Курс: Компьютерные сети
Урок 8. Шифрование туннеля.
Выполнил: Кузнецов Сергей (Факультет Geek University Python-разработки)

Домашнее задание:

1. Настроить туннель между R0 и R2 роутерами
2. Настроить шифрование туннеля
3. Проверить

---

1. Настройка туннеля

Первичная настройка роутеров и хостов:

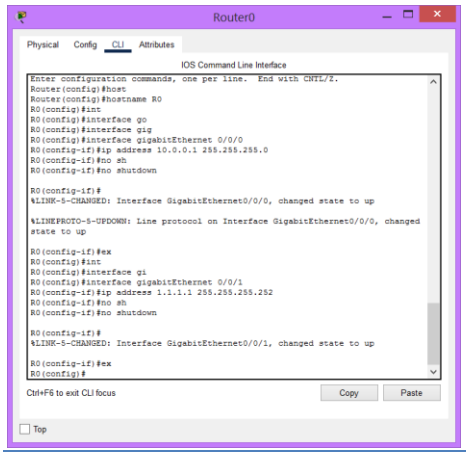
Настройка «R0»:

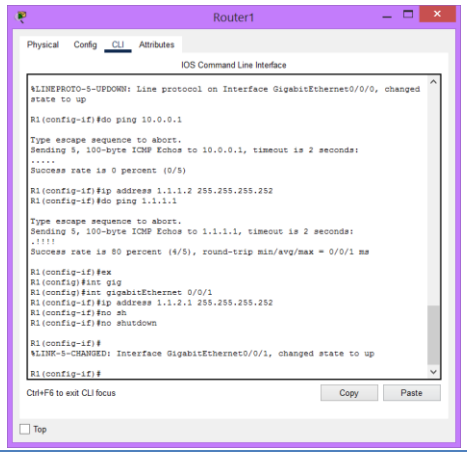
Router>	Enable	Переход в привилегированный режим
Router#	configure terminal	Переход в режим конфигурирования терминала
Router(config)#	hostname R0	Назовем Роутер
R0(config)#	interface gigabitEthernet 0/0/0	Создаем саб-интерфейс «10»
R0(config-subif)#	ip address 10.0.0.1 255.255.255.0	Установим IP адрес
R0(config-subif)#	no shutdown	Поднимаем порт
R0(config-subif)#	exit	Выйти на уровень ниже
R0(config)#	interface gigabitEthernet 0/0/1	Создаем саб-интерфейс «20»
R0(config-subif)#	ip address 1.1.1.1 255.255.255.252	Установим IP адрес
R0(config-subif)#	no shutdown	Поднимаем порт

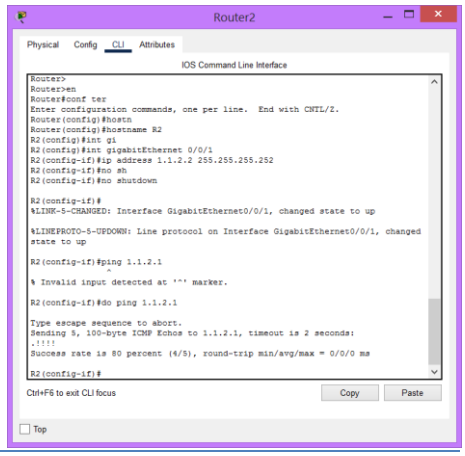
Аналогично, настраиваем физические порты роутеров «R1» и «R2»:

Не забываем проверять пингованием «do ping…»...

Роутер	Порт	Адрес	маска
R0	Gig 0/0/0	10.0.0.1	255.255.255.0
R0	Gig 0/0/1	1.1.1.1	255.255.255.252
R1	Gig 0/0/0	1.1.1.2	255.255.255.252
R1	Gig 0/0/1	1.1.2.1	255.255.255.252
R2	Gig 0/0/1	1.1.2.2	255.255.255.252
R2	Gig 0/0/0	192.168.0.1	255.255.255.0

