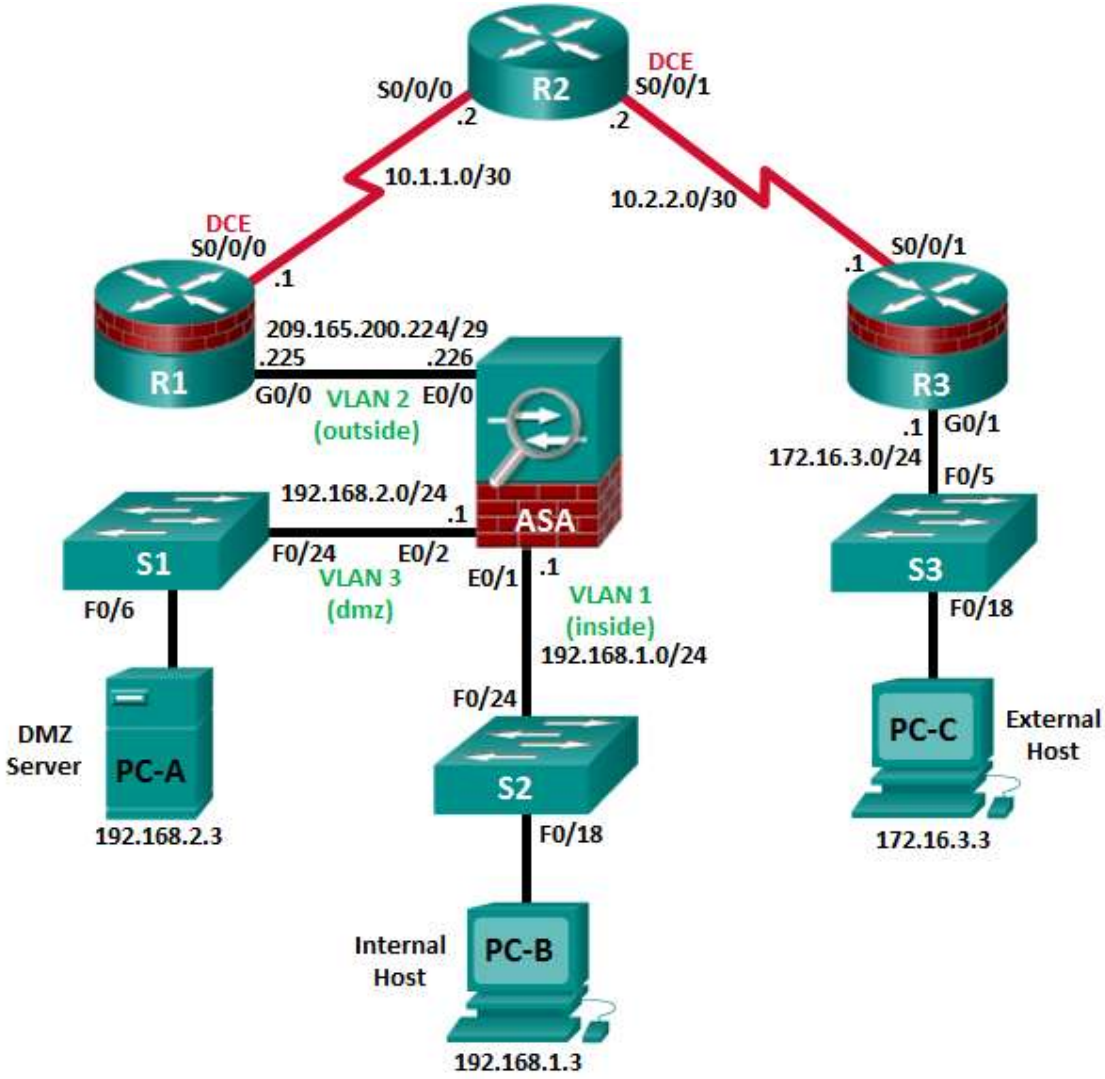
CCNA Security

Глава 10. Конфигурирование сетей SSL VPN удаленного доступа без использования клиента 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 сетей SSL VPN удаленного доступа без использования клиента с помощью ASDM

- Запуск мастера VPN
- Настройка интерфейса пользователя для SSL VPN
- Настройка аутентификации пользователей AAA
- Настройка групповой политики VPN
- Настройка списка закладок (только для соединений без клиента)
- Проверка сводки по конфигурации и отправка команд на ASA

- Проверка профиля подключения ASDM SSL VPN
- Проверка доступа к VPN из удаленного хоста
- Доступ к странице веб-портала
- Просмотр удаленного сеанса пользователя без клиента с помощью монитора ASDM

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 без использования клиента и проверки доступа с помощью браузера на удаленном ПК.

В вашей компании имеется 2 площадки, подключенных 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 без использования клиента, с помощью SSL и браузера для доступа клиентов.

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 с 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.

a. 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, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. 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.

a. 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.

a. 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
 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.

Между устройствами, подключенными к ASA, не будет связи, так как ASA является центральным узлом для сетевых зон и оно не было сконфигурировано. 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 запрос завершается 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 командной строки 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.

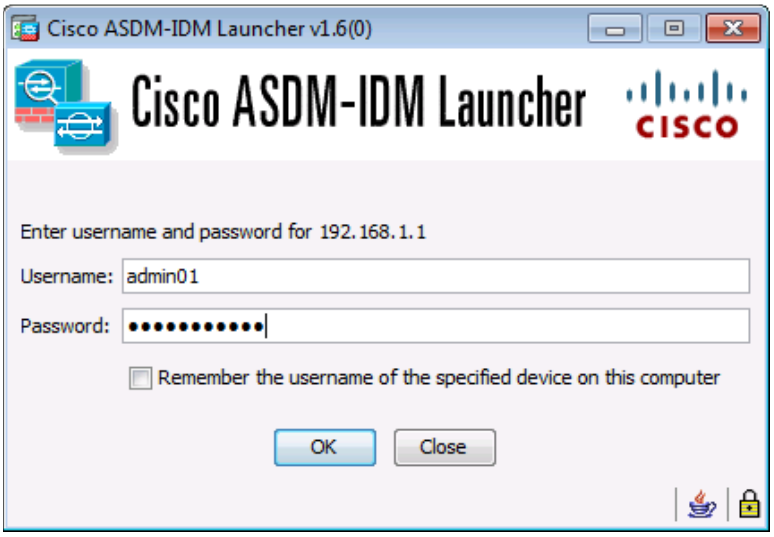
Шаг 4: Доступ к ASDM.

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.

