Федеральное агентство связи

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича »

Протоколы туннелирования.

Лабораторный практикум.

Санкт-Петербург

2017

Лабораторная работа №3
Построение VPN.

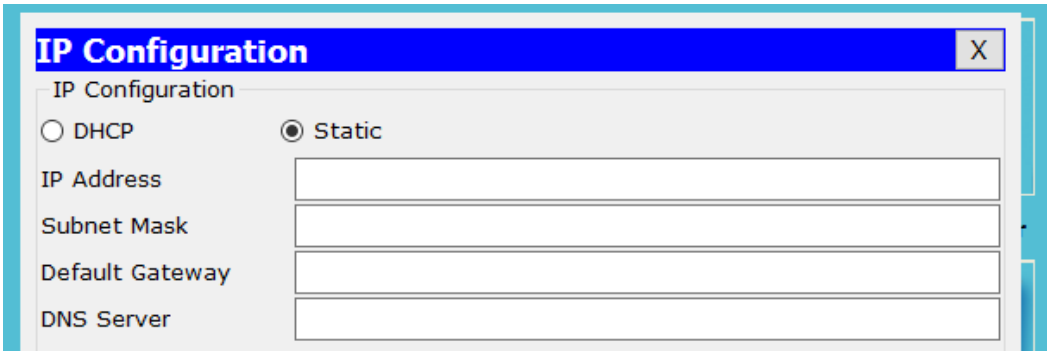
Цель работы: Получение практических навыков организации VPN соединения, а также знакомство с NAT(Network Address Translation).

Теоретические сведения:

Концепция построения защищенных виртуальных частных сетей основывается на простой идее, которая заключается в следующем: если в глобальной сети есть два узла, которым необходимо обмениваться информацией (при этом важно обеспечить конфиденциальность и целостность данных), то между ними нужно создать виртуальный туннель. Туннель должен отвечать требованию чрезвычайной труднодоступности к нему всеми возможными внешними наблюдателями.

Настройка ip-адресов компьютеров производится следующим образом:

1. Клик на устройство открывает меню его конфигураций.
2. В появившемся окне выбирается поле "IP Configuration" (В дальнейшем для выполнения команды ping необходимо будет выбрать "Command Prompt").
3. Для данной лабораторной работы нужно заполнить поля "IP-Address", "Subnet Mask", "Default Gateway":



4. Закрыть окно конфигурации.

Настройка адресов маршрутизаторов выполняется в CLI(Command Line Interface) следующим образом:

1. Клик на устройство открывает меню его конфигураций.
2. Выбирается вкладка CLI.
3. Поочередно выполняются команды:

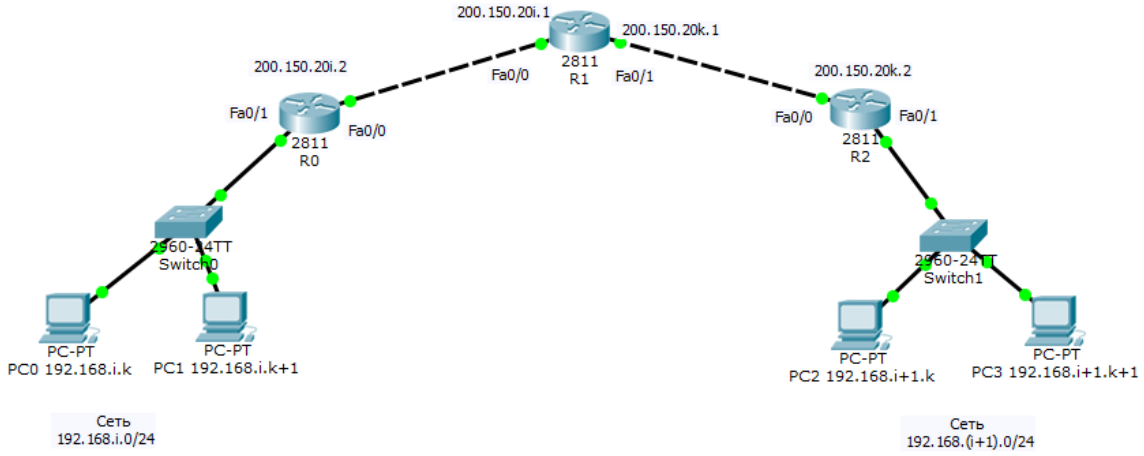
   R>enable
   R#configure terminal
   R2(config)#interface fastEthernet N **(где N-номер интерфейса)**
   R2(config-if)#ip address A.B.C.D A1.B1.C1.D1 **(где A.B.C.D-ip-адрес, A1.B1.C1.D1 - маска сети)**
   R2(config-if)#exit **(выход из настроек интерфейса)**

Варианты:

Варианты заданий выбираются в соответствии с номером зачётной книжки студента, где i - предпоследняя цифра в зачётной книжке студента, k - последняя.

