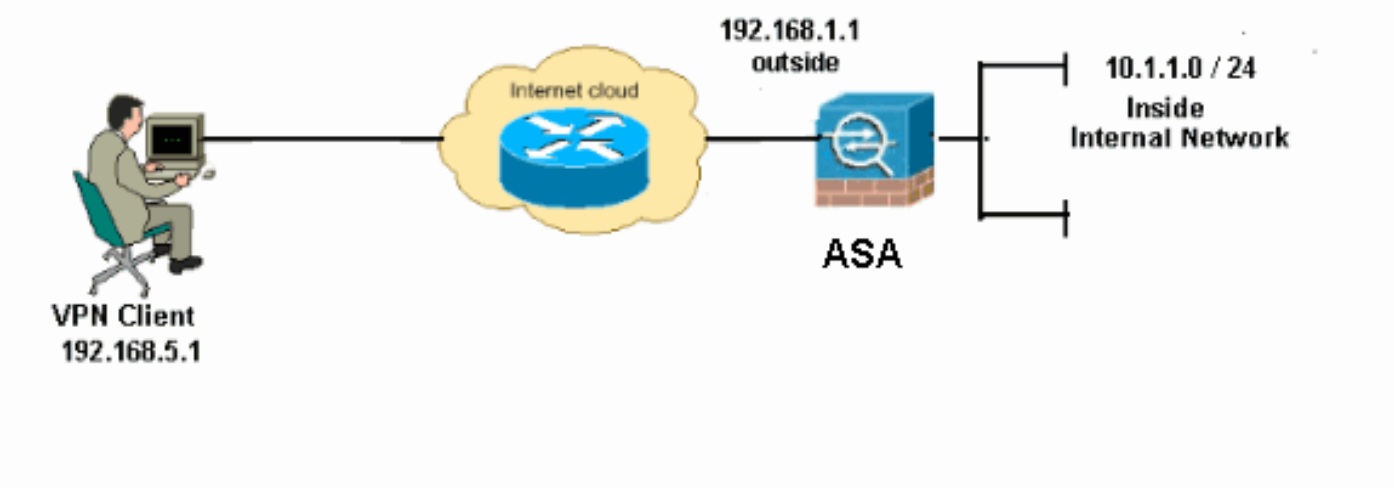
Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



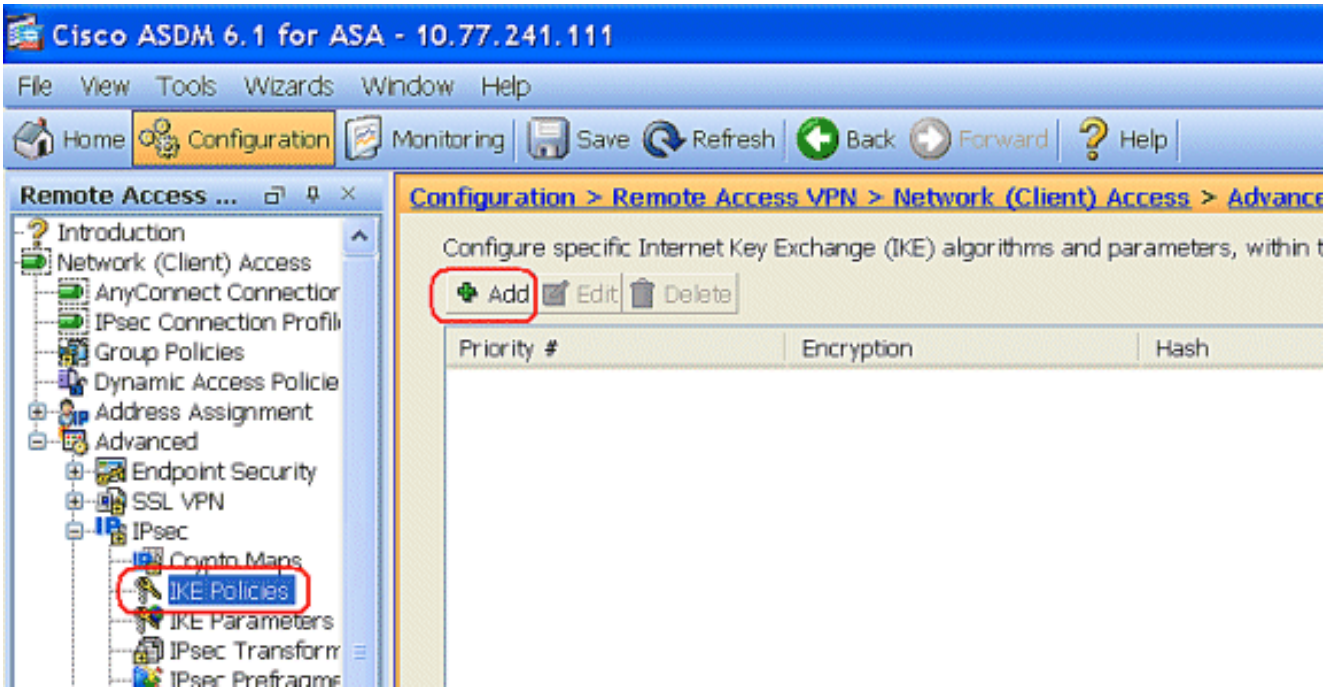
Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Настройка VPN для удаленного доступа (IPSec)

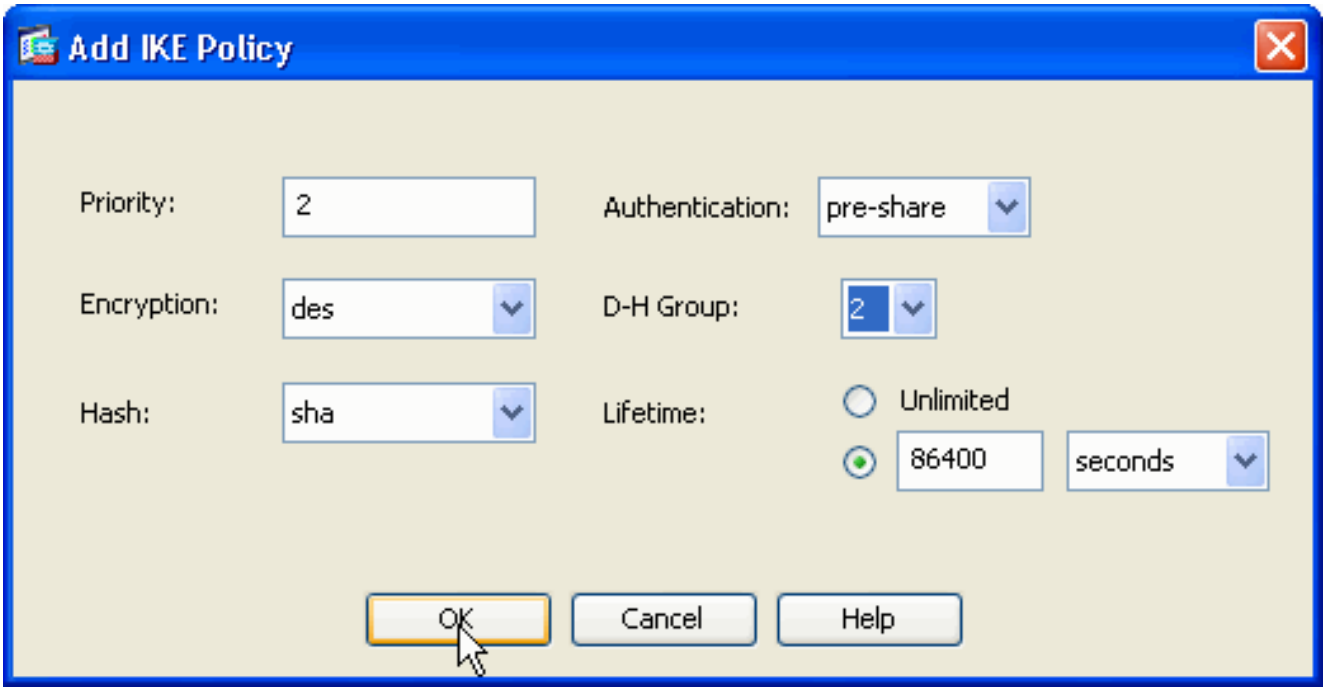
Порядок действий в диспетчере ASDM

Выполните эти шаги, чтобы настроить удаленный доступ через сеть VPN:

1. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> IPSec> IKE Policies> Add** для создания Политики ISAKMP.

