Лабораторная работа № 16. Настройка VPN

16.1. Цель работы

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

16.2. Задание

Настроить VPN-туннель между сетью Университета г. Пиза (Италия) и сетью «Донская» в г. Москва (см. рис. 16.1).

При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

16.3. Предварительные сведения

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

Для организации защищённого VPN-туннеля может использоваться протокол общей инкапсуляции маршрутов (Generic Routing Encapsulation, GRE) компании Cisco. Основное назначение GRE — инкапсуляция пакетов сетевого уровня сетевой модели взаимодействия открытых систем (Open Systems Interconnection Basic Reference Model), например, IP, CLNP, IPX, AppleTalk и др., в IP пакеты.

16.4. Модельные предположения

Сеть Университета г. Пиза (Италия) содержит маршрутизатор Cisco 2811 `pisa-inipi-gw-1`, коммутатор Cisco 2950 `pisa-unipi-sw-1` и конечное устройство PC `pc-unipi-1` (см. общую схему сети на рис. 16.1).

Адреса для организации VPN-туннеля представлены в табл. 16.1.

Таблица 16.1

Адреса туннеля VPN

IP-адреса	Примечание
10.128.255.252/30	Линк VPN
10.128.255.253	msk-donskaya-gw-1
10.128.255.254	pisa-unipi-gw-1

Для идентификации маршрутизаторов предполагается использовать loopback-адреса (табл. 16.2).

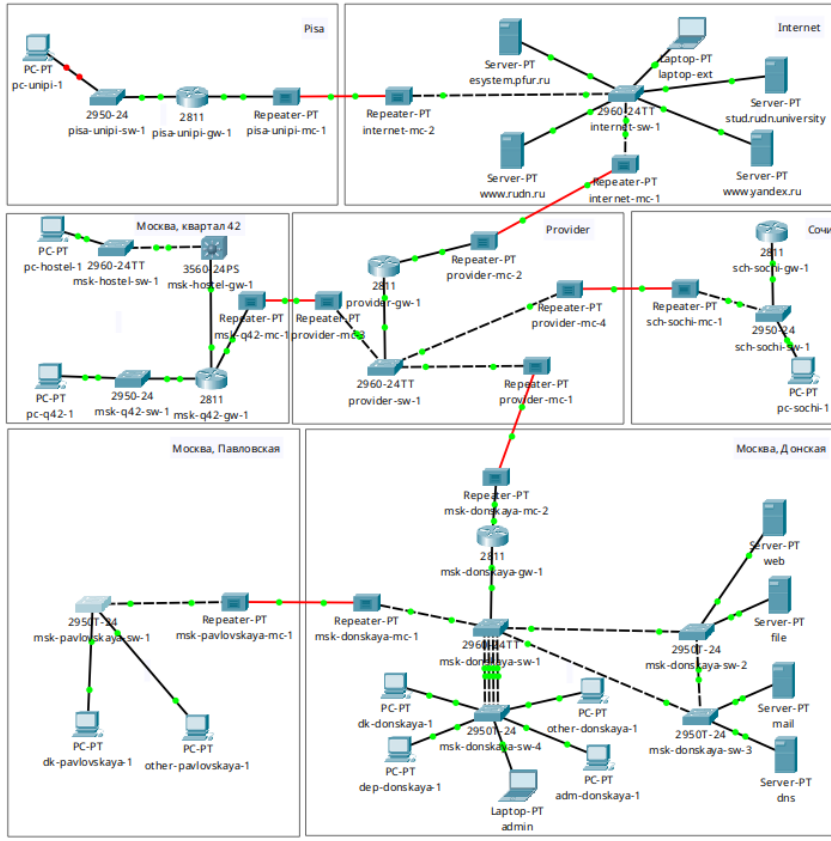

Рис. 16.1. Схема сети с дополнительными площадками

16.5. Последовательность выполнения работы

1. Разместить в рабочей области проекта в соответствии с модельными предположениями оборудование для сети Университета г. Пиза.
2. В физической рабочей области проекта создать город Пиза, здание Университета г. Пиза. Переместить туда соответствующее оборудование.
3. Сделать первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза (см. раздел 16.5.1).
4. Настроить VPN на основе протокола GRE [25] (см. раздел 16.5.2).
5. Проверить доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская».

Таблица 16.2

Адреса интерфейсов loopback

IP-адреса	Примечание
10.128.254.0/24	Сеть адресов loopback интерфейсов
10.128.254.1/32	msk-donskaya-gw-1
10.128.254.2/32	msk-q42-gw-1
10.128.254.3/32	msk-hostel-gw-1
10.128.254.4/32	sch-sochi-gw-1
10.128.254.5/32	pisa-unipi-gw-1

16.5.1. Настройка площадки в г. Пиза

16.5.1.1. Первоначальная настройка маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#line vty 0 4
pisa-unipi-gw-1(config-line)#password cisco
pisa-unipi-gw-1(config-line)#login
pisa-unipi-gw-1(config-line)#exit

pisa-unipi-gw-1(config)#line console 0
pisa-unipi-gw-1(config-line)#password cisco
pisa-unipi-gw-1(config-line)#login
pisa-unipi-gw-1(config-line)#exit

pisa-unipi-gw-1(config)#enable secret cisco
pisa-unipi-gw-1(config)#service password-encryption
pisa-unipi-gw-1(config)#username admin privilege 1 secret cisco

pisa-unipi-gw-1(config)#ip domain-name unipi.edu
pisa-unipi-gw-1(config)#crypto key generate rsa
pisa-unipi-gw-1(config)#line vty 0 4
pisa-unipi-gw-1(config-line)#transport input ssh
```

16.5.1.2. Первоначальная настройка коммутатора pisa-unipi-sw-1

