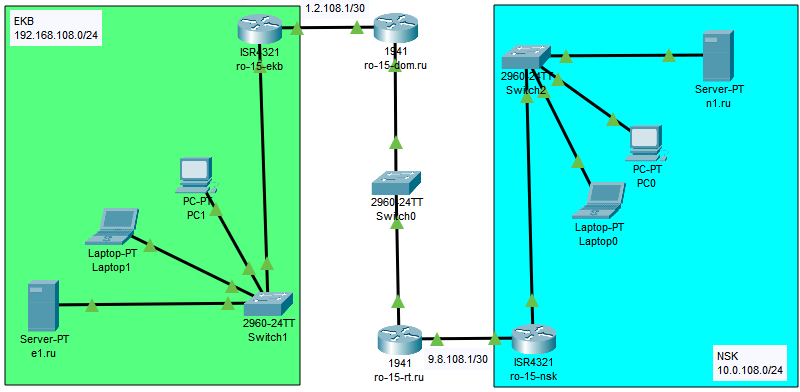
Лабораторная работа № 15. VPN

В данной работе мы познакомимся с механизмом виртуальных частных сетей (VPN: Virtual Private Network), который позволяет пересылать данные между двумя (и более) локальными сетями через публичные сети, гарантируя их целостность и конфиденциальность.

Существует огромное количество протоколов, обеспечивающих создание VPN, мы познакомимся с одним из наиболее широко применяемых – IPsec. Это очень сложный протокол, имеющий широчайшие варианты настройки. В его работе принято выделять две фазы:

1. Установка безопасного канала между двумя узлами (IKE security association, IKE SA)
2. Собственно пересылка пакетов внутри канала

На обоих этапах все пересылаемые данные шифруются (во избежание утечки) и подписываются (во избежание подделки), причём возможно разными алгоритмами.



1. Выберем нумерацию

| **Сеть** | **Екатеринбург** | **Провайдер в Екатеринбурге** | **«Интернет»** | **Провайдер в Новосибирске** | **Новосибирск** |
| --- | --- | --- | --- | --- | --- |
| IP | 192.168.108.0 | 1.2.108.0 | 5.5.108.0 | 9.8.108.0 | 10.0.108.0 |
| Маска | 255.255.255.0 | 255.255.255.252 | 255.0.0.0 | 255.255.255.252 | 255.255.255.0 |
| /Маска | /24 | /30 | /8 | /30 | /24 |
| Шлюз | 192.168.108.1 | 1.2.108.2 | - | 9.8.108.2 | 10.0.108.1 |
| Сервер | 192.168.108.50 |  |  |  | 10.0.108.50 |
| Routers | 192.168.108.1 | 1.2.108.1 |  |  |  |
|  | 1.2.108.2 | 5.5.108.1 |  |  |
|  |  | 5.5.108.2 | 9.8.108.2 |  |
|  |  |  | 9.8.108.1 | 10.0.108.1 |

