Лабораторная работа 16

Настройка VPN

Ланцова Яна Игоревна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков настройки VPN-туннеля через незащищённое Интернет-соединение.

2 Задание

Настроить VPN-туннель между сетью Университета г. Пиза (Италия) и сетью «Донская» в г. Москвas

3 Выполнение лабораторной работы

3.1 Размещение оборудования

Разместим в рабочей области проекта оборудование для сети Университета г. Пиза.(рис. 3.1).

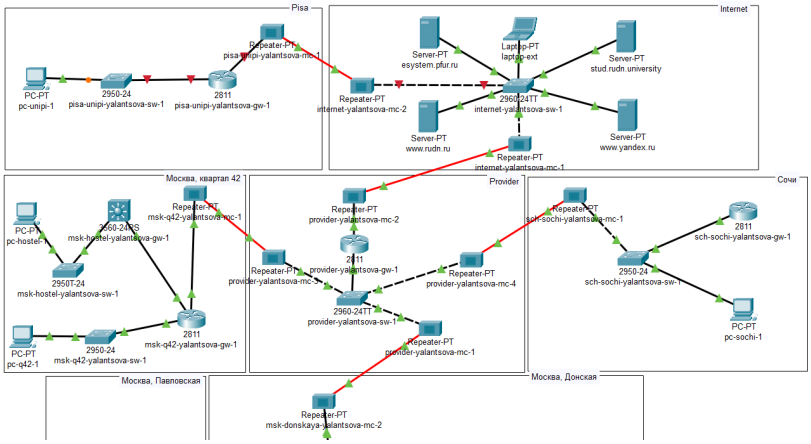

Рис. 3.1: Схема сети

В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование.(рис. 3.2, 3.3):