Порядок выполнения работы:

1. В программе Cisco Packet Tracer создать следующую схему:



2. Настроить ip-адреса, как показано на рисунке согласно своему варианту.
3. На роутерах R0 и R2 установить настройки NAT, например:

   R0(config)#interface fastEthernet 0/0
   R0(config-if)#ip nat outside **(указание на внешний NAT-интерфейс)**
   R0(config-if)#exit
   R0(config)#int fa0/1
   R0(config-if)#ip nat **inside (указание на внутренний NAT-интерфейс)**
   R0(config-if)#exit
   R0(config)#ip access-list standard vpnlab **(выбрать называние листа доступа)**

R0(config-std-nacl)#permit 192.168.i.0 0.0.0.255 **(добавить разрешение на применение NAT к адресам локальной сети маршрутизатора)**
R0(config-std-nacl)#exit
R0(config)#ip nat inside source list vpnlab interface fastEthernet 0/0 overload **(указываем трансляцию созданного нами листа и внешний интерфейс маршрутизатора)**
R0(config)#

4. Проверить доступность интерфейса маршрутизатора R1(200.150.20i.1) с одного из компьютеров сети 192.168.i.0, используя утилиту PING.
5. Аналогичным образом настроить NAT на маршрутизаторе R2 и произвести проверку доступности второго интерфейса R1 с одного из компьютеров второй сети 192.168.(i+1).0
6. Приступить к настройке VPN на R0, используя следующие команды:

R0>
R0>enable
R0#configure terminal
R0(config)#crypto isakmp policy 1 (создание политики, далее ее параметры)
R0(config-isakmp)#encryption 3des **(шифрование 3des - алгоритм симметричного шифрования)**
R0(config-isakmp)#hash md5 **(хэш-функция md5(алгоритм хэширования))**
R0(config-isakmp)#authentication pre-share**(алгоритм дефи-хэлмана для обмена прешард ключами)**
R0(config-isakmp)#group 2 **(2 Diffie-Hellman group 2)**
R0(config-isakmp)#exit
R0(config)#

Теперь нужно создать сам pre-shared ключ и задать ip-адрес роутера, с которым будет производиться соединение по VPN:
R0(config)#crypto isakmp key vpnkey address 200.150.20k.2
Указать параметры, необходимые для построения IPSec-туннеля:
R0(config)#crypto ipsec transform-set TrSet esp-3des esp-md5-hmac **(алгоритм шифрования и алгоритм хэширования)**

Настройка access-листа, который указывает, какой трафик отправлять в туннель:

R0>enable
R0#configure terminal
R0(config)#ip access-list extended vpntun
R0(config-ext-nacl)#permit ip 192.168.i.0 0.0.0.255 192.168.(i+1).0 0.0.0.255 **(помещение в туннель пакетов, направляющихся из сети i в сеть (i+1))**
R0(config-ext-nacl)#exit

Создание криптокарты:

R0(config)#crypto map CrMap 10 ipsec-isakmp (**для данной записи будет использоваться процедура согласования параметров IKE**)
R0(config-crypto-map)#set peer 200.150.20k.2 **(внешний интерфейс R2, удалённого устройства)**
R0(config-crypto-map)#set transform-set TrSet

R0(config-crypto-map)#match address vpntun **(допускаем созданный ранее access-list)**
R0(config-crypto-map)#exit
R0(config)#interface fastEthernet 0/0
R0(config-if)#crypto map CrMap **(прикрепляет криптокарту к внешнему интерфейсу)**

7. Аналогичным образом настроить маршрутизатор R2.
8. Запустить PING от компьютера в левой подсети до компьютера в правой.
9. Убедиться в том, что хост недоступен.
10. Повторно запустить PING и не прерывая его, выполнить на R0 команду:

R0#show ip nat translations

11. Ознакомиться с появившейся информации о недопуске пакетов механизмом NAT, который не пропускает все пакеты.
12. Удалить созданный ранее access-list и создать новый с указанием допуска пакетов, направляющихся из данной сети в удалённую:

R0(config)#no ip access-list standard vpntun
R0(config)#ip access-list extended vpntun
R0(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255 **(исключение)**
R0(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 any **(все остальные подвергать обработке NAT)**
R0(config-ext-nacl)#exit
R0(config)#exit

13. Аналогичным образом настроить лист доступа на R2.
14. Проверить доступность компьютеров разных сетей друг для друга, используя утилиту PING.
15. Убедиться в том, что теперь пакеты доходят успешно.

Представление работы:

В отчёте к данной работе должны содержаться: снимок экрана составленной схемы с подписанными ip-адресами интерфейсов и с пометкой на рабочем поле с именем, фамилией и группой студента; тексты команд, выполняемых для достижения результатов, требуемых в данной лабораторной работе; вывод.

Контрольные вопросы:

1. Какие возможности предоставляет VPN и кто чаще является пользователями данной технологии?
2. Какие функции выполняет NAT?
3. Какие меры были предприняты в данной лабораторной работе после того, как оказалось, что трансляция сетевых адресов мешает отправке пакетов через туннель VPN?