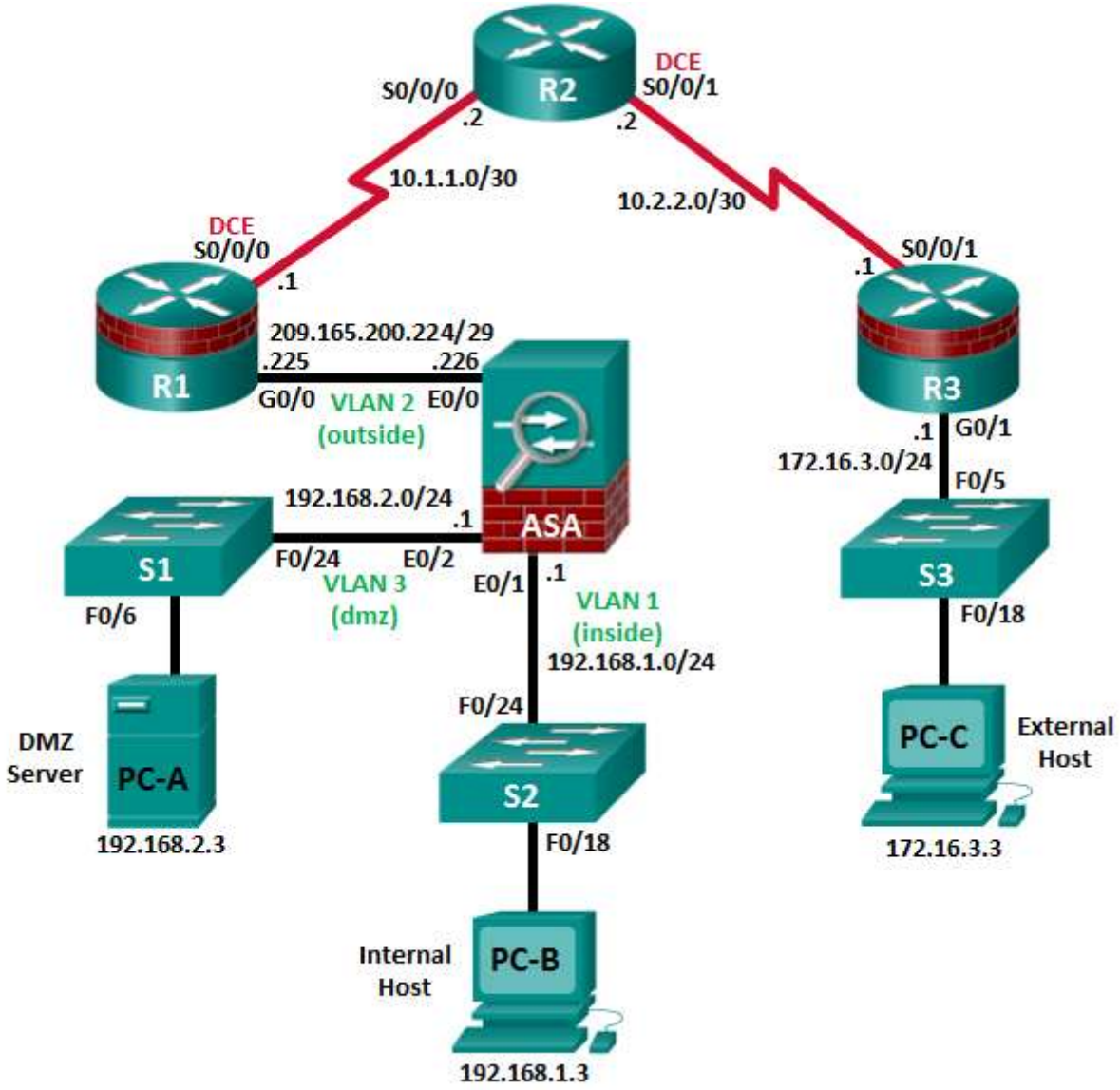
CCNA Security

Глава 10. Конфигурирование сетей SSL VPN AnyConnect для удаленного доступа с помощью ASDM

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet вместо GigabitEthernet.

Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/0	209.165.200.225	255.255.255.248	Н/П	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Задачи

Часть 1. Базовая настройка маршрутизатора/коммутатора/ПК

- Подключение сетевых кабелей и сброс предыдущих настроек на устройствах, как показано на топологической схеме
- Конфигурирование основных параметров для маршрутизаторов
- Конфигурирование параметров IP для хостов
- Проверка связи
- Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора

Часть 2. Доступ к консоли ASA и ASDM

- Доступ к консоли ASA
- Сброс предыдущих настроек конфигурации ASA
- Пропуск режима настройки
- Настройка ASA с помощью скрипта CLI
- Доступ к ASDM

Часть 3. Настройка сети SSL VPN с использованием клиента AnyConnect с помощью ASDM

- Запуск мастера VPN
- Выбор протокола шифрования VPN
- Выбор образа клиента, который нужно загрузить пользователям AnyConnect
- Настройка локальной аутентификации AAA
- Настройка назначения клиентских адресов
- Настройка разрешения сетевых имен

- Исключение преобразования адресов для VPN-трафика
- Обзор варианта развертывания клиента AnyConnect
- Обзор экрана Summary и применение конфигурации для ASA

Часть 4. Подключение к AnyConnect SSL VPN

- Проверка профиля клиента AnyConnect
- Вход в систему с удаленного хоста
- Обнаружение платформы (при необходимости)
- Автоматическая установка клиента AnyConnect VPN (при необходимости)
- Установка вручную клиента AnyConnect VPN (при необходимости)
- Проверка связи по VPN

Исходные данные/сценарий

Помимо межсетевого экрана с сохранением состояния и других функций безопасности, ASA может предоставлять функции site-to-site VPN и VPN для удаленного доступа. ASA поддерживает два основных режима развертывания, используемых для создания сетей VPN для удаленного доступа с поддержкой Cisco SSL.

- **Сеть SSL VPN без использования клиента –** сеть VPN без использования клиента, на основе браузера, позволяющая пользователям устанавливать безопасный VPN-туннель для удаленного доступа к ASA при помощи браузера и встроенного протокола SSL для защиты VPN-трафика. После аутентификации пользователи попадают на страницу портала и могут получать доступ к необходимым, предварительно определенным внутренним ресурсам.
- **Сеть SSL VPN с использованием клиента** позволяет установить туннельное соединение по VPN SSL, но требует установки клиентского приложения VPN на удаленном хосте. После аутентификации пользователи могут получать доступ к любому внутреннему ресурсу, как если бы они физически находились в локальной сети. ASA поддерживает сети VPN с использованием клиента SSL и IPsec.

В части 1 этой лабораторной работы необходимо сконфигурировать топологию и устройства, отличные от ASA. В части 2 необходимо подготовить ASA к доступу через ASDM. В части 3 необходимо использовать мастер ASDM VPN для настройки сети SSL VPN для удаленного доступа с использованием клиента AnyConnect. В части 4 необходимо установить соединение и проверить связь.

В вашей компании имеется 2 площадки, подключенные к ISP. Маршрутизатор R1 представляет собой конечное устройство (CPE), работой которого управляет ISP. R2 – это промежуточный интернет-маршрутизатор. Маршрутизатор R3 подключает пользователей удаленного филиала к ISP. ASA – это граничное устройство безопасности, подключающее внутрикорпоративную сеть и DMZ к ISP и одновременно предоставляющее сервисы NAT внутренним хостам.

Менеджмент компании попросил вас предоставить доступ по VPN для удаленных сотрудников, используя ASA в качестве концентратора VPN. Они хотят, чтобы вы проверили модель доступа с использованием клиента Cisco AnyConnect и SSL.

Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатора Cisco 1941 с ПО Cisco IOS Release 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. В зависимости от модели маршрутизатора и версии Cisco IOS, доступные команды и выходные данные могут отличаться от указанных в данной лабораторной работе.

ASA в данной лабораторной работе представляет собой модель Cisco 5505 со встроенным 8-портовым коммутатором, с ОС версии 9.2(3) и ASDM версии 7.4(1) и имеет базовую лицензию, поддерживающую максимум три сети VLAN.

Примечание. Перед началом работы убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Необходимые ресурсы

- Одно устройство ASA 5505 (версия ОС 9.2 (3), ASDM версии 7.4(1), базовая или сопоставимая лицензия)
- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 3 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 3 ПК (Windows 7 или 8.1, с установленным SSH-клиентом)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Базовая настройка маршрутизатора/коммутатора/ПК

В части 1 необходимо определить топологию сети и сконфигурировать основные параметры на маршрутизаторах, такие как IP-адреса интерфейсов и статическая маршрутизация.

Примечание. На данном этапе не конфигурируйте параметры ASA.

Шаг 1: Подключение сетевых кабелей и сброс предыдущих настроек на устройствах.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Шаг 2: Настройка маршрутизатора R1 с помощью скрипта CLI.

На данном шаге для конфигурирования основных параметров маршрутизатора R1 используйте следующий скрипт CLI. Скопируйте и вставьте перечисленные ниже скриптовые команды. Наблюдайте за сообщениями, появляющимися при исполнении команд, чтобы убедиться в отсутствии ошибок или предупреждений.

Примечание. В зависимости от модели маршрутизатора, интерфейсы могут быть пронумерованы по-другому, нежели в примере. В таком случае необходимо внести соответствующие изменения.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, а сами пароли были упрощены для облегчения выполнения лабораторной работы. В производственной сети рекомендуется использовать более сложные пароли.

```
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/0
```



```
 ip address 209.165.200.225 255.255.255.248
 no shut
exit
int serial 0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
crypto key generate rsa general-keys modulus 1024
```

Шаг 3: Настройка маршрутизатора R2 с помощью скрипта CLI.