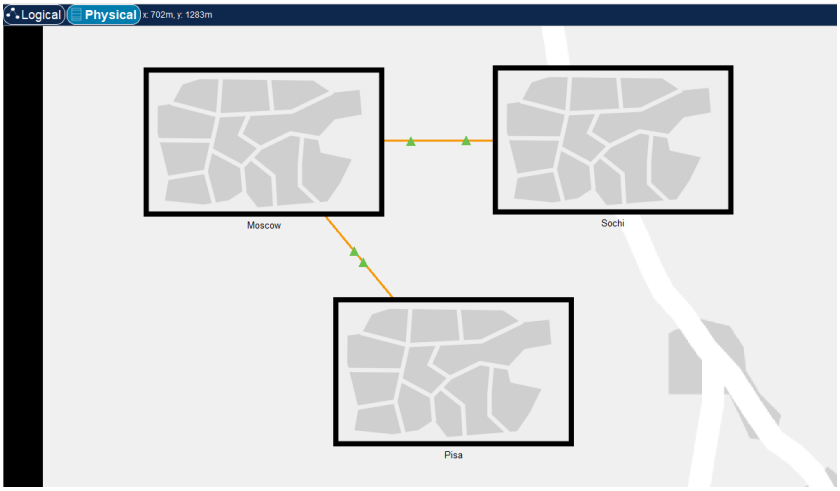

Рис. 3.2: Города сети

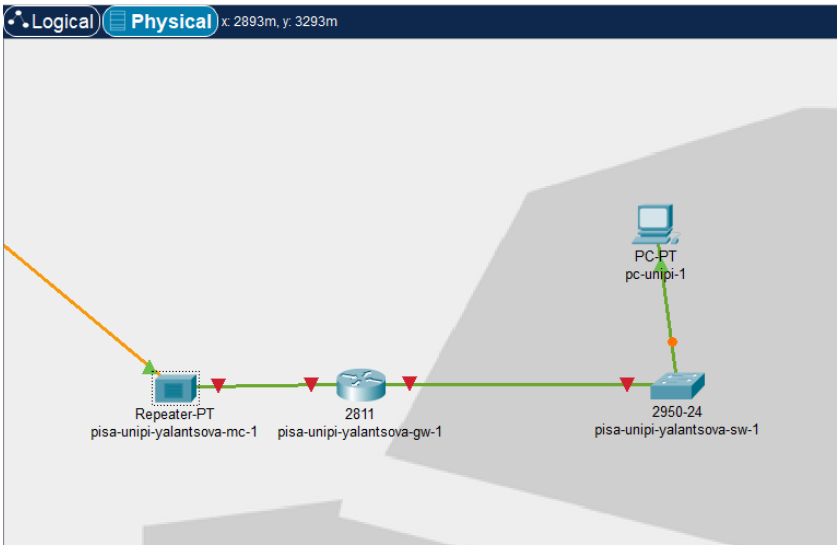

Рис. 3.3: Физическая область города Пиза

3.2 Первоначальная настройка оборудования

Для коммутатора и маршрутизатора на территории города Пиза установим имя хоста, доступ по паролю, telnet и ssh(рис. 3.4, 3.5).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname pisa-unipi-yalantsova-gw-1
pisa-unipi-yalantsova-gw-1(config)#
pisa-unipi-yalantsova-gw-1(config)#line vty 0 4
pisa-unipi-yalantsova-gw-1(config-line)#password cisco
pisa-unipi-yalantsova-gw-1(config-line)#login
pisa-unipi-yalantsova-gw-1(config-line)#exit
pisa-unipi-yalantsova-gw-1(config)#line console 0
pisa-unipi-yalantsova-gw-1(config-line)#password cisco
pisa-unipi-yalantsova-gw-1(config-line)#login
pisa-unipi-yalantsova-gw-1(config-line)#exit
pisa-unipi-yalantsova-gw-1(config)#enable secret cisco
pisa-unipi-yalantsova-gw-1(config)#service password-encryption
pisa-unipi-yalantsova-gw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-yalantsova-gw-1(config)#ip domain-name unipi.edu
pisa-unipi-yalantsova-gw-1(config)#crypto key generate rsa
The name for the keys will be: pisa-unipi-yalantsova-gw-1.unipi.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-yalantsova-gw-1(config)#line vty 0 4
*Mar 1 0:12:26.629: %SSH-5-ENABLED: SSH 1.99 has been enabled
pisa-unipi-yalantsova-gw-1(config-line)#transport input ssh
```

Рис. 3.4: Настройка маршрутизатора pisa-unipi-yalantsova-gw-1

```
pisa-unipi-yalantsova-sw-1(config)#line vty 0 4
pisa-unipi-yalantsova-sw-1(config-line)#password cisco
pisa-unipi-yalantsova-sw-1(config-line)#login
pisa-unipi-yalantsova-sw-1(config-line)#exit
pisa-unipi-yalantsova-sw-1(config)#line console 0
pisa-unipi-yalantsova-sw-1(config-line)#password cisco
pisa-unipi-yalantsova-sw-1(config-line)#login
pisa-unipi-yalantsova-sw-1(config-line)#exit
pisa-unipi-yalantsova-sw-1(config)#enable secret cisco
pisa-unipi-yalantsova-sw-1(config)#service password-encryption
pisa-unipi-yalantsova-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-yalantsova-sw-1(config)#ip domain-name unipi.edu
pisa-unipi-yalantsova-sw-1(config)#crypto key generate rsa
The name for the keys will be: pisa-unipi-yalantsova-sw-1.unipi.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-yalantsova-sw-1(config)#line vty 0 4
*Mar 1 0:13:44.489: %SSH-5-ENABLED: SSH 1.99 has been enabled
pisa-unipi-yalantsova-sw-1(config-line)#transport input ssh
pisa-unipi-yalantsova-sw-1(config-line)#exit
```

Рис. 3.5: Настройка коммутатора pisa-unipi-yalantsova-sw-1

Теперь настроим интерфейсы на сетевых устройтсвах Пизы(рис. 3.6, 3.7). Для машрутизатора поднимем интерфейс f0/0, а на нем субинтерфейс f0/0.401 для основного 401 vlan Пизы, и зададим ip-адрес. Также поднимем f0/1 и зададим ip-адрес для связи с подсетью Интернет, указав маршрут по умолчанию к маршрутизатору из сети Интернет. На коммутаторе поднимем интерфейс f0/24 и сделаем его транковым, а на интерфейсе f0/1 дадим доступ к vlan 401 Пизы.

