## **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 установившееся VPN-соединение на каждом роутере командой: “show crypto session”. Статус должен быть UP-ACTIVE. Сделайте скриншот.
4. Ответ внесите в комментарии к решению задания в личном кабинете Нетологии

—--------------------------------------------

**Ответы и решение:**

1. Сначала настроил сетевую связанность и NAT-ы как в прошлом задании. Все было ок, например шли пинги и было:

Head\_office#sh ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 188.144.0.2:16 192.168.0.2:16 87.250.0.1:16 87.250.0.1:16

icmp 188.144.0.2:17 192.168.0.2:17 87.250.0.1:17 87.250.0.1:17

icmp 188.144.0.2:18 192.168.0.2:18 87.250.0.1:18 87.250.0.1:18

icmp 188.144.0.2:19 192.168.0.2:19 87.250.0.1:19 87.250.0.1:19

* т.е. NAT работал и с IP все ок.

1. Далее настроил VPN:

В главном офисе:

| Head\_office#en  Head\_office#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Head\_office(config)#crypto isakmp policy 1  Head\_office(config-isakmp)#encr 3des  Head\_office(config-isakmp)#hash md5  Head\_office(config-isakmp)#authentication pre-share  Head\_office(config-isakmp)#group 2  Head\_office(config-isakmp)#lifetime 86400  Head\_office(config-isakmp)#crypto isakmp key mykey address 87.250.0.2  Head\_office(config)#ip access-list extended VPN-TRAFFIC  Head\_office(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.15 192.168.1.0 0.0.0.255  Head\_office(config-ext-nacl)#exit  Head\_office(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac  Head\_office(config)#crypto map CMAP 10 ipsec-isakmp  Head\_office(config-crypto-map)#set peer 87.250.0.2  Head\_office(config-crypto-map)#set transform-set TS  Head\_office(config-crypto-map)#match address VPN-TRAFFIC  Head\_office(config-crypto-map)#int GigabitEthernet0/0/0  Head\_office(config-if)#crypto map CMAP  \*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON  Head\_office(config-if)# |
| --- |

Аналогично на другом офисе на роутере:

| Router>en  Router#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#crypto isakmp policy 1  Router(config-isakmp)#encr 3des  Router(config-isakmp)#hash md5  Router(config-isakmp)#authentication pre-share  Router(config-isakmp)#group 2  Router(config-isakmp)#lifetime 86400  Router(config-isakmp)#crypto isakmp key mykey address 188.144.0.2  Router(config)#ip access-list extended VPN-TRAFFIC  Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.15  Router(config-ext-nacl)#exit  Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac  Router(config)#crypto map CMAP 10 ipsec-isakmp  % NOTE: This new crypto map will remain disabled until a peer  and a valid access list have been configured.  Router(config-crypto-map)#set peer 188.144.0.2  Router(config-crypto-map)#set transform-set TS  Router(config-crypto-map)#match address VPN-TRAFFIC  Router(config-crypto-map)#interface GigabitEthernet0/0/0  Router(config-if)#crypto map CMAP  \*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON  Router(config-if)# |
| --- |

Далее отключил NAT на главном:

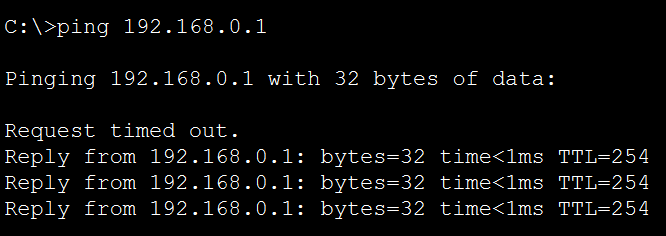
| Head\_office>en  Head\_office#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Head\_office(config)#interface GigabitEthernet0/0/0  Head\_office(config-if)#no ip nat outside  Head\_office(config-if)#interface GigabitEthernet0/0/1  Head\_office(config-if)#no ip nat inside  Head\_office(config-if)#no ip nat inside source list MYLISTNAT interface GigabitEthernet0/0/0 overload  Head\_office(config-if)#no ip access-list standard MYLISTNAT  Head\_office(config)# |
| --- |

Аналогично отключил на другом:

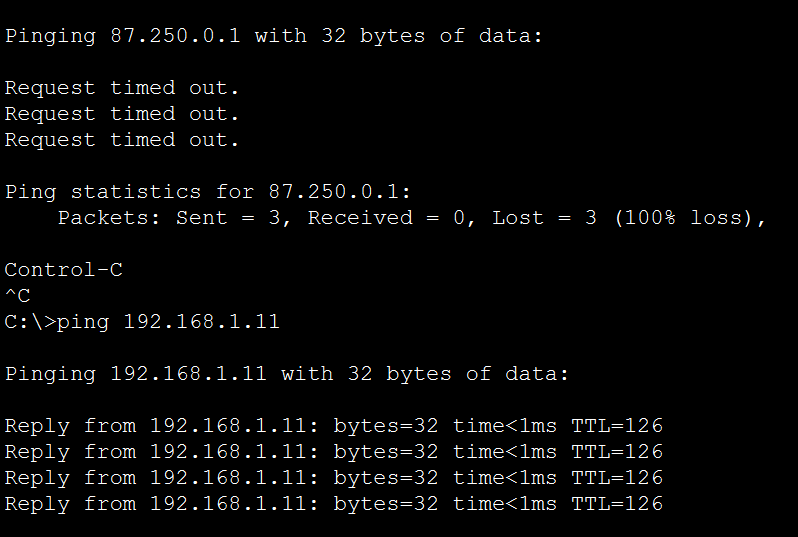
| Router#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#interface GigabitEthernet0/0/0  Router(config-if)#no ip nat outside  Router(config-if)#interface GigabitEthernet0/0/1  Router(config-if)#no ip nat inside  Router(config-if)#no ip nat inside source list MYLISTNAT interface GigabitEthernet0/0/0 overload  Router(config-if)#no ip access-list standard MYLISTNAT |
| --- |

Еще отключили переадресацию по локальным IP на роутере ISP (ранее настраивал для проверки связи).

Проверил пинги из филиала в главный офис:



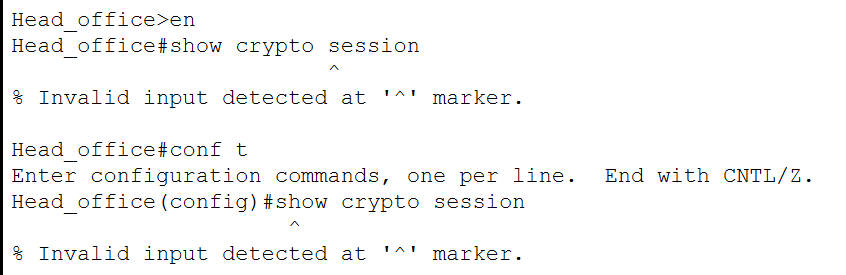
из главного офиса:



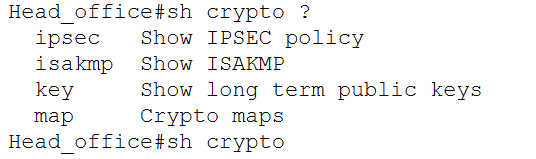
Но, не получилось посмотреть статус VPN:

1. Проверьте установившееся VPN-соединение на каждом роутере командой: “show crypto session”. Статус должен быть UP-ACTIVE. Сделайте скриншот.

Выдает что нет такой команды:



Посмотрел по справке:



команды session нет в списке.

Как посмотреть?

и я так понял что по хорошему еще нужно так настроить NAT, чтобы при доступе в интернет был бы NAT а при доступе в другую сеть не было бы NAT.

Если я правильно понял, то, это нужно сделать не через Standard список, а через Extended , т.к. в нем можно прописать гибкие условия, так?

И еще вопрос, можете ли объяснить суть этой команды:

ip nat inside source list MYLISTNAT int GigabitEthernet0/0/0 overload

Я догадываюсь, что это что это настраивает использование списка доступа для NAT для интерфейса. Но, не понял что значит слова inside и overload?

inside - это видимо от куда идут запросы для которых применять список, вроде бы так.

А что значит overload?

И как настроить NAT что бы интернет все шло а в другой офис не шло через NAT?

Я смотрел пример в Интернете, но, он у меня не заработал:

R1(config)# ip nat inside source list 100 interface fastethernet0/1 overload

R1(config)# access-list 100 deny ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255

R1(config)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any

Спасибо.