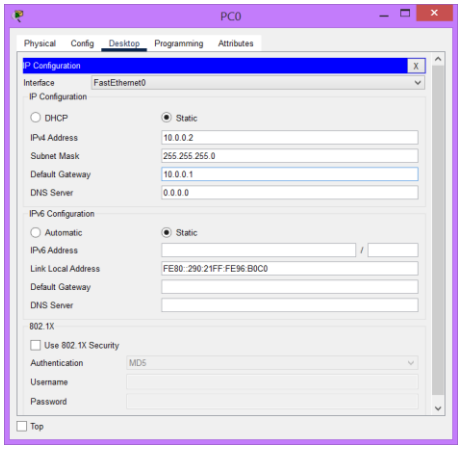


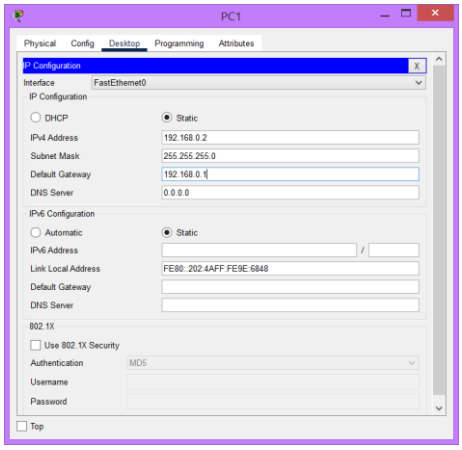


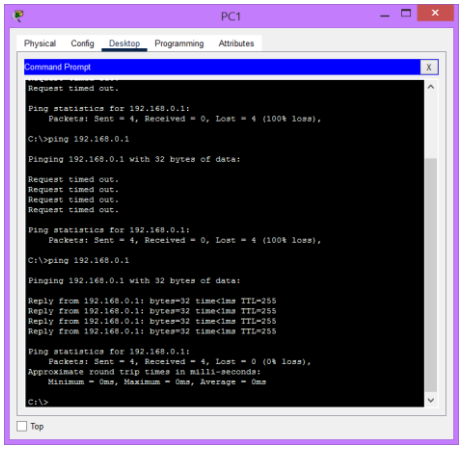


Настраиваем статические адреса на «PC0» и «PC1»:

Проверяем пингами до ближайших роутеров (DefaultGateway) – все Ок.







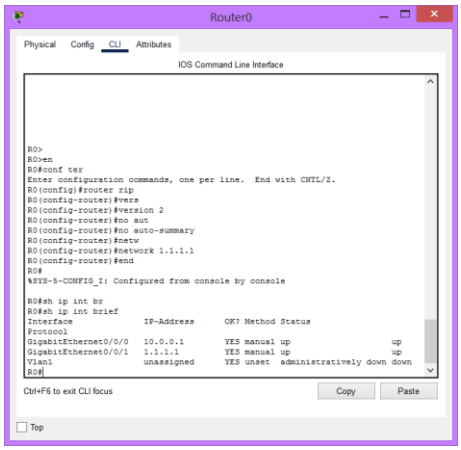
Настроим маршрутизацию по протоколу RIP2

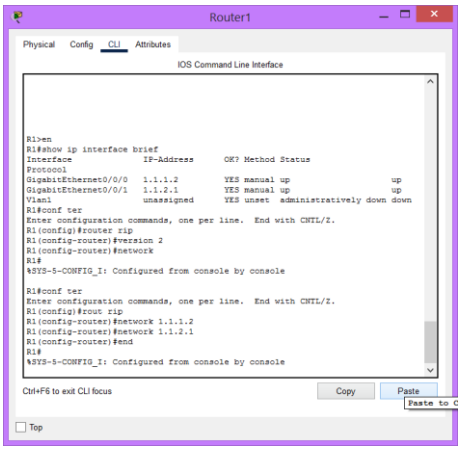
Настроим «R0» через CLI:

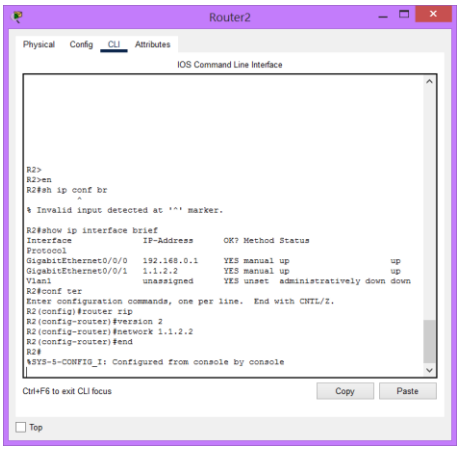
R1#	show ip interface brief	Показывает настроенные порты и IP-адреса (впоследствии их удобно копировать для команды network)
R1#	configure terminal	Переход в режим конфигурирования терминала
R1 (config)#	router rip	Переход в конфигурирование протокола RIP
R1 (config-router)#	version 2	Выбираем вторую версию протокола RIP_2
R1 (config-router)#	no auto-summary	Отключаем суммирование маршрутов
R1 (config-router)#	network 1.1.1.1	Подключаем протокол к сети…
R1 (config-router)#	network 172.16.0.1	Подключаем протокол к сети…
R1 (config-router)#	End	
не будем анонсировать/публиковать локальные сети «10.0.0.0/24»		

Аналогично настроим остальные роутеры:

Роутер	сеть
R0	1.1.1.0/30
R1	1.1.1.0/30 *(RIP2, встречая адрес, начинающийся с «1.» воспринимает сеть класса «А» и заменяет все на «1.0.0.0»)*
R1	1.1.2.0/30 *(не требуется, см выше)*
R2	1.1.2.0/30 *(локальную сеть «192.168.0.0/24» не публикуем)*







Убедимся, что «R0» по динамической маршрутизации видит «R2» - все Ок.

Поднятие туннеля между «R0» и «R2»:

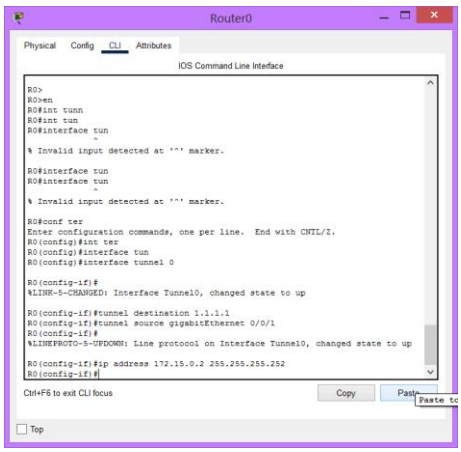
Начнем с «R0»:

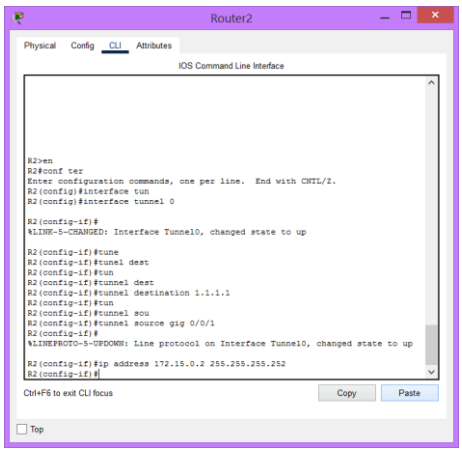
R0#	configure terminal	Переход в режим конфигурирования терминала
R0 (config)#	interface tunnel 0	Заходим в настройки интерфейса «0»
R0 (config-if)#	tunnel source gigabitEthernet 0/0/1	порт начала туннеля
R0 (config-if)#	tunnel destination 1.1.2.2	адрес конца туннеля (порт «R2»)
R0 (config-if)#	ip address 172.15.0.1 255.255.255.252	Назначим туннелю вымышленный IP (не конфликтует с имеющимися сетями) и сеть с двумя адресами (достаточно для подключения «точка-точка»)
R0 (config-if)#	tunnel mode gre ip	Режим туннеля по протоколу «gre» поверх IP
Настроим статические маршруты:		
R0 (config)#	ip route 192.168.0.0 255.255.255.0 172.15.0.2	Укажем, что искать сеть «192.168.0.0/24» по адресу виртуального порта «R2»
R0#	show running-config	Посмотрим итоговые настройки

