Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Безопасность компьютерных сетей»

Лабораторная работа №4  
«*VPN*. *IPSec*»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Сборка схемы 3](#_Toc135781319)

[2. Выбор плана адресации IPv4 3](#_Toc135781320)

[3. Базовая настройка маршрутизаторов и конечных устройств 4](#_Toc135781321)

[4. Настройка GRE туннеля между маршрутизаторами 4](#_Toc135781322)

[5. Защита туннеля средствами IPSec (AH, ESP). 6](#_Toc135781323)

[6. Настройка SPAN на коммутаторе Switch0 8](#_Toc135781324)

[7. Проверка наличия связи и анализ передаваемых пакетов 9](#_Toc135781325)

[Вывод 13](#_Toc135781326)

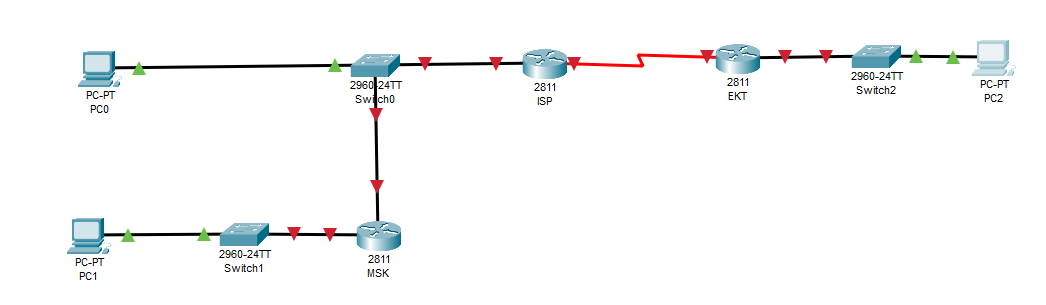
**Цель работы:**

Знакомство с технологией туннелирования и шифрования туннелированного трафика посредством *GRE*/*IPSec* в *Cisco* *Packet* *Tracer*.

**Ход работы:**

## Сборка схемы

Открываем *Cisco* *Packet* *Tracer* и собираем схему, указанную в методических материалах.



**Рисунок 1.** Схема сети

Важно отметить, что для соединения маршрутизаторов *ISP* и *EKT* понадобится подключения физического модуля *WIC*-2*T*, который поддерживает интерфейсы *Serial*.

## Выбор плана адресации IPv4

Простой *IP*-план сети:

|  |  |
| --- | --- |
| **Устройство** | **IP-адрес** |
| *ISP* *Router* | * MSK 1.1.1.2/24 * EKT 2.2.2.1/30 |
| *MSK* *Router* | **Local Net (Fa0/0)** 10.10.1.1/24  **ISP (Fa0/1)** 1.1.1.1/24 |
| *EKT* *Router* | **Local Net (Fa0/0)** 10.10.2.1/24  **ISP (Serial)** 2.2.2.2/30 |
| *Switch*0 | - |
| *Switch*1 | - |
| *Switch*2 | - |
| *PC*0 | 1.1.1.3/24 |
| *PC*1 | 10.10.1.2/24 |
| *PC*2 | 10.10.2.2/24 |

Выставление *IP* адресов для маршрутизаторов и конечных устройств будет производиться во время базовой настройки.

## Базовая настройка маршрутизаторов и конечных устройств

* 1. Базовая настройка конечных устройств.

Настраиваем статическую адресацию, указав *IPv*4 адрес, маску сети и шлюз по умолчанию.

* 1. Базовая настройка маршрутизатора.

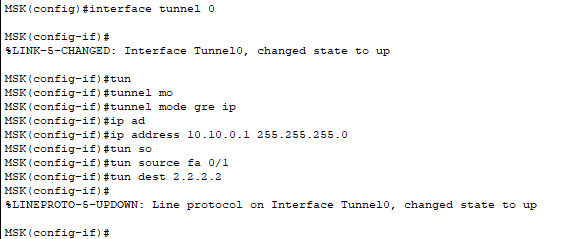
Устанавливаем имя хоста, указываем *IPv*4 адреса и маски сети для используемых интерфейсов (*ISP* и локальная сеть), указываем маршруты по умолчанию от граничных маршрутизаторов к *ISP*. Переводим маршрутизаторы в «*no* *shutdown*» режим. Сохраняем настройки.

Проверяем видимость компьютеров в соседней сети командой *ping*. Видимости нет.

## Настройка GRE туннеля между маршрутизаторами

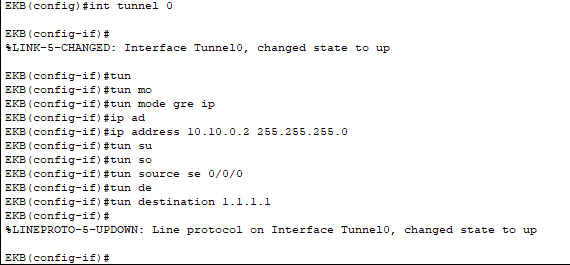
Настройка туннеля будет проводиться на каждом граничном маршрутизаторе локальных сетей (*EKB* и *MSK*)

* 1. Настройка на маршрутизаторе *MSK*:



**Рисунок 2.** Настройка GRE туннеля на маршрутизаторе MSK

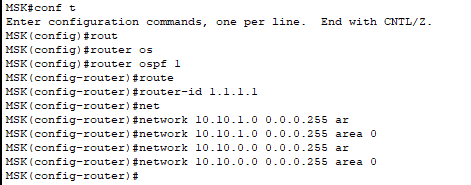
* 1. Настройка на маршрутизаторе *EKT*:



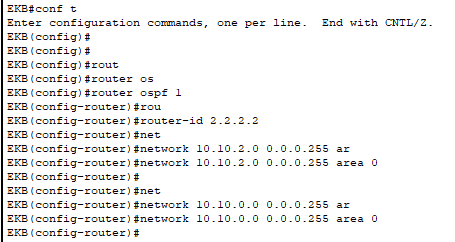
**Рисунок 3.** Настройка GRE туннеля на маршрутизаторе EKT

Вновь проверяем видимость компьютеров в соседней сети. Снова нет видимости. Нужно настроить маршрутизацию граничных маршрутизаторов (*OSPF*).

* 1. Настройка *OSPF*.



**Рисунок 4.** Настройка OSPF на MSK



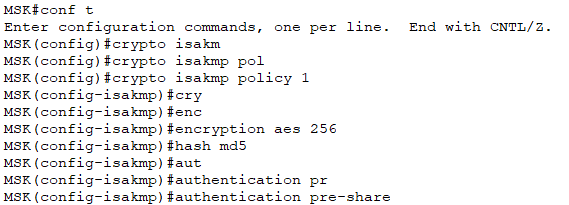
**Рисунок 5.** Настройка OSPF на EKT

Теперь маршрутизаторы будут «знать» своих соседей, а компьютеры одной сети смогут видеть компьютеры соседней сети.

## Защита туннеля средствами IPSec (AH, ESP).

Настройка производится на обоих пограничных маршрутизаторах.

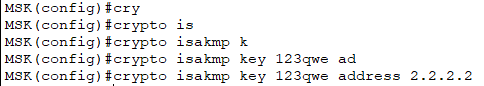
* 1. Задание политики



**Рисунок 6.** Задание политики для MSK.

Аналогично для *EKT*.

* 1. Задание ключа



**Рисунок 7.** Задание ключа для MSK

Аналогично (но с другим адресом – 1.1.1.1) для *EKT*.

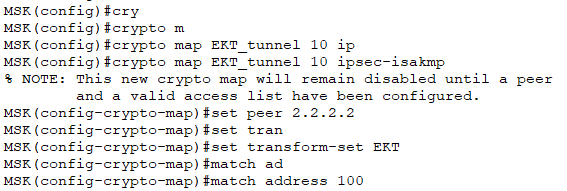
* 1. Задание набора преобразований – списка используемых комбинаций алгоритмов и протоколов



**Рисунок 8.** Задание набора преобразований для MSK

Аналогично (но с именем *MSK*) для *EKT*.

* 1. Задание крипто-карты туннеля



**Рисунок 9.** Задание крипто-карты туннеля

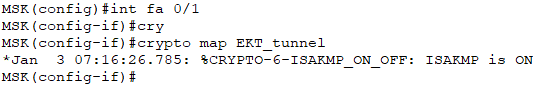
Аналогично (но с именем *MSK\_tunnel* и *set* *peer* 1.1.1.1, *set* *transform*-*set* *MSK*) для *EKT*.



**Рисунок 10.** Задание access-list для MSK

Аналогично (но с инверсивным порядком указания хостов) для *EKT*.

* 1. Применение крипто-карты на интерфейс



**Рисунок 11.** Применение крипто-карты на интерфейс для MSK

Аналогично (но уже с указанием интерфейса *Serial*0/0/0) для *EKT*.

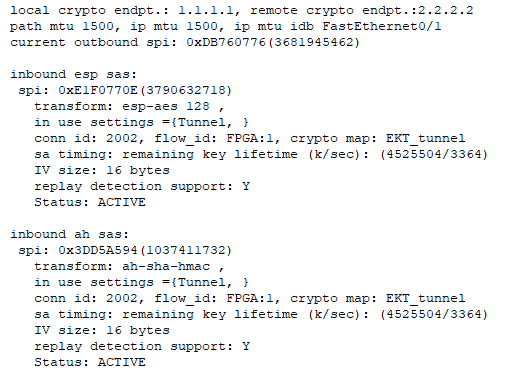
## Настройка SPAN на коммутаторе Switch0



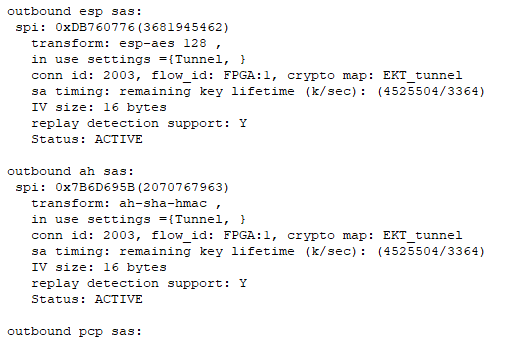
**Рисунок 12.** Настройка SPAN на коммутаторе Switch0

## Проверка наличия связи и анализ передаваемых пакетов

Запускаем режим симуляции пакетов и отправляем простой *ICMP* пакет от компьютера в сети 10.10.1.0 до компьютера в сети 10.10.2.0. Симуляция проходит успешно, пакет доставляется до адресата. Проверяем *SPI* (*Inbound*/*Outbound*) на маршрутизаторе *MSK* в привилегированном режиме командой «*show* *crypto* *ipsec* *sa*».

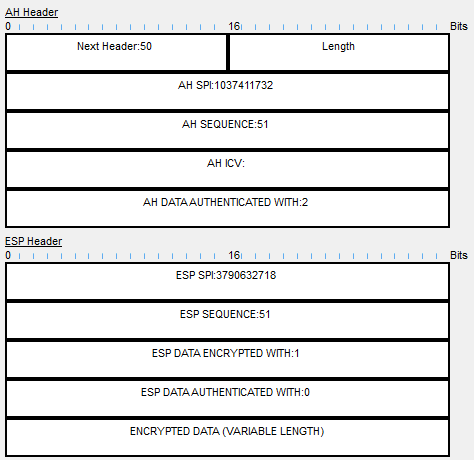


**Рисунок 13.** SPI (Inbound)

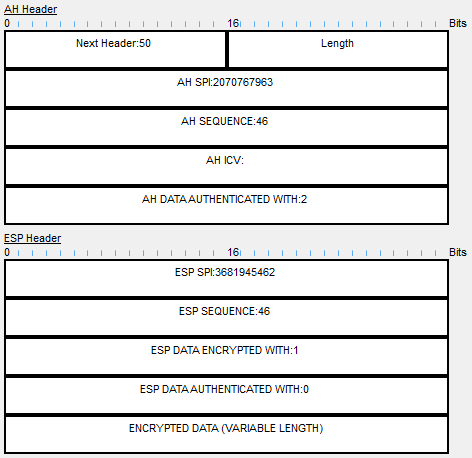


**Рисунок 14.** SPI (Outbound)

Теперь берем пакет (изначально отправленный пакет), пересланный с маршрутизатора *MSK* на коммутатор *Switch*0 и ищем заголовки *SPI* (*Inbound*/*Outbound*). При этом при просмотре кадров пакетов нужно учитывать, что значение *SPI* (*AH*/*ESP*) *Inbound* нужно искать во входящем трафике, а *SPI* (*AH*/*ESP*) *Inbound* – в исходящем.



**Рисунок 15.** AH и ESP заголовки с SPI (Inbound), маршрут Switch0-MSK



**Рисунок 16.** AH и ESP заголовки с SPI (Outbound), маршрут MSK-Switch0

Равенство значений *SPI* в заголовках кадров и информации, полученной в выводе в *CLI* маршрутизатора *MSK* свидетельствует об успешном шифровании трафике через туннель.

## Вывод

В ходе выполнения лабораторной работы были изучены основы туннелирования трафика, а также настройка шифрования туннелированного трафика посредством *GRE* и *IPSec*.

В *Cisco* *Packet* *Tracer* собрана схема, выполнена базовая настройка маршрутизаторов и конечных устройств; проведен туннель между граничными маршрутизаторами двух локальных сетей; настроена крипто-карта, которая в дальнейшем установлена на исходящие из локальной сети интерфейсы граничных маршрутизаторов.

После настройки *GRE*/*IPSec* проверено наличие связи и соответствие *SPI*, установленного на маршрутизаторе *MSK*, и *SPI*, находящегося в кадрах пакетов, для входящего и исходящего трафика.