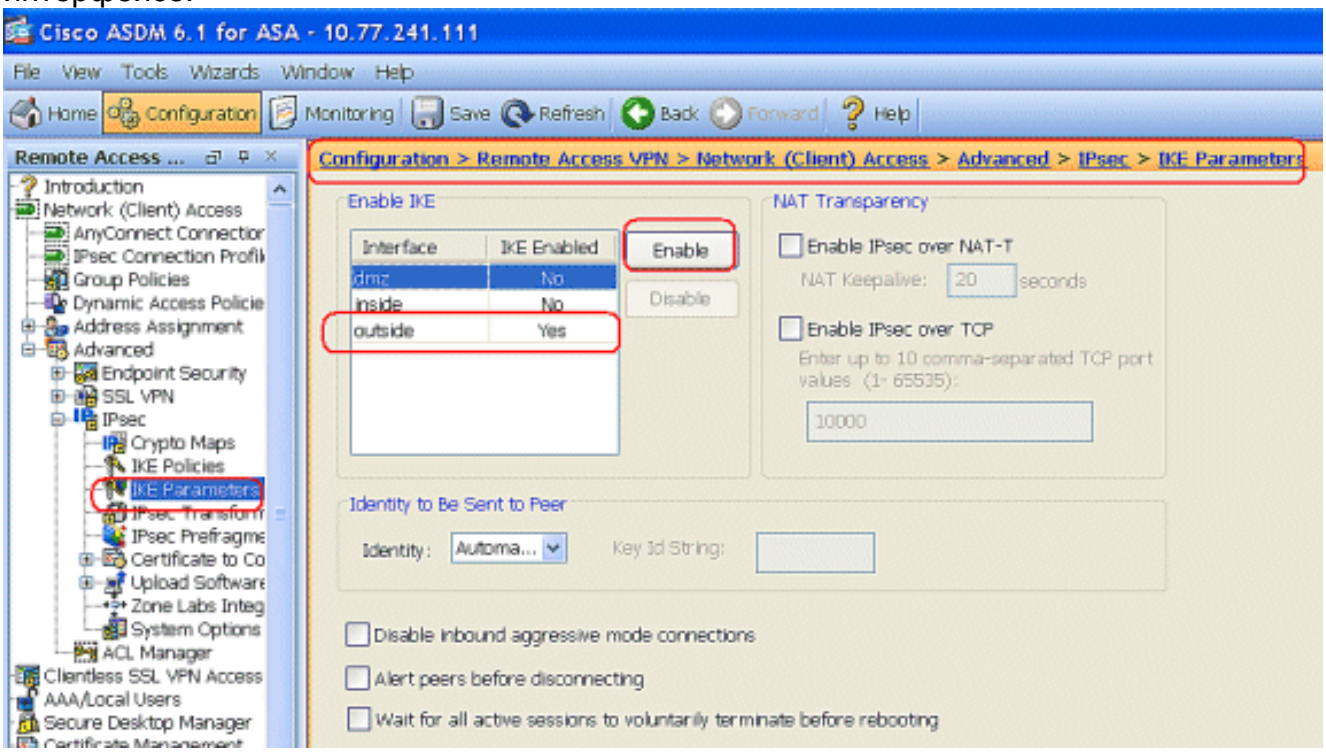


2. Предоставьте подробную информацию Политики ISAKMP.

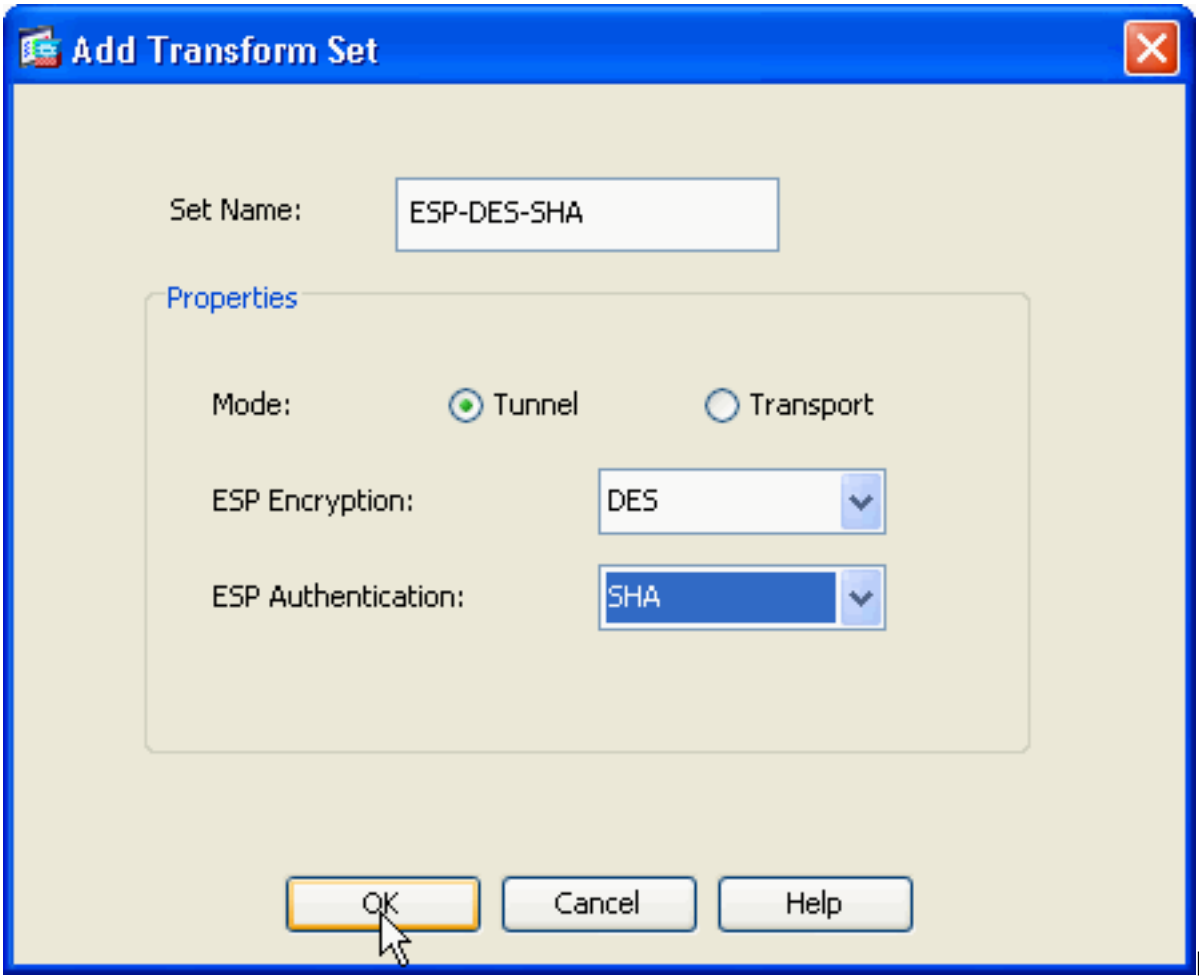


Нажмите кнопку OK и Apply.

3. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> IPSec> IKE Parameters** для включения IKE на Внешнем интерфейсе.