На данном шаге для конфигурирования основных параметров маршрутизатора R2 используйте следующий скрипт CLI. Скопируйте и вставьте перечисленные ниже скриптовые команды. Наблюдайте за сообщениями, появляющимися при исполнении команд, чтобы убедиться в отсутствии ошибок или предупреждений.

```
hostname R2
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface serial 0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
exit
interface serial 0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 209.165.200.224 255.255.255.248 Serial0/0/0
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```


Шаг 4: Настройка маршрутизатора R3 с помощью скрипта CLI.

На данном шаге для конфигурирования основных параметров маршрутизатора R3 используйте следующий скрипт CLI. Скопируйте и вставьте перечисленные ниже скриптовые команды. Наблюдайте за сообщениями, появляющимися при исполнении команд, чтобы убедиться в отсутствии ошибок или предупреждений.

```
hostname R3
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/1
 ip address 172.16.3.1 255.255.255.0
 no shut
exit
int serial 0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

Шаг 5: Конфигурирование параметров IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A, PC-B и PC-C, как показано в таблице IP-адресов.

Шаг 6: Проверка связи.

ASA является основным пунктом между сетевыми зонами, и оно еще не было сконфигурировано. Поэтому между подключенными к нему устройствами связи не будет. Однако у компьютера PC-C должна быть возможность отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. С компьютера PC-C отправьте эхо-запрос на IP-адрес интерфейса G0/0 маршрутизатора R1 (**209.165.200.225**). Если запросы завершаются с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запросы с компьютера PC-C на интерфейсы G0/0 и S0/0/0 маршрутизатора R1 выполнены успешно, это означает, что адресация настроена верно и статическая маршрутизация настроена и работает исправно.

Шаг 7: Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора.

Часть 2: Доступ к консоли ASA и ASDM

Шаг 1: Сброс предыдущих настроек конфигурации ASA.

a. С помощью команды **write erase** удалите файл **startup-config** из флеш-памяти.

Примечание. Команда IOS **erase startup-config** не поддерживается на ASA.

b. Используйте команду **reload** для перезапуска ASA. При этом ASA загрузится в режиме настройки CLI. Если вы увидите сообщение **System config has been modified. Save? [Y]es/[N]o:,** введите **no** и нажмите **Enter**.

Шаг 2: Пропуск режима настройки.

После перезагрузки устройство ASA должно определить, что не хватает файла startup-config, и перейти в режим настройки (Setup). Если переход в данный режим не выполняется, повторите шаг 2.

a. При запросе на предварительную настройку межсетевого экрана с помощью интерактивных подсказок (режим установки) ответьте **no.**

b. Войдите в привилегированный режим при помощи команды **enable**. На данном этапе пароль должен быть пустым (отсутствовать).

Шаг 3: Настройка ASA с помощью скрипта CLI.

На данном шаге с помощью скрипта CLI необходимо сконфигурировать основные параметры, межсетевой экран и DMZ.

a. С помощью команды **show run** убедитесь, что в ASA не осталось предыдущих настроек, отличных от значений по умолчанию, которые автоматически применяет данное устройство.

b. Войдите в режим глобальной настройки. На запрос анонимной отправки отчетности (call-home reporting) ответьте **no.**

c. Скопируйте и вставьте перечисленные ниже команды скрипта для предварительного конфигурирования VPN в запросе в режиме глобальной настройки ASA, чтобы запустить процесс настройки сетей SSL VPN.

Наблюдайте за сообщениями, появляющимися при исполнении команд, чтобы убедиться в отсутствии ошибок или предупреждений. При получении запроса на замену пары ключей RSA ответьте **yes**.

```
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password cisco12345
!
interface Ethernet0/0
 switchport access vlan 2
 no shut
!
interface Ethernet0/1
 switchport access vlan 1
 no shut
!
interface Ethernet0/2
 switchport access vlan 3
 no shut
!
interface Vlan1
```



```
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
object network dmz-server
 host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
 nat (inside,outside) dynamic interface
!
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
username admin01 password admin01pass
!
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 10
ssh timeout 10
```



```
!
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
   inspect icmp
!
crypto key generate rsa modulus 1024
```

d. В запросе в привилегированном режиме введите команду **write mem** (или **copy run start**), чтобы сохранить текущую конфигурацию в качестве конфигурации запуска и ключей RSA в энергонезависимой памяти.

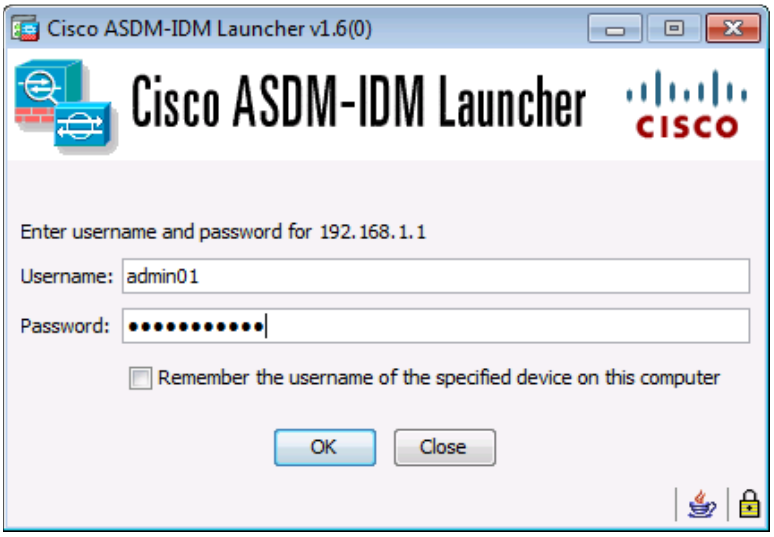
Шаг 4: Доступ к ASDM.

a. Откройте браузер на компьютере PC-B и проверьте HTTPS-доступ к ASA, введя строку https://192.168.1.1. После ввода указанного выше URL-адреса (https://192.168.1.1) должно появиться предупреждение системы безопасности о сертификате безопасности сайта. Щелкните **Continue to this website**. На все другие предупреждения системы безопасности нажимайте **Yes.**

Примечание. Убедитесь, что в URL-адресе указан протокол HTTPS.

b. На стартовой странице ASDM нажмите **Run ASDM**. Появится окно ASDM-IDM Launcher.

c. Войдите в систему как пользователь **admin01** с паролем **admin01pass.**

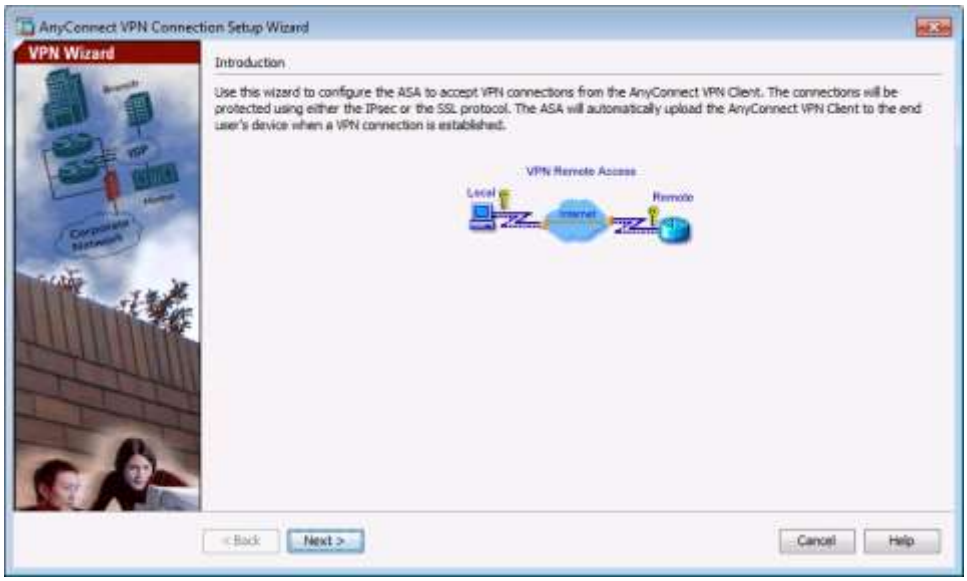


Часть 3: Настройка сети SSL VPN с использованием клиента AnyConnect с помощью ASDM

Шаг 1: Запуск мастера VPN.

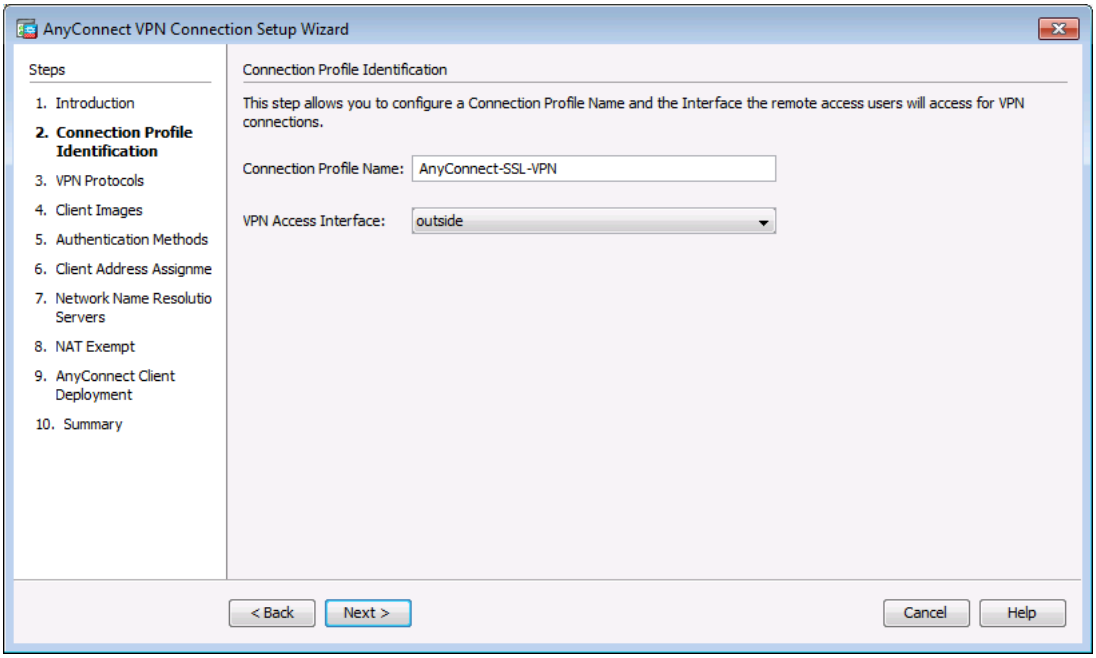
a. В главном меню ASDM выберите **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**.

b. Прочитайте текст на экране и проверьте топологическую схему. Нажмите **Next**, чтобы продолжить.



