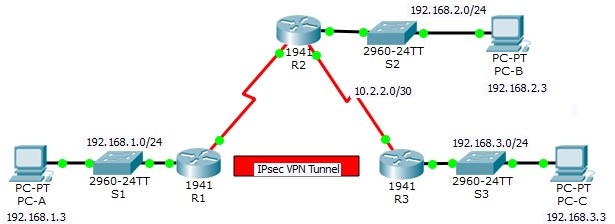
**Packet Tracer. Конфигурирование и проверка IPsec VPN между двумя пунктами (site-to-site) с помощью интерфейса командной строки**

**Топология**



**Таблица адресации**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** | **Порт коммутатора** |
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | Н/П | S1 F0/1 |
| S0/0/0 (DCE) | 10.1.1.2 | 255.255.255.252 | Н/П | Н/П |
| R2 | G0/0 | 192.168.2.1 | 255.255.255.0 | Н/П | S2 F0/2 |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | Н/П | Н/П |
| S0/0/1 (DCE) | 10.2.2.1 | 255.255.255.252 | Н/П | Н/П |
| R3 | G0/0 | 192.168.3.1 | 255.255.255.0 | Н/П | S3 F0/5 |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | Н/П | Н/П |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | S2 F0/1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 F0/18 |

**Задачи**

* Проверка связи в сети
* Настройка маршрутизатора R1 для поддержки сети Site-to-Site IPsec VPN с маршрутизатором R3

**Исходные данные/сценарий**

Топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (между двумя пунктами) при передаче трафика между соответствующими локальными сетями. 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.

очерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

**Параметры политики ISAKMP, фаза 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметры** | | **R1** | **R3** |
| **Метод распределения ключей** | Вручную или **ISAKMP** | **ISAKMP** | **ISAKMP** |
| **Алгоритм шифрования** | **DES**, 3DES или AES | AES 256 | AES 256 |
| **Алгоритм хеширования** | MD5 или **SHA-1** | **SHA-1** | **SHA-1** |
| **Метод аутентификации** | Общие ключи или **RSA** | pre-share | pre-share |
| **Обмен ключами** | Группа DH 1, 2 или 5 | DH 5 | DH 5 |
| **Время существования IKE SA** | 86 400 с или меньше | 86400 | 86400 |
| **Ключ ISAKMP** |  | vpnpa55 | vpnpa55 |

**Примечание.** Полужирным шрифтом выделены параметры по умолчанию. Явно настраивать требуется только невыделенные параметры.

**Параметры политики IPsec, фаза 2**

|  |  |  |
| --- | --- | --- |
| **Параметры** | **R1** | **R3** |
| **Имя набора преобразований** | VPN-SET | VPN-SET |
| **Шифрование преобразования ESP** | esp-aes | esp-aes |
| **Аутентификация преобразования ESP** | esp-sha-hmac | esp-sha-hmac |
| **IP-адрес узла** | 10.2.2.2 | 10.1.1.2 |
| **Трафик, подлежащий шифрованию** | access-list 110 (source  192.168.1.0 dest  192.168.3.0) | access-list 110 (source  192.168.3.0 dest  192.168.1.0) |
| **Имя криптографической карты** | VPN-MAP | VPN-MAP |
| **Установление SA** | ipsec-isakmp | ipsec-isakmp |

На маршрутизаторах были предварительно настроены следующие параметры.

* Пароль для линии консоли: **ciscoconpa55**
* Пароль для линий VTY: **ciscovtypa55**
* Пароль привилегированного доступа: **ciscoenpa55**
* Имя пользователя и пароль SSH: **SSHadmin**/**ciscosshpa55**  OSPF 101

# Часть 1: Настройка параметров IPsec на маршрутизаторе R1

**Шаг 1: Проверка связи.**

Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C.

**Шаг 2: Включение пакета Security Technology.**

1. На маршрутизаторе R1введите команду **show version** для просмотра сведений о лицензии Security Technology Package.
2. Если пакет Security Technology не активирован, сделайте это с помощью следующей команды.

R1(config)# **license boot module c1900 technology-package securityk9**

1. Примите условия лицензионного соглашения с конечным пользователем.
2. Сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы активировать лицензию Technology Package.
3. Убедитесь, что пакет Security Technology включен, с помощью команды **show version**.

**Шаг 3: Определение «интересного» трафика на маршрутизаторе R1.**

Настройте список ACL 110, чтобы идентифицировать как «интересный» трафик, направляющийся из локальной сети на маршрутизаторе R1 в локальную сеть на маршрутизаторе R3. Этот трафик будет инициировать создание сети IPsec VPN при наличии трафика между локальными сетями маршрутизаторов R1 и R3. Весь остальной трафик, исходящий из локальных сетей, не будет шифроваться. Из-за неявного условия **deny all** не нужно настраивать оператор **deny ip any any**.

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

**Шаг 4: Настройка политики ISAKMP фазы 1 IKE на маршрутизаторе R1.**

Настройте свойства **crypto ISAKMP policy 10** на маршрутизаторе R1 с общим ключом шифрования **vpnpa55**.

Конкретные параметры для настройки см. в таблице ISAKMP, фаза 1. Значения по умолчанию настраивать не нужно. Следовательно, необходимо настроить только метод шифрования, метод обмена ключами и метод DH.

**Примечание.** В настоящее время Packet Tracer поддерживает группы DH с номером не выше 5. В производственной сети потребуется настроить, как минимум, DH14.

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

R1(config-isakmp)# **encryption aes 256**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 5**

R1(config-isakmp)# **exit**

R1(config)# **crypto isakmp key vpnpa55 address 10.2.2.2**

**Шаг 5: Настройка политики IPsec фазы 2 IKE на маршрутизаторе R1.**

1. Создайте набор преобразований VPN-SET, чтобы использовать **esp-aes** и **esp-sha-hmac**.

R1(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

1. Создайте криптографическую карту VPN-MAP, связывающую друг с другом все параметры фазы 2.

Используйте порядковый номер 10 и определите его как карту ipsec-isakmp.

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

R1(config-crypto-map)# **match address 110**

R1(config-crypto-map)# **exit**

**Шаг 6: Настройка криптографической карты на исходящем интерфейсе.**

Привяжите криптографическую карту **VPN-MAP** к исходящему интерфейсу Serial 0/0/0.

R1(config)# **interface s0/0/0**

R1(config-if)# **crypto map VPN-MAP**

# Часть 2: Настройка параметров IPsec на маршрутизаторе R3

**Шаг 1: Включение пакета Security Technology.**

1. На маршрутизаторе R3 введите команду **show version**, чтобы проверить, активирована ли лицензия Security Technology Package.
2. Если нет, активируйте пакет и перезагрузите маршрутизатор R3.

**Шаг 2: Настройка маршрутизатора R3 для поддержки сети site-to-site VPN с маршрутизатором R1.**

Настройте соответствующие параметры на маршрутизаторе R3. Настройте список ACL 110, чтобы идентифицировать как «интересный» трафик, направляющийся из локальной сети на маршрутизаторе R3 в локальную сеть на маршрутизаторе R1.

R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**

**Шаг 3: Настройка свойств ISAKMP фазы 1 IKE на маршрутизаторе R3.**

Настройте свойства криптополитики ISAKMP 10 на маршрутизаторе R3 с общим ключом шифрования vpnpa55.

R3(config)# **crypto isakmp policy 10**

R3(config-isakmp)# **encryption aes 256**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 5**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key vpnpa55 address 10.1.1.2**

**Шаг 4: Настройка политики IKE фазы 2 IPsec на маршрутизаторе R3.**

1. Создайте набор преобразований VPN-SET, чтобы использовать **esp-aes** и **esp-sha-hmac**.

R3(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

1. Создайте криптографическую карту VPN-MAP, связывающую друг с другом все параметры фазы 2.

Используйте порядковый номер 10 и определите его как карту ipsec-isakmp.

R3(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R3(config-crypto-map)# **description VPN connection to R1**

R3(config-crypto-map)# **set peer 10.1.1.2**

R3(config-crypto-map)# **set transform-set VPN-SET**

R3(config-crypto-map)# **match address 110** R3(config-crypto-map)# **exit**

**Шаг 5: Настройка криптографической карты на исходящем интерфейсе.**

Привяжите криптографическую карту VPN-MAP к исходящему последовательному интерфейсу 0/0/1. **Примечание.** Этот шаг не оценивается.

R3(config)# **interface s0/0/1**

R3(config-if)# **crypto map VPN-MAP**

# Часть 3: Проверка IPsec VPN

**Шаг 1: Проверка туннеля до передачи «интересного» трафика.**

Введите команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что количество инкапсулированных, зашифрованных, декапсулированных и дешифрованных пакетов установлено на 0.

**Шаг 2: Создание «интересного» трафика.**

Отправьте эхо-запрос на компьютер PC-C с компьютера PC-A.

**Шаг 3: Проверка туннеля после передачи «интересного» трафика.**

Введите снова команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что количество пакетов больше 0, и это означает, что туннель IPsec VPN работает.

**Шаг 4: Создание «неинтересного» трафика.**

Отправьте эхо-запрос на компьютер PC-B с компьютера PC-A. **Примечание.** Отправка эхо-запроса с маршрутизатора R1 на компьютер PC-C или с маршрутизатора R3 на компьютер PC-A представляет собой «неинтересный» трафик.

**Шаг 5: Проверка туннеля.**

Снова введите команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что количество пакетов не изменилось, что означает, что «неинтересный» трафик не зашифрован.

**Шаг 6: Проверка результатов.**

Вы полностью выполнили задание. Нажмите **Check Results (Проверить результаты)** для просмотра отзыва и проверки завершенных обязательных компонентов.