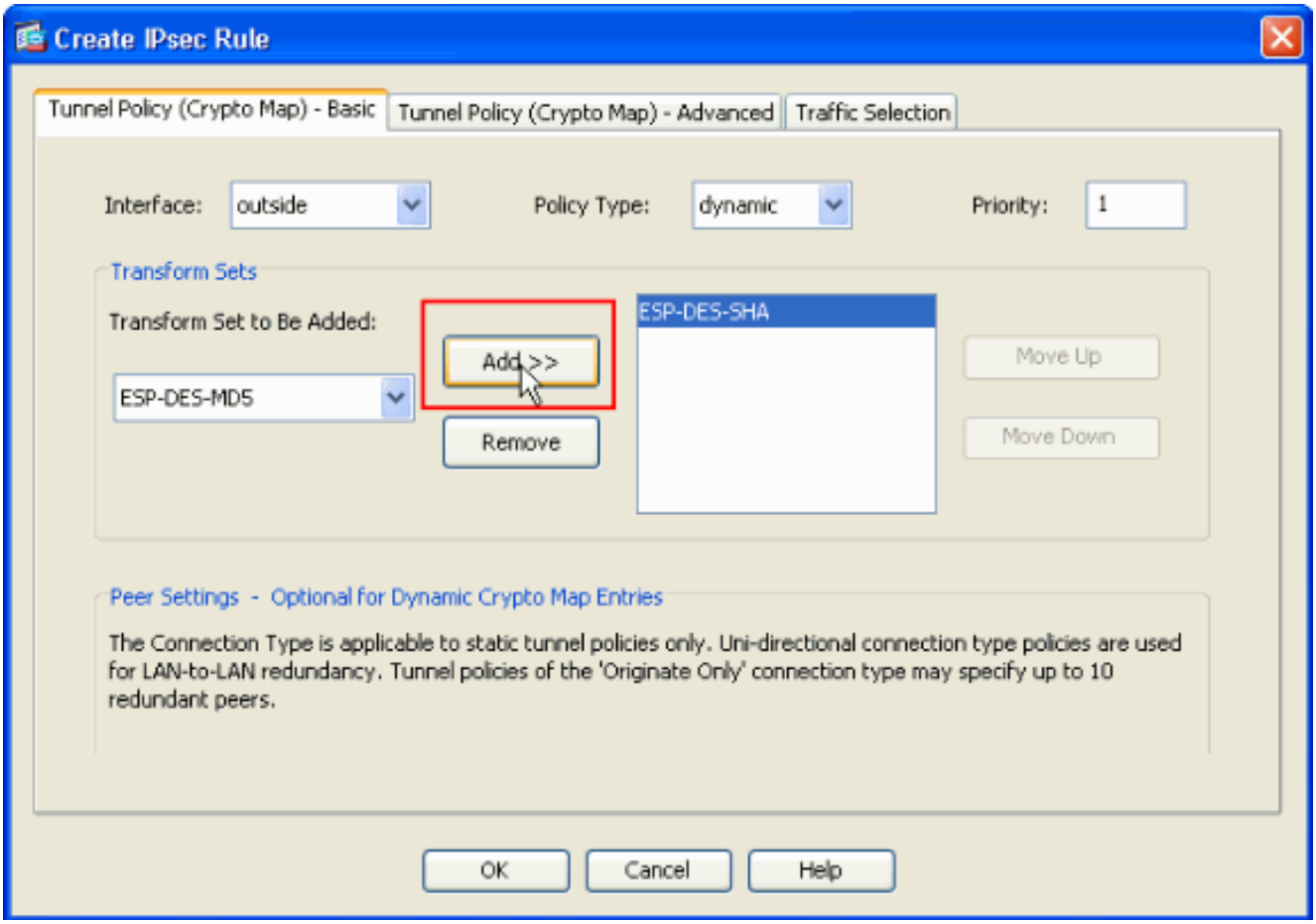


4. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> IPSec> IPSec Transform Sets> Add** для создания набора преобразований **SHA ESP-DES**, как показано.



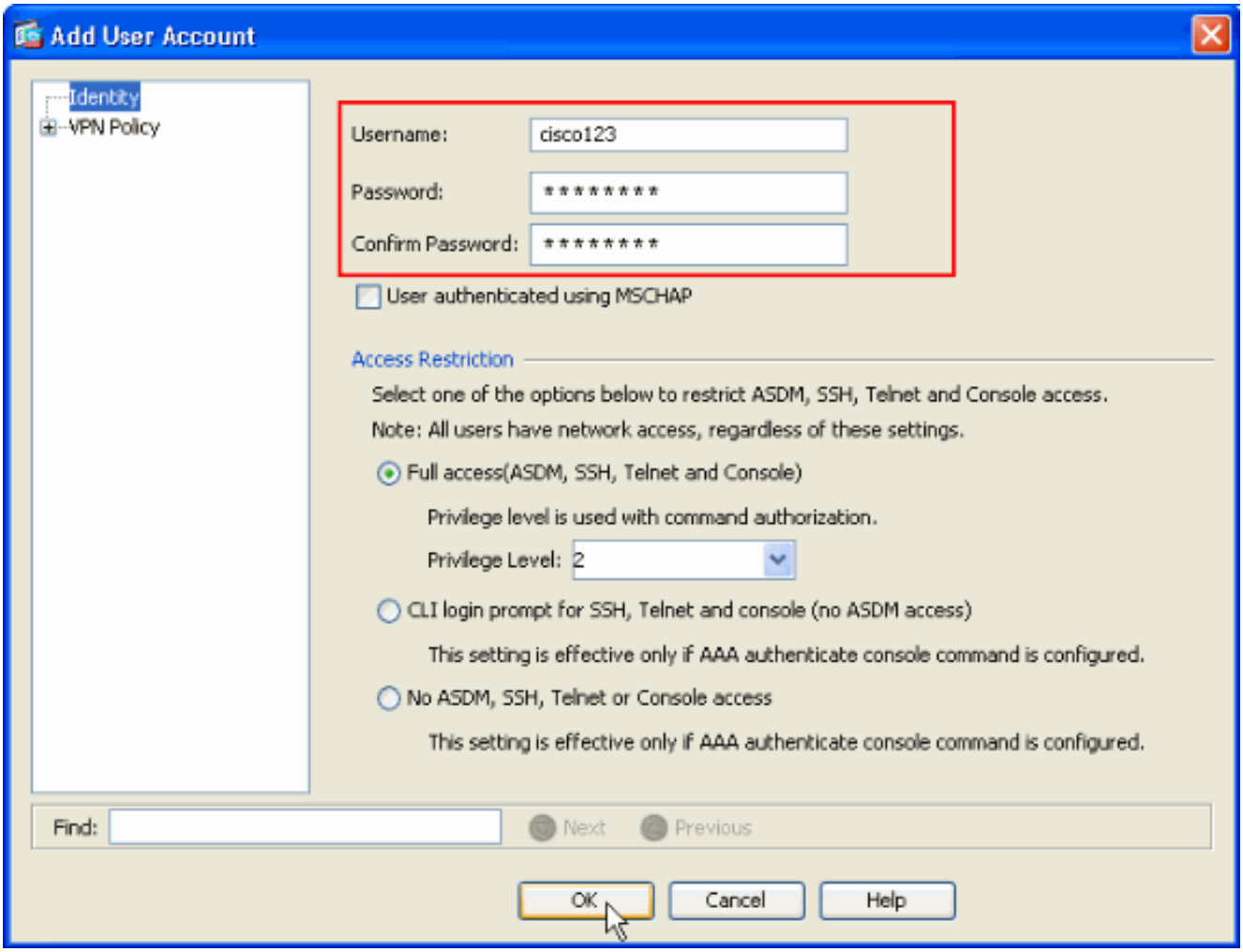
Нажмите кнопку OK и Apply.

5. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Дополнительно > IPSec > Криптографические карты > Добавить), чтобы создать криптографическую карту с приоритетом динамической политики равным 1, как показано на рисунке.