1. Нарисуем схему сети
2. Расставим оборудование
   * Клиентские рабочие станции
   * Коммутаторы в локальных сетях клиентов (Cisco 2960)
   * Маршрутизаторы клиента (Cisco 4321)
   * Маршрутизаторы провайдеров (Cisco 1941)
   * Коммутатор Интернет (Cisco 2960)
3. Соединим оборудование
   * Сетевое оборудование – Gigabit Ethernet
   * Конечные узлы – Fast Ethernet
4. Настроим маршрутизаторы провайдеров
   * Включим порты
   * Настроим IP-адреса
   * Включим протокол маршрутизации OSPF (вместо BGP)
     + interface range GigabitEthernet0/0-1
     + ip ospf 1 area 2
5. Настроим клиентские маршрутизаторы
   * Включим порты
   * Настроим IP-адреса
   * Зададим шлюз по умолчанию в сторону провайдера
   * Настроим службу DHCP
     + Раздайте шлюз по умолчанию
     + В качестве DNS-сервера укажите один из клиентских серверов
6. Настройка серверов
   * Настройте статические IP
   * Настройте DNS-сервер на одном из серверов
   * Настройте веб-серверы на обоих серверах
7. Получим IP-адреса на всех рабочих станциях
8. Настройка IPsec на (обоих!) клиентских маршрутизаторах
   * Установка канала (фаза I)
     + crypto isakmp policy 1
     + encr aes
     + hash sha
     + authentication pre-share
     + group 2
     + lifetime 300
     + Зададим пароль:
       - crypto isakmp key preved! address 3.5.108.2
   * Шифрование трафика (фаза II)
     + crypto ipsec transform-set EKB-NSK esp-aes 256 esp-sha-hmac
   * Выделим трафик, подлежащий туннелированию
     + ip access-list extended EKB2NSK
     + permit ip 192.168.108.0 0.0.0.255 192.168.108.0 0.0.0.255
   * Создадим карту
     + crypto map EKB-NSK 10 ipsec-isakmp
     + set peer 3.5.108.2
     + set transform-set EKB-NSK
     + match address EKB2NSK
   * Привяжем её к внешнему интерфейсу
     + interface GigabitEthernet0/0/1
     + crypto map EKB-NSK
9. Установим VPN-подключение
   * С одной из рабочих станций пошлём ping в другую локальную сеть
   * Визуально рассмотрим, как модифицируются пакеты
   * Show crypto ipsec sa
   * Проверьте доступность веб-серверов

Приложение

## Примерная конфигурация маршрутизаторов

hostname **ro-15-ekb**

ip dhcp excluded-address 192.168.108.0 192.168.108.100

ip dhcp pool EKB

network 192.168.108.0 255.255.255.0

default-router 192.168.108.1

dns-server 10.0.108.50

crypto isakmp policy 1

encr aes

hash sha

authentication pre-share

group 2

lifetime 300

crypto isakmp key preved! address 9.8.108.1

crypto ipsec transform-set EKB-NSK esp-aes 256 esp-sha-hmac

crypto map EKB-NSK 10 ipsec-isakmp

set peer 9.8.108.1

set transform-set EKB-NSK

match address EKB2NSK

interface GigabitEthernet0/0/0

no shutdown

ip address 192.168.108.1 255.255.255.0

interface GigabitEthernet0/0/1

no shutdown

ip address 1.2.108.1 255.255.255.252

crypto map EKB-NSK

ip route 0.0.0.0 0.0.0.0 1.2.108.2

ip access-list extended EKB2NSK

permit ip 192.168.108.0 0.0.0.255 10.0.108.0 0.0.0.255

hostname **ro-15-nsk**

ip dhcp excluded-address 10.0.108.0 10.0.108.99

ip dhcp pool NSK

network 10.0.108.0 255.255.255.0

default-router 10.0.108.1

dns-server 10.0.108.50

crypto isakmp policy 1

encr aes

hash sha

authentication pre-share

group 2

lifetime 300

crypto isakmp key preved! address 1.2.108.1

crypto ipsec transform-set NSK-EKB esp-aes 256 esp-sha-hmac

crypto map NSK-EKB 10 ipsec-isakmp

set peer 1.2.108.1

set transform-set NSK-EKB

match address NSK2EKB

interface GigabitEthernet0/0/0

no shutdown

ip address 10.0.108.1 255.255.255.0

interface GigabitEthernet0/0/1

no shutdown

ip address 9.8.108.1 255.255.255.252

crypto map NSK-EKB

ip route 0.0.0.0 0.0.0.0 9.8.108.2

ip access-list extended NSK2EKB

permit ip 10.0.108.0 0.0.0.255 192.168.108.0 0.0.0.255

hostname **ro-15-dom.ru**

interface GigabitEthernet0/0

no shutdown

ip address 5.5.108.1 255.0.0.0

ip ospf 1 area 2

interface GigabitEthernet0/1

no shutdown

ip address 1.2.108.2 255.255.255.252

ip ospf 1 area 2

hostname **ro-15-rt.ru**

interface GigabitEthernet0/0

no shutdown

ip address 5.5.108.2 255.0.0.0

ip ospf 1 area 2

interface GigabitEthernet0/1

no shutdown

ip address 9.8.108.2 255.255.255.252

ip ospf 1 area 2