

Министерство образования Республики Беларусь

Учреждение образования  
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Защита информации в информационных системах

ОТЧЕТ  
по лабораторной работе № 6  
на тему  
«Создание защищённого туннеля для обмена трафиком.  
Настройка протокола IPSec»

Студент:

Преподаватель:

МИНСК 2024

## 1 ЦЕЛЬ РАБОТЫ

Изучить возможности настройки режимов работы протокола IPSec.

## 2 ИСХОДНЫЕ ДАННЫЕ К РАБОТЕ

В данной лабораторной работе необходимо:

- Сконфигурировать в среде моделирования сеть;
- Настроить протокол IPSec

## 3 ВЫПОЛНЕНИЕ РАБОТЫ

Сконфигурированная сеть изображена на рисунке 3.1.

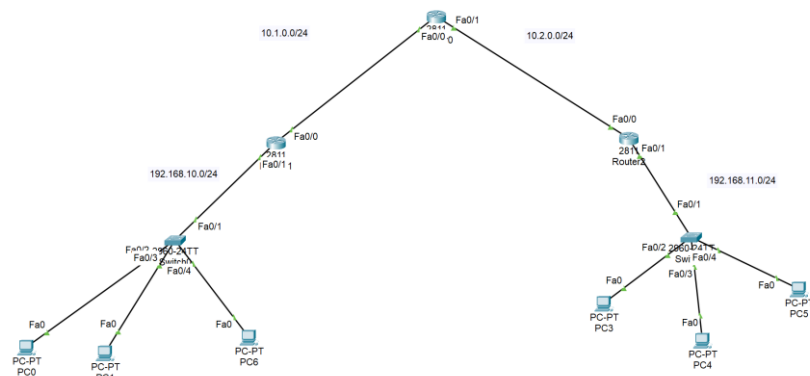


Рисунок 3.1 – Сконфигурированная сеть

Все последующие действия, которые были выполнены на R1, аналогично применяются к R2.

Для настройки протокола IPSec необходимо выполнить следующие действия:

1) Создать расширенный список доступа:

```
access-list 100 permit ip 192.168.10.0 0.0.0.255  
192.168.11.0 0.0.0.255  
access-list 100 remark ACL for IPSec
```

2) Настроить криптографический протокол, отвечающий за генерацию и распределение ключей, аутентификацию и шифрование трафика, установить ему политику в отношении ключей с указанием приоритета:

```
crypto isakmp policy 10
```

3) Выбрать подходящий алгоритм генерации ключа шифрования данных:

```
authentication pre-share  
encryption aes 256  
group 5
```

4) Присвоить значение общего секретного ключа с указанием адреса интерфейса маршрутизатора сети получателя:

```
crypto isakmp key 1111 address 10.1.0.1
```

5) Создать туннель, включив протокол IPSec:

```
crypto ipsec transform-set tunnel1 esp-aes 256 esp-sha-hmac
```

6) Создать криптокарту, в которую внести параметры уже созданного IPSec-туннеля; указать узел назначения, с которым требуется создать защищенный туннель; запустить уже выбранный алгоритм безопасного обмена ключами; определить время жизни ключа:

```
crypto map map1 10 ipsec-isakmp
set peer 10.1.0.1
set pfs group5
set security-association lifetime seconds 86400
```

7) Подключить установленный набор преобразований (ассоциаций) с указанием названия уже существующего туннеля:

```
set transform-set tunnel1
```

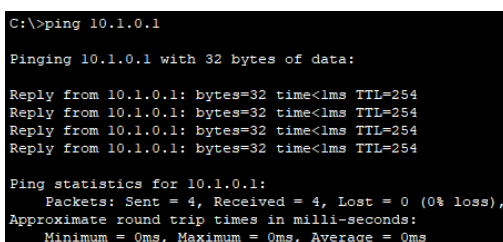
8) Привязать к данному туннелю выделенный с помощью списка доступа трафик:

```
Match address 100
```

9) Определить созданную криптокарту на нужный интерфейс:

```
interface f0/0
crypto map map1
```

Проверка передачи пакетов данных из одной сети в другую изображена на рисунках 3.2 и 3.3.



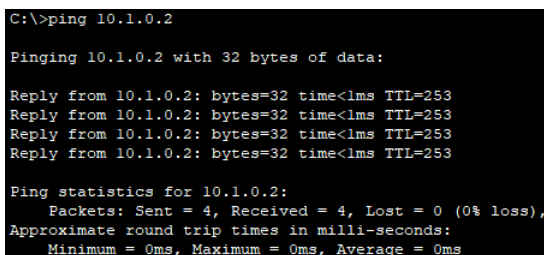
```
C:\>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:

Reply from 10.1.0.1: bytes=32 time<1ms TTL=254
Reply from 10.1.0.1: bytes=32 time<1ms TTL=254
Reply from 10.1.0.1: bytes=32 time<1ms TTL=254
Reply from 10.1.0.1: bytes=32 time<1ms TTL=254

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.2 – Проверка передачи пакетов



```
C:\>ping 10.1.0.2

Pinging 10.1.0.2 with 32 bytes of data:

Reply from 10.1.0.2: bytes=32 time<1ms TTL=253
Reply from 10.1.0.2: bytes=32 time<1ms TTL=253
Reply from 10.1.0.2: bytes=32 time<1ms TTL=253
Reply from 10.1.0.2: bytes=32 time<1ms TTL=253

Ping statistics for 10.1.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.3 – Проверка передачи пакетов

На рисунке 3.4 изображен протокол ESP в режиме симуляции.

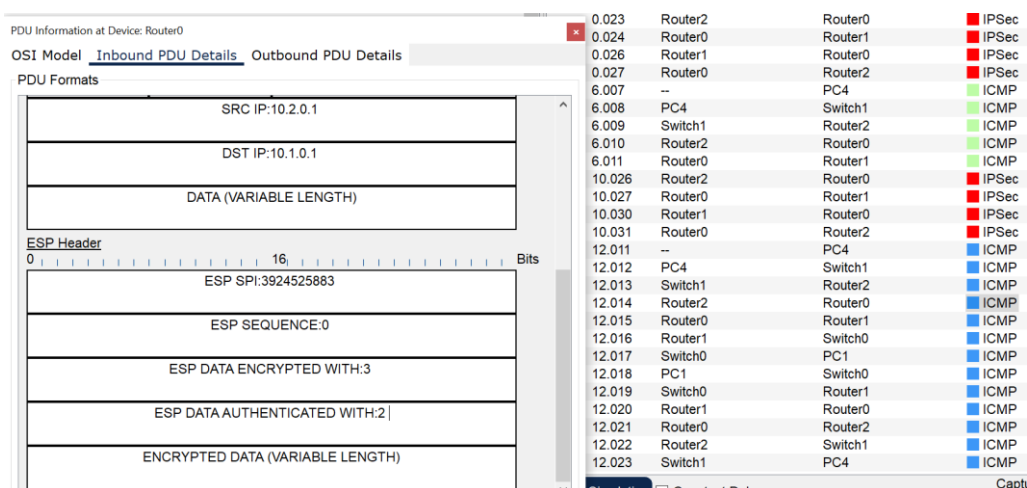


Рисунок 3.4 – Протокол ESP в режиме симуляции

На рисунке 3.5 изображена настройка IPsec.

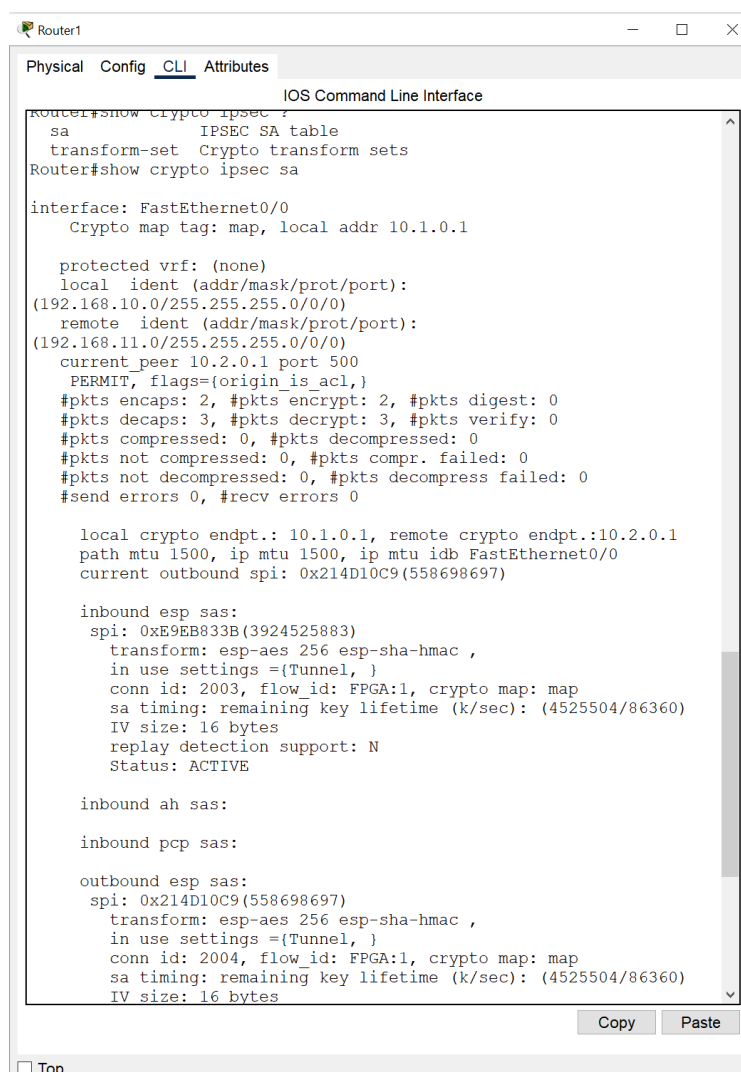


Рисунок 3.5 – Настройка IPsec

На рисунке 3.6 изображена криптографическая карта.

```
map      Crypto maps
Router#show crypto m
Crypto Map map 10 ipsec-isakmp
  Peer = 10.2.0.1
  Extended IP access list 100
    access-list 100 permit ip 192.168.10.0 0.0.0.255
192.168.11.0 0.0.0.255
    access-list 100 remark ACL for IPSec
  Current peer: 10.2.0.1
  Security association lifetime: 4608000 kilobytes/86400
seconds
  PFS (Y/N): Y
  Transform sets={
    R1-R2,
  }
  Interfaces using crypto map map:
    FastEthernet0/0
```

Рисунок 3.6 – Криптографическая карта

#### 4 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое IPSec? С какими протоколами совместимо?

IPSec (Internet Protocol Security) — это набор протоколов, предназначенный для обеспечения безопасности сетевого трафика на уровне IP. Он совместим с протоколами туннелирования (L2TP и PPTP), IKE, IKEv2.

2. Что понимается под ассоциацией безопасности? Для чего используется?

Ассоциация безопасности (Security Association, SA) — это концепция, используемая в области сетевой безопасности, особенно в контексте протоколов IPSec. Она представляет собой набор параметров, которые определяют, как будет осуществляться защита данных в сети. Эти параметры могут включать в себя алгоритмы шифрования, методы аутентификации, ключи шифрования и другие настройки, необходимые для обеспечения безопасного соединения. Она используется для установления защищённых соединений, управления безопасностью и обеспечения совместимости.

3. Что такое ISAKMP? За что отвечает в семействе протоколов IPSec и какие протоколы позволяет подключить?

ISAKMP (Internet Security Association and Key Management Protocol) — это протокол, определенный в RFC 2408, который отвечает за установление и управление ассоциациями безопасности (SA) в рамках протоколов IPSec. Он обеспечивает структуру для обмена сообщениями, необходимыми для согласования параметров безопасности, таких как алгоритмы шифрования и аутентификации, а также для управления ключами. Он отвечает за

установление ассоциаций безопасности, управление ключами и поддержку различных режимов обмена сообщениями (main mode и aggressive mode) и позволяет подключить IKE, IKEv2, KINK.

4. Из каких трех основных протоколов состоит IPSec?

Из AH, ESP и ISAKMP.

5. Какой протокол отвечает за аутентификацию? Какую дополнительную функцию также выполняет?

AH. Он выполняет функцию обеспечения целостности данных.

6. Что такое ESP и за что отвечает?

ESP (Encapsulating Security Payload) — это протокол, входящий в состав IPSec, который отвечает за шифрование и защиту конфиденциальности данных, передаваемых по сети. Он обеспечивает защиту содержимого пакетов, что делает их недоступными для несанкционированного доступа во время передачи.

7. За что отвечает протокол IKE?

IKE (Internet Key Exchange) — это протокол, который отвечает за установление защищённого канала, управление ключами, аутентификацию и поддерживает различные алгоритмы шифрования.

8. Перечислите основные достоинства и недостатки IPSec.

Достоинства:

- Высокий уровень безопасности
- Гибкость
- Прозрачность для приложений
- Совместимость

Недостатки:

- Сложность настройки
- Производительность
- Проблемы с NAT
- Зависимость от инфраструктуры

9. В каких двух режимах могут работать протоколы семейства IPSec? В чем особенность каждого из них?

В транспортном и туннельном. В транспортном режиме IPSec шифрует только полезную нагрузку (данные) пакета, оставляя оригинальный IP-заголовок неизменным. Это означает, что только данные, передаваемые в TCP или UDP, защищаются, а информация о маршруте остается открытой.

В туннельном режиме IPSec создает виртуальный "туннель" для передачи данных. Он шифрует как полезную нагрузку, так и оригинальный

IP-заголовок, добавляя новый IP-заголовок, который указывает на конечный пункт назначения.

10. Какие параметры необходимо согласовывать между сторонами защищенного обмена данными по протоколу IPSec?

Алгоритмы шифрования и аутентификации, параметры обмена ключами, сроки действия ключей, параметры IPSec SA (время жизни SA, протокол (AH или ESP), режим работы (туннельный или транспортный)).

## **5 ВЫВОД**

Изучил возможности настройки режимов работы протокола IPSec.