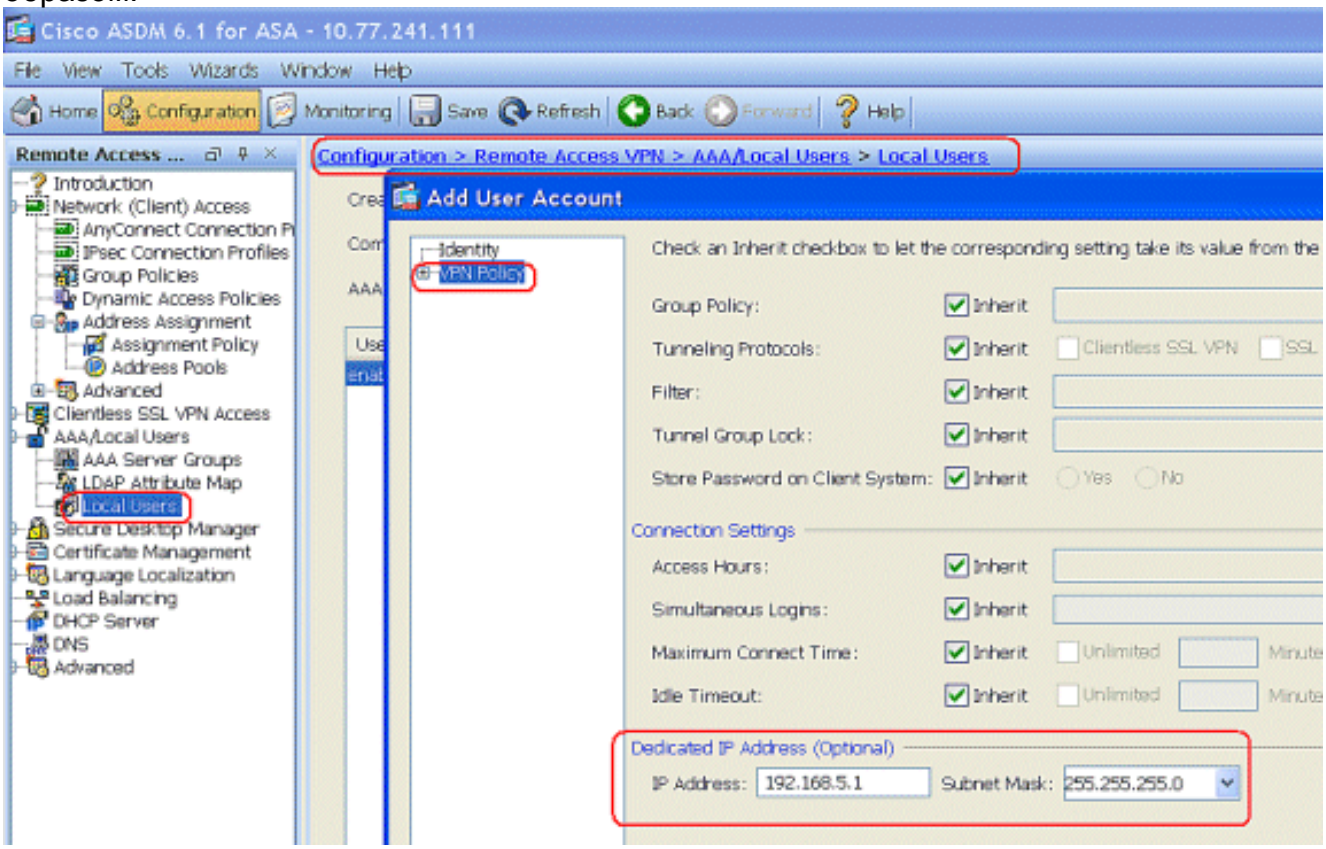


Нажмите кнопку OK и Apply.

6. Выберите **Configuration> Remote Access VPN> AAA Setup> Local Users> Add** для создания учетной записи пользователя (например, имя пользователя - cisco123 и Пароль - cisco123) для доступа клиента
VPN.

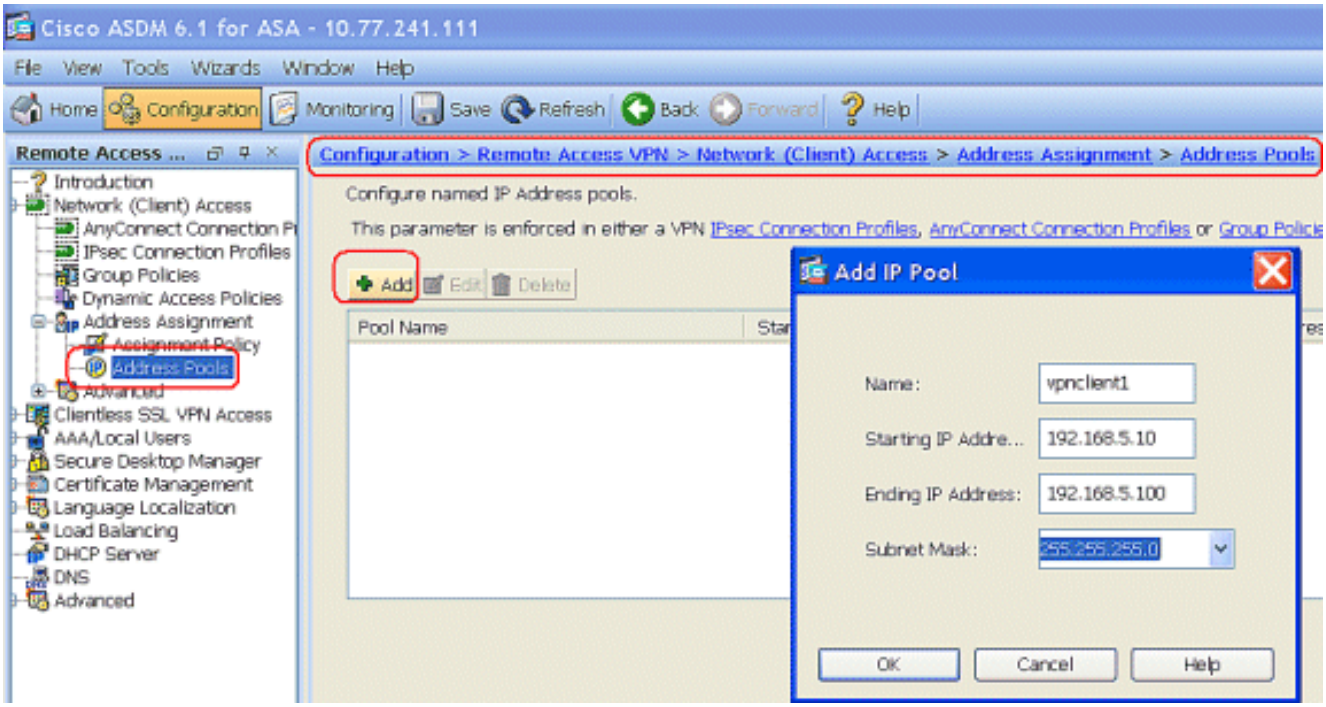


7. Перейдите **к Политике VPN** и добавьте **Статический/Специализированный IP-адрес** для пользователя "cisco123", следующим образом.