```
pisa-unipi-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-yalantsova-gw-1(config)#interface f0/0
pisa-unipi-yalantsova-gw-1(config-if)#no shutdown

pisa-unipi-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

pisa-unipi-yalantsova-gw-1(config-if)#exit
pisa-unipi-yalantsova-gw-1(config)#interface f0/0.401
pisa-unipi-yalantsova-gw-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.401, changed state to up

pisa-unipi-yalantsova-gw-1(config-subif)#encapsulation dot1Q 401
pisa-unipi-yalantsova-gw-1(config-subif)#ip address 10.131.0.1 255.255.255.0
pisa-unipi-yalantsova-gw-1(config-subif)#description unipi main
pisa-unipi-yalantsova-gw-1(config-subif)#description unipi-main
pisa-unipi-yalantsova-gw-1(config-subif)#exit
pisa-unipi-yalantsova-gw-1(config)#interface f0/1
pisa-unipi-yalantsova-gw-1(config-if)#no shutdown

pisa-unipi-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

pisa-unipi-yalantsova-gw-1(config-if)#ip address 192.0.2.20 255.255.255.0
pisa-unipi-yalantsova-gw-1(config-if)#description internet
pisa-unipi-yalantsova-gw-1(config-if)#exit
pisa-unipi-yalantsova-gw-1(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1
```

Рис. 3.6: Настройка интерфейсов маршрутизатора pisa-unipi-yalantsova-gw-1

```
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-yalantsova-sw-1(config)#interface f0/24
pisa-unipi-yalantsova-sw-1(config-if)#switchport mode trunk
pisa-unipi-yalantsova-sw-1(config-if)#exit
pisa-unipi-yalantsova-sw-1(config)#interface f0/1
pisa-unipi-yalantsova-sw-1(config-if)#switchport mode access
pisa-unipi-yalantsova-sw-1(config-if)#switchport access vlan 401
% Access VLAN does not exist. Creating vlan 401
pisa-unipi-yalantsova-sw-1(config-if)#exit
pisa-unipi-yalantsova-sw-1(config)#vlan 401
pisa-unipi-yalantsova-sw-1(config-vlan)#name unipi main
                                       ^
% Invalid input detected at '^' marker.

pisa-unipi-yalantsova-sw-1(config-vlan)#name unipi-main
pisa-unipi-yalantsova-sw-1(config-vlan)#interface vlan401
pisa-unipi-yalantsova-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan401, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan401, changed state to up

