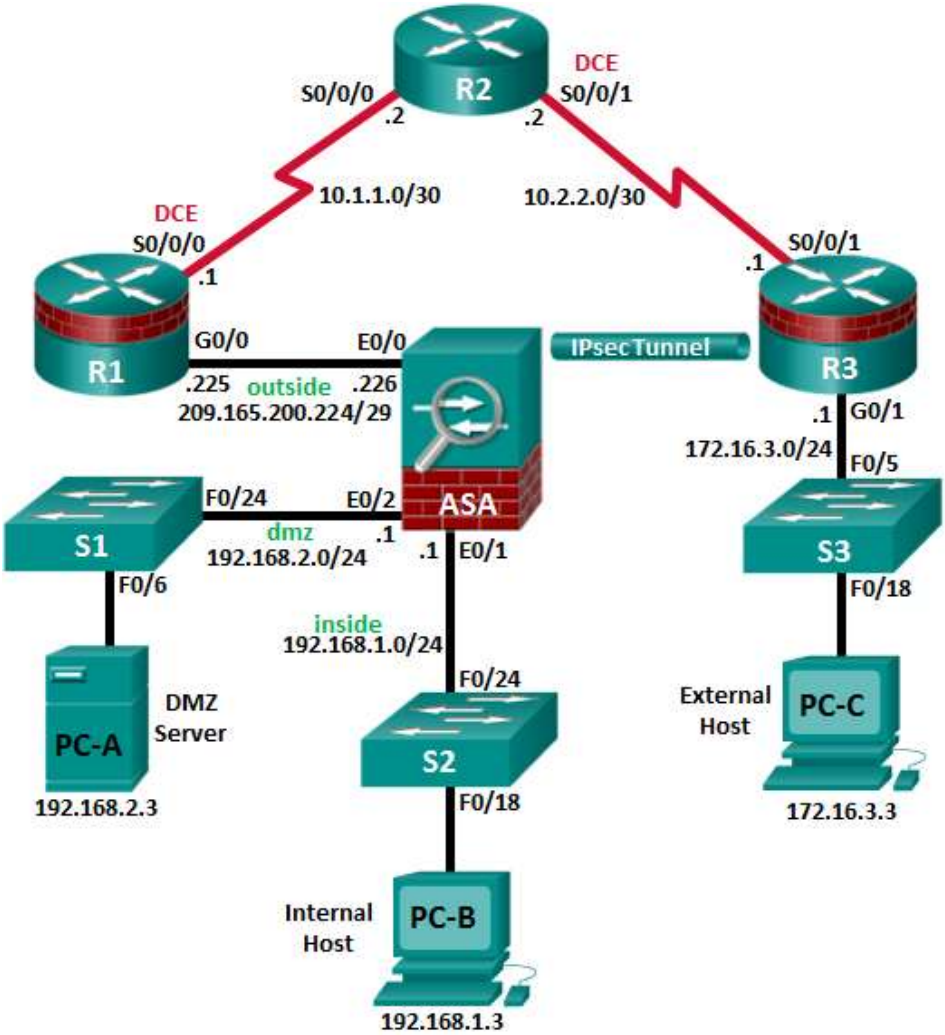
CCNA Security

Глава 10. Настройка сети Site-to-Site IPsec VPN между ISR и ASA

Топология



Примечание. Устройства ISR G2 используют 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 Fa0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 F0/0
	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 командного скрипта CLI
- Проверка доступа к ASDM по HTTP

Часть 3. Настройка ISR в качестве конечного устройства сети Site-to-Site IPsec VPN с помощью CLI

- Настройка основных параметров подключения VPN
- Настройка параметров политики IKE
- Настройка набора преобразований
- Указание трафика, который необходимо защитить
- Просмотр сводной информации по конфигурации
- Проверка конфигурации туннеля в site-to-site VPN

Часть 4. Настройка ASA в качестве конечного устройства сети Site-to-Site IPsec VPN с помощью ASDM

- Доступ к ASDM
- Обзор главной страницы ASDM
- Запуск мастера VPN
- Настройка идентификации другого устройства
- Указание трафика, который необходимо защитить
- Настройка аутентификации
- Настройка дополнительных параметров
- Проверка сводки по конфигурации и отправка команд на ASA
- Проверка профиля подключения VPN в ASDM
- Использование мониторинга ASDM для проверки туннеля

Исходные данные/сценарий

Помимо того что ASA функционирует как концентратор VPN удаленного доступа, это устройство может обеспечивать туннелирование IPsec VPN между двумя пунктами (site-to-site). Туннель может быть установлен как между двумя ASA, так и между ASA и другим устройством, поддерживающим IPsec VPN, например, как в данной лабораторной работе, ISR.

В вашей компании имеется 2 площадки, подключенные к ISP. Маршрутизатор R1 выступает в роли клиентского оборудования (CPE), работой которого управляет поставщик 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.

Руководство попросило вас организовать выделенный туннель site-to-site IPSec VPN между маршрутизатором ISR в удаленном офисе и устройством ASA в офисе корпорации. Этот туннель будет защищать трафик между LAN удаленного офиса и корпоративной LAN при его передаче через Интернет. Сеть site-to-site VPN не требует наличия VPN-клиента на ПК в удаленном или главном офисах. Трафик, поступающий из любой LAN в другие места назначения в Интернете, маршрутизируется поставщиком ISP и не защищается с помощью VPN-туннеля. VPN-туннель будет проходить через маршрутизаторы R1 и R2. Оба маршрутизатора не располагают информацией о наличии туннеля.

В части 1 данной лабораторной работы будет необходимо сконфигурировать топологию и устройства, отличные от ASA. В части 2 необходимо подготовить ASA к доступу через ASDM. В части 3 с помощью CLI необходимо настроить маршрутизатор R3 ISR в качестве конечного устройства туннеля site-to-site IPsec VPN. В части 4 необходимо настроить ASA в качестве конечного устройства site-to-site IPSec VPN при помощи мастера ASDM VPN.

Примечание. В данной лабораторной работе используются команды и соответствующие им выходные данные маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. В конце этой лабораторной работы приведена сводная таблица по интерфейсам маршрутизаторов, с помощью которой можно определить идентификаторы 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.

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.

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.

Сохраните **текущую конфигурацию** для каждого маршрутизатора.