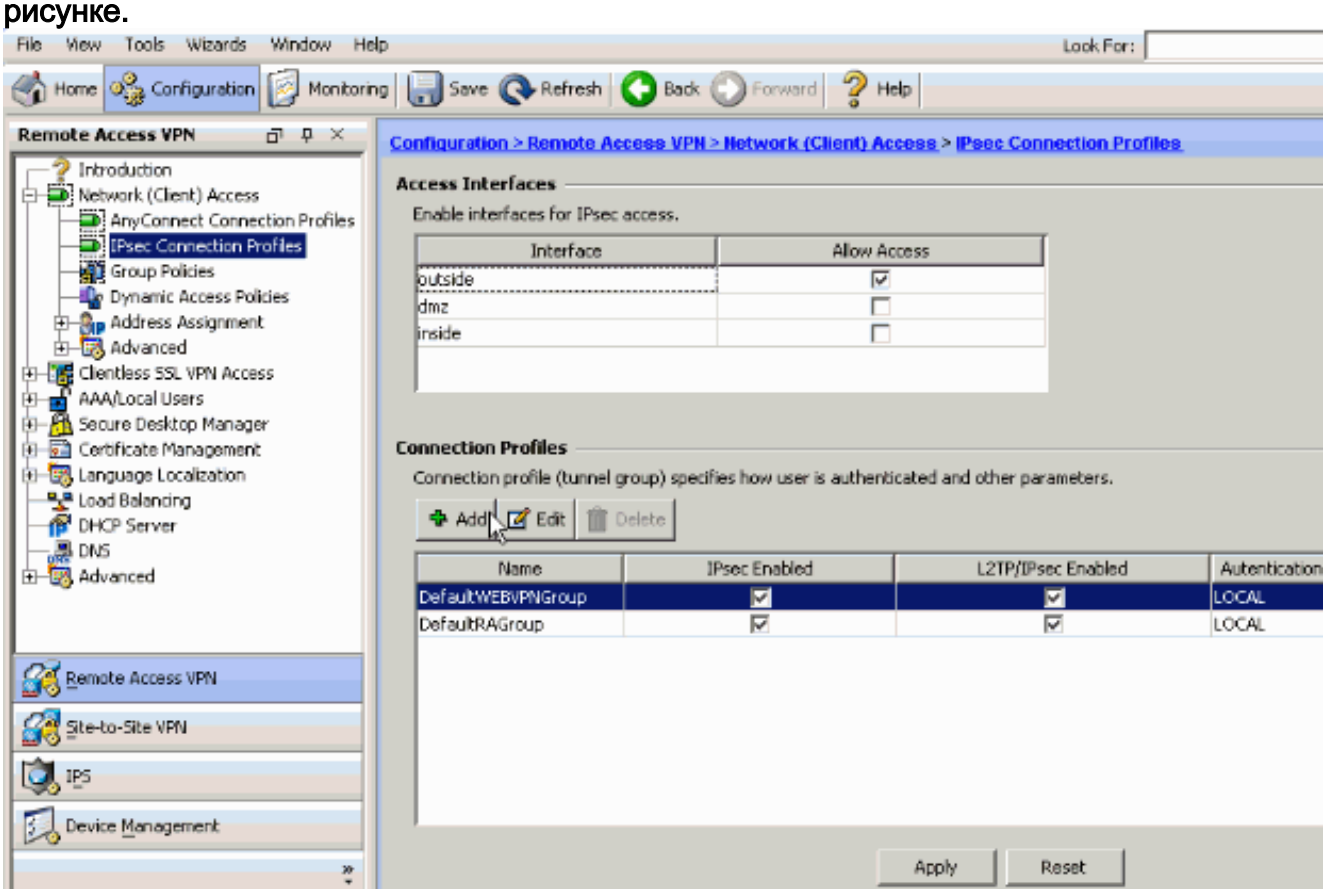


8. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Address**

Assignment> Address Pools и **нажмите Add** для добавления Клиента VPN для Пользователей VPN-
клиента.

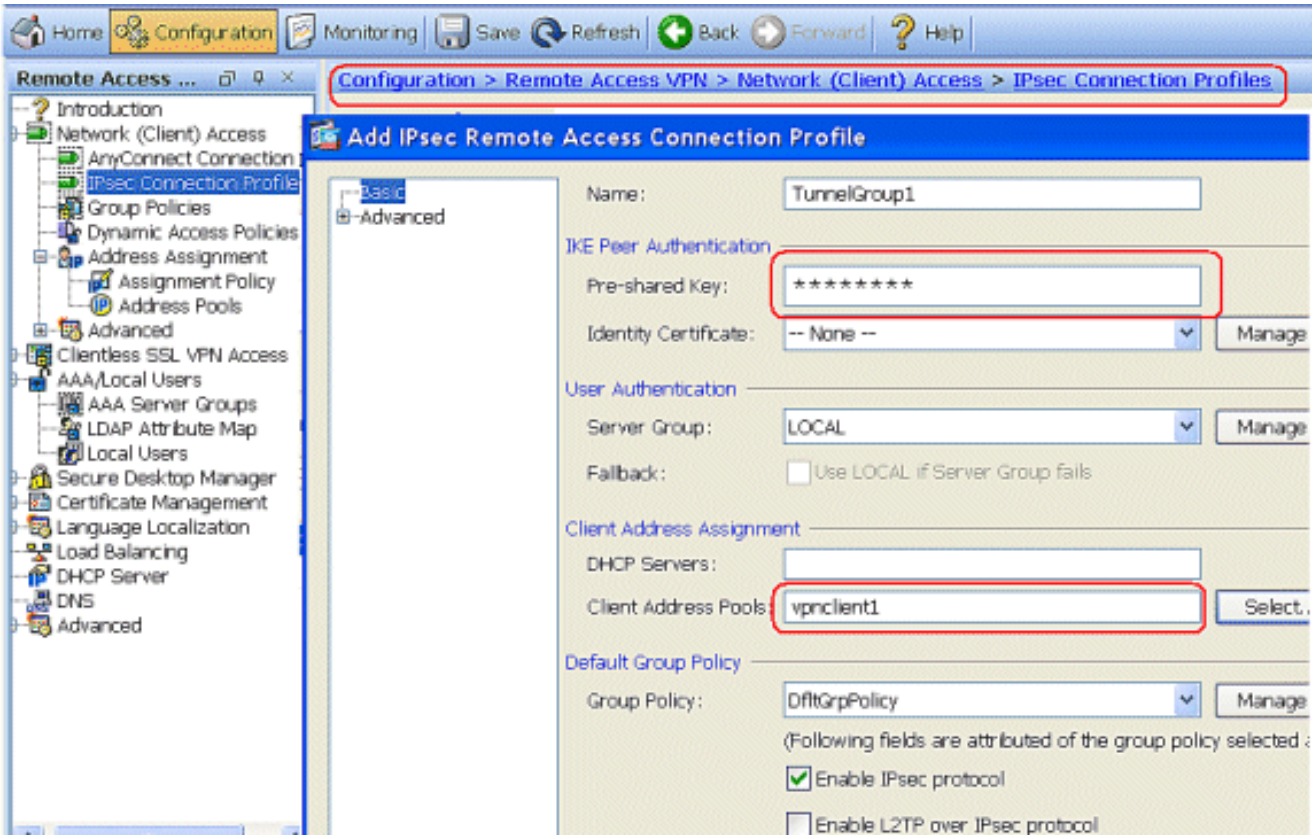


9. **Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Add (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Профили подключений IPSec > Добавить), чтобы добавить группу туннеля, например TunnelGroup1, и предварительно согласованный ключ cisco123, как показано на**
рисунке.



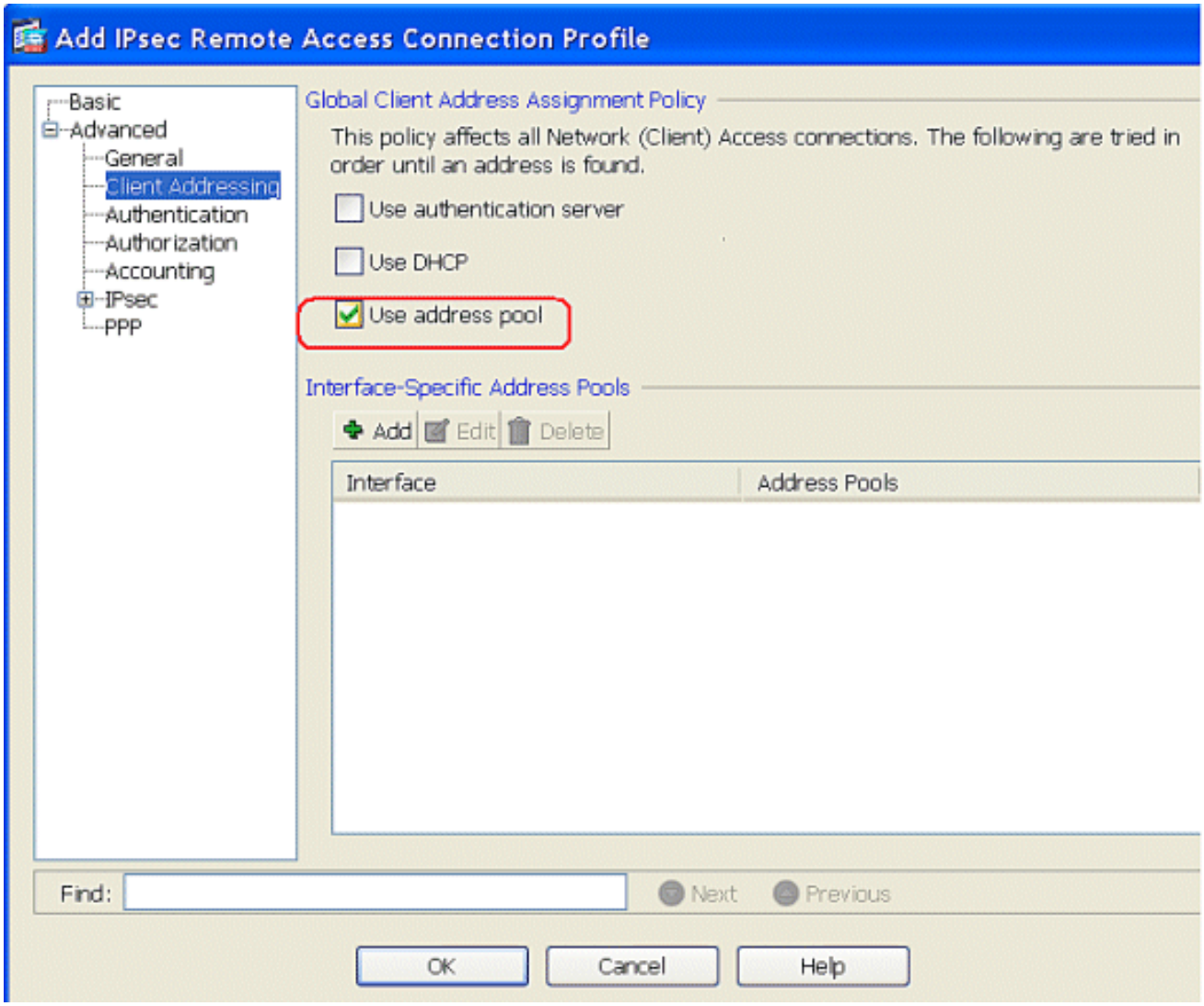
Под вкладкой **Basic** выберите группу серверов в качестве **ЛОКАЛЬНОЙ** для поля User Authentication.Выберите **vpnclient1** в качестве Пулов Адреса клиента для

Пользователей VPN-клиента.