pisa-unipi-yalantsova-sw-1(config-if)#no shutdown
pisa-unipi-yalantsova-sw-1(config-if)#exit
```

Рис. 3.7: Настройка интерфейсов маршрутизатора pisa-unipi-yalantsova-sw-1

Проверим связь устройств внутри Пизы, пропинговав марщрутизатор с ПК(рис. 3.8).

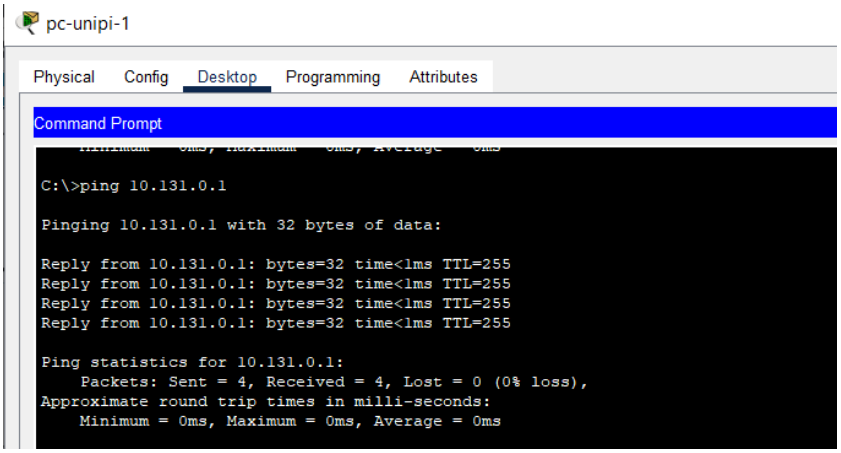

Рис. 3.8: Проверка связи между устройствами в городе Пиза

3.3 Настройка VPN на основе GRE

Настроим VPN на основе протокола GRE. Для этого на маршрутизаторе с Донской зададим интерфейс и ip-адрес для туннеля, указав источником интерфейс f0/1.4(vlan в Интернет), а точкой назначения адрес 192.0.2.20(маршрутизатор Университета Пизы в сети Интернет). Также поднимем loopback-интерфейс, на котором зададим loopback-адрес машрутизатора и маршрут по умолчанию до Пизы, указав, что надо посылать на loopback-адрес, идя через туннельный адрес маршрутизатора в г. Пиза(рис. 3.9).

```
msk-donskaya-yalantsova-gw-1>en
Password:
msk-donskaya-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-yalantsova-gw-1(config)#interface Tunnel0

msk-donskaya-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

msk-donskaya-yalantsova-gw-1(config-if)#ip address 10.128.255.253 255.255.255.252
msk-donskaya-yalantsova-gw-1(config-if)#tunnel source f0/1.4
msk-donskaya-yalantsova-gw-1(config-if)#tunnel destination 192.0.2.20
msk-donskaya-yalantsova-gw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

msk-donskaya-yalantsova-gw-1(config-if)#exit
msk-donskaya-yalantsova-gw-1(config)#interface loopback0

msk-donskaya-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

msk-donskaya-yalantsova-gw-1(config-if)#ip address 10.128.254.1 255.255.255.255
msk-donskaya-yalantsova-gw-1(config-if)#exit
msk-donskaya-yalantsova-gw-1(config)#ip route 10.128.254.5 255.255.255.255 10.128.255.254
```

Рис. 3.9: Настройка VPN на маршрутизаторе msk-donskaya-yalantsova-gw-1

Теперь на маршрутизаторе в Пизе зададим интерфейс и ip-адрес для туннеля, указав источником интерфейс f0/1(свзяь с сетью Интернет), а точкой назначения адрес 198.51.100.2(внешний адрес маршрутизатора Донской). Также поднимем loopback-интерфейс, на котором зададим loopback-адрес машрутизатора и маршрут по умолчанию до Донской, указав, что надо посылать на loopback-адрес, идя через туннельный адрес маршрутизатора на Донской. Кроме того настроим протокол OSPF(рис. 3.10):

```
pisa-unipi-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-yalantsova-gw-1(config)#interface Tunnel0

pisa-unipi-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

pisa-unipi-yalantsova-gw-1(config-if)#ip address 10.128.255.254 255.255.255.252
pisa-unipi-yalantsova-gw-1(config-if)#tunnel source f0/1
pisa-unipi-yalantsova-gw-1(config-if)#tunnel destination 198.51.100.2
pisa-unipi-yalantsova-gw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

pisa-unipi-yalantsova-gw-1(config-if)#exit
pisa-unipi-yalantsova-gw-1(config)#interface loopback0

