**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сетевая безопасность»

Отчет по лабораторной работе №2

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-73Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Симонов Михаил Фёдорович  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

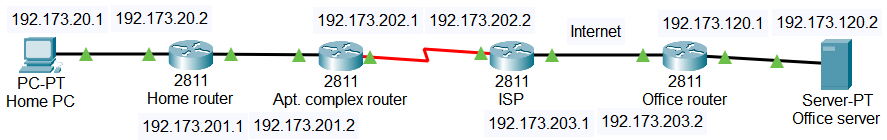
Москва, 2024 г.

Цель работы:

Изучить протоколы защиты данных в Cisco Packet Tracer на примере PPP и IPsec.

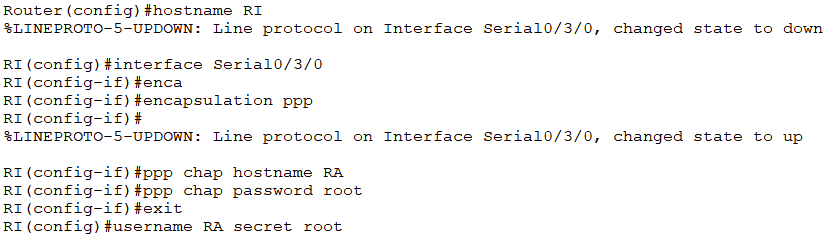
Ход работы:

1. Построить виртуальную сеть с IP-адресами подсетей по варианту:



1. Настроить PPP с аутентификацией CHAP между Apt. Complex Router и ISP:

Настройка одного из роутеров:



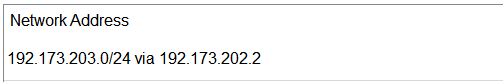
Настройка второго роутера осуществляется аналогично.

1. Настроить шлюзы по умолчанию и маршрутизацию всех сетей, кроме сети за Home router и сети за Office router:

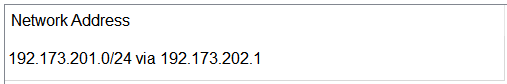
Роутер Home router:



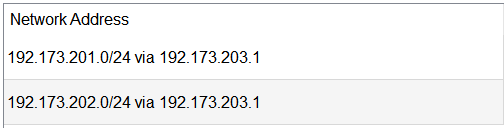
Роутер Apt. complex router:



Роутер ISP:



Роутер Office router:



1. Настроить IPsec туннель между Home router и Office router:

Сначала необходимо настроить непосредственно туннель:

*Router(config)#interface tunnel1*

*Router(config-if)#ip address 50.73.20.(n) 255.255.255.0*

*Router(config-if)#tunnel source (внутренний интерфейс туннеля)*

*Router(config-if)#tunnel destination (внутренний порт туннеля на том конце)*

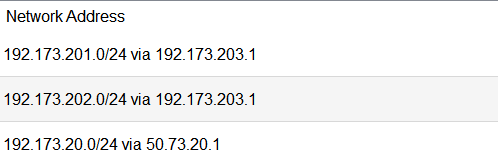
*Router(config-if)#end*

После создания туннеля необходимо обновить маршрутизацию:

Роутер Home router:



Роутер Office router:



Для настройки IPsec сначала необходимо настроить ISAKMP - протокол из набора IPsec для аутентификации и обмена ключами:

*Router(config)#crypto isakmp policy 10*

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

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

*Router(config-isakmp)#group 5*

*Router(config-isakmp)#exit*

Для Home router:

*Router(config)#crypto isakmp key password address 192.173.120.1*

*Router(config)#crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac*

*Router(config)#access-list 100 permit ip 192.173.20.0 0.0.0.255 192.173.120.0 0.0.0.255*

*Router(config)#crypto map IPSec 100 ipsec-isakmp*

*Router(config-crypto-map)#set peer 192.173.120.1*

Для Office router:

*Router(config)#crypto isakmp key password address 192.173.20.2*

*Router(config)#crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac*

*Router(config)#access-list 100 permit ip 192.173.120.0 0.0.0.255 192.173.20.0 0.0.0.255*

*Router(config)#crypto map IPSec 100 ipsec-isakmp*

*Router(config-crypto-map)#set peer 192.173.20.2*

Снова для обоих роутеров:

*Router(config-crypto-map)#set pfs group5*

*Router(config-crypto-map)#set security-association lifetime seconds 86400*

*Router(config-crypto-map)#set transform-set set1*

*Router(config-crypto-map)#match address 100*

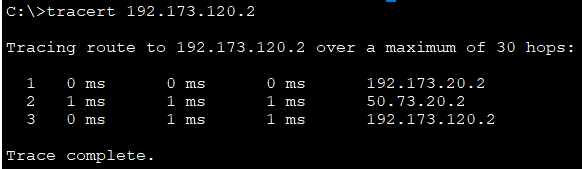
(выбрать внешний интерфейс туннеля)

*Router(config-if)#crypto map IPSec*

1. Продемонстрировать доступ к серверу Office server с компьютера Home PC:



С компьютера при помощи команды tracert:



Результаты выполнения работы:

В процессе выполнения лабораторной работы я вспомнила протокол IPSec и построение туннелей, а также научилась применять протокол РРР.