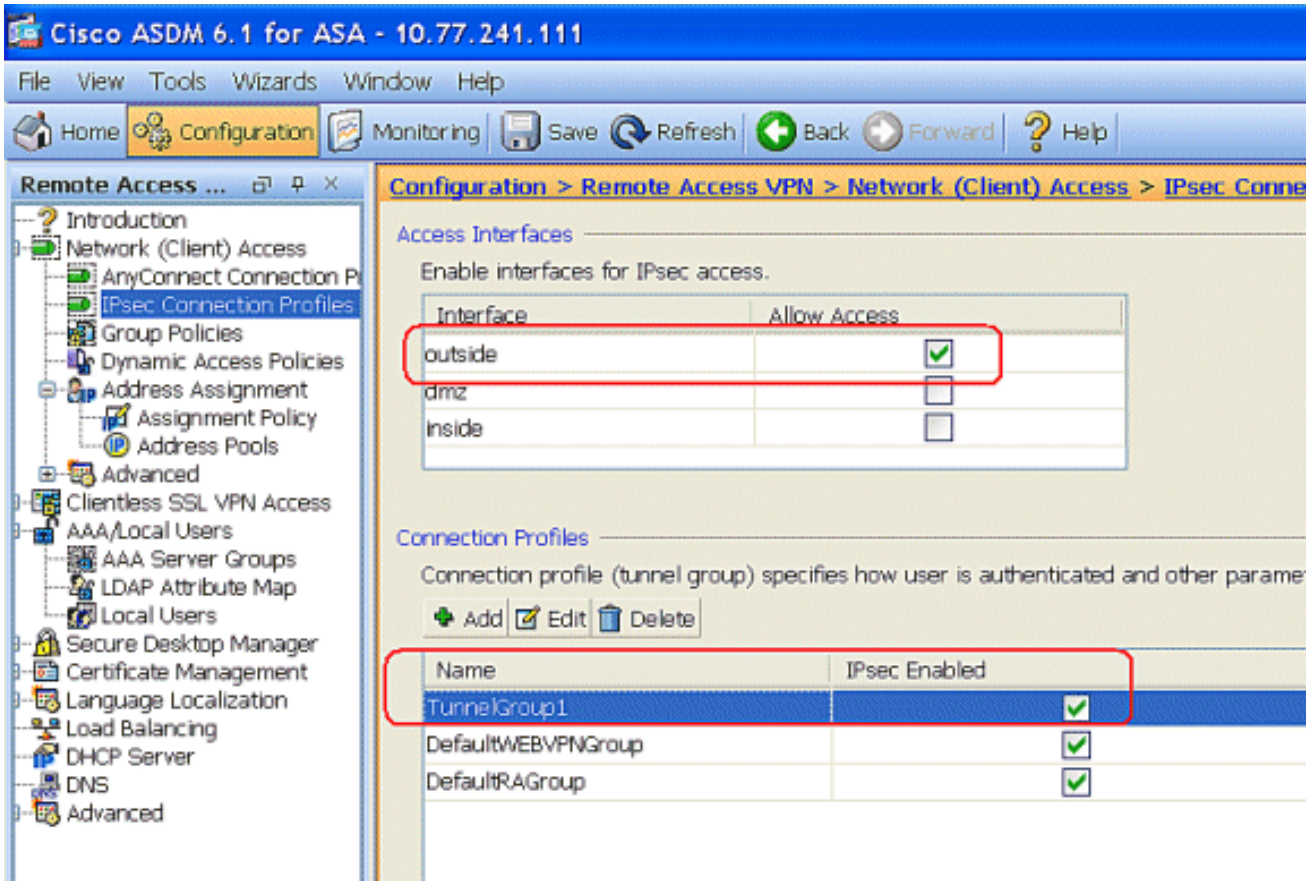
Нажмите кнопку OK.

10. Выберите **Advanced> Client Addressing** и проверьте флажок **пула адресов Использования** для присвоения IP-адреса на клиенты VPN.**Примечание:** Удостоверьтесь, что сняли флажок с флажками для **сервера проверки подлинности Использования** и **DHCP Использования**.



Нажмите кнопку OK.

11. Включите внешний интерфейс для доступа IPSec. Для продолжения нажмите кнопку Apply
(Применить).



Настройка ASA/PIX в интерфейсе командной строки

Для настройки сервера DHCP на предоставление IP-адресов VPN-клиентам из командной строки выполните следующие шаги. Дополнительные сведения о каждой из используемых команд см. в документах Настройка сетей VPN для удаленного доступа и Справочник по командам устройств адаптивной защиты Cisco ASA серии 5500.