pisa-unipi-yalantsova-gw-1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

pisa-unipi-yalantsova-gw-1(config-if)#ip address 10.128.254.5 255.255.255.255
pisa-unipi-yalantsova-gw-1(config-if)#exit
pisa-unipi-yalantsova-gw-1(config)#ip route 10.128.254.1 255.255.255.255 10.128.255.253
pisa-unipi-yalantsova-gw-1(config)#router ospf 1
pisa-unipi-yalantsova-gw-1(config-router)#router-id 10.128.254.5
pisa-unipi-yalantsova-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
```

Рис. 3.10: Настройка VPN на маршрутизаторе pisa-unipi-yalantsova-gw-1

Проверим доступность узлов сети Университета г. Пиза, пропинговав Пк в Пизе с ноутбука администратора сети «Донская»(рис. 3.11):

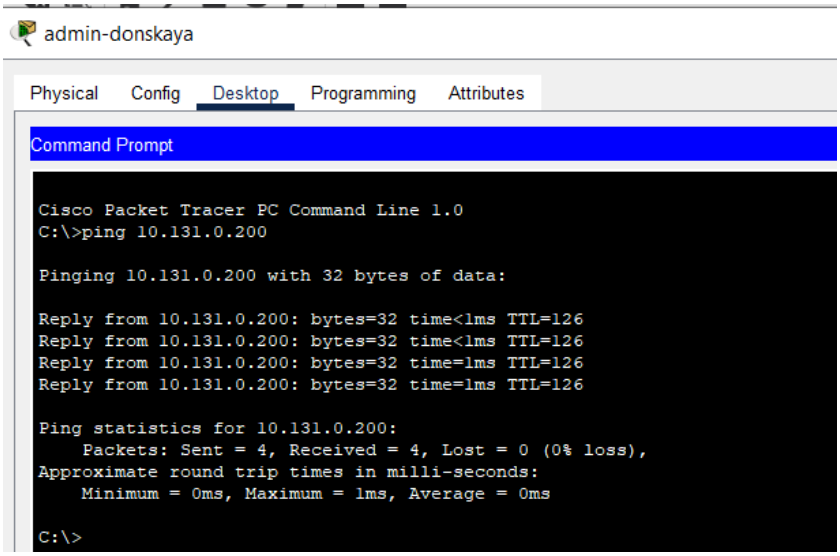

Рис. 3.11: Проверка доступности узлов сети Университета г. Пиза из сети Донская

4 Выводы

В результате выполнения лабораторной были приобретены практические навыки по настройке VPN-туннеля через незащищённое Интернет-соединение.

5 Контрольные вопросы

1. Что такое VPN?

Виртуальная частная сеть (Virtual Private Network, VPN) — технология, обеспечивающая одно или несколько сетевых соединений поверх другой сети (например, Интернет).

2. В каких случаях следует использовать VPN?

- Обеспечение безопасности и конфиденциальности: VPN шифрует ваше интернет-соединение, что позволяет защитить ваши данные от несанкционированного доступа и прослушивания. Это особенно важно при использовании общественных Wi-Fi сетей, где ваша информация может быть уязвима.
- Обход географических ограничений: VPN позволяет обойти географические ограничения и получить доступ к контенту, который может быть недоступен в вашей стране. Например, вы можете получить доступ к стриминговым сервисам, социальным сетям или новостным сайтам, которые ограничены в вашем регионе.
- Анонимность и защита личной информации: VPN скрывает ваш реальный IP-адрес и заменяет его на IP-адрес сервера VPN. Это помогает сохранить вашу анонимность и защитить вашу личную информацию от отслеживания и сбора данных о вас.
- Работа из удаленного офиса: Если вы работаете из удаленного офиса или подключаетесь к корпоративной сети из дома, VPN обеспечивает безопасное соединение и защищает корпоративные данные от утечки.

3. Как с помощью VPN обойти NAT?

При подключении к VPN-серверу устройство получает новый виртуальный IP-адрес, который не связан с реальным IP-адресом. Это позволяет обойти ограничения NAT и получить доступ к ресурсам в Интернете, которые могут быть недоступны из-за NAT.