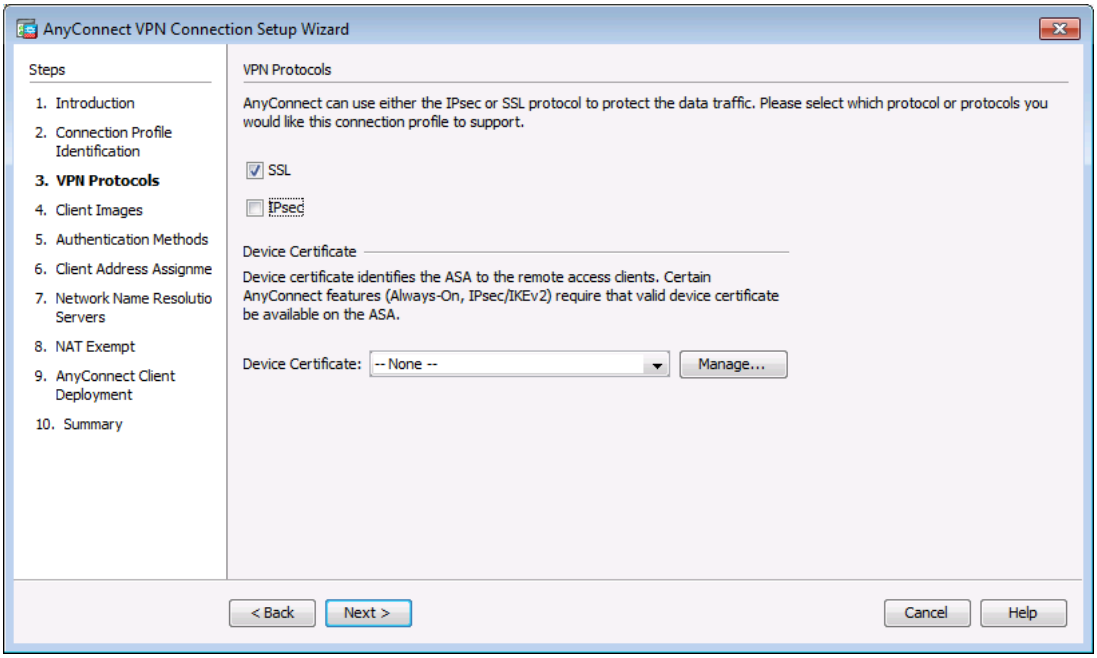
Шаг 2: Настройка профиля подключения интерфейса SSL VPN.

На экране Connection Profile Identification в поле Connection Profile Name введите **AnyConnect-SSL-VPN** и укажите интерфейс **outside** в поле VPN Access Interface. Нажмите **Next**, чтобы продолжить.



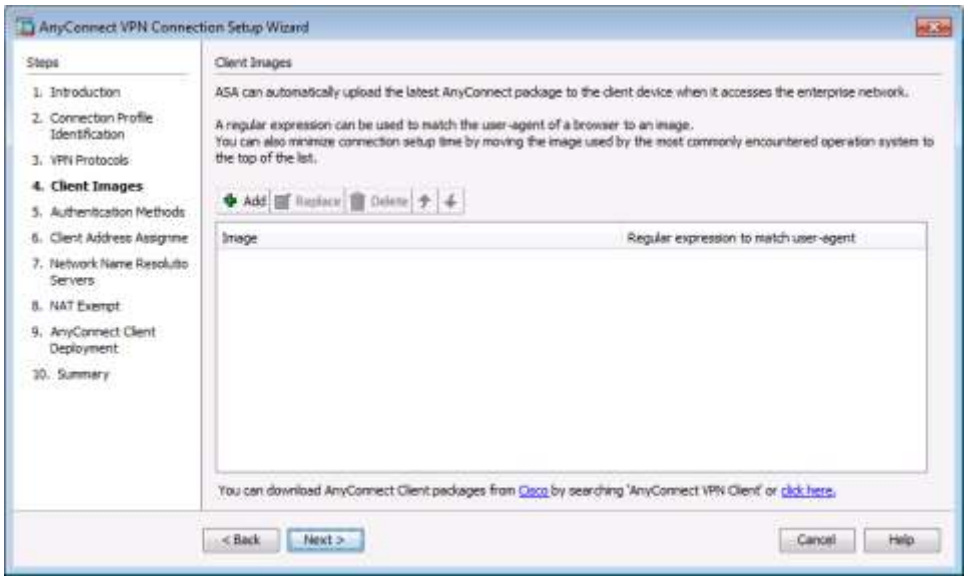
Шаг 3: Выбор протокола шифрования VPN.

На экране VPN Protocols снимите флажок **IPsec**. Оставьте флажок **SSL.** Не указывайте сертификат устройства. Нажмите **Next**, чтобы продолжить.

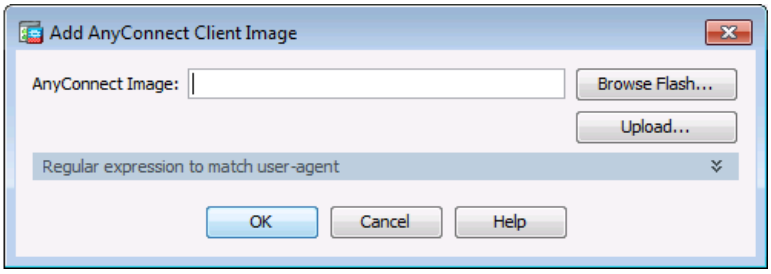


Шаг 4: Выбор образа клиента, который нужно загрузить пользователям AnyConnect.

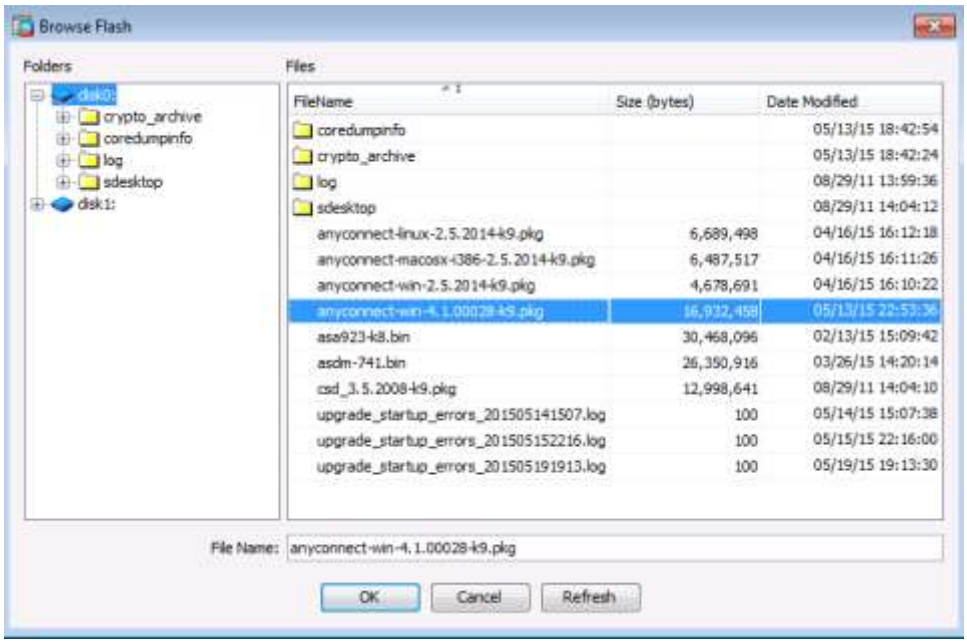
a. На экране Client Images нажмите **Add**, чтобы указать путь к файлу с образом клиента AnyConnect.



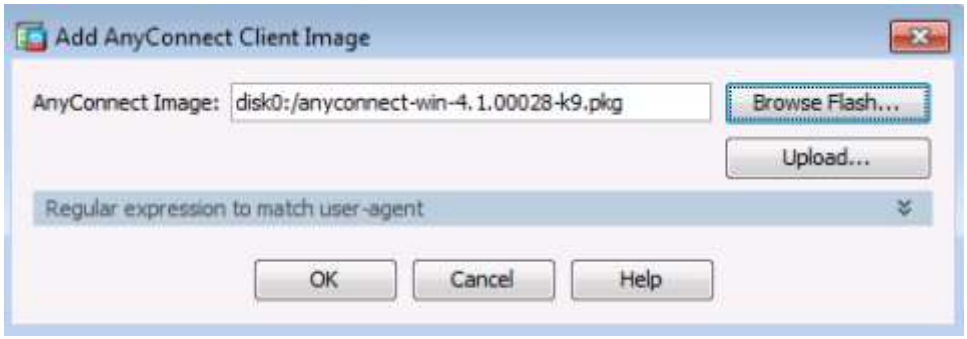
b. В окне Add AnyConnect Client Image нажмите **Browse Flash**.