Рабочая конфигурация на устройстве ASA

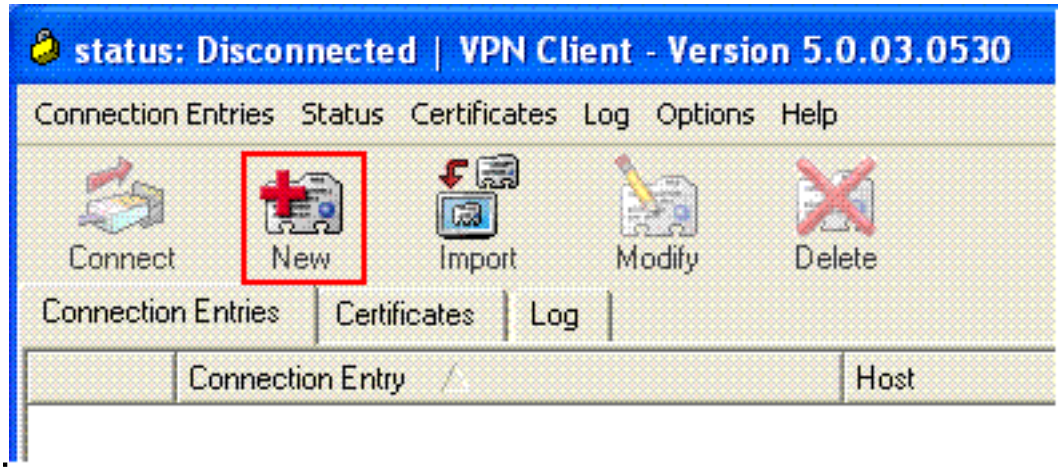
```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0 no failover icmp unreachable rate-
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0
```

```
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the local and not by AAA or dhcp. The CLI
vpn-addr-assign local for VPN address assignment through
ASA is hidden in the CLI provided by show run command.
no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global ! group-policy DfltGrpPolicy
attributes vpn-tunnel-protocol IPSec webvpn group-policy
GroupPolicy1 internal !--- In order to identify remote
access users to the Security Appliance, !--- you can
also configure usernames and passwords on the device. !-
-- specify the IP address to assign to a particular
user, use the vpn-framed-ip-address command !--- in
username mode username cisco123 password
ffIRPGpDSOJh9YLq encrypted username cisco123 attributes
vpn-framed-ip-address 192.168.5.1 255.255.255.0 !---
Create a new tunnel group and set the connection !---
type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

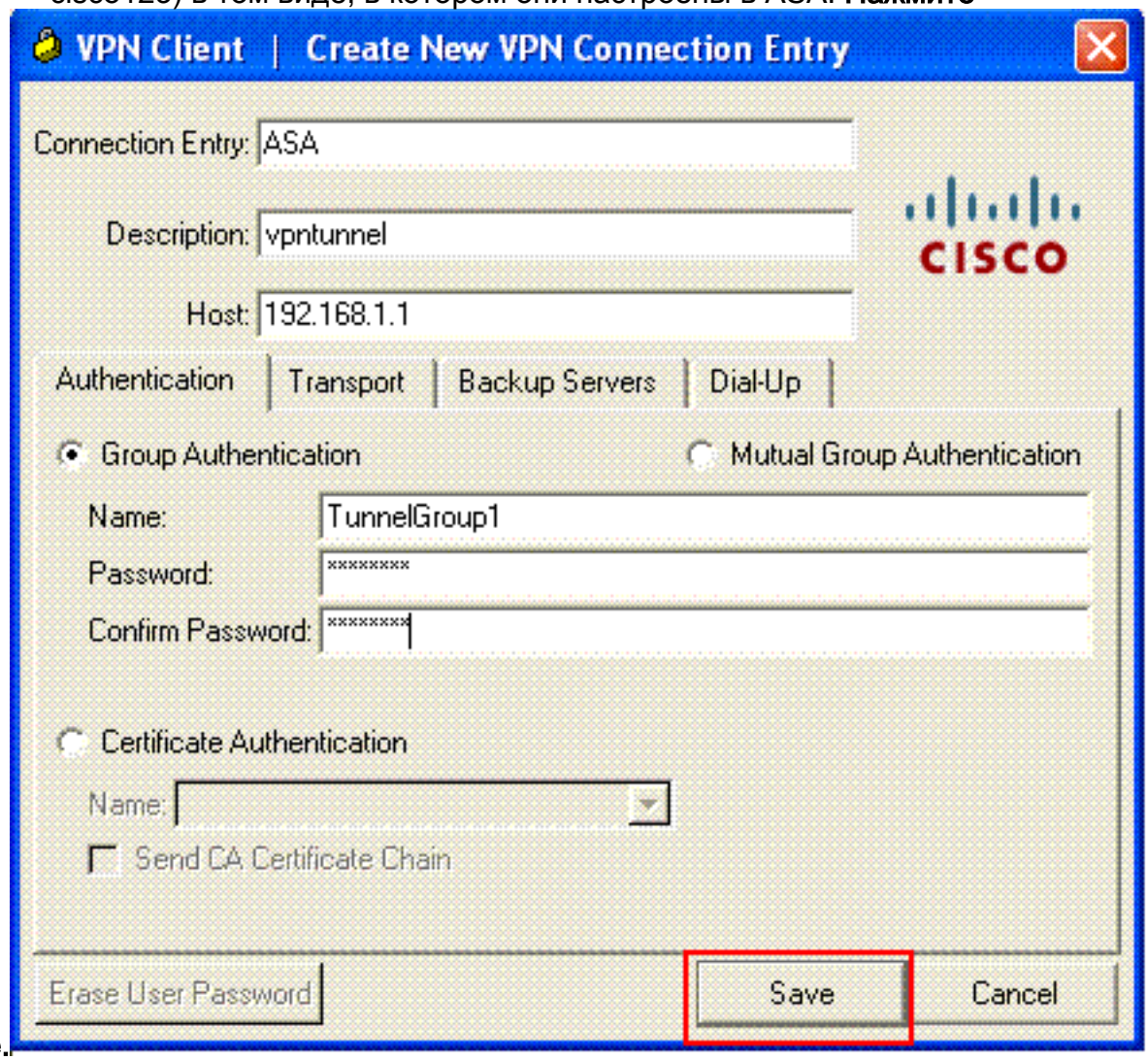
Настройка VPN-клиента Cisco VPN Client

Попробуйте подключиться к маршрутизатору Cisco с помощью VPN-клиента Cisco VPN Client, чтобы убедиться, что устройство ASA настроено правильно.

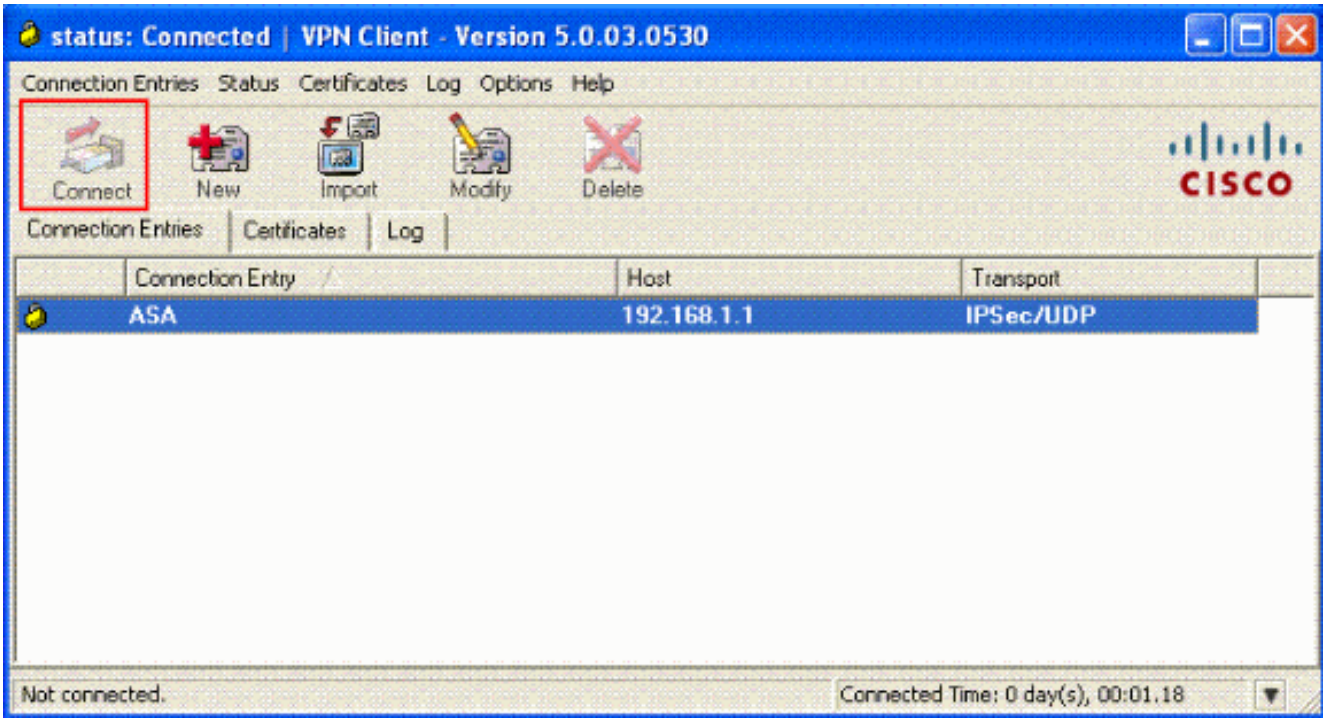
1. Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client.
2. Нажмите кнопку New (Создать), чтобы открыть окно Create New VPN Connection Entry (Создание записи нового VPN-



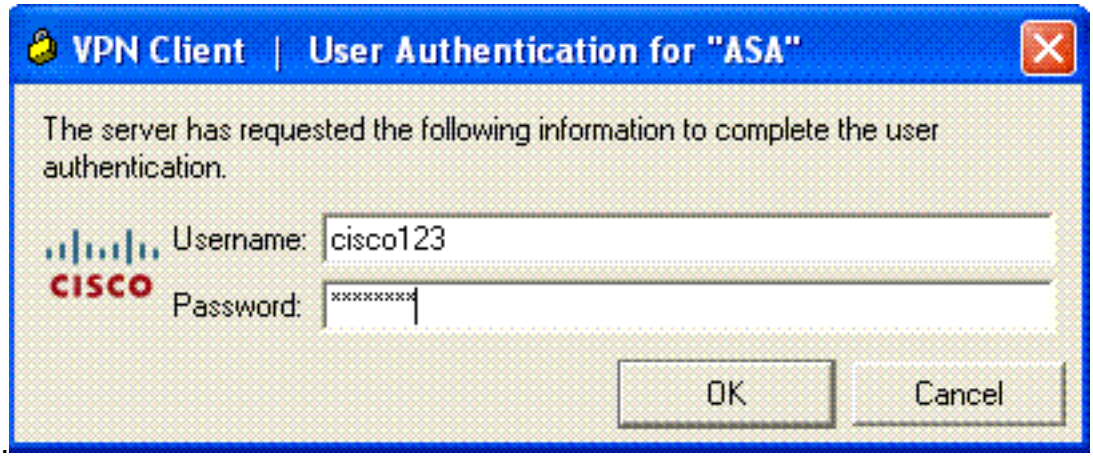
подключения).
3. Введите данные нового подключения.Введите имя записи и описание подключения. **Введите внешний IP-адрес устройства ASA в поле Host (Хост).** Затем введите имя (TunnelGroup1) группы туннеля сети VPN и пароль (предварительно согласованный ключ — cisco123) в том виде, в котором они настроены в ASA. **Нажмите**



Save.
4. Выберите подключение, которое необходимо использовать, и нажмите Connect (Подключить) в главном окне клиента VPN Client.

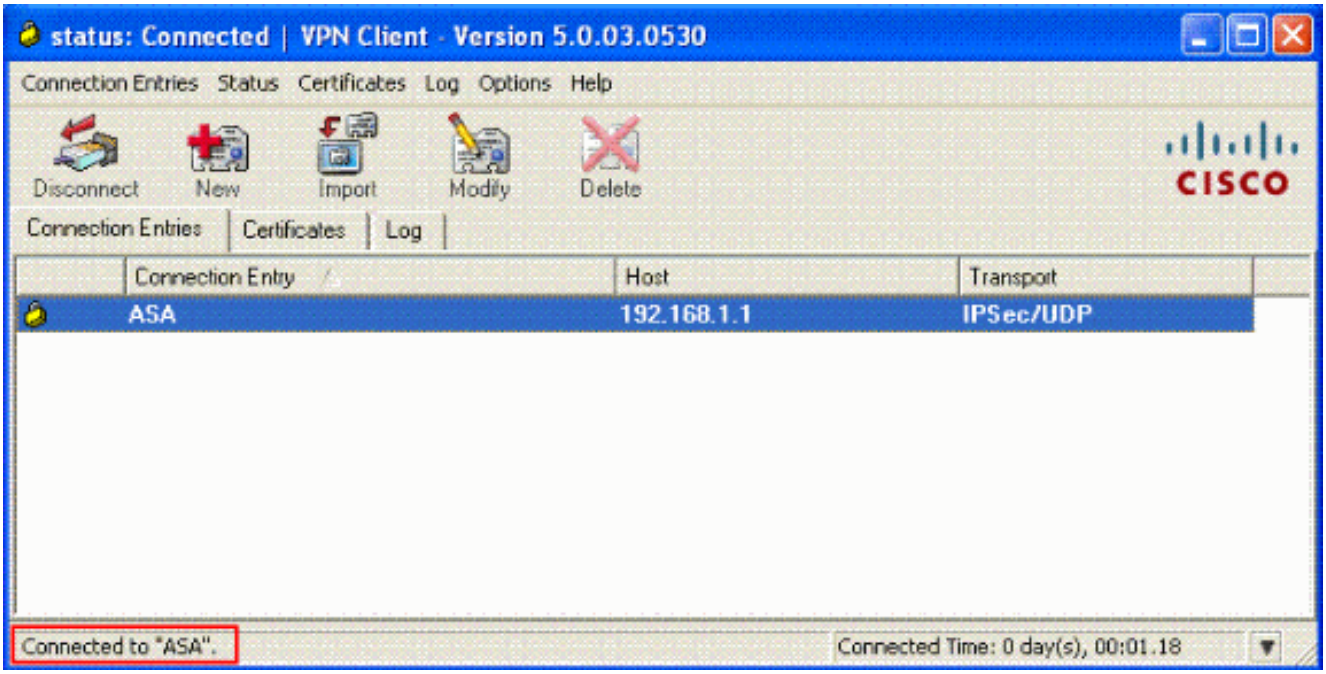