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.

d. 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 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
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
```

e. 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.

Часть 3: Настройка ISR в качестве конечного устройства сети Site-to-Site IPsec VPN с помощью CLI

В части 3 данной лабораторной работы будет необходимо настроить маршрутизатор R3 в качестве конечного устройства сети IPsec VPN для туннеля между маршрутизатором R3 и ASA. Маршрутизаторы R1 и R2 не имеют информации о туннеле.

Шаг 1: Проверка связи между LAN маршрутизатора R3 и ASA.

На данном шаге необходимо убедиться, что с компьютера PC-C в LAN маршрутизатора R3 можно отправить эхо-запрос на внешний интерфейс ASA.

Отправьте с компьютера PC-C эхо-запрос на IP-адрес ASA **209.165.200.226.**

```
PC-C:\> ping 209.165.200.226
```

Если запросы завершаются с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Шаг 2: Включение политик IKE на маршрутизаторе R3.

IPsec – это открытая платформа, поддерживающая обмен протоколами безопасности по мере появления новых технологий и алгоритмов шифрования.

В процессе реализации сети IPsec VPN особое значение играют две операции конфигурирования:

- реализация параметров протокола Internet Key Exchange (IKE),
- реализация параметров IPsec.

a. Убедитесь, что IKE поддерживается и включен.

Фаза 1 IKE определяет метод обмена ключами, используемый для передачи политик IKE между узлами и проверки этих политик. На фазе 2 IKE узлы обмениваются и сопоставляют политики IPsec для аутентификации и шифрования передаваемых данных.

Чтобы IPsec работал, необходимо включить IKE. IKE по умолчанию включен в образах IOS с наборами криптографических функций. Если этот протокол выключен, его можно включить с помощью команды **crypto isakmp enable**. Эта команда позволяет проверить, что IOS маршрутизатора поддерживает IKE и что этот протокол включен.

```
R3(config)# crypto isakmp enable
```

Примечание. Если вы не можете выполнить эту команду на маршрутизаторе, необходимо обновить образ IOS до версии, которая содержит криптографические сервисы Cisco.

b. Установите политику ISAKMP и ознакомьтесь с доступными опциями.

Для обеспечения согласования на фазе 1 IKE необходимо создать политику ISAKMP и настроить ассоциацию узлов, содержащую эту политику. Политика ISAKMP определяет алгоритмы аутентификации и шифрования, а также хеш-функцию, используемую для отправки управляющего трафика между двумя конечными устройствами VPN. Как только ассоциация безопасности ISAKMP будет принята узлами IKE, фаза 1 IKE будет завершена. Параметры фазы 2 IKE будут настроены позднее.

Введите в режиме глобальной настройки команду **crypto isakmp** *policy number* на маршрутизаторе R1 для политики 10.

```
R1(config)# crypto isakmp policy 10
```


c. Для просмотра значений параметров IKE введите знак вопроса (**?**) в справке по Cisco IOS.

```
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Шаг 3: Настройка параметров политики ISAKMP на маршрутизаторе R3.

Степень конфиденциальности канала управления между двумя конечными устройствами определяется алгоритмом шифрования. Хеш-алгоритм контролирует целостность данных, то есть проверяет, что данные, полученные из узла, не были несанкционированно изменены при пересылке. Тип аутентификации гарантирует, что пакет был отправлен и подписан на удаленном узле. Для создания секретного ключа, используемого совместно узлами, но не пересылаемого по сети, используется группа Диффи-Хеллмана (Diffie-Hellman).

a. Установите для политики ISAKMP приоритет **10**. Используйте общий ключ (**pre-share**) в качестве типа аутентификации, **3des** – в качестве алгоритма шифрования, **sha** – в качестве хеш-алгоритма и группу Diffie Hellman **2** – для обмена ключами.

Примечание. Старые версии Cisco IOS не поддерживают шифрование AES 256 и SHA в качестве хеш-алгоритма. Замените указанные алгоритмы шифрования и хеширования на любые, поддерживаемые вашим маршрутизатором. Убедитесь также, что аналогичные изменения были проведены на маршрутизаторе R3.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 2
R3(config-isakmp)# end
```

b. Проверьте политику IKE с помощью команды **show crypto isakmp policy**.

```
R3# show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
       encryption algorithm:      Three key triple DES
       hash algorithm:            Secure Hash Standard
       authentication method:     Pre-Shared Key
       Diffie-Hellman group:      #2 (1024 bit)
       lifetime:           3600 seconds, no volume limit
```

Шаг 4: Настройка общих ключей.

На каждом маршрутизаторе, подключенном к другому конечному устройству в сети VPN, должен быть сконфигурирован ключ, так как в качестве метода аутентификации в политике IKE применяются общие ключи. Для успешной аутентификации эти ключи должны совпадать. Для ввода общего ключа применяется команда **crypto isakmp key** *key-string* **address** *ip-address* в режиме глобальной настройки. Используйте IP-адрес удаленного узла. Это должен быть IP-адрес удаленного интерфейса, который узел будет использовать для маршрутизации трафика на локальный маршрутизатор.

Какой IP-адрес необходимо использовать для настройки узла IKE, учитывая заданную топологическую схему и таблицу IP-адресов?

_____

_____

_____

a. В качестве IP-адреса удаленного устройства в VPN также можно применять каждый IP-адрес, используемый для настройки узлов IKE. На маршрутизаторе R3 сконфигурируйте общий ключ **SECRET-KEY**. В производственных сетях следует использовать сложный ключ. Эта команда указывает на внешний IP-адрес удаленного ASA.

```
R3(config)# crypto isakmp key SECRET-KEY address 209.165.200.226
```

Шаг 5: Конфигурирование набора преобразований и времени жизни Ipsec.

a. Набор преобразований Ipsec – это еще один криптографический параметр, который маршрутизаторы согласуют друг с другом для создания ассоциации безопасности. Его можно сконфигурировать с помощью команды **crypto ipsec transform-set** *tag* в режиме глобальной настройки. Сконфигурируйте набор преобразований с тегом **ESP-TUNNEL**. Для просмотра доступных параметров используйте **?**.

```
R3(config)# crypto ipsec transform-set ESP-TUNNEL ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform on R3
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
```

b. В сети VPN Site-to-site с ASA мы будем использовать два выделенных параметра. Добавьте в команду два выделенных параметра.

```
R3(config)# crypto ipsec transform-set ESP-TUNNEL esp-3des esp-sha-hmac
```

Какую функцию выполняет набор преобразований IPsec?

_____

_____

_____

_____

Шаг 6: Определение «интересного» трафика.

Чтобы использовать шифрование IPsec в сети VPN, необходимо определить расширенные списки доступа, с помощью которых маршрутизатор сможет понимать, какой трафик следует шифровать. Если сеанс IPsec сконфигурирован правильно, то пакет, разрешаемый в списке доступа, который применяется для определения трафика IPsec, будет шифроваться. Пакет, отклоняемый в одном из таких списков доступа, не отбрасывается. Такой пакет будет отправлен нешифрованным. Так же как и в любом другом списке доступа, в конце имеется оператор неявного отклонения. Это означает, что по умолчанию для трафика шифрование не выполняется. Если ассоциация безопасности IPsec сконфигурирована неправильно, трафик не шифруется и передается в нешифрованном виде.

В нашем сценарии с позиции маршрутизатора R3 мы хотим зашифровать трафик, идущий из Ethernet LAN маршрутизатора R3 во внутреннюю LAN ASA или в обратном направлении, если смотреть со стороны ASA.

a. Сконфигурируйте список ACL для «интересного» трафика в IPSec VPN на маршрутизаторе R3.

```
R3(config)# ip access-list extended VPN-ACL
R3(config-ext-nacl)# remark Link to the CCNAS-ASA
R3(config-ext-nacl)# permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
```

Проверяет ли IPsec наличие зеркальных списков доступа как необходимое условие для согласования ассоциации безопасности?

_____

_____

_____

Шаг 7: Создание и применение криптографической карты.

Криптографическая карта ассоциирует трафик, соответствующий списку доступа, с узлом и различными параметрами IKE и IPsec. После создания криптографической карты ее можно применить к одному или нескольким интерфейсам. Интерфейсы, к которым такая карта применяется, должны быть соединены с узлом IPsec.

Для создания криптографической карты используйте команду **crypto map** *name sequence-num type* в режиме глобальной настройки, чтобы ввести режим настройки криптографической карты для заданного порядкового номера. В одной криптографической карте может быть несколько криптографических операторов, которые анализируются в порядке возрастания номеров.

a. На маршрутизаторе R3 создайте криптографическую карту, назовите ее **S2S-MAP** и укажите 10 в качестве порядкового номера. Используйте тип **ipsec-isakmp,** чтобы указать, что для установления ассоциаций безопасности IPsec будет применяться IKE. После ввода команды будет выведено сообщение.

```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#
```

b. Используйте команду **match address** *access-list* для указания списка доступа, определяющего трафик, подлежащий шифрованию.

```
R3(config-crypto-map)# match address VPN-ACL
```

c. Требуется указать IP-адрес или имя хоста для узла. Укажите интерфейс удаленного конечного устройства VPN ASA с помощью следующей команды.

```
R3(config-crypto-map)# set peer 209.165.200.226
```

d. Используйте команду **set transform-set** *tag,* чтобы четко указать набор преобразований, который должен использоваться с этим узлом.

```
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# exit
```

e. Примените криптографическую карту к интерфейсам.

Примечание. Ассоциации SA будут установлены только после активации криптографической карты «интересным» трафиком. Маршрутизатор сгенерирует уведомление о том, что шифрование теперь активно.

Примените криптографические карты к последовательному интерфейсу 0/0/1 маршрутизатора R3.

```
R3(config)# interface Serial0/0/1
R3(config-if)# crypto map S2S-MAP
R3(config-if)# end
R3#
*Mar  9 06:23:03.863: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3#
```

Часть 4: Настройка ASA в качестве конечного устройства сети Site-to-Site IPsec VPN с помощью ASDM

В части 4 этой лабораторной работы необходимо настроить ASA в качестве конечного устройства туннеля Ipsec VPN. Туннель между ASA и маршрутизатором R3 проходит через маршрутизаторы R1 и R2.

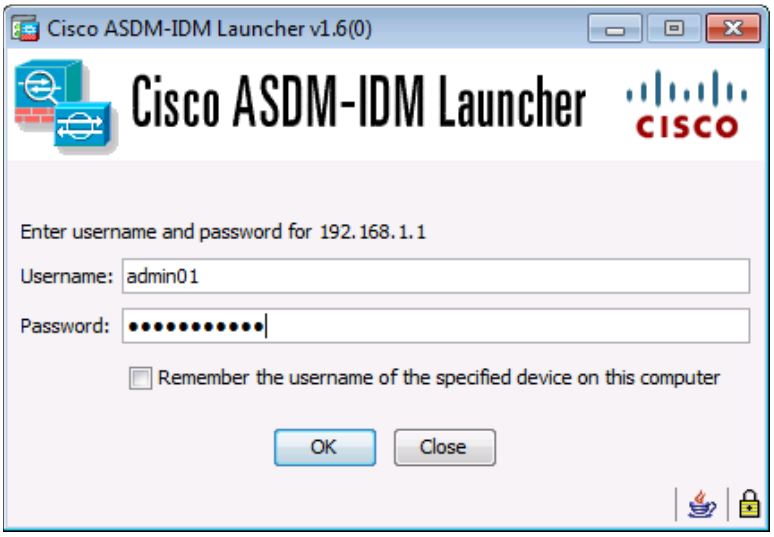
Шаг 1: Доступ к ASDM.

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.

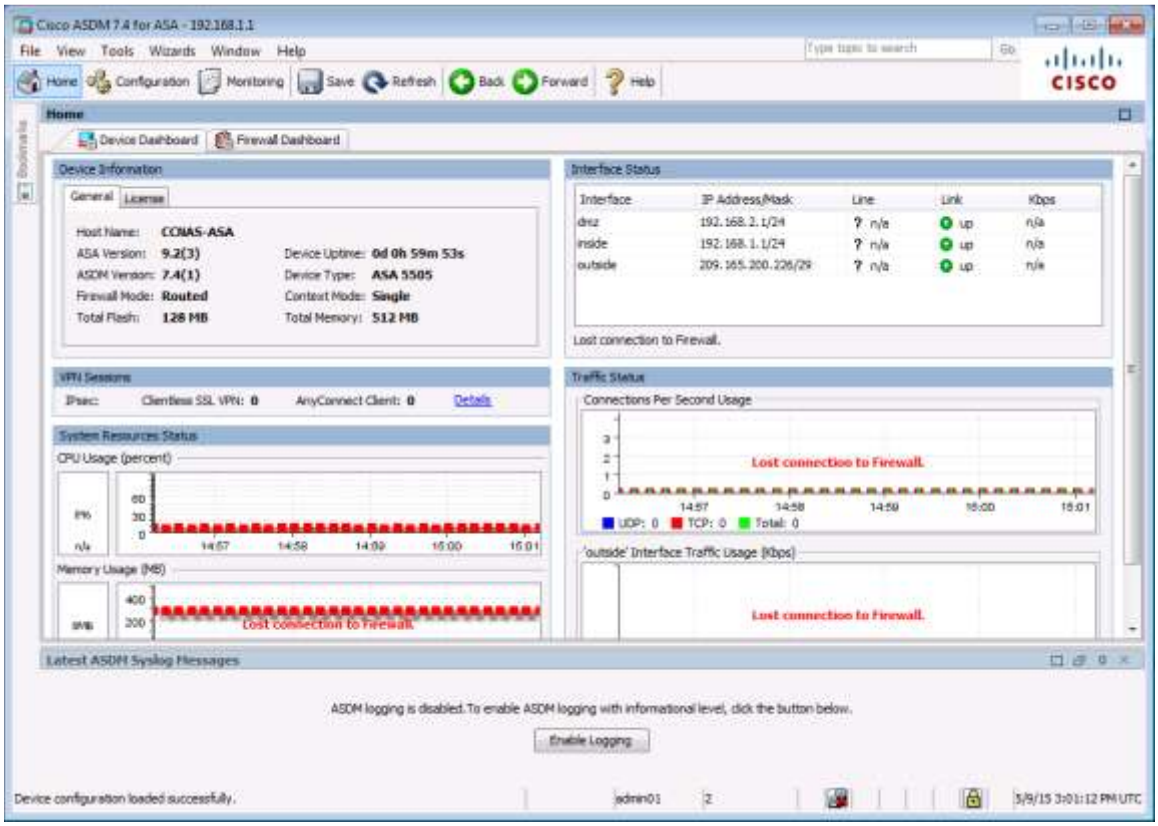
b. На стартовой странице ASDM нажмите **Run ASDM**. Появится окно ASDM-IDM Launcher.

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



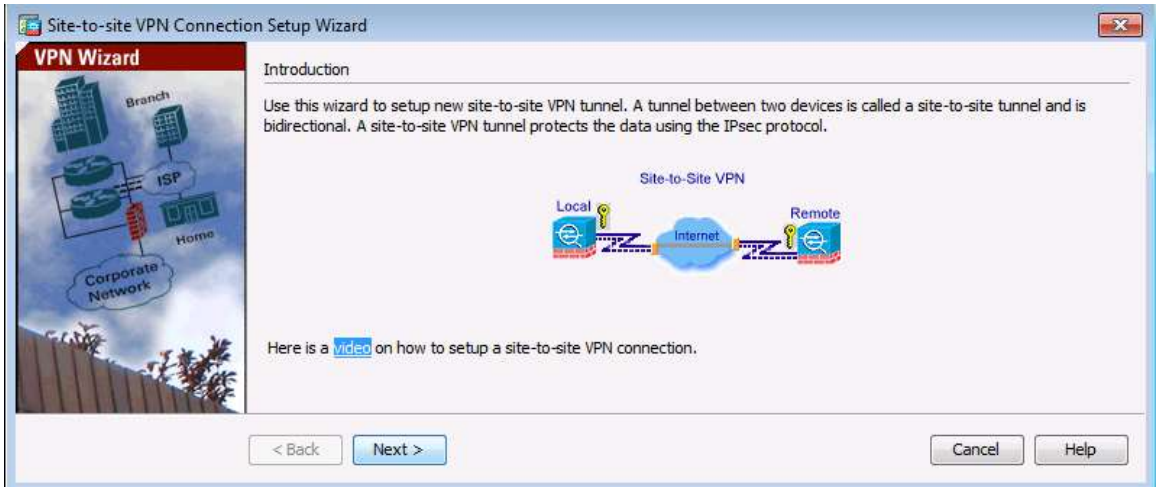
Шаг 2: Обзор главной страницы ASDM.

На главной странице отображается текущая конфигурация устройства ASA и статистика о потоке трафика. Обратите внимание на внешние и внутренние интерфейсы, а также интерфейсы dmz, сконфигурированные в части 2 данной лабораторной работы.



Шаг 3: Запуск мастера VPN.

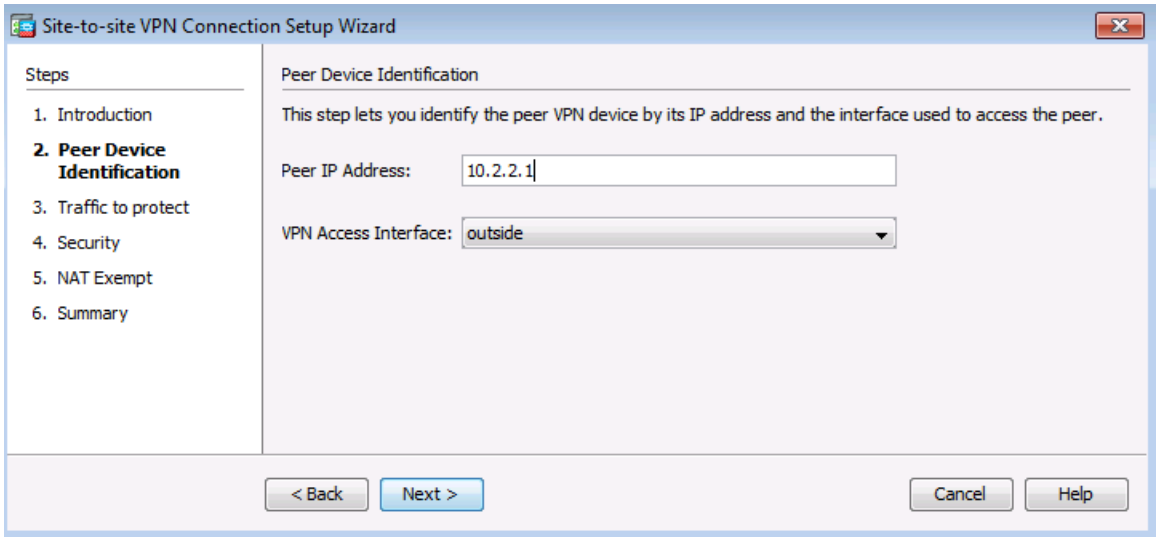
a. В главном меню ASDM выберите **Wizards** > **VPN Wizards** > **Site-to-Site VPN Wizard**, чтобы открыть окно Site to-Site VPN Connection Setup Wizard Introduction.



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

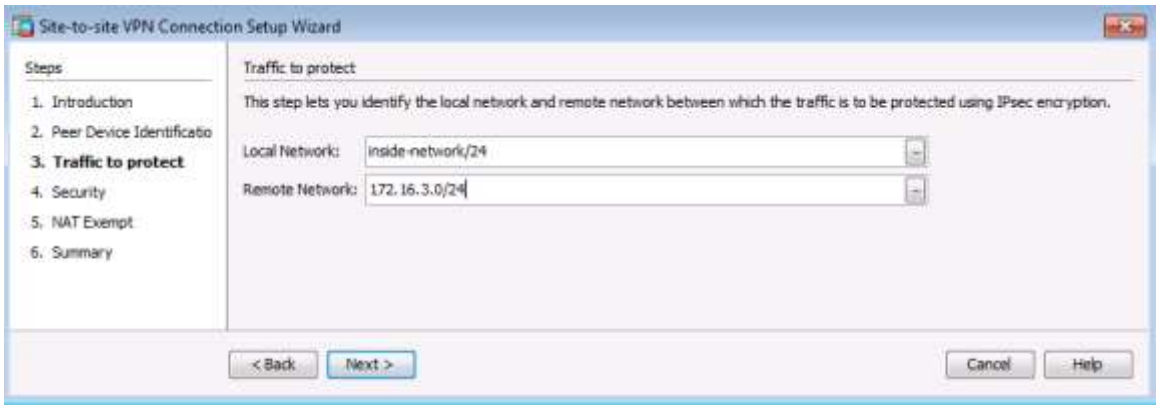
Шаг 4: Настройка идентификации другого устройства.

В окне Peer Device Identification введите IP-адрес последовательного интерфейса Serial0/0/1 маршрутизатора R3 (**10.2.2.1)** в качестве IP-адреса узла. Оставьте для интерфейса доступа к VPN по умолчанию значение **outside.** VPN-туннель будет установлен между интерфейсом S0/0/1 маршрутизатора R3 и внешним интерфейсом ASA (VLAN 2 E0/0). Нажмите **Next**, чтобы продолжить.



Шаг 5: Указание трафика, который необходимо защитить.

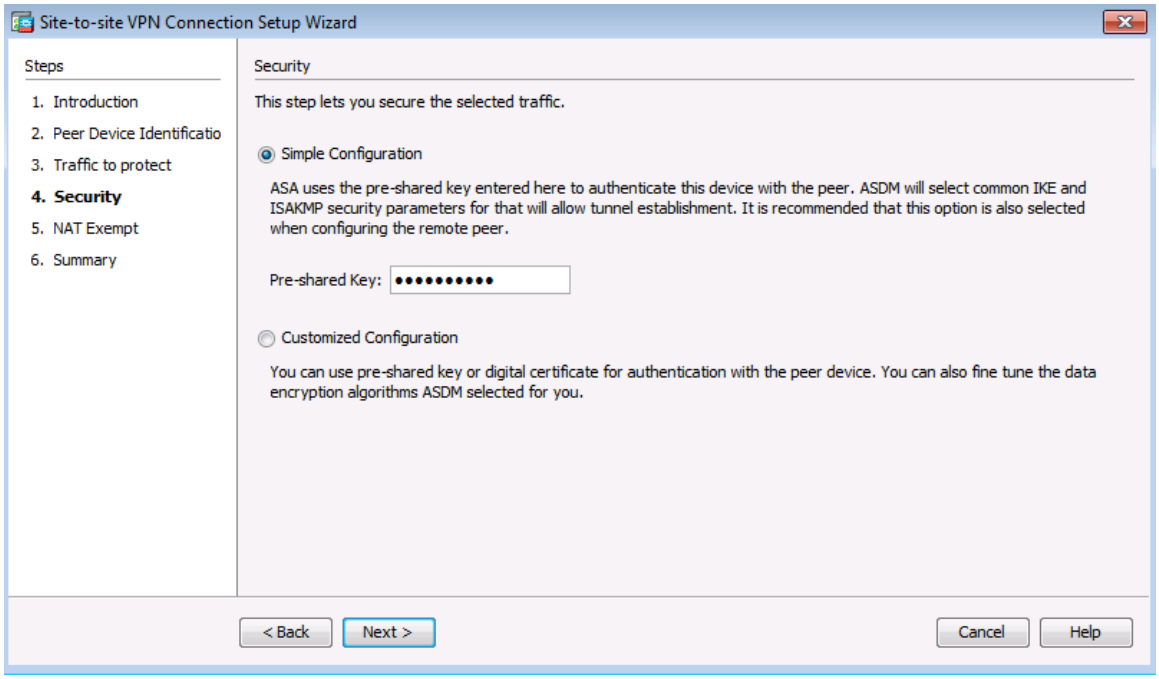
В окне Traffic to protect укажите **inside-network/24** (192.168.1.0/24) в качестве локальной сети и введите **172.16.3.0/24,** чтобы добавить LAN маршрутизатора R3 в качестве удаленной сети. Нажмите **Next**, чтобы продолжить. На экране может появиться сообщение о получении информации о сертификате.



Примечание. Если ASA не отвечает, возможно, придется закрыть окно и перейти к следующему шагу. При получении запроса на аутентификацию выполните вход как пользователь **admin01** с паролем **admin01pass.**

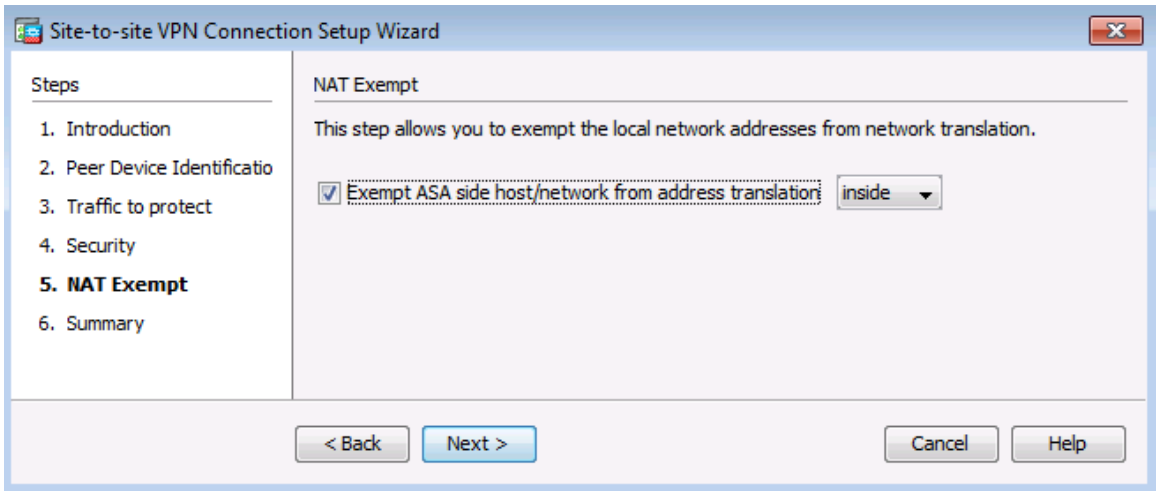
Шаг 6: Настройка аутентификации.

В окне Security введите общий ключ **SECRET-KEY**. Сертификат устройства использоваться не будет. Нажмите **Next**, чтобы продолжить.



Шаг 7: Настройка дополнительных параметров.

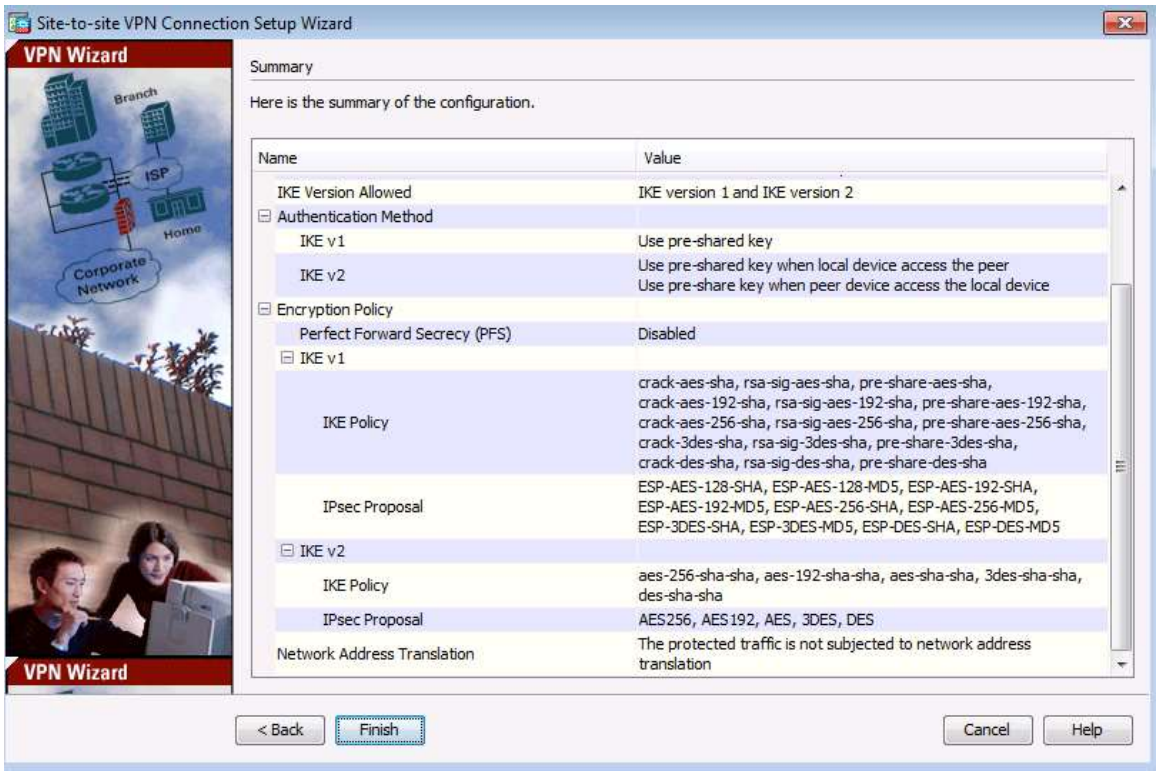
В окне NAT Exempt установите флажок **Exempt ASA** для интерфейса **inside.** Нажмите **Next**, чтобы продолжить.



Шаг 8: Проверьте сводку по конфигурации и отправьте команды на ASA.

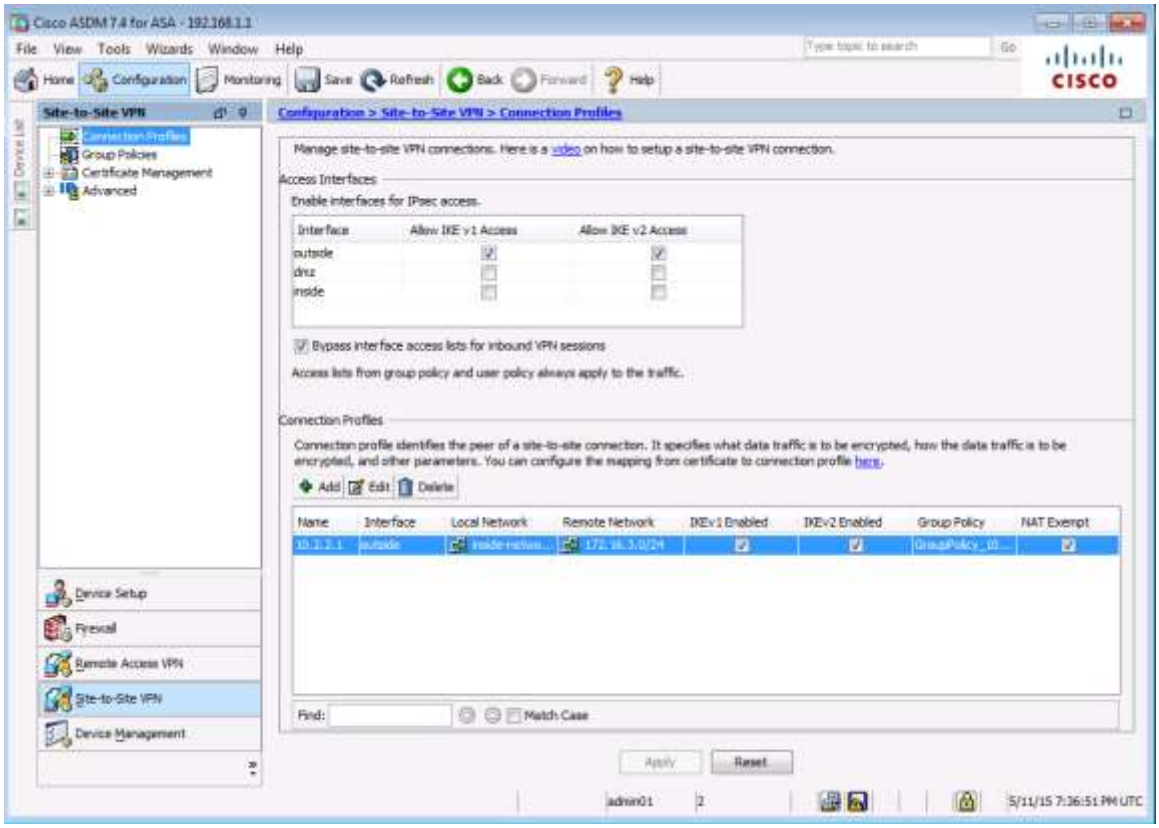
Появляется окно Summary. Убедитесь, что введена корректная информация о конфигурации. Вы можете нажать **Back,** если необходимо внести изменения, или **Cancel** и заново запустить мастер VPN (рекомендуется). Нажмите **Finish** для завершения процесса и отправки команд на ASA.

Примечание. При получении запроса на аутентификацию выполните вход как пользователь **admin01** с паролем **admin01pass.**



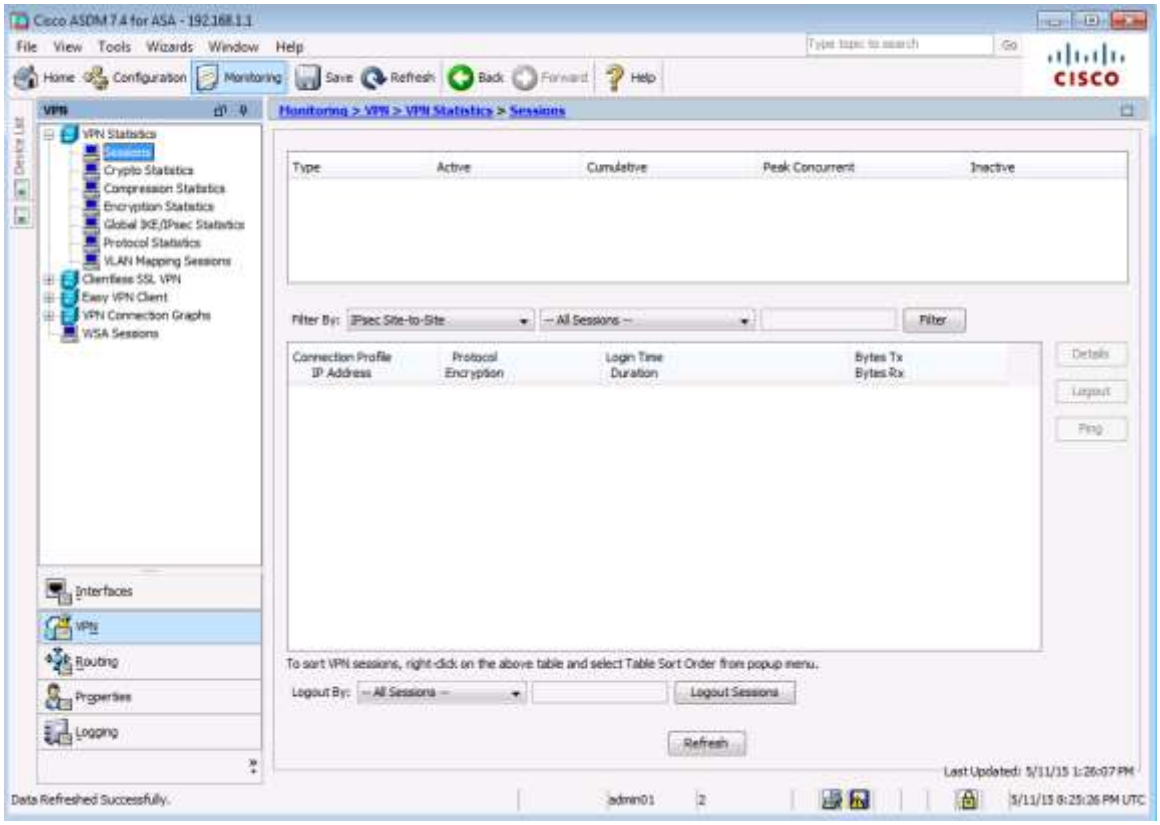
Шаг 9: Проверка профиля подключения VPN в ASDM.

На экране ASDM **Configurations** > **Site-to-Site VPN** > **Connection Profiles** отображаются сконфигурированные параметры. В этом окне можно проверить и изменить конфигурацию VPN.



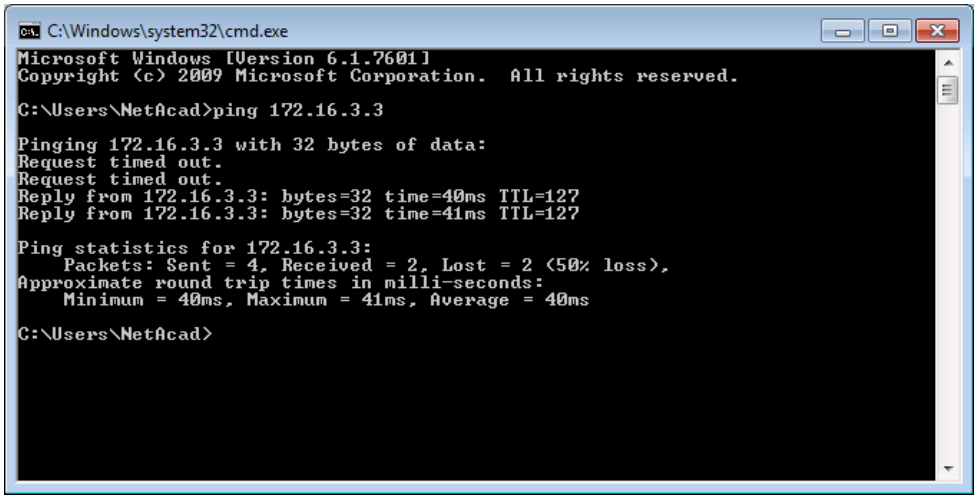
Шаг 10: Использование мониторинга ASDM для проверки туннеля.

В строке меню ASDM нажмите **Monitoring** > **VPN** на панели в левой нижней части экрана. Выберите **VPN Statistics** > **Sessions**. Обратите внимание, что в данный момент активных сеансов нет. Это объясняется тем, что VPN-туннель не установлен.



Шаг 11: Проверка конфигурации VPN из компьютера PC-B.

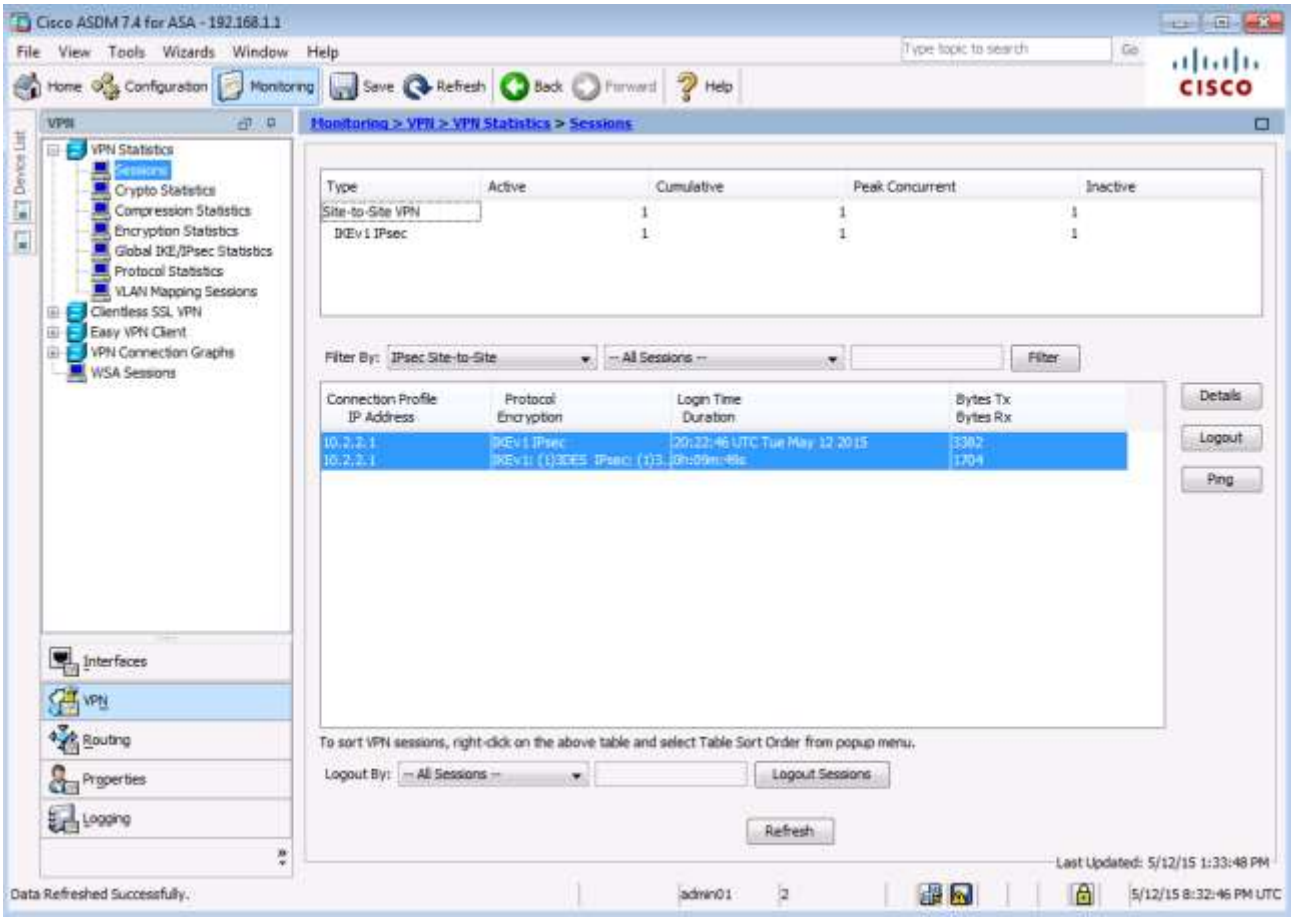
a. Для установки VPN-туннеля должен генерироваться «интересный» трафик. С компьютера PC-B отправьте эхо-запрос на компьютер PC-C.



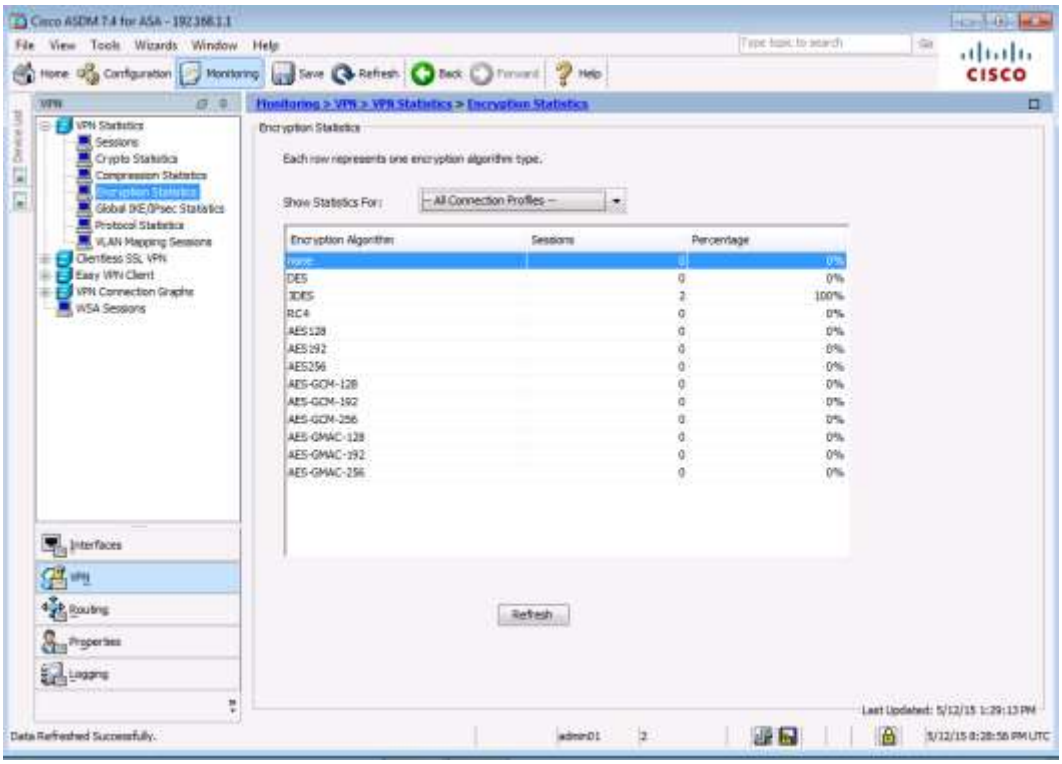
b. Это сгенерирует «интересный» трафик. Обратите внимание, что два эхо-запроса были выполнены с ошибкой, а следующие завершились успешно. Это объясняется тем, что сначала нужно было согласовать и установить туннель, и только после этого пакеты ICMP могли быть успешно переданы.

c. Теперь информация о VPN отображается на странице ASDM **Monitoring** > **VPN** > **VPN Statistics** > **Sessions.**

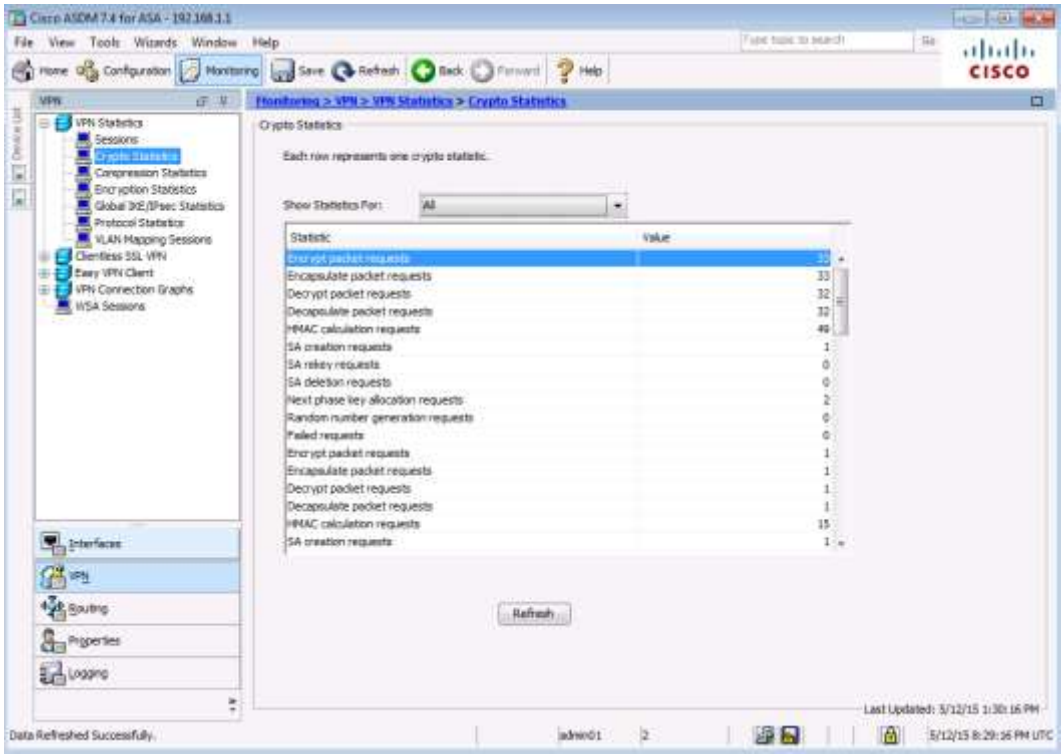
Примечание. Для обновления статистики, возможно, будет нужно нажать кнопку **Refresh.**



d. Нажмите **Encryption Statistics**. Вы должны увидеть один или несколько сеансов, использующих алгоритм шифрования 3DES.



e. Нажмите **Crypto Statistics**. Вы должны увидеть количество шифрованных и дешифрованных пакетов, запросов на установление ассоциации безопасности (SA) и т. д.



Вопросы для повторения

Опишите ситуацию, когда выгоднее использовать сеть site-to-site IPSec VPN, а не сети VPN другого типа.

_____

_____

_____

_____

_____

_____

_____

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.