```
pisa-unipi-sw-1>enable
pisa-unipi-sw-1#configure terminal

pisa-unipi-sw-1(config)#line vty 0 4
pisa-unipi-sw-1(config-line)#password cisco
pisa-unipi-sw-1(config-line)#login
pisa-unipi-sw-1(config-line)#exit

pisa-unipi-sw-1(config)#line console 0
pisa-unipi-sw-1(config-line)#password cisco
pisa-unipi-sw-1(config-line)#login
pisa-unipi-sw-1(config-line)#exit
```

```
pisa-unipi-sw-1(config)#enable secret cisco
pisa-unipi-sw-1(config)#service password-encryption
pisa-unipi-sw-1(config)#username admin privilege 1 secret cisco

pisa-unipi-sw-1(config)#ip domain-name unipi.edu
pisa-unipi-sw-1(config)#crypto key generate rsa
pisa-unipi-sw-1(config)#line vty 0 4
pisa-unipi-sw-1(config-line)#transport input ssh
```

16.5.1.3. Настройка интерфейсов маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#interface f0/0
pisa-unipi-gw-1(config-if)#no shutdown
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#interface f0/0.401
pisa-unipi-gw-1(config-subif)#encapsulation dot1Q 401
pisa-unipi-gw-1(config-subif)#ip address 10.131.0.1 255.255.255.0
pisa-unipi-gw-1(config-subif)#description unipi-main
pisa-unipi-gw-1(config-subif)#exit

pisa-unipi-gw-1(config)#interface f0/1
pisa-unipi-gw-1(config-if)#no shutdown
pisa-unipi-gw-1(config-if)#ip address 192.0.2.20 255.255.255.0
pisa-unipi-gw-1(config-if)#description internet
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1
```

16.5.1.4. Настройка интерфейсов коммутатора pisa-unipi-sw-1

```
pisa-unipi-sw-1>enable
pisa-unipi-sw-1#configure terminal

pisa-unipi-sw-1(config)#interface f0/24
pisa-unipi-sw-1(config-if)#switchport mode trunk
pisa-unipi-sw-1(config-if)#exit

pisa-unipi-sw-1(config)#interface f0/1
pisa-unipi-sw-1(config-if)#switchport mode access
pisa-unipi-sw-1(config-if)#switchport access vlan 401
pisa-unipi-sw-1(config-if)#exit

pisa-unipi-sw-1(config)#vlan 401
pisa-unipi-sw-1(config-vlan)#name unipi-main
pisa-unipi-sw-1(config-vlan)#exit

pisa-unipi-sw-1(config)#interface vlan401
pisa-unipi-sw-1(config-if)#no shutdown
pisa-unipi-sw-1(config-if)#exit
```

16.5.2. Настройка VPN на основе GRE

16.5.2.1. Настройка маршрутизатора msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface Tunnel0
msk-donskaya-gw-1(config-if)#ip address 10.128.255.253 255.255.255.252
msk-donskaya-gw-1(config-if)#tunnel source f0/1.4
msk-donskaya-gw-1(config-if)#tunnel destination 192.0.2.20
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#interface loopback0
msk-donskaya-gw-1(config-if)#ip address 10.128.254.1 255.255.255.255
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#ip route 10.128.254.5 255.255.255.255
    ↪ 10.128.255.254
```

16.5.2.2. Настройка маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#interface Tunnel0
pisa-unipi-gw-1(config-if)#ip address 10.128.255.254 255.255.255.252
pisa-unipi-gw-1(config-if)#tunnel source f0/1
pisa-inipi-gw-1(config-if)#tunnel destination 198.51.100.2
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#interface loopback0
pisa-unipi-gw-1(config-if)#ip address 10.128.254.5 255.255.255.255
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#ip route 10.128.254.1 255.255.255.255
    ↪ 10.128.255.253

pisa-unipi-gw-1(config)#router ospf 1
pisa-unipi-gw-1(config-router)#router-id 10.128.254.5
pisa-unipi-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
pisa-unipi-gw-1(config-router)#exit
```

16.6. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - подробное описание настроек сетевого оборудования в соответствии с заданием;
   - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

16.7. Контрольные вопросы

1. Что такое VPN?

2. В каких случаях следует использовать VPN?
3. Как с помощью VPN обойти NAT?

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155.
2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.
3. *A J.* Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_s.
4. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.
5. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.
6. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http://www.ietf.org/rfc/rfc3069.txt.
7. *Moy J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.
8. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.
9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
10. *Neumann J. C.* Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.
11. *Odom S., Nottingham H.* Cisco Switching: Black Book. — The Coriolis Group, 2001. — ISBN 9781576107065. — URL: http://books.google.sk/books?id=GYsLAAAACAAJ.
12. *Tetz E.* Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html.
13. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: http://protect.gost.ru/v.aspx?control=7&id=132355.
14. *Кларк К., Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.

15. *Королькова А. В.*, *Кулябов Д. С.* Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.

16. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.

17. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.

18. *Королькова А. В.*, *Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.

19. *Куроуз Д. Ф.*, *Росс К. В.* Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

20. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.

21. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

22. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.

23. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.

24. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science). — ISBN 978-5-496-00831-0.

25. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.

26. Цикл статей «Сети для самых маленьких». — URL: `http://linkmeup.ru/blog/11.html`.

27. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: `https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html`.