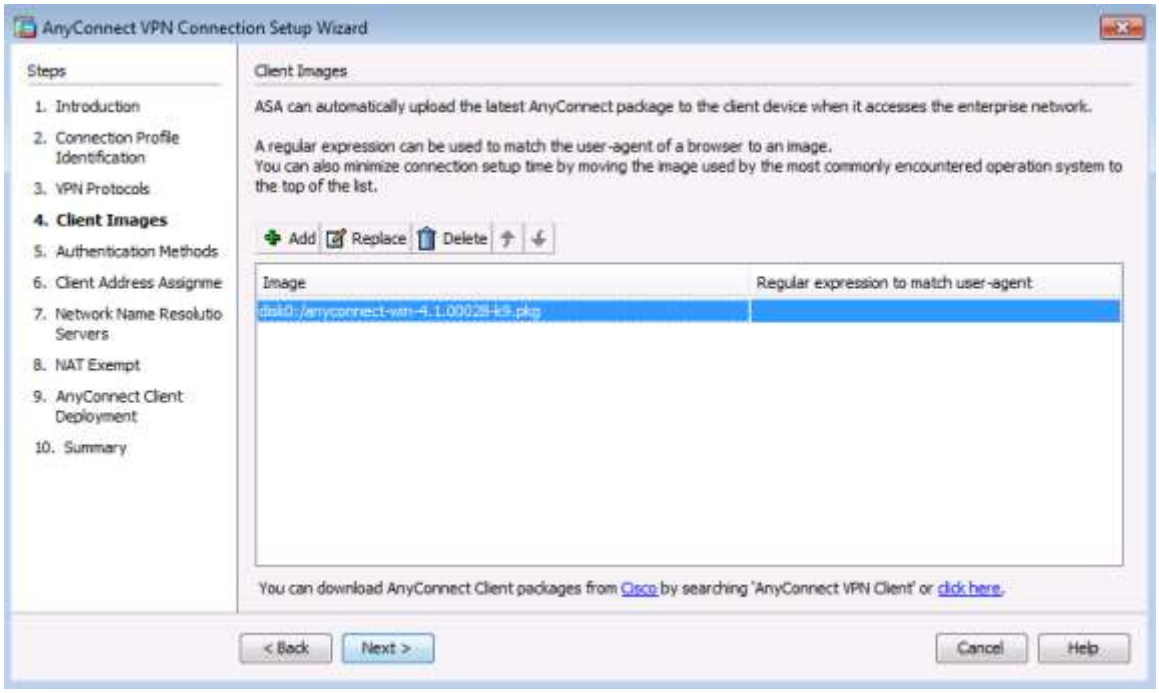
c. В окне Browse Flash выберите файл с пакетом AnyConnect для Windows (в примере – **anyconnect-win-4.1.00028-k9.pkg**). Нажмите **OK** для возврата в окно AnyConnect Client Image.



d. Снова нажмите **OK** для возврата в окно Client Image.



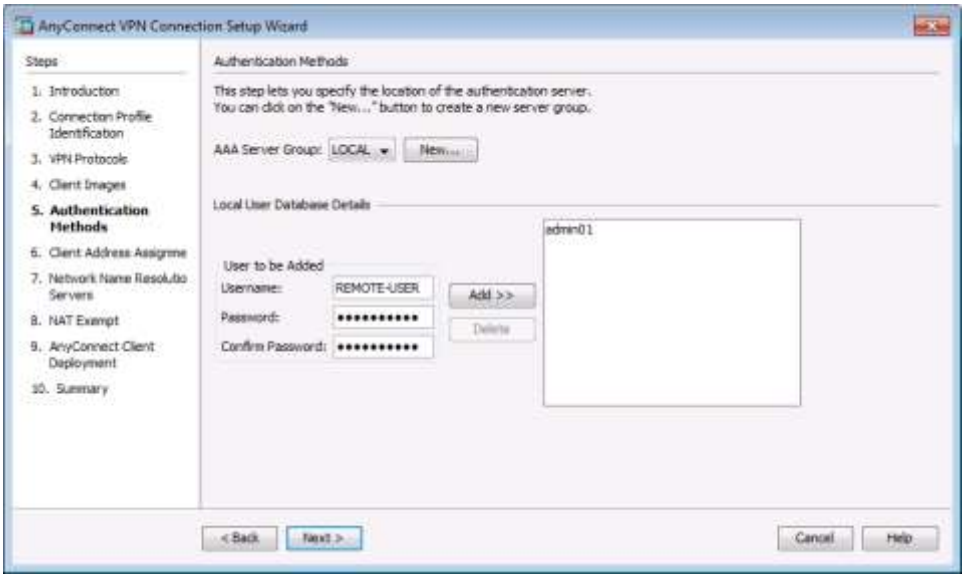
e. Выбранный образ теперь отображается в окне Client Image. Нажмите **Next**, чтобы продолжить.



Шаг 5: Настройка локальной аутентификации AAA.

a. На экране Authentication Methods убедитесь, что в поле AAA Server Group указано **LOCAL**.

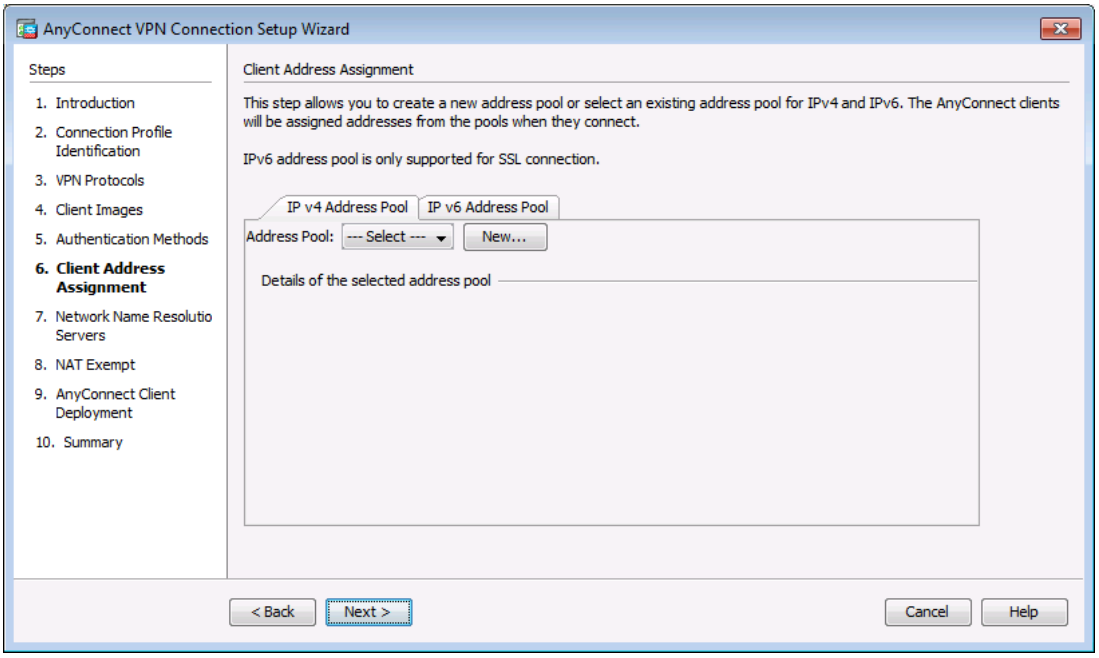
b. Введите нового пользователя с именем **REMOTE-USER** и паролем **cisco12345**. Нажмите **Add.**



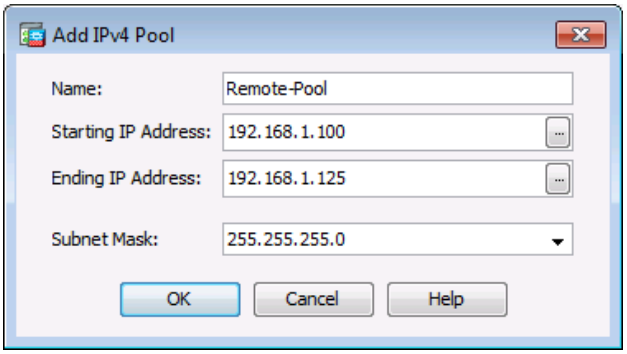
c. Нажмите **Next**, чтобы продолжить.

Шаг 6: Настройка назначения клиентских адресов.

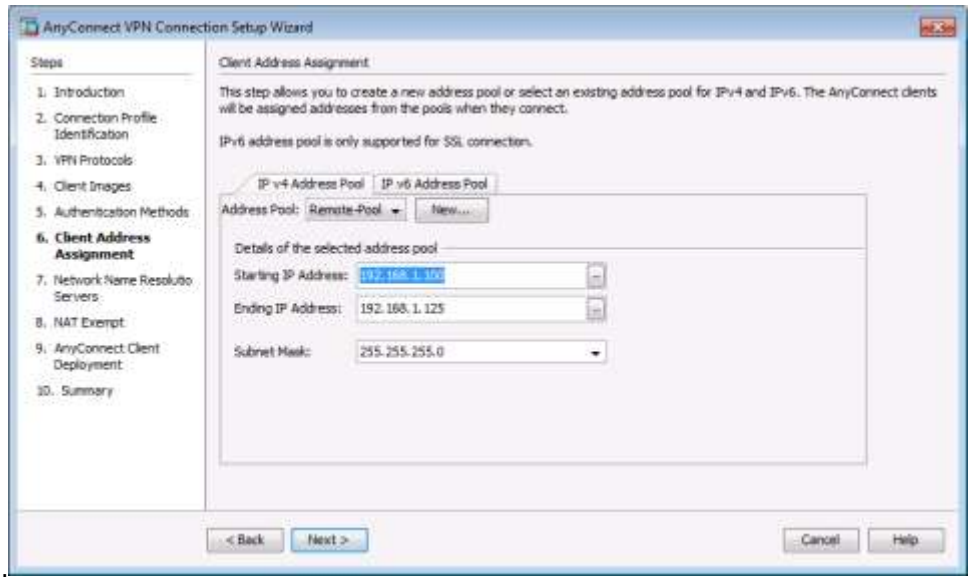
a. В окне Client Address Assignment нажмите **New,** чтобы создать пул адресов IPv4.



b. В окне Add IPv4 Pool введите наименование пула **Remote-Pool**, укажите начальный IP-адрес **192.168.1.100,** конечный адрес **192.168.1.125** и маску подсети **255.255.255.0.** Нажмите **OK** для возврата в окно Client Address Assignment, в котором теперь отображается только что созданный пул IP-адресов удаленных пользователей.



c. В окне Client Address Assignment теперь отображается только что созданный пул IP-адресов удаленных пользователей. Нажмите **Next**, чтобы продолжить.

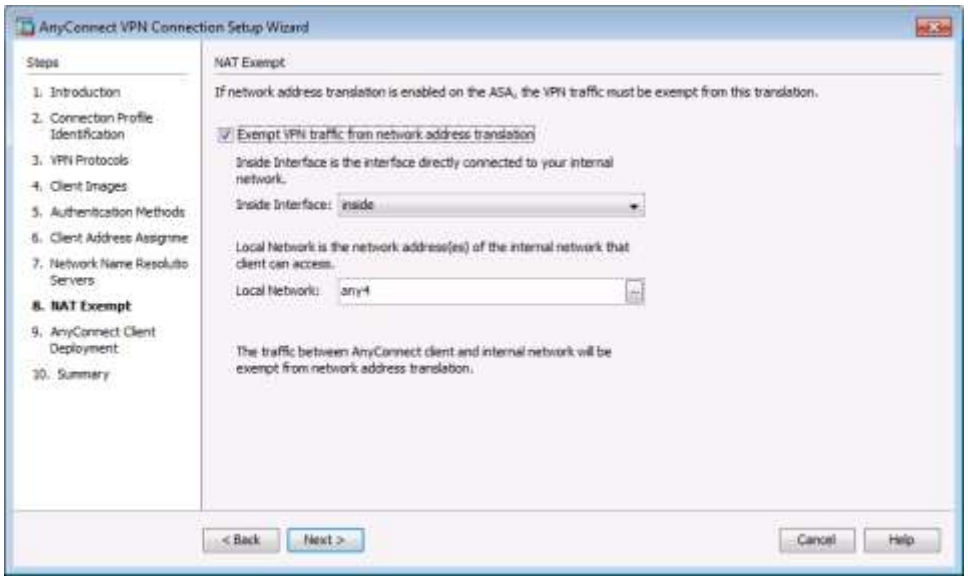


Шаг 7: Настройка разрешения сетевых имен.

На экране Network Name Resolution Servers введите IP-адрес DNS-сервера (**192.168.2.3**). Оставьте текущее доменное имя **ccnasecurity.com.** Нажмите **Next**, чтобы продолжить.

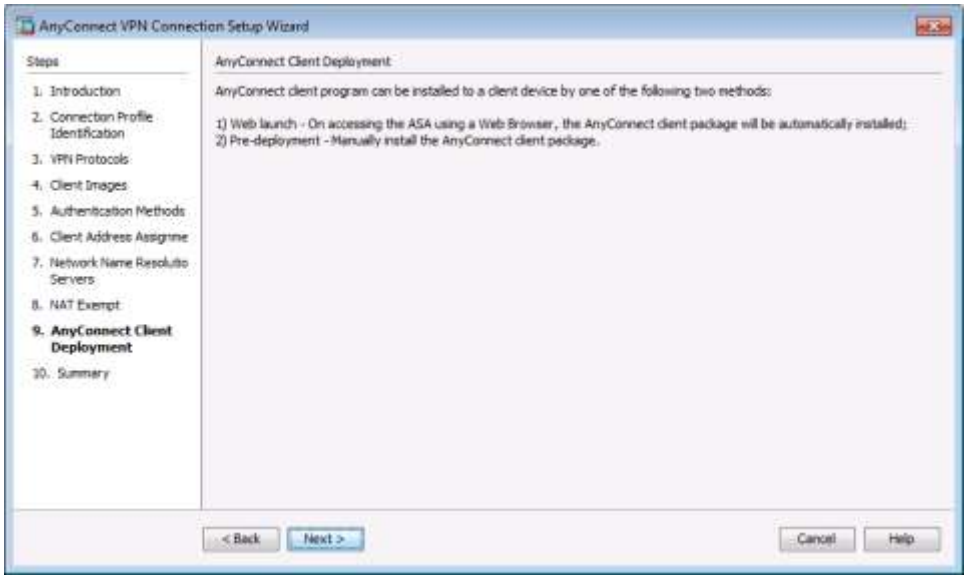
Шаг 8: Исключение преобразования адресов для VPN-трафика.

На экране NAT Exempt установите флажок **Exempt VPN traffic from network address translation**. Не меняйте установленные по умолчанию значения в полях Inside Interface (**inside**) и Local Network (**any4**). Нажмите **Next**, чтобы продолжить.



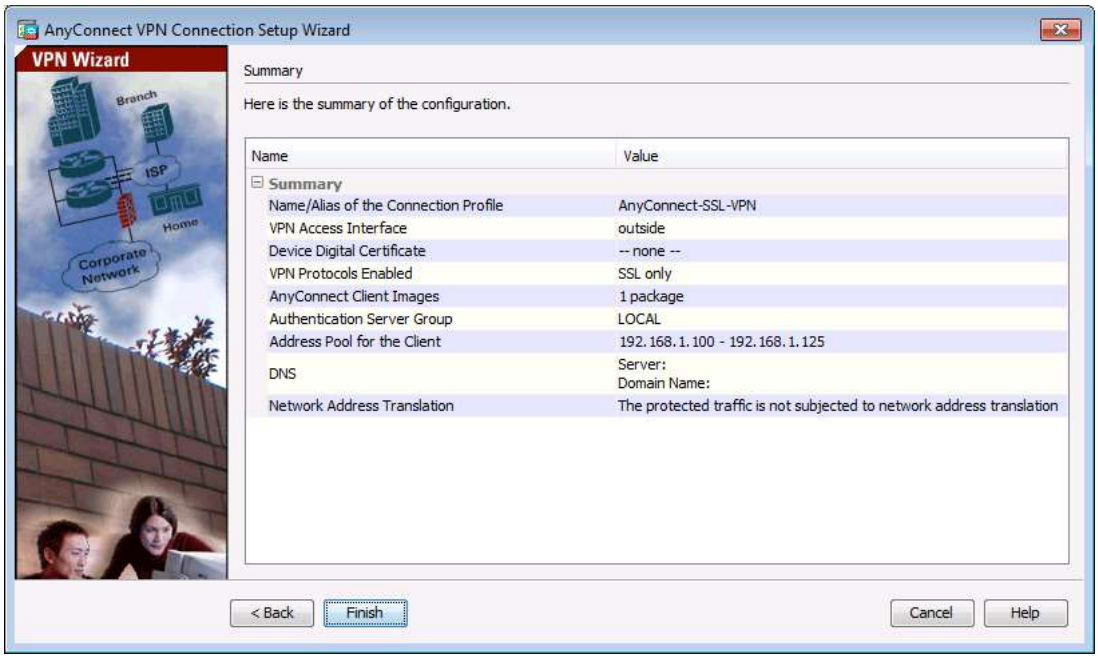
Шаг 9: Обзор варианта развертывания клиента AnyConnect.

На экране AnyConnect Client Deployment прочтите текст с описанием опций и нажмите **Next,** чтобы продолжить.



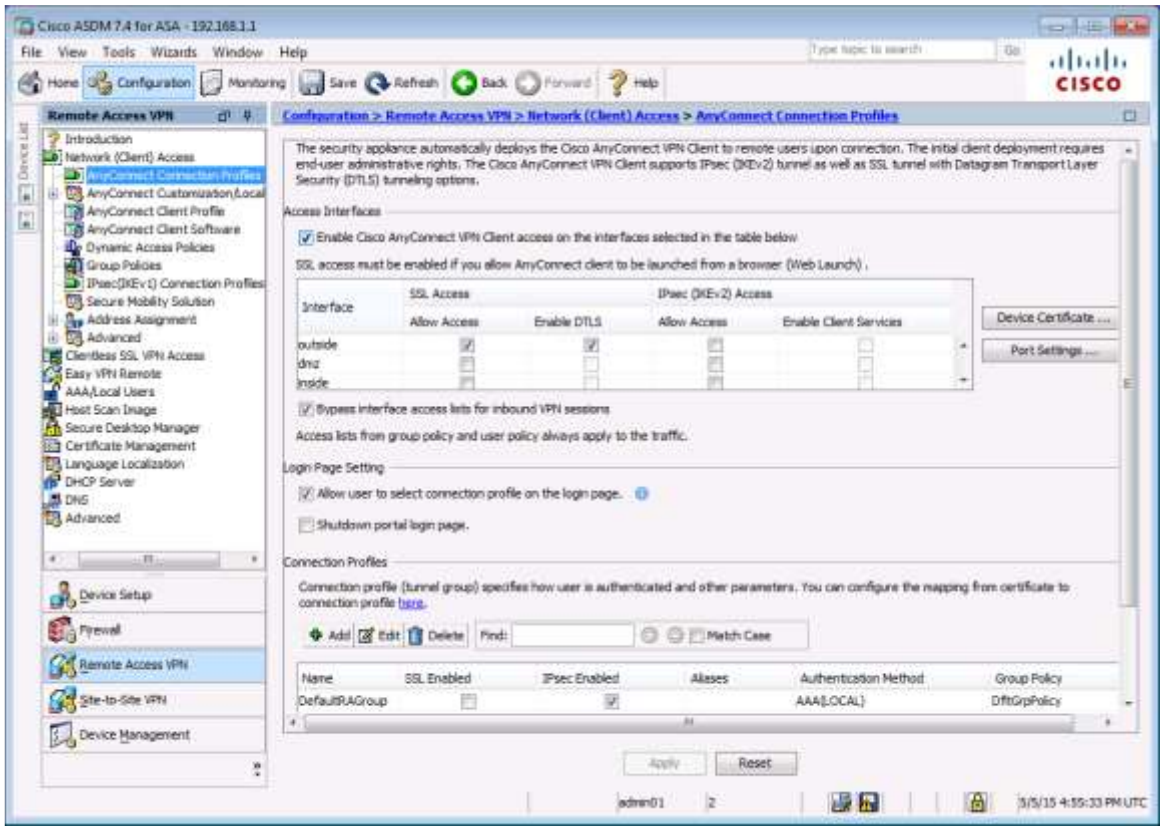
Шаг 10: Обзор экрана Summary и применение конфигурации для ASA.

На экране Summary проверьте описание конфигурации и нажмите **Finish**.



Шаг 11: Проверка профиля клиента AnyConnect.

После отправки конфигурации на устройство ASA появится экран AnyConnect Connection Profiles.

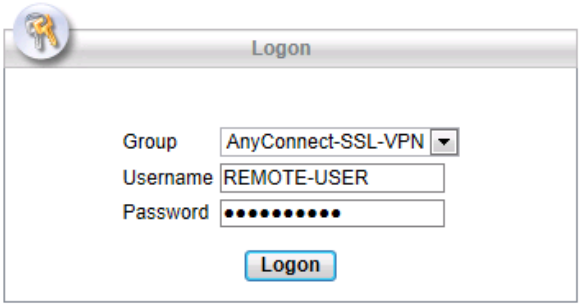


Часть 4: Подключение к AnyConnect SSL VPN

Шаг 1: Вход в систему с удаленного хоста.

a. Сначала необходимо установить соединение SSL VPN с ASA без использования клиента, чтобы скачать клиентское программное обеспечение AnyConnect. На компьютере PC-C откройте браузер. В поле адреса браузера введите **https://209.165.200.226** для SSL VPN. SSL требуется для подключения к ASA. Следовательно, используйте защищенный протокол HTTP (HTTPS).

b. Введите недавно созданные имя пользователя **REMOTE-USER** и пароль **cisco12345.** Для продолжения нажмите **Logon.**



Примечание. ASA может запросить подтверждение того, что это доверенный сайт. При получении такого запроса нажмите **Yes** для продолжения.

Шаг 2: Обнаружение платформы (при необходимости).

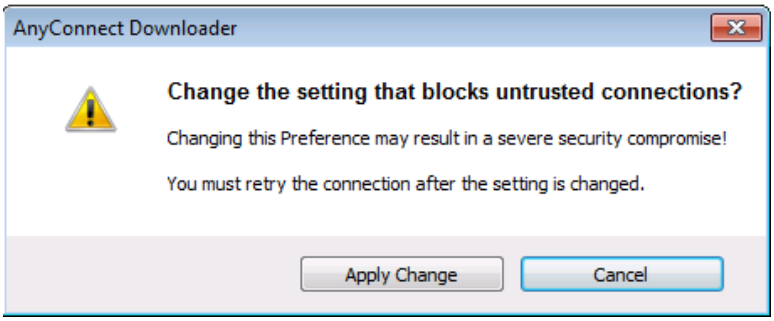
Если необходимо скачать клиент AnyConnect, на удаленном хосте будет выведено предупреждение системы безопасности. ASA определит, имеется ли ActiveX на хосте. Чтобы ActiveX корректно работал с Cisco ASA, важно, чтобы устройство безопасности было добавлено как доверенный сетевой сайт.

Примечание. Если ActiveX не обнаружен, необходимо вручную скачать и установить клиентское программное обеспечение AnyConnect. Чтобы получить инструкции о том, как вручную скачать клиентское программное обеспечение AnyConnect, перейдите к **шагу 3.**

a. ASA инициирует процесс автоматической загрузки программного обеспечения, состоящий из последовательности проверок на соответствие целевой системы. ASA определит платформу путем запроса клиентской системы, чтобы идентифицировать тип клиента, подключаемого к устройству безопасности. На основании полученных данных о платформе будет автоматически загружен требуемый программный пакет.

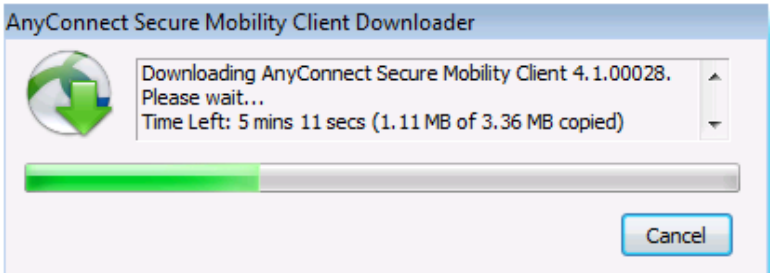
b. Если появится окно AnyConnect Downloader, в котором будет написано, что сервер AnyConnect 209.165.200.226 не удается верифицировать, нажмите кнопку **Change Setting.**

c. AnyConnect Downloader отобразит окно верификации, в котором можно изменить настройки, блокирующие недоверенные соединения. Нажмите **Apply Change**.

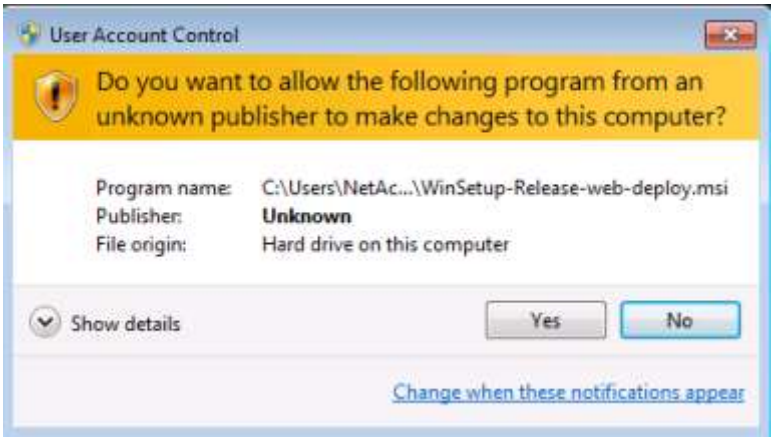


d. Если вы получите предупреждение Security Warning: Untrusted Server Certificate, нажмите **Connect Anyway.**

e. В окне AnyConnect Secure Mobility Client Downloader будет отображаться обратный отсчет времени загрузки.



f. После завершения загрузки начнется автоматическая установка загруженного программного обеспечения. При появлении запроса на внесение изменений на компьютере нажмите **Yes.**

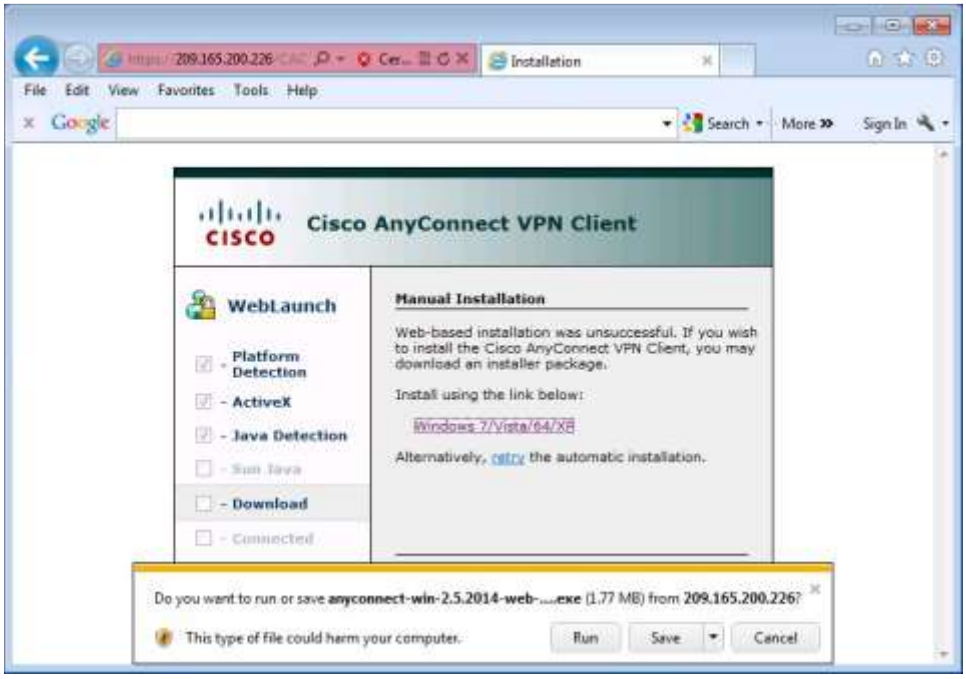


g. После завершения установки клиент AnyConnect установит подключение SSL VPN.

h. Если на панели слева установлен флажок Connected, перейдите к **шагу 5**. Если флажок Connected не установлен, перейдите к **шагу 3.**

Шаг 3: Установка вручную клиента AnyConnect VPN (при необходимости).

Если ActiveX не обнаружен, необходимо вручную скачать и установить клиентское программное обеспечение AnyConnect.

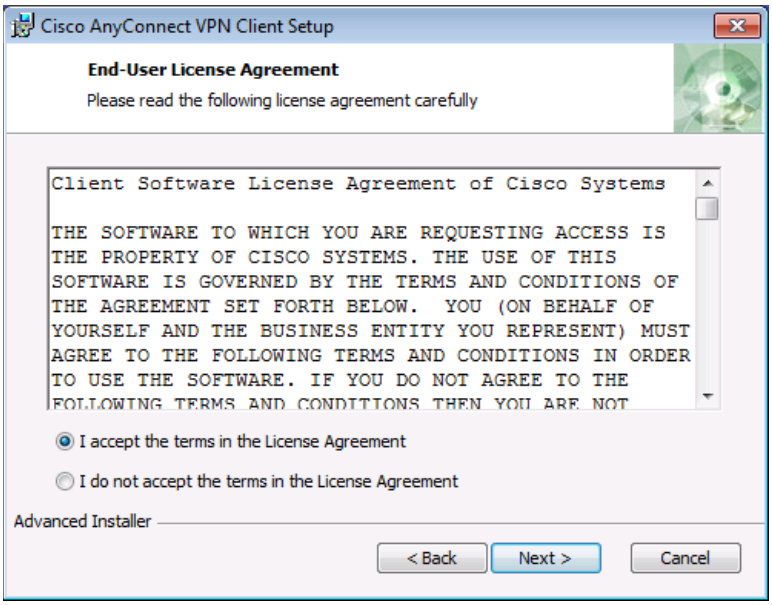


a. На экране Manual Installation нажмите **Windows 7/Vista/64/XP**.

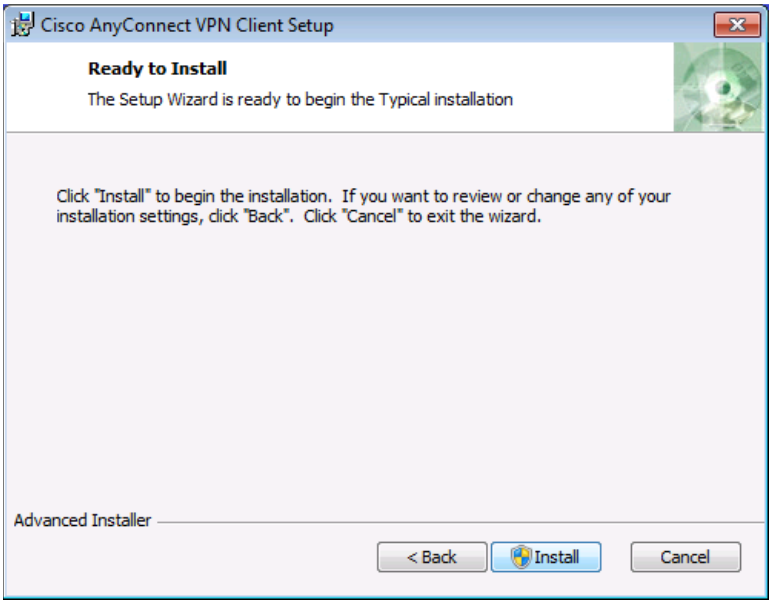
b. Нажмите **Run** для установки клиента AnyConnect VPN.

c. Как только загрузка будет завершена, начнется установка клиента Cisco AnyConnect VPN. Нажмите **Next**, чтобы продолжить.

d. Прочтите соглашение End-User License Agreement. Выберите опцию **I accept the terms in the License Agreement** и нажмите **Next,** чтобы продолжить.

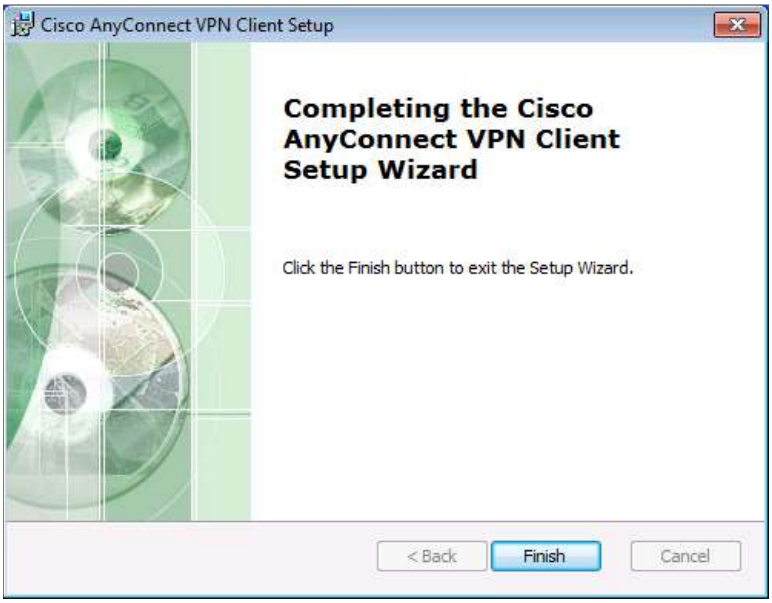


e. Появится окно Ready to Install. Нажмите **Install,** чтобы продолжить.



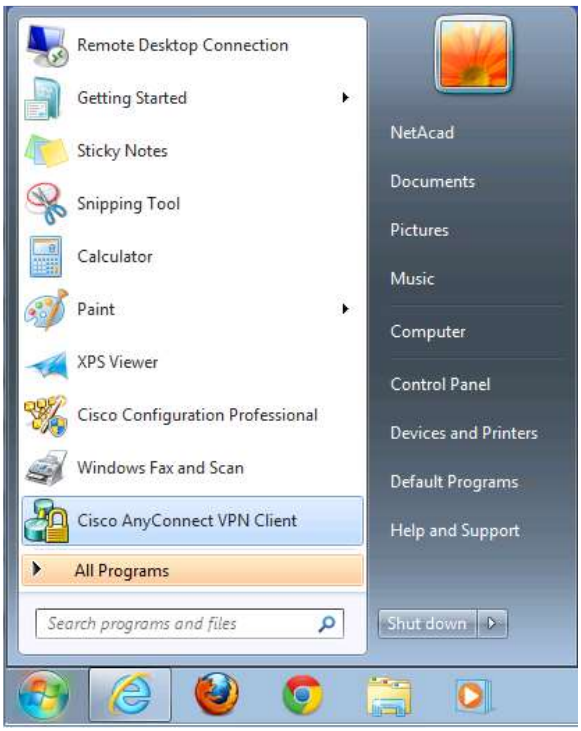
Примечание. Если появится предупреждение системы безопасности, нажмите **Yes**, чтобы продолжить.

f. Для завершения установки нажмите **Finish**.

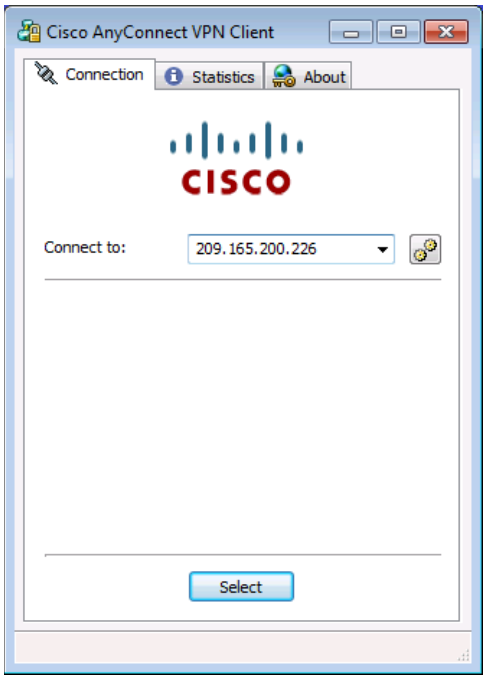


Шаг 4: Подключение к сети AnyConnect SSL VPN.

a. После установки клиента AnyConnect VPN запустите программу вручную, выбрав **Start > Cisco AnyConnect VPN Client**.

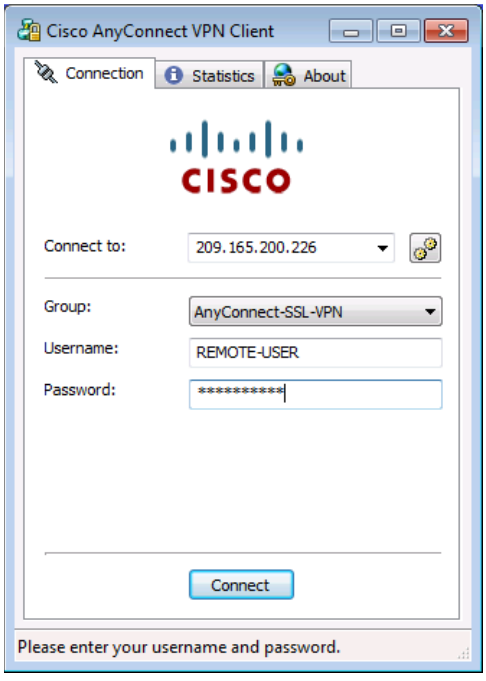


b. Программа предложит ввести адрес безопасного шлюза. Введите **209.165.200.226** в поле Connect to и нажмите **Select**.



Примечание. Если появится предупреждение системы безопасности, нажмите **Yes** для продолжения.

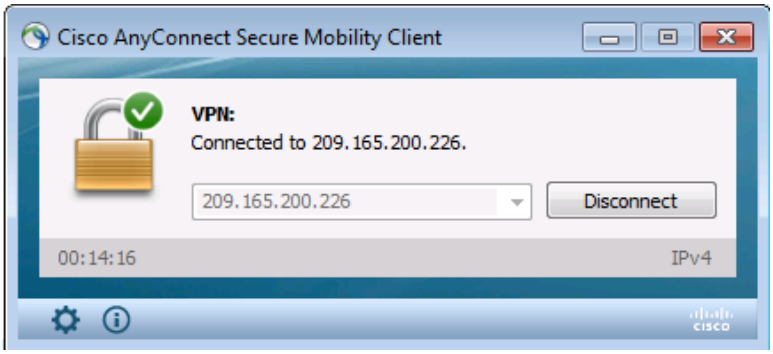
c. При получении запроса введите имя пользователя **REMOTE-USER** и пароль **cisco12345.**



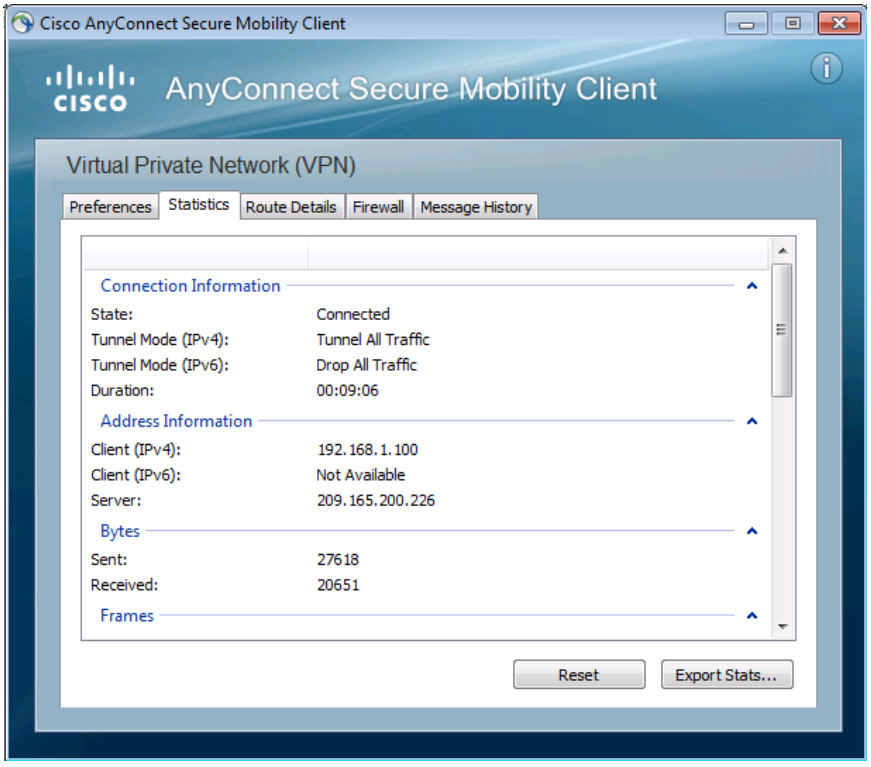
Шаг 5: Проверка связи по VPN.

После установления соединения SSL VPN по туннелю в области уведомлений системы появится значок, указывающий на успешное подключение клиента к сети SSL VPN.

a. Для отображения информации и статистики о соединении дважды щелкните значок **AnyConnect** в области уведомлений системы. Здесь же вы сможете прервать сеанс работы SSN VPN. Сейчас **НЕ** нажимайте кнопку **Disconnect.** Нажмите **значок шестеренки** в левом нижнем углу окна клиента Cisco AnyConnect Secure Mobility.

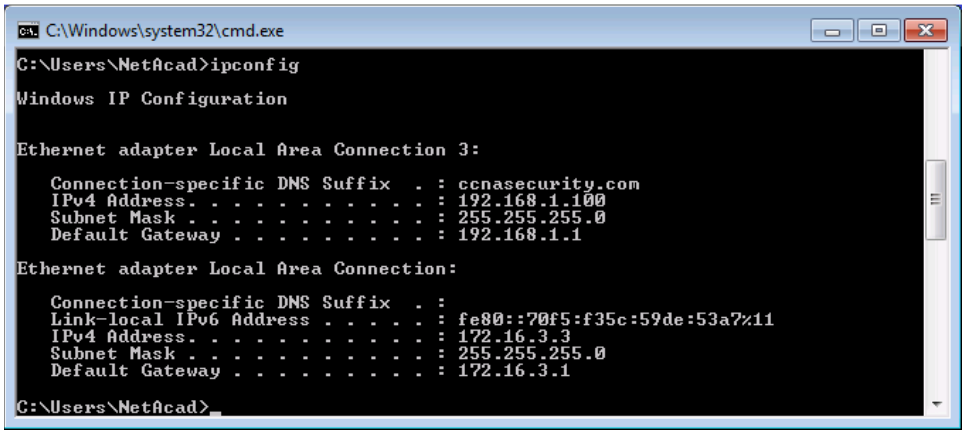


b. Чтобы получить дополнительную информацию о соединении, используйте полосу прокрутки в правой части вкладки Virtual Private Network (VPN) – Statistics.

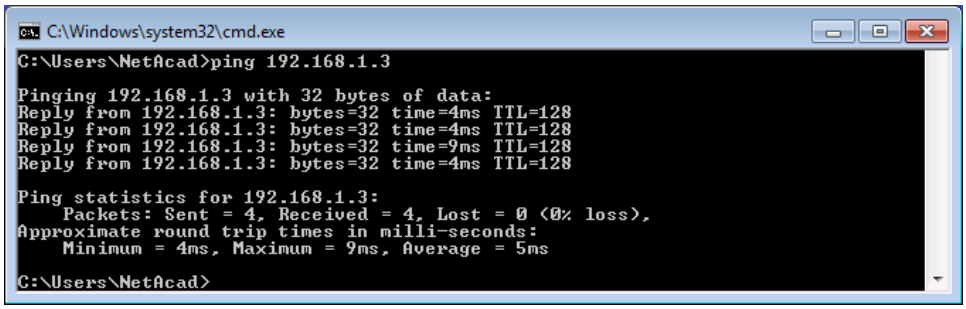


Примечание. Внутренний IP-адрес, назначенный клиенту из пула VPN, – 192.168.1.100-125.

c. В командной строке на удаленном хосте PC-C проверьте IP-адресацию с помощью команды **ipconfig.** Обратите внимание, что указаны два IP-адреса. Один из них – локальный IP-адрес удаленного хоста PC-C (172.16.3.3), а второй – IP-адрес, назначенный туннелю SSL VPN (192.168.1.100).



d. С удаленного хоста PC-C отправьте эхо-запрос на компьютер PC-B (**192.168.1.3**), чтобы проверить связь.

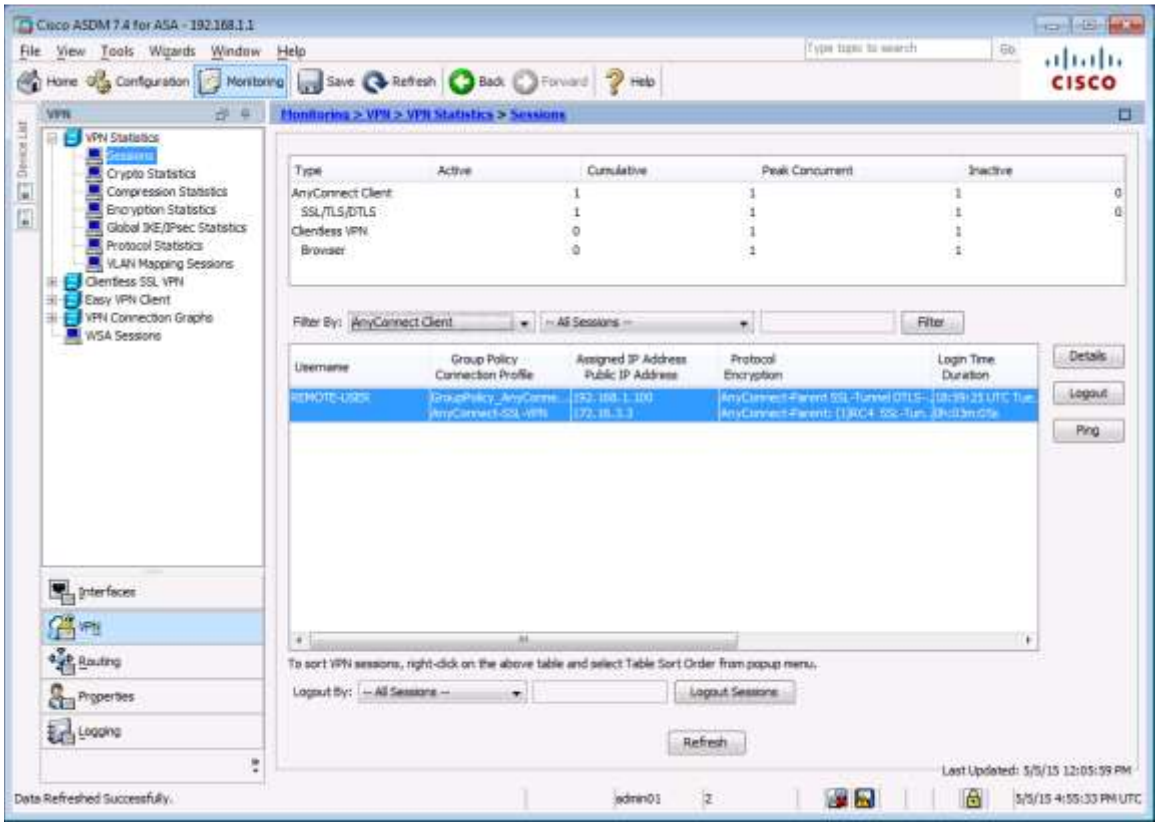


Шаг 6: Просмотр удаленного сеанса пользователя без клиента с помощью монитора ASDM.

Примечание. Последующие сеансы SSL VPN можно запустить на веб-портале или с помощью установленного клиента Cisco AnyConnect SSL VPN. Пока удаленный пользователь на компьютере PC-C находится в системе и использует клиент AnyConnect, вы с помощью монитора ASDM можете видеть статистику по сеансу.

В строке меню ASDM нажмите **Monitoring**, а затем выберите **VPN** > **VPN Statistics** > **Sessions**. Нажмите раскрывающийся список **Filter By** и выберите **AnyConnect Client**. Вы должны увидеть сеанс пользователя **VPN-User**, вошедшего в систему с компьютера PC-C, которому устройство ASA назначило внутренний сетевой IP-адрес 192.168.1.100.

Примечание. Для отображения сеанса удаленного пользователя может потребоваться нажать кнопку **Refresh.**



Вопросы для повторения

1. Укажите как минимум два преимущества сети VPN с использованием клиента по сравнению с сетью без использования клиента.

_____

_____

_____

_____

2. Укажите как минимум одно различие между вариантами использования SSL и IPsec для шифрования туннеля удаленного доступа.

_____

_____

_____

_____

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.