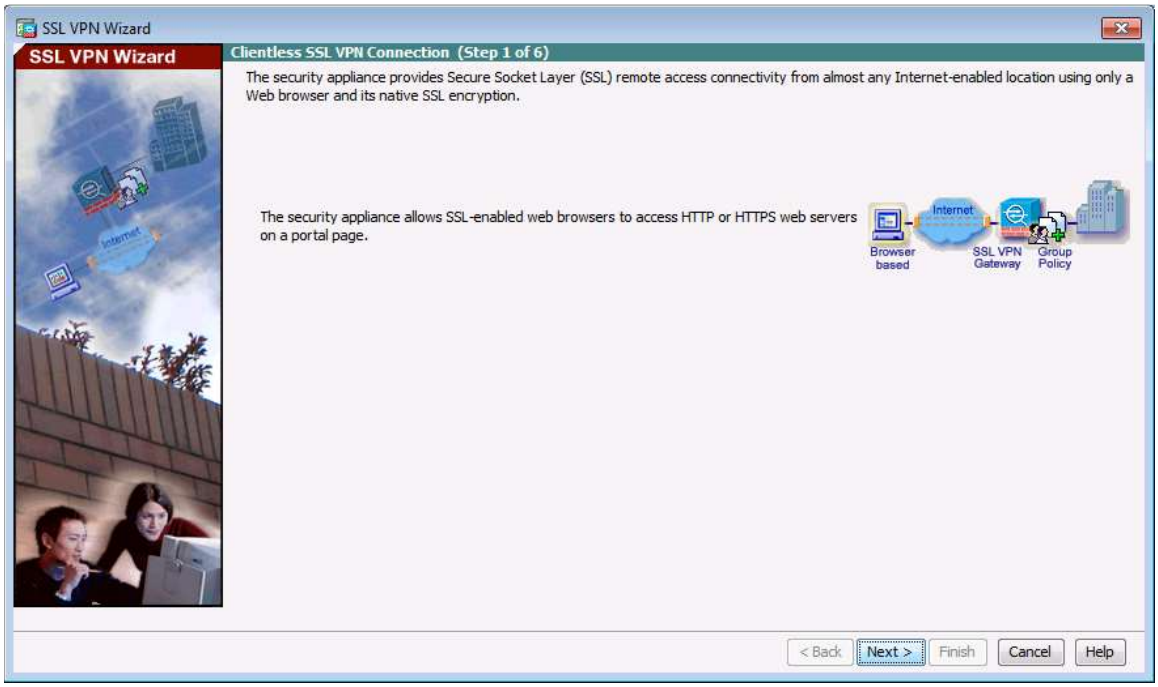
c. Войдите в систему как пользователь **admin01** с паролем **admin01pass.**



Часть 3: Настройка сетей SSL VPN удаленного доступа без использования клиента с помощью ASDM

Шаг 1: Запуск мастера VPN.

a. В главном меню ASDM выберите **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard.** Появится окно Clientless SSL VPN Connection мастера SSL VPN.



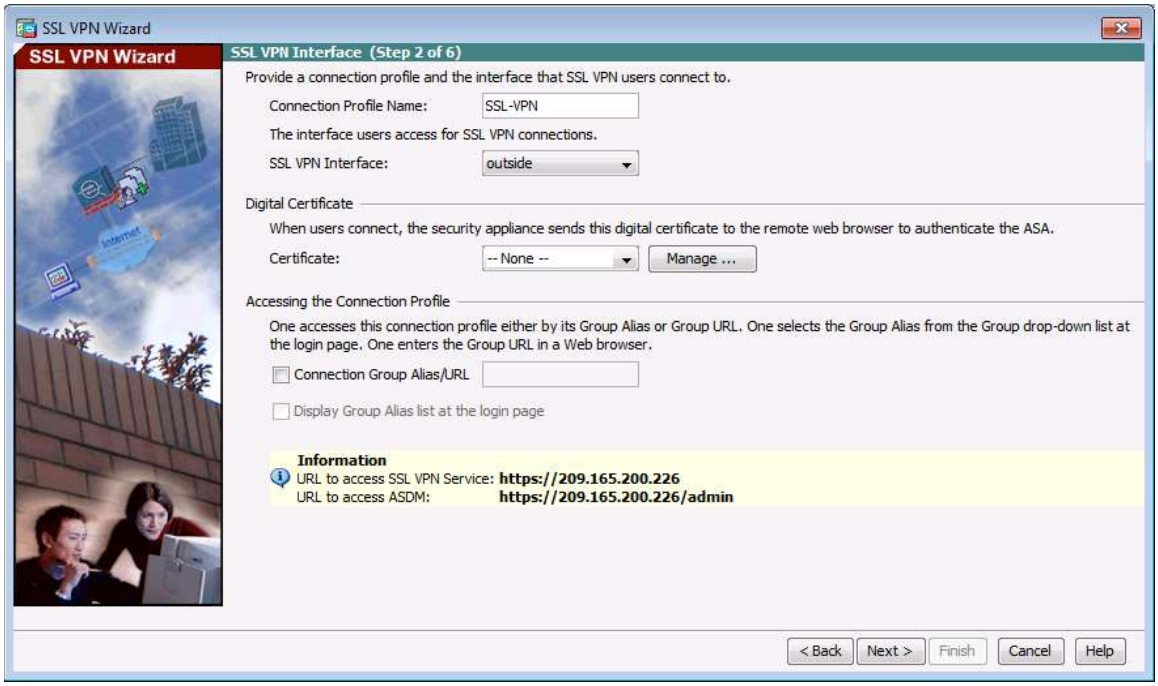
b. Прочтите текст на экране, проверьте топологическую схему и нажмите **Next,** чтобы продолжить.

Шаг 2: Настройка интерфейса пользователя для SSL VPN.

a. На экране SSL VPN Interface введите **SSL-VPN** в поле Connection Profile Name, а также укажите **outside** в качестве интерфейса, к которому будут подключаться внешние пользователи.

Примечание. По умолчанию ASA использует самоподписанный сертификат для авторизации клиента. При необходимости, ASA можно настроить так, чтобы для подключения клиентов это устройство использовало сторонний сертификат, приобретенный в широко известном центре сертификации, например в VeriSign. Если приобретен такой сертификат, его можно выбрать в раскрывающемся меню Digital Certificate.

Экран интерфейса SSL VPN содержит ссылки в разделе информации. Эти ссылки идентифицируют URL-адреса, которые необходимо использовать для доступа к сервисам SSL VPN (для входа в систему) и доступа к Cisco ASDM (доступ к программному обеспечению Cisco ASDM).