5. **При появлении приглашения введите имя пользователя Username : cisco123** и **Пароль: cisco123** согласно конфигурации в ASA для Xauth, и нажимает **OK** для соединения с удаленной

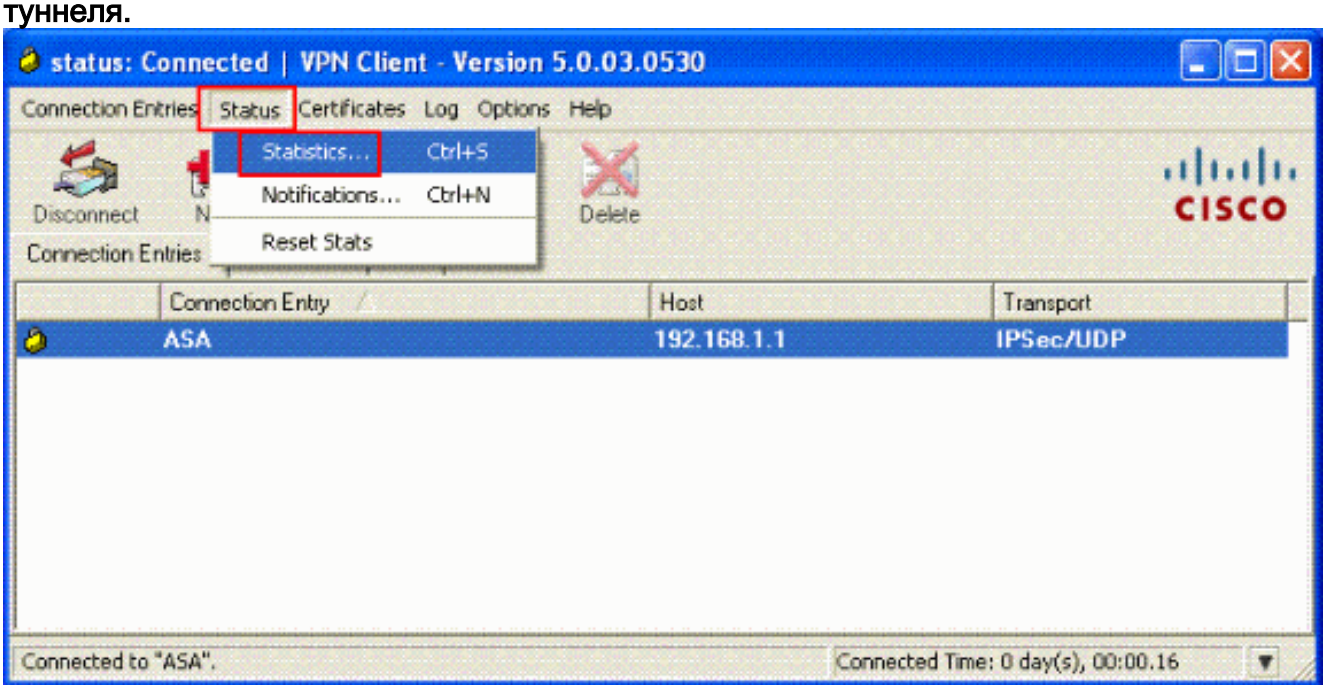


сетью.

6. ПО VPN Client соединится с устройством ASA на центральном узле.



7. После успешного установления соединения выберите пункт Statistics (Статистика) в меню Status (Состояние), чтобы проверить данные туннеля.



Проверка

команды "show"

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.

- show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.
- show crypto ipsec sa—отображает параметры, используемые текущими SA.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации. Также показан пример выходных данных команды debug.

Примечание: Для получения дополнительной информации об устранении проблем IPSEC VPN Удаленного доступа обращаются Решения для Устранения проблем IPSEC VPN Наиболее распространенного соединения L2L и Удаленного доступа.

Очистка ассоциаций безопасности

При работе по устранению неполадок не забывайте очищать существующие ассоциации безопасности после выполнения изменений. В привилегированном режиме PIX используйте следующие команды:

- **clear [crypto] ipsec sa— удаляет все активные ассоциации безопасности IPSec.** Ключевое слово crypto является необязательным.
- **clear crypto isakmp sa— удаляет активные ассоциации безопасности IKE.** Ключевое слово crypto является необязательным.

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 7 – отображает связь IPsec этапа 2.**
- **debug crypto isakmp 7 — отображает процесс установления связи по протоколу ISAKMP на этапе 1.**

Дополнительные сведения

- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- Справочники по командам устройств адаптивной защиты Cisco ASA серии 5500
- Страница поддержки устройств защиты Cisco PIX серии 500
- Справочник по командам устройств защиты Cisco PIX серии 500
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Страница технической поддержки протоколов согласования IPSec и IKE
- Страница поддержки Cisco VPN Client
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация