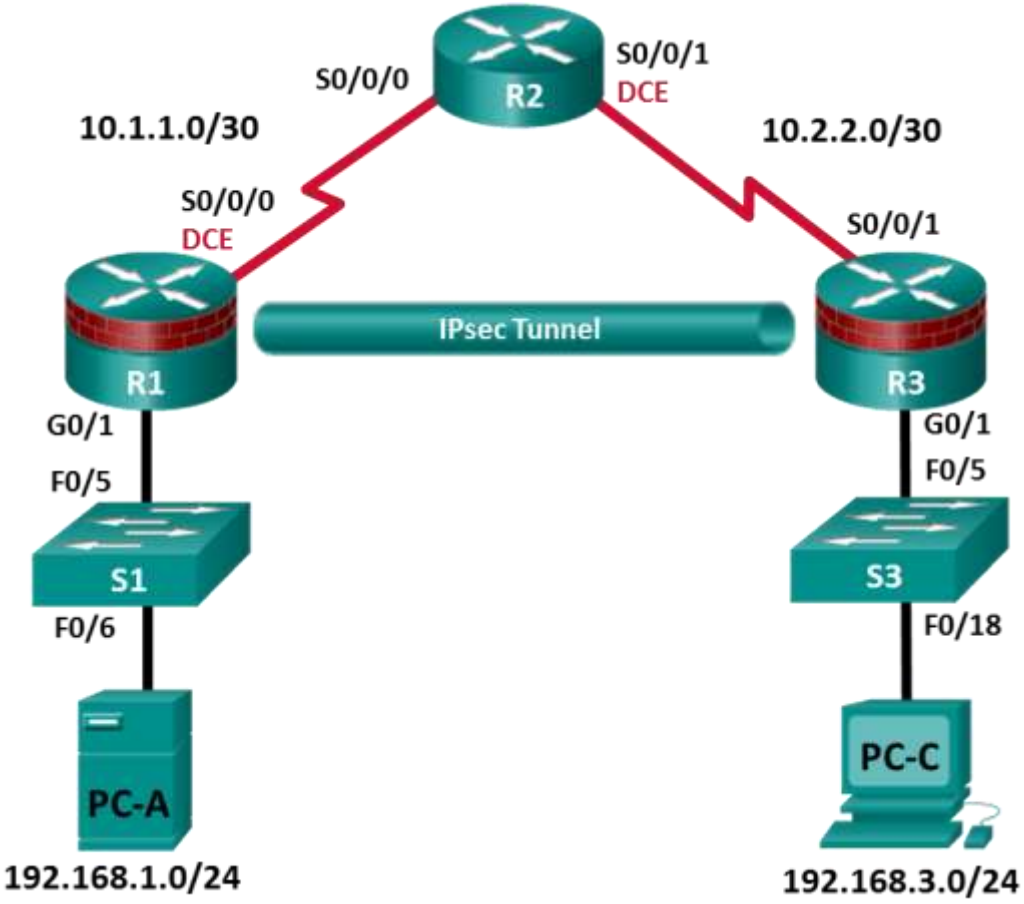
CCNA Security

Глава 8. Лабораторная работа. Настройка сети Site-to-Site VPN с помощью Cisco IOS

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	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	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	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

- Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте протокол динамической маршрутизации OSPF.

Часть 2. Настройка сети Site-to-Site VPN с помощью Cisco IOS

- Настройте параметры сети IPsec VPN на маршрутизаторах R1 и R3.
- Проверьте конфигурацию сети site-to-site IPsec VPN.
- Проверьте работоспособность сети IPsec VPN.

Исходные данные/сценарий

Сети VPN могут обеспечивать безопасную передачу данных через общедоступную сеть, например через Интернет. Соединения VPN позволяют снизить расходы, связанные с арендованными линиями. Сети типа Site-to-Site VPN обычно обеспечивают безопасный туннель (по IPsec или другому протоколу) между филиалами и центральным офисом. Другим распространенным способом реализации технологии VPN является удаленный доступ к офису компании для пользователя, который работает, например, в небольшом или домашнем офисе.

В данной лабораторной работе вы создадите и настроите сеть с несколькими маршрутизаторами, с помощью Cisco IOS настроите сеть site-to-site IPsec VPN (между двумя пунктами), а затем протестируете созданную сеть VPN. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPSec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям, например по Интернету. IPSec функционирует на сетевом уровне и выполняет функцию как защиты, так и аутентификации IP-пакетов между соответствующими устройствами IPsec (узлами), такими как маршрутизаторы Cisco.

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.

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

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 2 ПК (Windows 7 или 8.1, с установленным SSH-клиентом и WinRadius)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

В части 1 вы создадите топологию сети и настроите базовые параметры, такие как IP-адреса интерфейсов, динамическая маршрутизация, доступ к устройствам и пароли.

Примечание. На маршрутизаторах R1, R2 и R3 должны быть выполнены все задачи. В качестве примера здесь показана процедура для R1.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов, как показано на топологической схеме.

b. Настройте IP-адреса интерфейсов, как показано в таблице IP-адресов.

c. Настройте тактовую частоту (64000) для последовательных интерфейсов маршрутизаторов с помощью DCE-кабеля.

Шаг 3: Отключите поиск DNS.

Чтобы предотвратить попытки маршрутизатора неправильно интерпретировать введенные команды, отключите функцию DNS-поиска.

Шаг 4: Настройте протокол OSPF на маршрутизаторах R1, R2 и R3.

a. На маршрутизаторе R1 используйте следующие команды.

```
R1(config)# router ospf 101
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

b. На маршрутизаторе R2 используйте следующие команды.

```
R2(config)# router ospf 101
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

c. На маршрутизаторе R3 используйте следующие команды.

```
R3(config)# router ospf 101
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Шаг 5: Настройте параметры IP для хоста.

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

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

Шаг 6: Проверьте базовую связь по сети.

a. Отправьте эхо-запрос с маршрутизатора R1 на интерфейс Fa0/1 маршрутизатора R3 по IP-адресу 192.168.3.1.

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, это означает, что протокол маршрутизации OSPF настроен правильно и работает корректно. Если эхо-запрос выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами **show run** и **show ip route**, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 7: Настройте и зашифруйте пароли.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. В рабочих сетях рекомендуется использовать более сложные пароли.

Установите аналогичные настройки на маршрутизаторах R1 и R3. В качестве примера показан маршрутизатор R1.

a. Задайте минимальную длину пароля.

Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

b. Установите на обоих маршрутизаторах пароль привилегированного доступа **cisco12345**. Используйте алгоритм хеширования type 9 (SCRYPT).

c. Создайте локальную учетную запись **admin01,** установите для нее пароль **admin01pass.** Используйте алгоритм хеширования type 9 (SCRYPT).

Шаг 8: Настройте линию консоли.

Настройте консоль на использование локальной базы для входа в систему. В целях дополнительной безопасности настройте эти линии на выход из системы через 5 минут при отсутствии активности. Используйте команду **logging synchronous** для предотвращения прерывания ввода команд сообщениями консоли.

Шаг 9: Настройте сервер SSH.

a. Укажите доменное имя **ccnasecurity.com**.

b. Задайте количество битов модуля 1024 для RSA-ключей.

c. Введите команду ip ssh version 2 для принудительного использования SSH версии 2.

d. Настройте линии VTY на маршрутизаторах R1 и R3 таким образом, чтобы использовать локальную базу данных для входа. Удаленный доступ к маршрутизаторам должен быть доступен только по SSH. Настройте линии vty на выход из системы спустя 5 минут в случае отсутствия активности.

Шаг 10: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме на маршрутизаторах R1, R2 и R3.

```
R1# copy running-config startup-config
```

Часть 2: Настройка сети Site-to-Site VPN с помощью Cisco IOS

В части 2 этой лабораторной работы необходимо настроить туннель IPSec VPN между маршрутизаторами R1 и R3, проходящий через R2. Настройте маршрутизаторы R1 и R3 с помощью Cisco IOS CLI. Затем вы проверите итоговую конфигурацию.

Задача 1: Настройка параметров сети IPsec VPN на маршрутизаторах R1 и R3.

Шаг 1: Проверьте связь из локальной сети маршрутизатора R1 в локальную сеть маршрутизатора R3.

В этой задаче вы убедитесь, что с компьютера PC-A в локальной сети маршрутизатора R1 можно отправить эхо-запрос на PC-C в локальной сети маршрутизатора R3 при отсутствии туннеля.

Отправьте эхо-запрос с PC-A на IP-адрес компьютера PC-C **192.168.3.3.**

```
PC-A:\> ping 192.168.3.3
```

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Шаг 2: Включите политики IKE на маршрутизаторах R1 и 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.

```
R1(config)# crypto isakmp enable


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, применяющую 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: Настройте политику ISAKMP фазы 1 IKE на маршрутизаторах R1 и 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 тип аутентификации **pre-shared key**, алгоритм шифрования **aes 256,** алгоритм хеширования **sha** и группу Diffie-Hellman **14** для обмена ключами. Установите время действия политики на 3600 секунд (один час).

   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 внесены на маршрутизаторе R3.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
```

b. Настройте аналогичную политику на маршрутизаторе R3.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash sha
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 14
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# end
```

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

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
```

Шаг 4: Настройте общие ключи.

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. Это должен быть IP-адрес удаленного интерфейса, который узел будет использовать для маршрутизации трафика на локальный маршрутизатор.

Какие IP-адреса необходимо использовать для настройки узлов 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. Настройте общий ключ **cisco123** на маршрутизаторе R1. В производственных сетях следует использовать сложный ключ. Эта команда указывает на IP-адрес интерфейса S0/0/1 удаленного маршрутизатора R3.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1
```

b. Настройте общий ключ **cisco123** на маршрутизаторе R3. Данная команда относится к маршрутизатору R3 и указывает на IP-адрес интерфейса S0/0/0 маршрутизатора R1.

```
R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```

Шаг 5: Настройте набор преобразований и время жизни IPsec.

a. Набор преобразований Ipsec – это еще один криптографический параметр, который маршрутизаторы согласуют друг с другом для создания ассоциации безопасности. Для создания набора преобразований IPsec используйте команду **crypto ipsec transform-set <tag>.** Для просмотра доступных параметров используйте ?.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA 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-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
```

b. На маршрутизаторах R1 и R3 создайте набор преобразований с тегом 50, используйте преобразование ESP с шифром AES 256 с ESP и хеш-функцией SHA. Наборы преобразований должны совпадать.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)# exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

Какую функцию выполняет набор преобразований IPsec?

_____

_____

_____

_____

c. Вы можете также изменить время жизни ассоциации безопасности IPSec и не использовать значение по умолчанию 3600 секунд. На маршрутизаторах R1 и R3 установите время жизни ассоциации безопасности 30 минут или 1800 секунд.

```
R1(config)# crypto ipsec security-association lifetime seconds 1800

R3(config)# crypto ipsec security-association lifetime seconds 1800
```

Шаг 6: Определите «интересный» трафик.

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 одним из таких списков доступа, не отбрасывается, а отправляется незашифрованным. 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 R1 мы хотим зашифровать трафик, поступающий из локальной сети Ethernet маршрутизатора R1 в локальную сеть Ethernet маршрутизатора R3, или наоборот, если смотреть со стороны маршрутизатора R3. Данные списки доступа используются для исходящего трафика на интерфейсах устройств VPN и должны зеркально отражать друг друга.

a. Сконфигурируйте список ACL для «интересного» трафика в IPSec VPN на маршрутизаторе R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

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

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

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

_____

_____

_____

Шаг 7: Создайте и примените криптографическую карту.

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 подключены к узлу IPsec.

Для создания криптографической карты используйте команду **crypto map <name> <sequence-num> <type>** в режиме глобальной настройки, чтобы войти в режим настройки криптографической карты для заданного порядкового номера. В одной криптографической карте может быть несколько криптографических операторов, которые анализируются в порядке возрастания номеров. Войдите в режим настройки криптографический карты на маршрутизаторе R1. Используйте тип ipsec-isakmp, чтобы указать, что для установления ассоциаций безопасности IPsec будет применяться IKE.

a. Создайте криптографическую карту на маршрутизаторе R1, назовите ее **CMAP** и укажите 10 в качестве порядкового номера. После ввода команды будет выведено сообщение.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

b. Используйте команду **match address <access-list>** для указания списка доступа, определяющего трафик, который нужно шифровать.

```
R1(config-crypto-map)# match address 101
```


c. Для просмотра списка возможных команд **set**, которые можно применить к криптографической карте, используйте функцию справки.

```
R1(config-crypto-map)# set ?
  identity              Identity restriction.
  ip                    Interface Internet Protocol config commands
  isakmp-profile        Specify isakmp Profile
  nat                   Set NAT translation
  peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings
  reverse-route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in priority order
```

d. Требуется указать IP-адрес или имя хоста для узла. Укажите интерфейс конечного устройства VPN маршрутизатора R3 с помощью следующей команды.

```
R1(config-crypto-map)# set peer 10.2.2.1
```

e. Используйте команду **set transform-set <tag>**, чтобы четко указать набор преобразований, который должен использоваться с этим узлом. Установите тип perfect forwarding secrecy с помощью команды **set pfs <type>** и измените время жизни ассоциации безопасности IPsec, заданное по умолчанию, с помощью команды **set security-association lifetime seconds <seconds>**.

```
R1(config-crypto-map)# set pfs group14
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

f. Создайте такую же криптографическую карту на маршрутизаторе R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set pfs group14
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R3(config-crypto-map)# exit
```

g. 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 соответствующим интерфейсам на маршрутизаторах R1 и R3.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end

R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```


Задача 2: Проверка конфигурации сети site-to-site IPsec VPN.

Шаг 1: Проверьте конфигурацию IPsec на маршрутизаторах R1 и R3.

a. Ранее вы использовали команду **show crypto isakmp policy** для отображения настроенных на маршрутизаторе политик ISAKMP. Команда **show crypto ipsec transform-set** отображает настроенные политики IPsec в виде наборов преобразований.

```
R1# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

R3# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

b. Используйте команду **show crypto map** для отображения криптографических карт, которые будут применены на маршрутизаторе.

```
R1# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/0

R3# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```



```
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/1
```

Примечание. Выходные данные этих команд **show** не изменяются, если «интересный» трафик проходит по соединению. В следующей задаче вы проверите разные виды трафика.

Задача 3: Проверка работы сети IPsec VPN.

Шаг 1: Отобразите ассоциации безопасности ISAKMP.

Команда **show crypto isakmp sa** показывает, что в данный момент ассоциации IKE SA не существуют. После отправки «интересного» трафика выходные данные команды изменятся.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

Шаг 2: Отобразите ассоциации безопасности IPsec.

Команда **show crypto ipsec sa** показывает неиспользуемую ассоциацию SA между маршрутизаторами R1 и R3.

Примечание. Количество переданных пакетов равно нулю, и в нижней части выходных данных ассоциации безопасности не указаны. Ниже приведены выходные данные для маршрутизатора R1.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```



```
PFS (Y/N): N, DH group: none

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:
```

Почему не было согласовано ни одной SA?

_____

_____

_____

Шаг 3: Создайте «неинтересный» тестовый трафик и проверьте результаты.

a. Отправьте эхо-запрос с маршрутизатора R1 на интерфейс S0/0/1 маршрутизатора R3 по IP-адресу 10.2.2.1. Этот запрос должен быть выполнен успешно.

b. Введите команду **show crypto isakmp sa**.

c. Отправьте эхо-запрос с маршрутизатора R1 на интерфейс G0/1 маршрутизатора R3 по IP-адресу **192.168.3.1.** Этот запрос должен быть выполнен успешно.

d. Введите команду **show crypto isakmp sa** еще раз. Была ли создана SA для этих эхо-запросов? Поясните ответ.

_____

_____

_____

e. Введите команду **debug ip ospf hello**. Вы должны увидеть пакеты OSPF hello, передаваемые между маршрутизаторами R1 и R3.

```
R1# debug ip ospf hello
OSPF hello events debugging is on
R1#
*Apr  7 18:04:46.467: OSPF: Send hello to 224.0.0.5 area 0 on GigabitEthernet0/1 from 192.168.1.1
*Apr  7 18:04:50.055: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from 10.1.1.1
*Apr  7 18:04:52.463: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
*Apr  7 18:04:52.463: OSPF: End of hello processing
*Apr  7 18:04:55.675: OSPF: Send hello to 224.0.0.5 area 0 on GigabitEthernet0/1 from 192.168.1.1
*Apr  7 18:04:59.387: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from 10.1.1.1
*Apr  7 18:05:02.431: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
*Apr  7 18:05:02.431: OSPF: End of hello processing
```

f. Выключите отладку с помощью команды **no debug ip ospf hello** или **undebug all**.

g. Снова введите команду **show crypto isakmp sa**. Была ли создана SA между маршрутизаторами R1 и R3? Поясните ответ.

_____

_____

_____

Шаг 4: Создайте «интересный» тестовый трафик и проверьте результаты.

a. Отправьте расширенный эхо-запрос с маршрутизатора R1 на интерфейс G0/1 маршрутизатора R3 по IP-адресу 192.168.3.1. Расширенный эхо-запрос позволяет контролировать адрес источника пакетов. Ответьте так, как показано в примере. Нажмите клавишу **Enter** для принятия значений по умолчанию везде, кроме тех позиций, где показан другой ответ.

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1
..!!!
Success rate is 100 percent (3/5), round-trip min/avg/max = 92/92/92 ms
```

b. Снова введите команду **show crypto isakmp sa**.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.2.2.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Почему на этот раз между маршрутизаторами R1 и R3 была создана ассоциация SA?

_____

_____

_____

Что является конечными точками туннеля IPSec VPN?

_____

_____

_____

c. Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C. Если он был выполнен успешно, введите команду **show crypto ipsec sa**. Сколько пакетов было преобразовано между маршрутизаторами R1 и R3?

_____

_____

_____

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC1DD058(203280472)
```



```
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:6, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

d. В предыдущем примере для генерации «интересного» трафика были использованы эхо-запросы. Какие еще типы трафика приведут к созданию ассоциации SA и установлению туннеля?

_____

_____

_____

_____

_____

_____

Вопросы для повторения

1. Будет ли трафик, передаваемый по каналу Gigabit Ethernet между компьютером PC-A и интерфейсом G0/0 маршрутизатора R1, шифроваться туннелем site-to-site IPsec VPN? Поясните ответ.

_____

_____

_____

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 (Fa0/0)	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 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	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, хотя в конкретном 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.

