МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №11

Configure and Verify a Site-to-Site IPsec VPN using CLI

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студенты:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Жиляков Г. В., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

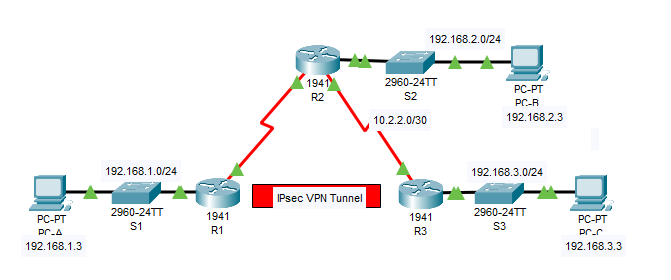
*(Ф.И.О., № группы) (подпись)*

Проверил:

К.т.н., доцент каф. ЗСС, Кушнир Д. В.

*(подпись)*

# 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 – настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (между двумя пунктами) при передаче трафика между их соответствующими локальными сетями. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. R2 играет роль транзитного узла и не имеет информации о VPN. IPsec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям, например через Интернет. IPsec работает на сетевом уровне, обеспечивая защиту и аутентификацию IP-пакетов между соответствующими устройствами IPsec (узлами), такими как маршрутизаторы 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. Необходимо настраивать в явном виде 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**

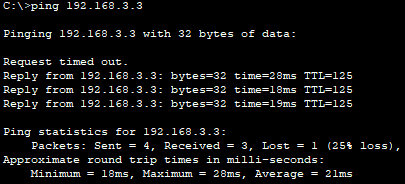
·         Имя пользователя и пароль SSH: **SSHadmin**/**ciscosshpa55**

·         OSPF 101

**Часть 1. Настройка параметров IPsec на маршрутизаторе R1**

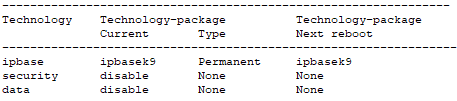
**Шаг 1. Проверьте связь.**

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



**Шаг 2. Включите пакет Security Technology.**

a.     На маршрутизаторе R1 введите команду **show version** для просмотра сведений о лицензии Security Technology.



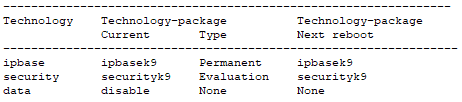
b.     Если пакет Security Technology не активирован, сделайте это с помощью следующей команды.

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

c.     Примите условия лицензионного соглашения с конечным пользователем.

d.     Сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы активировать лицензию Security Technology.

e.     Убедитесь, что пакет Security Technology активирован, с помощью команды **show version**.



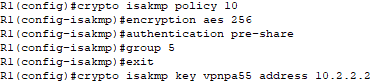
**Шаг 3. Определите «интересный» трафик на маршрутизаторе R1.**

Настройте список ACL 110, чтобы определить трафик, направляющийся из локальной сети на маршрутизаторе R1 в локальную сеть на маршрутизаторе R3, как «интересный». 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. Поскольку косвенно указано **deny all**, не нужно настраивать оператор **deny ip any any**.



**Шаг 4. Настройте политику ISAKMP фазы 1 IKE на маршрутизаторе R1.**

Настройте свойства **crypto ISAKMP policy** **10** на маршрутизаторе R1 с общим криптоключом **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.

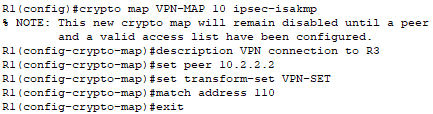
****

**Шаг 5. Настройте политику IPsec фазы 2 IKE на маршрутизаторе R1.**

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



b.     Затем создайте криптографическую карту VPN-MAP, связывающую друг с другом все параметры фазы 2. Используйте порядковый номер 10 и определите его как карту ipsec-isakmp.

****

**Шаг 6. Настройте криптографическую карту на исходящем интерфейсе.**

Свяжите криптографическую карту **VPN-MAP** с исходящим интерфейсом Serial 0/0/0.



**Часть 2. Настройка параметров IPsec на маршрутизаторе R3**

**Шаг 1. Включите пакет Security Technology.**

a.     На маршрутизаторе R3 выполните команду **show version**, чтобы проверить, активирована ли лицензия Security Technology.

b.     Если нет, сделайте это и перезагрузите маршрутизатор R3.

**Шаг 2. Настройте маршрутизатор R3 для поддержки сети site-to-site VPN с маршрутизатором R1.**

Настройте соответствующие параметры на маршрутизаторе R3. Настройте список ACL 110, идентифицирующий трафик, который передается из локальной сети на маршрутизаторе R3 в локальную сеть на маршрутизаторе R1, как «интересный».

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. Настройте свойства ISAKMP фазы 1 IKE на маршрутизаторе R3.**

Настройте свойства криптополитики ISAKMP 10 на маршрутизаторе R3 и общий ключ 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. Настройте политику IPsec фазы 2 IKE на маршрутизаторе R3.**

a.     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**

b.     Затем 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**

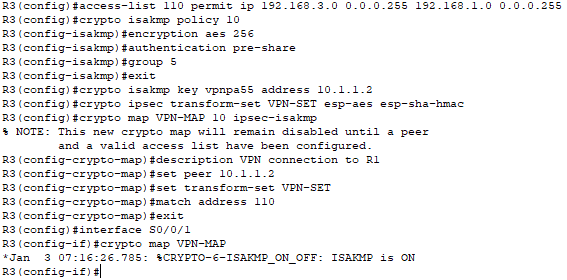
R3(config-crypto-map)# **exit**

**Шаг 5. Настройте криптографическую карту на исходящем интерфейсе.**

Свяжите криптографическую картуVPN-MAP с исходящим интерфейсом Serial 0/0/1. **Примечание**. Этот шаг не оценивается.

R3(config)# **interface s0/0/1**

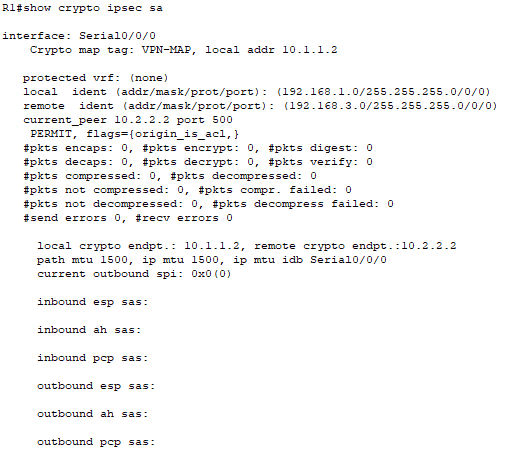
R3(config-if)# **crypto map VPN-MAP**



**Часть 3. Проверка сети IPsec VPN**

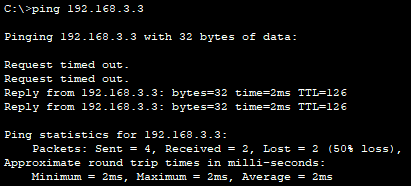
**Шаг 1. Проверьте туннель до передачи «интересного» трафика.**

Введите команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что число инкапсулированных, зашифрованных, декапсулированных и дешифрованных пакетов равно нулю.



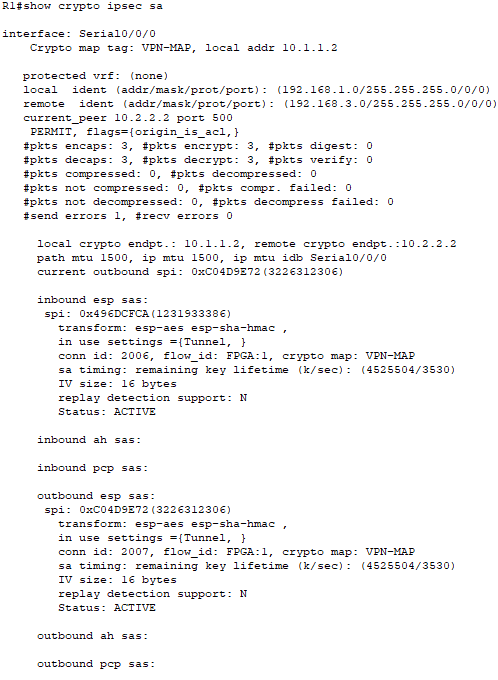
**Шаг 2. Создайте «интересный» трафик.**

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



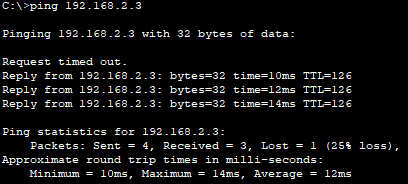
**Шаг 3. Проверьте туннель после передачи «интересного» трафика.**

Введите снова команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что число пакетов больше 0. Это свидетельствует о работоспособности туннеля IPsec VPN.



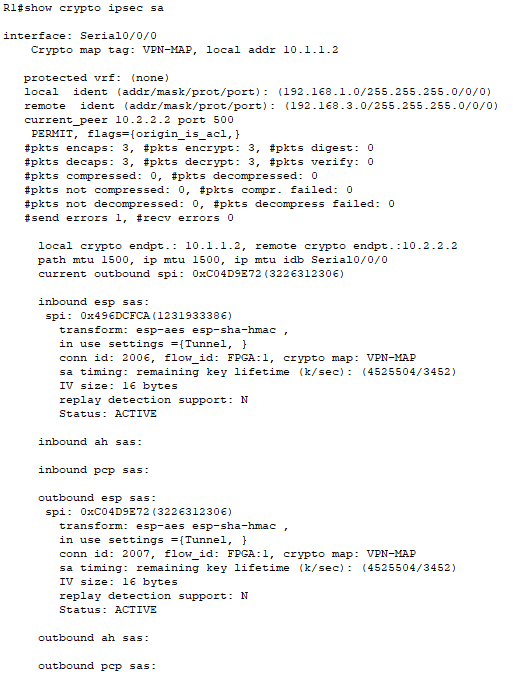
**Шаг 4. Создайте «неинтересный» трафик.**

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. Проверьте работу туннеля.**

Введите снова команду **show crypto ipsec sa** на маршрутизаторе R1. Обратите внимание, что число пакетов не изменилось. Это подтверждает, что «неинтересный» трафик не зашифрован.



**Шаг 6. Проверьте результаты.**

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