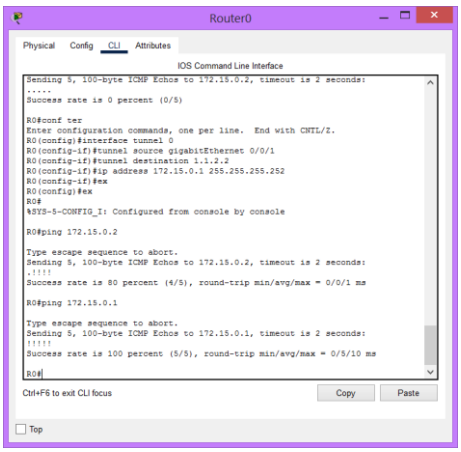
Аналогично с «R2»:

R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	interface tunnel 0	Заходим в настройки интерфейса «0»
R2 (config-if)#	tunnel destination 1.1.1.1	адрес конца туннеля (порт «R0»)
R2 (config-if)#	tunnel source gigabitEthernet 0/0/1	порт начала туннеля
R2 (config-if)#	ip address 172.15.0.2 255.255.255.252	Назначим туннелю вымышленный IP (не конфликтует с имеющимися сетями) и сеть с двумя адресами (достаточно для подключения «точка-точка»)
R2 (config-if)#	tunnel mode gre ip	Режим туннеля по протоколу «gre» поверх IP
Настроим статические маршруты:		
R2 (config)#	ip route 10.0.0.0 255.255.255.0 172.15.0.1	Укажем, что искать сеть с DHCP сервером по адресу виртуального порта «R5»
R2#	show running-config	Посмотрим итоговые настройки

Убедимся, что туннель поднят пингуя адреса «172.15.0.1» и «172.15.0.2»







2. Настройка шифрования туннеля

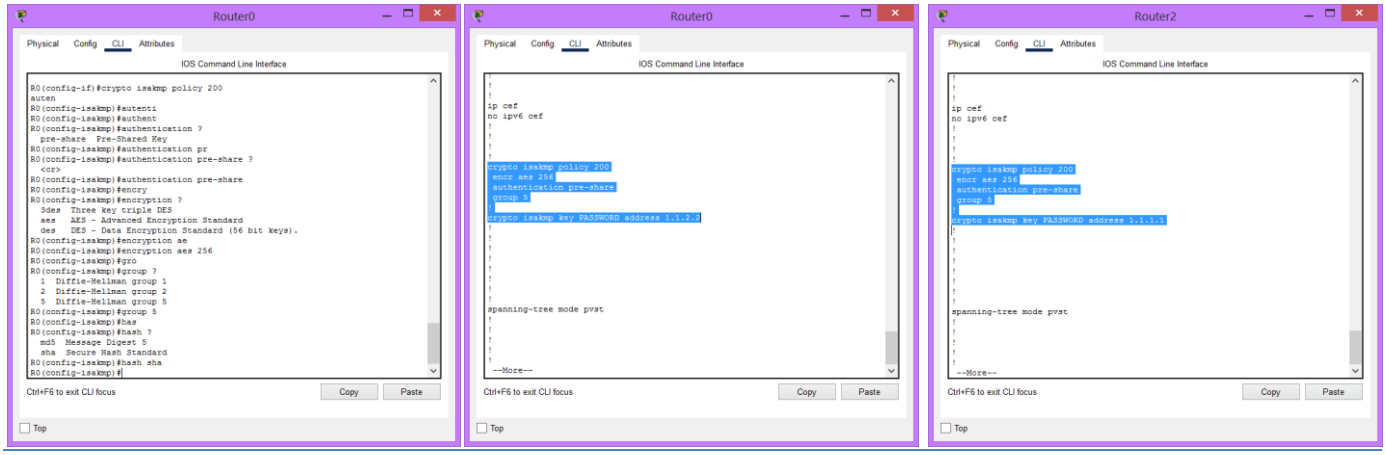
Первый этап/фаза «ISAKMP» (как будут договариваться)

Начнем с «R0»:

R0#	configure terminal	Переход в режим конфигурирования терминала
R0 (config)#	crypto isakmp key PASSWORD address 1.1.2.2	Объявляем, что ждем пакет запроса на шифрование с адреса порта «R2» «1.1.2.2» с паролем «PASSWORD»
R0 (config)#	crypto isakmp policy 200	Объявляем группу «200» для учета конкретных настроек нашего шифрования туннеля (групповая политика)
R0(config-isakmp)#	authentication pre-share	Вариант аутентификации «pre-share», т.к. уже указали пароль (см. выше)
R0(config-isakmp)#	encryption aes 256	Выбираем алгоритм шифрования «aes» (современный) с длиной ключа 256 бит
R0(config-isakmp)#	group 5	Выбираем группу самую криптоустойчивую – «5»
R0(config-isakmp)#	hash sha	Хэширование
R0(config-isakmp)#	ex	
R0#	show running-config	Посмотрим итоговые настройки

Симметрично, на «R2» повторяем все команды:

R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	crypto isakmp key PASSWORD address 1.1.1.1	Объявляем, что ждем пакет запроса на шифрование с адреса порта «R0» «1.1.1.1» с паролем «PASSWORD»
R2 (config)#	…	



Второй этап/фаза «IPSEC» (как будут «работать»)

«IPSEC»:

Начнем с «R0»:

R0#	configure terminal	Переход в режим конфигурирования терминала
R0 (config)#	crypto ipsec transform-set ts_IPSEC esp-aes esp-sha-hmac	Назначаем групповую политику с именем «ts_IPSEC» (сами придумали) с алгоритмом шифрования «esp-aes» и ХЭШированием «esp-sha-hmac»

Симметрично, на «R2» повторяем:

R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	crypto ipsec transform-set ts_IPSEC esp-aes esp-sha-hmac	Назначаем групповую политику с именем «ts_IPSEC» (сами придумали) с алгоритмом шифрования «esp-aes» и ХЭШированием «esp-sha-hmac»

«ACL» (какой трафик будем шифровать):

Начнем с «R0»:

R0#	configure terminal	Переход в режим конфигурирования терминала
R0 (config)#	ip access-list extended acl_IPSEC	создаем расширенный «extended» список доступа «acl_IPSEC»
R0(config-ext-nacl)#	permit gre host 1.1.1.1 host 1.1.2.2	Список разрешения «permit» под протокол «gre» между внешними «host» адресами роутеров «R0» «1.1.1.1» и «R2» «1.1.2.2»

Симметрично, на «R2» повторяем:

R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	ip access-list extended acl_IPSEC	создаем расширенный «extended» список доступа «acl_IPSEC»
R2(config-ext-nacl)#	permit gre host 1.1.2.2 host 1.1.1.1	Список разрешения «permit» под протокол «gre» между внешними «host» адресами роутеров «R0» «1.1.1.1» и «R2» «1.1.2.2»

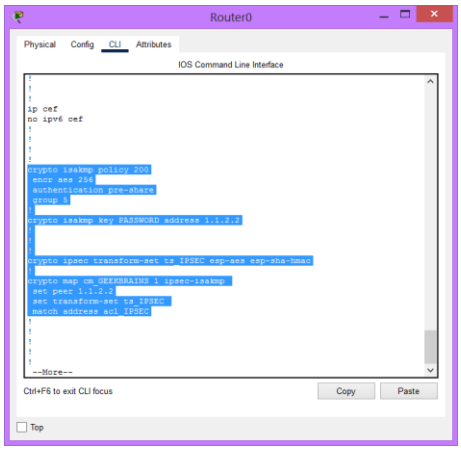
Заключительный этап «CRYPTO MAP»

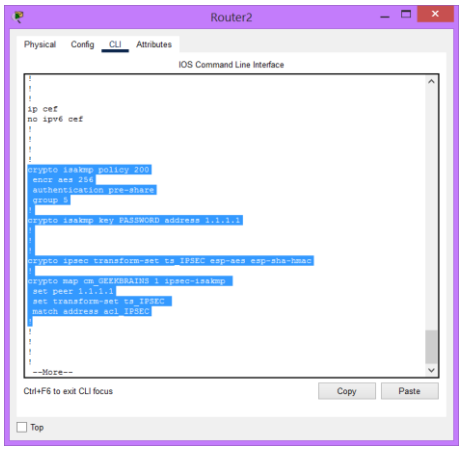
Начнем с «R0»:

R0#	configure terminal	Переход в режим конфигурирования терминала
R0 (config)#	crypto map cm_GEEKBRAINS 1 ipsec-isakmp	Создадим «crypto map» с именем «cm_GEEKBRAINS» под номером «1»
R0(config-crypto-map)#	match address acl_IPSEC	Укажем ранее определенные адреса «acl_IPSEC», трафик с которых будет подвергаться шифрованию
R0(config-crypto-map)#	set peer 1.1.2.2	Укажем, в сторону кого идет шифрованный трафик (порт «R2»)
R0(config-crypto-map)#	set transform-set ts_IPSEC	Укажем, какие правила использовать (заранее создали «ts_IPSEC»)
R0(config-crypto-map)#	do show running-config	Посмотрим итоговые настройки
R0(config-crypto-map)#	ex	
R0 (config)#	int gigabitEthernet 0/0/1	Перейдем в редактирование порта «0/0/1»
R0(config-if)#	crypto map cm_GEEKBRAINS	Привяжем шифрованный трафик к интерфейсу «0/0/1»

Симметрично, на «R2» повторяем:

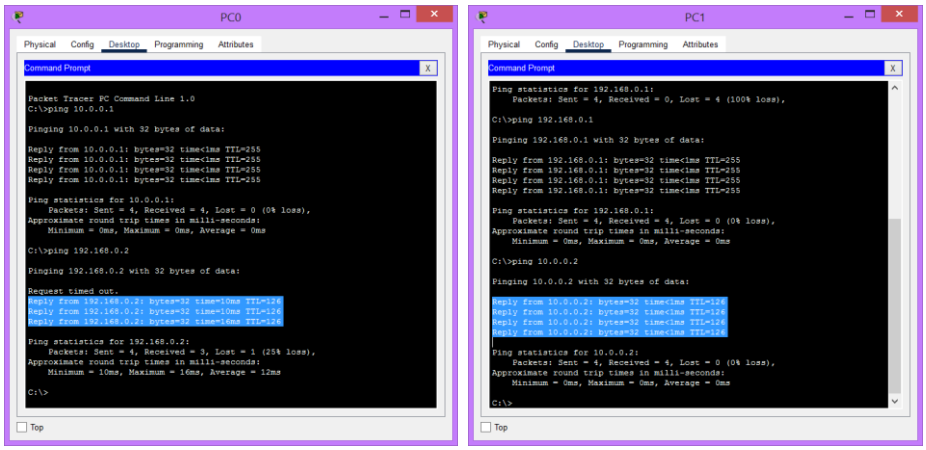
R2#	configure terminal	Переход в режим конфигурирования терминала
R2 (config)#	crypto map cm_GEEKBRAINS 1 ipsec-isakmp	Создадим «crypto map» с именем «cm_GEEKBRAINS» под номером «1»
R2(config-crypto-map)#	match address acl_IPSEC	Укажем ранее определенные адреса «acl_IPSEC», трафик с которых будет подвергаться шифрованию
R2(config-crypto-map)#	set peer 1.1.1.1	Укажем, в сторону кого идет шифрованный трафик (порт «R0»)
R2(config-crypto-map)#	set transform-set ts_IPSEC	Укажем, какие правила использовать (заранее создали «ts_IPSEC»)
R2(config-crypto-map)#	do show running-config	Посмотрим итоговые настройки
R2(config-crypto-map)#	ex	
R2 (config)#	int gigabitEthernet 0/0/1	Перейдем в редактирование порта «0/0/1»
R2(config-if)#	crypto map cm_GEEKBRAINS	Привяжем шифрованный трафик к интерфейсу «0/0/1»





3. Финальная проверка

Пропингуем «PC0» и «PC1» между собой – все Ок



Убедимся, что шифрование производится, введя на «R0» команду «show crypto ipsec sa», запомним количество зашифрованных/расшифрованных пакетов «7/7». Снова пропингуемся и запустим команду вновь. Количество пакетов изменилось «15/15» - мы достигли цели.