## **Задание. Создание дополнительного офиса и настройка ISAKMP-туннеля для согласования параметров протокола.**

### **Описание задания**

Руководство решило открыть новый филиал в соседней области. Перед вами стоит задача между главным офисом и филиалом создать VPN-туннель. Новый филиал подключен к тому же интернет-провайдеру. Но имеет другие “белые” ip-адреса для подключения: 87.250.0.0/30

### **Требование к результату**

* Вы должны отправить файл .pkt с выполненным заданием
* К выполненной задаче добавьте скриншоты с доступностью “внешней сети” и ответы на вопросы.

### **Процесс выполнения**

1. Запустите программу Cisco Packet Tracer
2. В программе Cisco Packet Tracer загрузите [файл с сетью](https://github.com/netology-code/snet-homeworks/blob/snet-22/VPN%20(8.2.0).pkt)
3. Настройте связность сети нового филиала, состоящую из 3 ПК, 1 коммутатора и 1 маршрутизатора. Адресацию внутри сети филиала можно использовать любую.
4. Создайте сетевую связность между маршрутизатором филиала и маршрутизатором интернет-провайдера, согласно условиям.
5. На маршрутизаторе филиала и главного офиса создайте NAT-трансляции с помощью access-листов для внутренней сети.
6. На маршрутизаторе главного офиса настройте политики ISAKMP:

*R1(config)# crypto isakmp policy 1*

*R1(config-isakmp)# encr 3des - метод шифрования*

*R1(config-isakmp)# hash md5 - алгоритм хеширования*

*R1(config-isakmp)# authentication pre-share - использование предварительного общего ключа (PSK) в качестве метода проверки подлинности*

*R1(config-isakmp)# group 2 - группа Диффи-Хеллмана, которая будет использоваться*

*R1(config-isakmp)# lifetime 86400 - время жизни ключа сеанса*

И укажите Pre-Shared ключ для аутентификации с маршрутизатором филиала.Проверьте доступность с любого конечного устройства доступность роутера интернет-провайдера, командой ping.

1. Создайте набор преобразования (Transform Set), используемого для защиты наших данных.

*crypto ipsec transform-set <название> esp-3des esp-md5-hmac*

1. Создайте крипто-карту с указанием внешнего ip-адреса интерфейса и привяжите его к интерфейсу.

*R1(config)# crypto map <название> 10 ipsec-isakmp*

*R1(config-crypto-map)# set peer*

*R1(config-crypto-map)# set transform-set <название>*

*R1(config-crypto-map)# match address <название access-листа>*

*R1(config- if)# crypto map <название крипто-карты>*

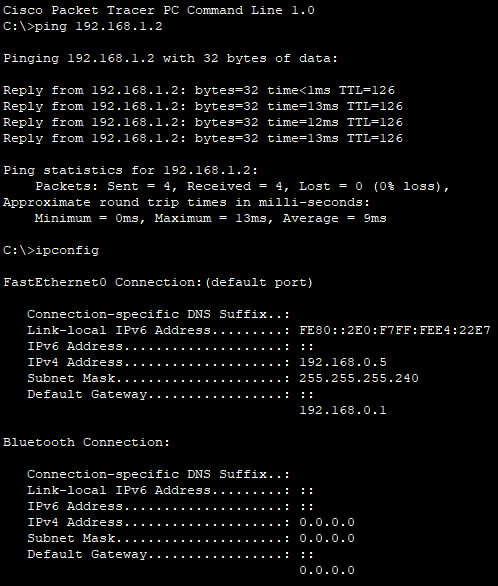
1. Проделайте вышеуказанные операции на маршрутизаторе филиала в соответствии ip-адресов и access-листов и отключите NAT-трансляцию сетевых адресов.
2. Проверьте сетевую доступность между роутерами командой ping.
3. Проверьте, что установившееся VPN-соединения на каждом маршрутизаторе активны. Для этого:

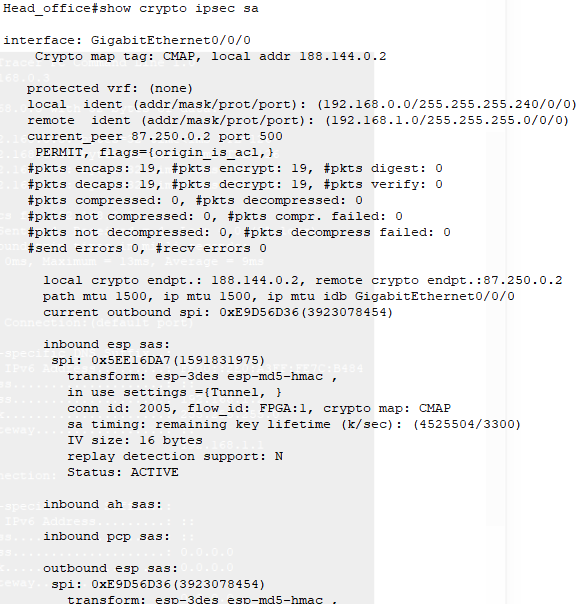
* проверьте, что установлены SA первой фазы командой: "show crypto isakmp sa". Статус должен быть ACTIVE.
* проверьте, что установлены SA второй фазы командой: "show crypto ipsec sa". При взаимодействии устройств между офисами можно сделать косвенный вывод, что оно работает по изменению счетчика пакетов в выводе второй команды (pkts encaps\pkts decaps).

1. Ответ внесите в комментарии к решению задания в личном кабинете Нетологии.

### **Решение**

Сеть офиса:





Сеть филиала:  