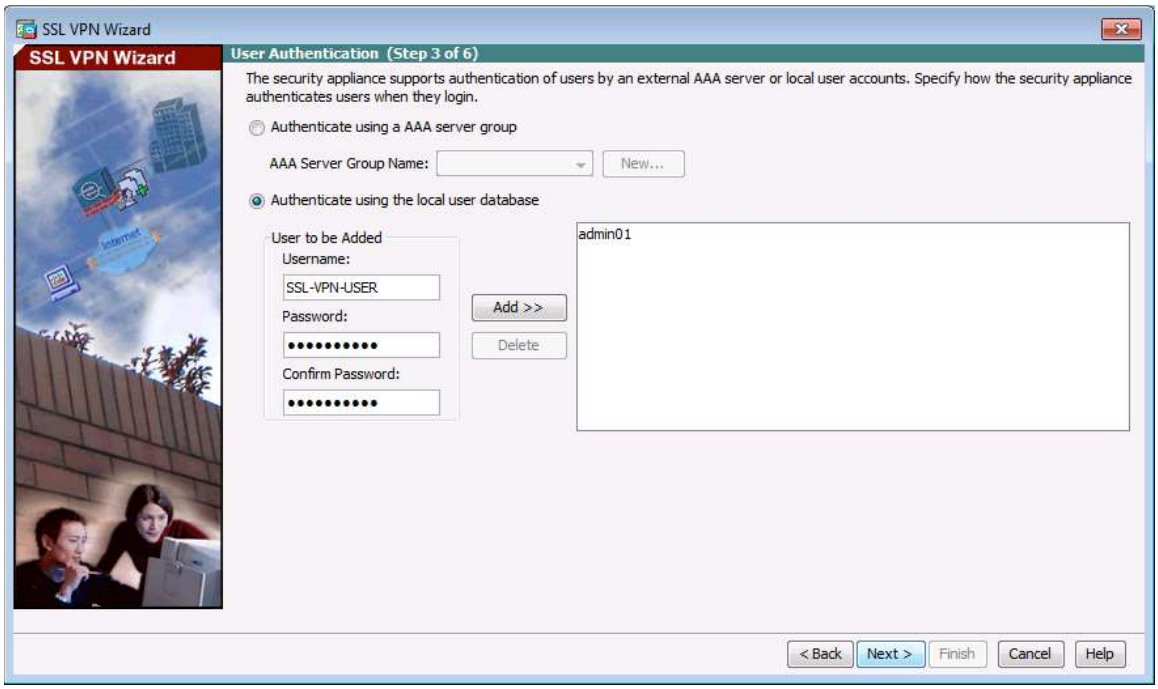
b. Нажмите **Next**, чтобы продолжить.

Шаг 3: Настройка аутентификации пользователей AAA.

a. На экране User Authentication нажмите **Authenticate using the local user database.**

b. Введите имя пользователя **SSL-VPN-USER** и пароль **cisco12345**.

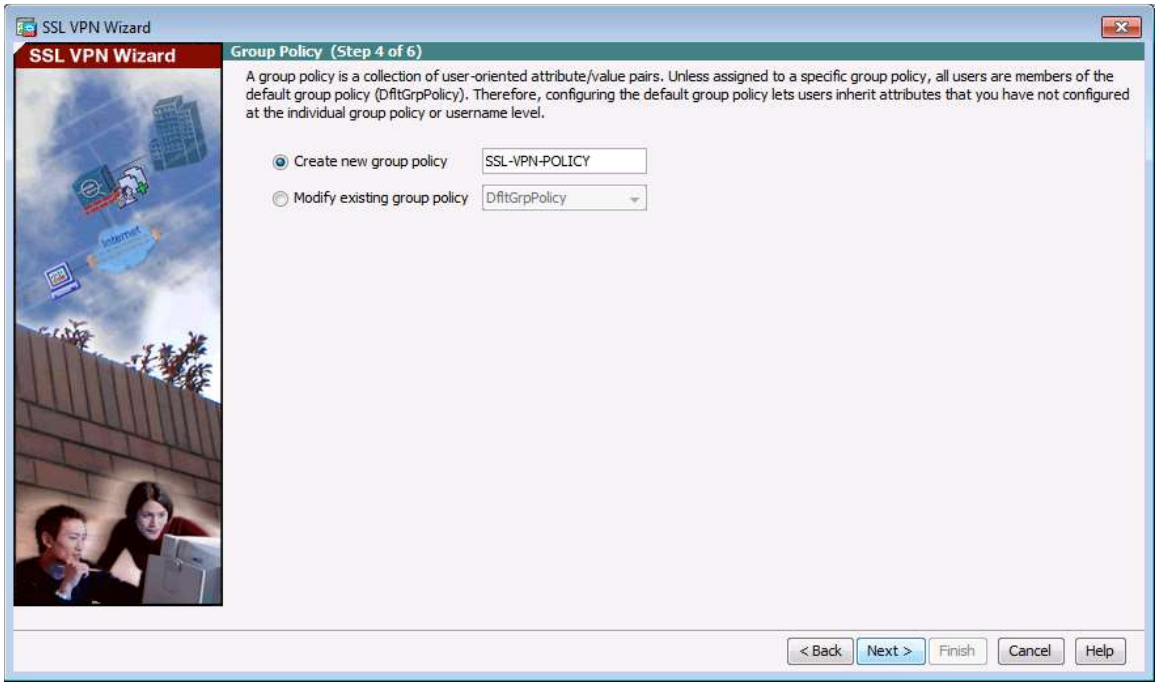
c. Нажмите **Add,** чтобы создать нового пользователя, а затем **Next,** чтобы продолжить.



Шаг 4: Настройка групповой политики VPN.

a. На экране Group Policy создайте новую групповую политику с именем **SSL-VPN-POLICY**.
(При конфигурировании новой политики следует иметь в виду, что ее имя не должно содержать пробелы.)

Примечание. По умолчанию созданная групповая политика наследует параметры из политики DfltGrpPolicy. Эти настройки можно изменить после завершения работы мастера. Выберите **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > подменю **Group Policies**.



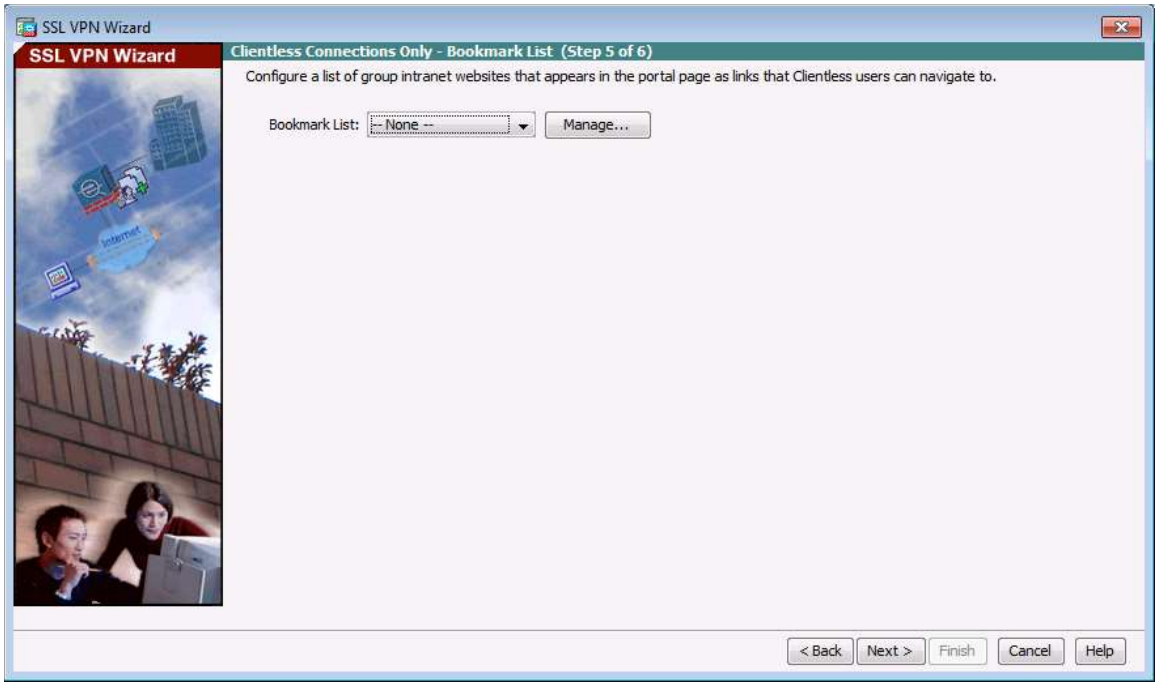
b. Нажмите **Next**, чтобы продолжить.

Шаг 5: Настройка списка закладок (только для соединений без клиента).

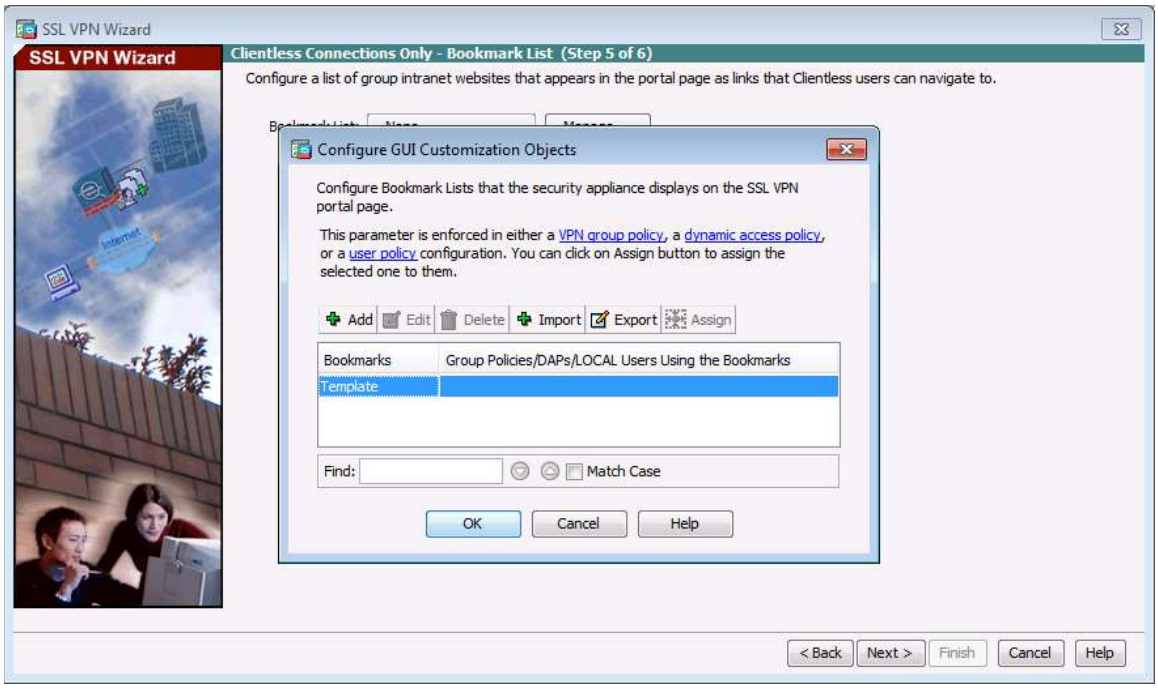
Список закладок – это набор URL-адресов, предназначенных для применения в веб-портале SSL VPN без использования клиента. Если такие закладки уже существуют, используйте раскрывающийся список **Bookmark List,** выберите нужную закладку и нажмите **Next,** чтобы продолжить работу с мастером SSL VPN.

Примечание. По умолчанию списков закладок нет. Поэтому они должны быть настроены сетевым администратором.

a. На экране Clientless Connections Only – Bookmark List нажмите **Manage**, чтобы создать закладку HTTP-сервера в списке закладок.

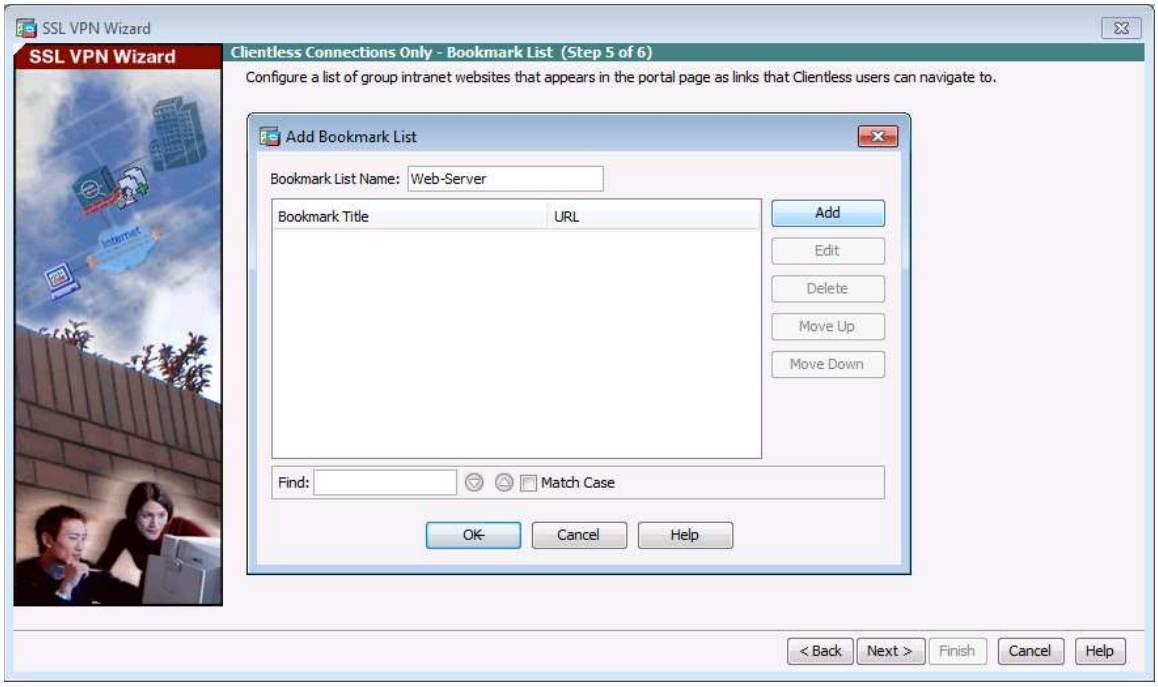


b. В окне Configure GUI Customization Objects нажмите **Add,** чтобы открыть окно Add Bookmark List. Введите для списка имя **Web-Server**.

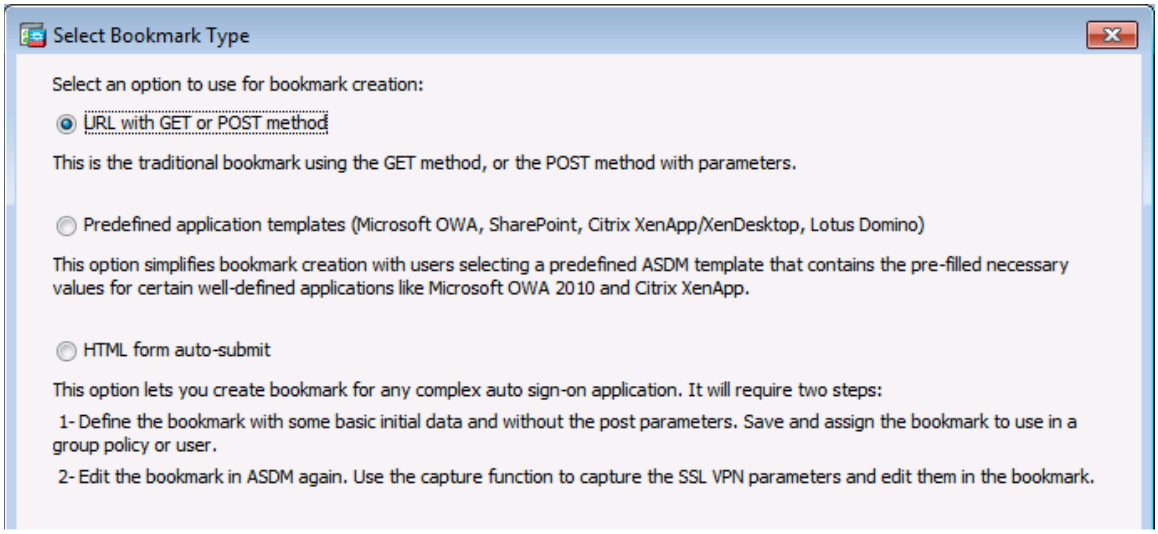


Примечание. Если уже отображается список закладок Web-Server из предыдущих конфигураций, его можно удалить в ASDM и создать заново.

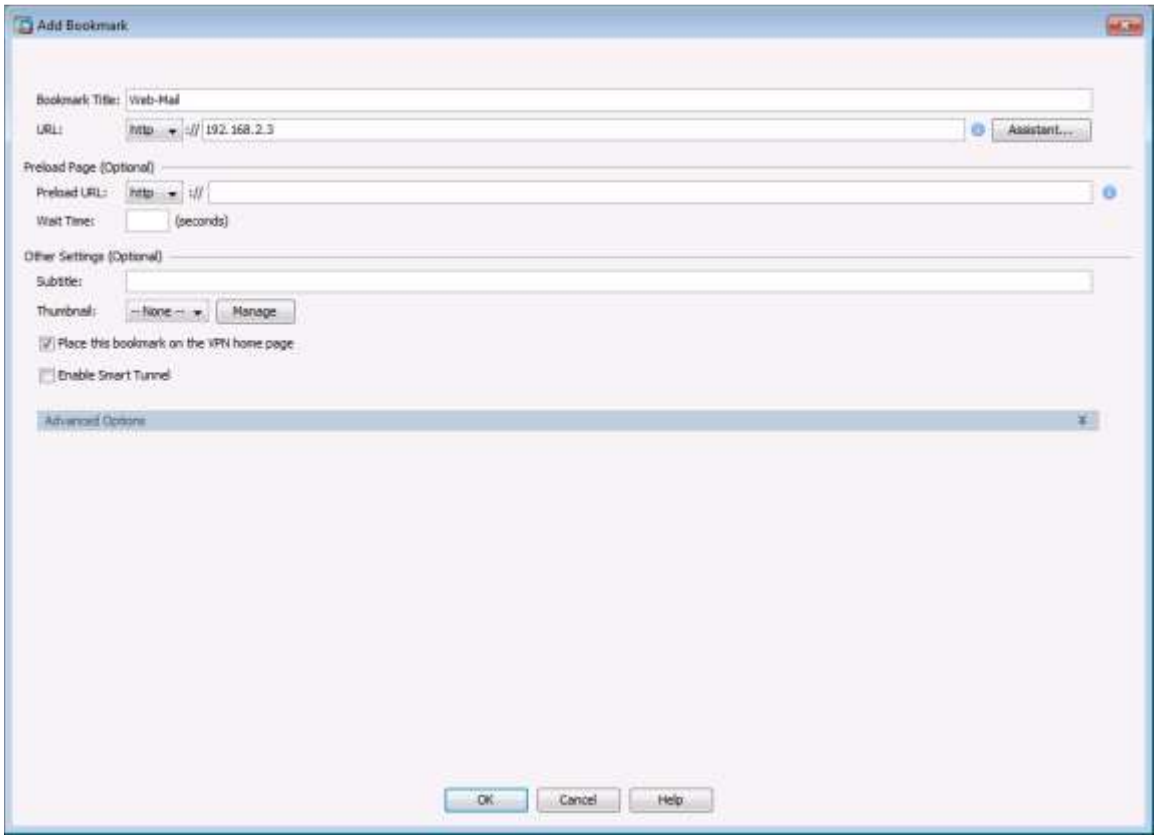
c. В окне Add Bookmark List нажмите **Add,** чтобы открыть окно Select Bookmark Type.



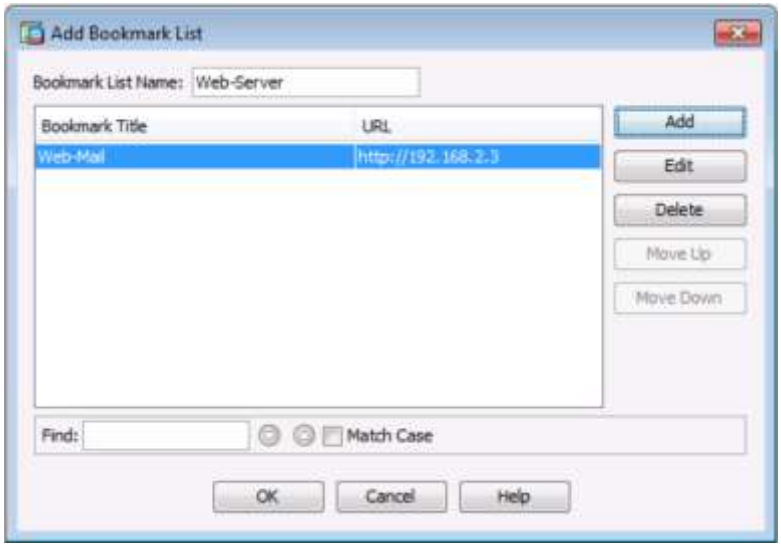
d. Как показано на рисунке, ASDM может создать закладки трех типов. Выберите опцию URL with GET or POST method и нажмите кнопку **OK**.



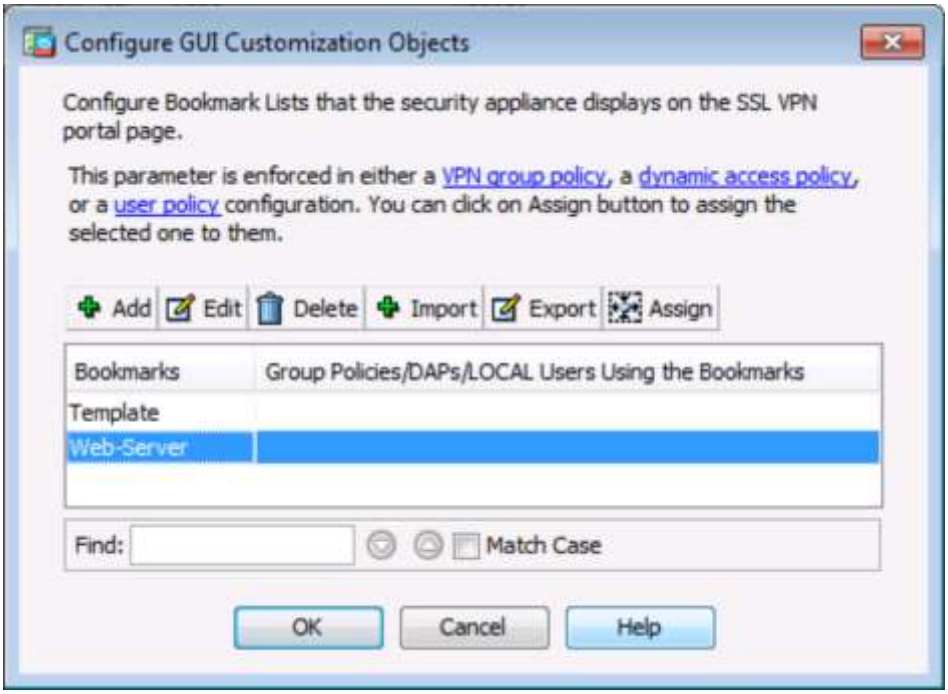
e. Введите название закладки и IP-адрес назначения сервера или имя хоста в качестве URL-адреса, который должен будет использоваться с адресом закладки. В данном примере указано название закладки **Web-Mail** и внутренний IP-адрес **192.168.2.3** (сервер DMZ). Если на этом сервере работают веб-сервисы HTTP, а также установлен и функционирует почтовый веб-сервер, то внешние пользователи смогут при подключении получить доступ к серверу с портала ASA.



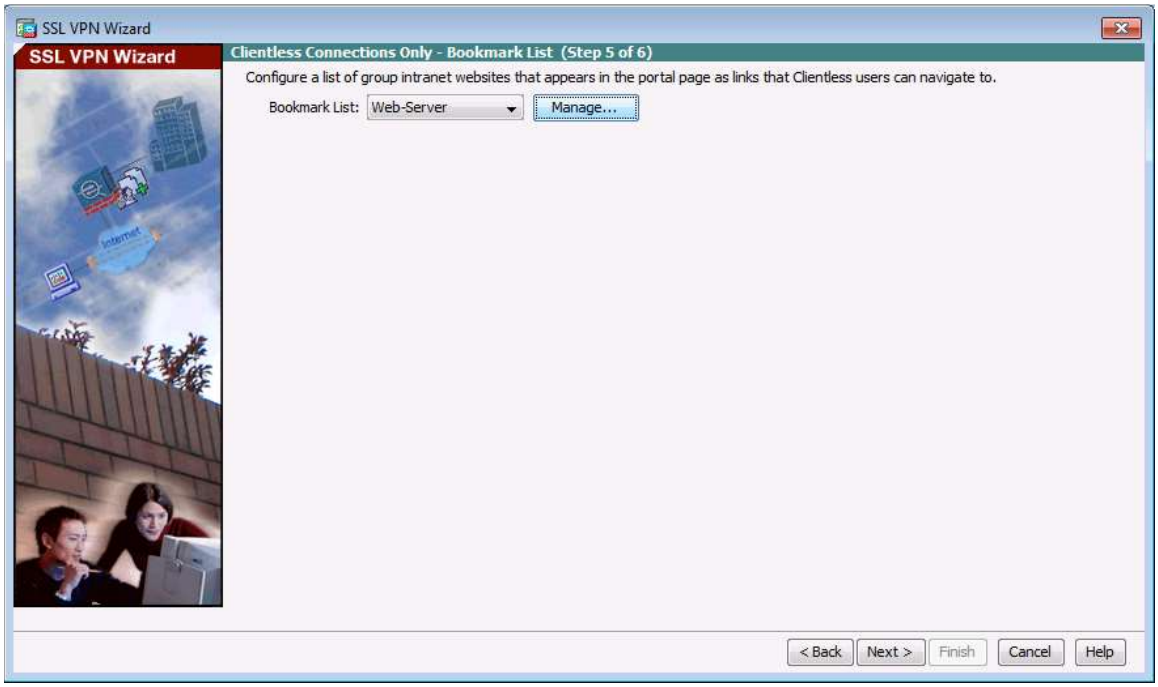
f. Нажмите кнопку **OK**, чтобы продолжить и вернуться в окно Add Bookmark List, в котором сейчас отображается название закладки Web-Server и ее URL-адрес.



g. Нажмите кнопку **OK**, чтобы продолжить и вернуться в окно Configure GUI Customization Objects, в котором теперь отображается закладка Web-Server.

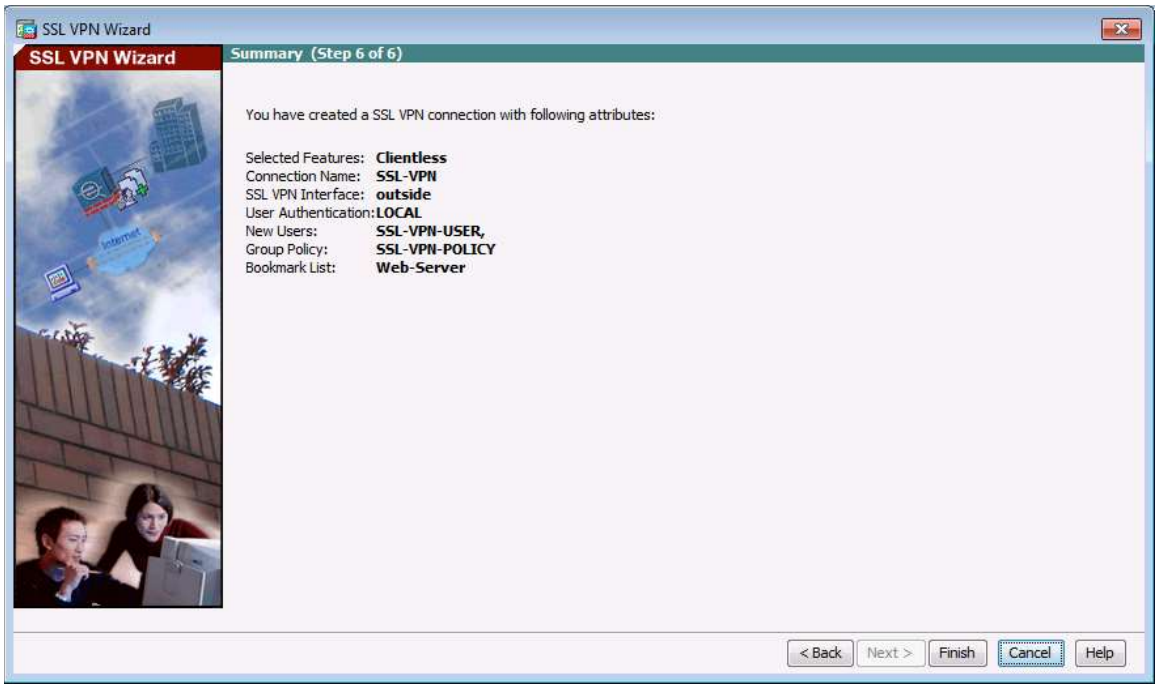


h. Нажмите кнопку **OK**, чтобы продолжить и вернуться в окно Bookmark List, а затем **Next**, чтобы продолжить.



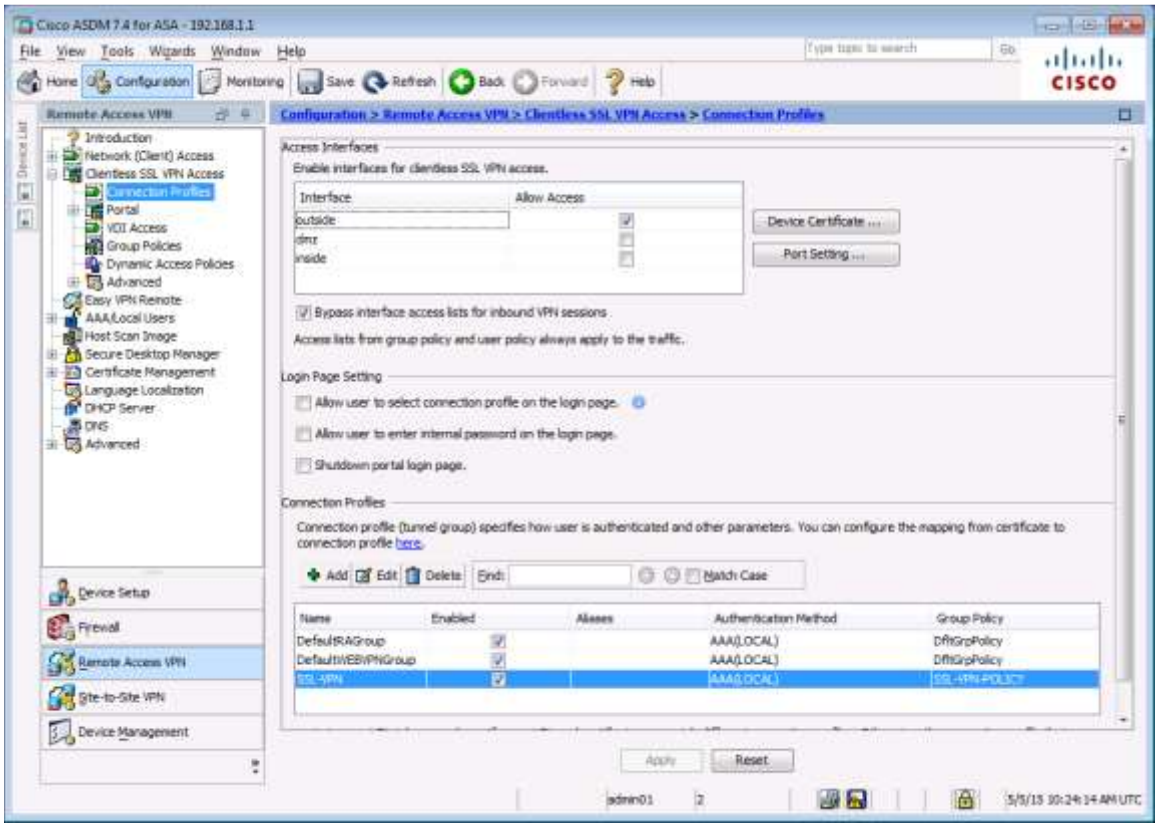
Шаг 6: Проверка сводки по конфигурации и отправка команд на ASA.

Появляется окно Summary. Убедитесь, что информация о настройках в мастере SSL VPN корректна. Для внесения изменений нажмите **Back** или нажмите **Cancel** и перезапустите мастер VPN. Нажмите **Finish**, чтобы завершить процесс и отправить команды в ASA.



Шаг 7: Проверка профиля подключения ASDM SSL VPN.

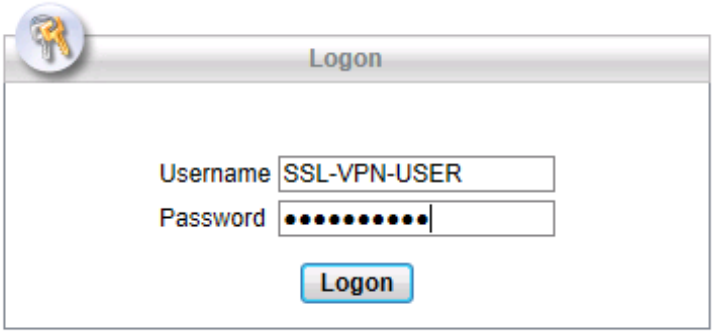
В ASDM выберите **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**. В этом окне можно проверить и изменить конфигурацию VPN.



Шаг 8: Проверка доступа к VPN из удаленного хоста.

a. Откройте браузер на компьютере PC-C и введите URL-адрес входа для SSL VPN в поле адреса (**https://209.165.200.226**). Используйте защищенный протокол HTTP (HTTPS), так как для подключения к ASA требуется SSL.

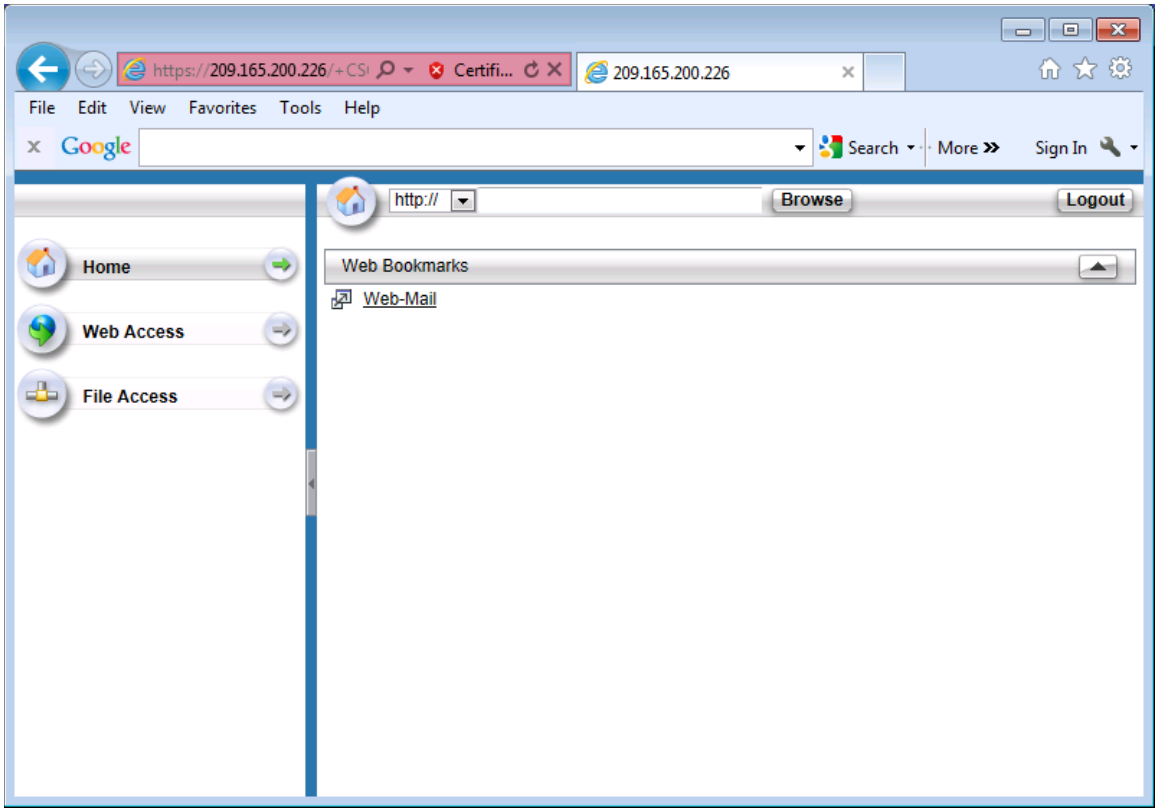
b. Должно появиться окно Logon. Введите указанное ранее имя пользователя **SSL-VPN-USER,** пароль **cisco12345** и нажмите кнопку **Logon.**



Шаг 9: Доступ к странице веб-портала.

После аутентификации пользователя на странице веб-портала ASA SSL появятся различные закладки, ранее назначенные данному профилю. Если закладка указывает на действительный IP-адрес сервера или имя хоста, на котором установлены и работают веб-сервисы HTTP, то внешний пользователь сможет получить доступ к этому серверу через портал ASA.

Примечание. В этой лабораторной работе почтовый веб-сервер не установлен.

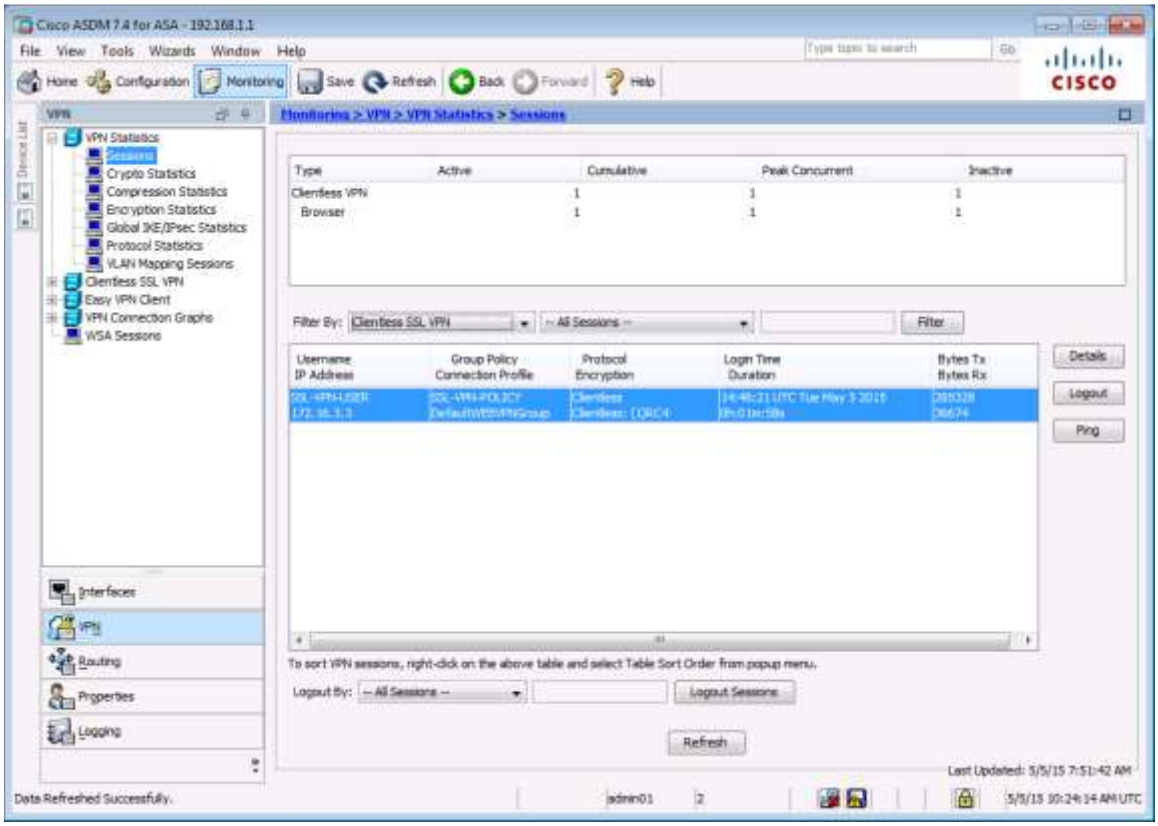


Шаг 10: Просмотр удаленного сеанса пользователя без клиента с помощью монитора ASDM.

Пока удаленный пользователь на компьютере PC-C находится в системе и на странице портала ASA, вы с помощью монитора ASDM можете просматривать статистику сеансов.

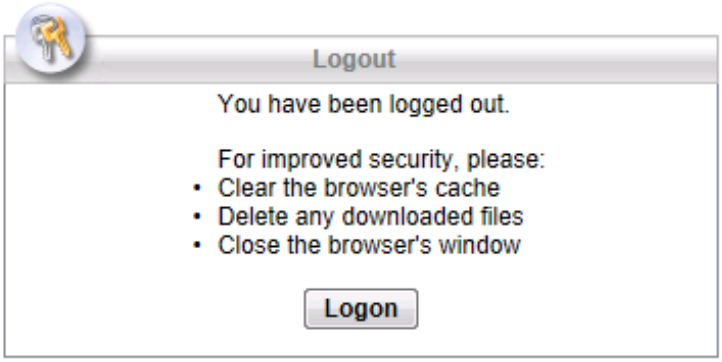
В строке меню ASDM на компьютере PC-B нажмите **Monitoring** и затем выберите **VPN** > **VPN Statistics** > **Sessions**. Щелкните раскрывающийся список **Filter By** и выберите **Clientless SSL VPN**. Вы должны увидеть сеанс пользователя SSL-VPN-USER, который выполнил вход с компьютера PC-C (172.16.3.3).

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



Шаг 11: Выход из веб-портала.

По окончании работы пользователь должен выйти из своей учетной записи на странице веб-портала на компьютере PC-C, используя кнопку **Logout** (см. шаг 10). Тем не менее выход из учетной записи также будет произведен через какое-то время в случае отсутствия активности. В любом случае отображается окно выхода из системы, в котором пользователь информируется о том, что для большей безопасности следует очистить кэш браузера, удалить загруженные файлы и закрыть окно браузера.



Вопросы для повторения

1. Каковы преимущества сетей VPN без использования клиента по сравнению с такими же сетями с использованием клиента?

_____

_____

_____

_____

_____

_____

2. Каковы различия в применении 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 (F0/1)	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.

