Packet Tracer. Настройка GRE поверх IPsec (дополнительно)

Топология

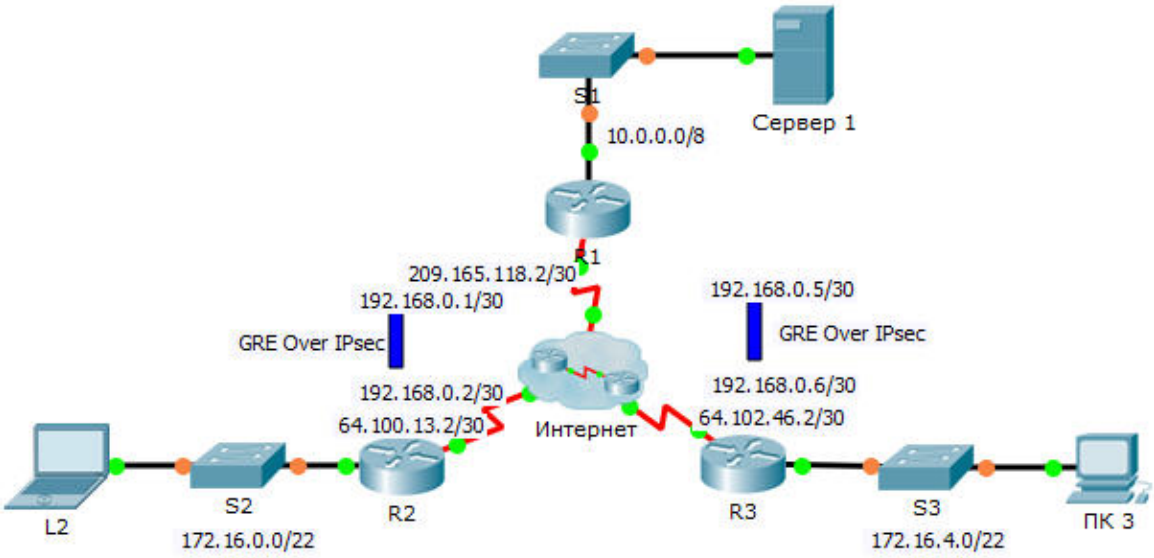

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	10.0.0.1	255.0.0.0	Недоступно
	S0/0/0	209.165.118.2	255.255.255.252	Недоступно
	Tunnel 0	192.168.0.1	255.255.255.252	Недоступно
	Tunnel 1	192.168.0.5	255.255.255.252	Недоступно
R2	G0/0	172.16.0.1	255.255.252.0	Недоступно
	S0/0/0	64.100.13.2	255.255.255.252	Недоступно
	Tunnel 0	192.168.0.2	255.255.255.252	Недоступно
R3	G0/0	172.16.4.1	255.255.252.0	Недоступно
	S0/0/0	64.102.46.2	255.255.255.252	Недоступно
	Tunnel 0	192.168.0.6	255.255.255.252	Недоступно
Сервер 1	NIC	10.0.0.2	255.0.0.0	10.0.0.1
L2	NIC	172.16.0.2	255.255.252.0	172.16.0.1
PC3	NIC	172.16.4.2	255.255.252.0	172.16.4.1

Задачи

Часть 1. Проверка связи между маршрутизаторами

Часть 2. Включение функций безопасности

Часть 3. Настройка параметров IPsec

Часть 4. Настройка туннелей GRE поверх IPsec

Часть 5. Проверка связи

Сценарий

Вы — администратор сети компании, которой нужно настроить туннель GRE поверх IPsec к сетям удалённых офисов. Все сети уже настроены локально, вам необходимо настроить только туннель и шифрование.

Часть 1: Проверка связи между маршрутизаторами

Шаг 1: Отправьте эхо-запрос с маршрутизатора R1 на маршрутизаторы R2 и R3.

a. С маршрутизатора **R1** отправьте эхо-запрос на IP-адрес интерфейса S0/0/0 маршрутизатора **R2**.

b. С маршрутизатора **R1** отправьте эхо-запрос на IP-адрес интерфейса S0/0/0 маршрутизатора **R3**.

Шаг 2: Отправьте эхо-запрос на сервер Сервер 1 от L2 и ПК 3.

Попытайтесь отправить с **L2** эхо-запрос на IP-адрес **Сервера 1**. Мы повторим этот тест после настройки туннеля GRE поверх IPsec. Каковы результаты эхо-запроса? Почему?

Шаг 3: Отправьте эхо-запрос с L2 на ПК 3.

Попытайтесь отправить с **L2** эхо-запрос на IP-адрес компьютера **ПК 3**. Мы повторим этот тест после настройки туннеля GRE поверх IPsec. Каковы результаты эхо-запроса? Почему?

Часть 2: Включение функций безопасности

Шаг 1: Активируйте модуль securityk9.

Для выполнения этого задания должна быть включена лицензия пакета технологий обеспечения безопасности (Security).

a. Введите команду **show version** в пользовательском или привилегированном режиме, чтобы убедиться, что лицензия пакета технологий безопасности активирована.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None
```

```
Configuration register is 0x2102
```

b. Если это не так, активируйте модуль **securityk9** для следующей загрузки маршрутизатора, примите лицензию, сохраните настройку и перезагрузите маршрутизатор.

```
R1(config)# license boot module c2900 technology-package securityk9
<Accept the License>
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. После перезагрузки снова выполните команду **show version** для проверки активации лицензии пакета технологий безопасности.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Повторите шаги 1a-1c для маршрутизаторов **R2** и **R3**.

Часть 3: Настройка параметров IPsec

Шаг 1: Определите интересующий трафик на маршрутизаторе R1.

a. Настройте список ACL 102 для определения трафика из локальной сети маршрутизатора **R1** до локальной сети маршрутизатора **R2** как интересующего. Данный интересующий трафик будет активировать IPsec VPN при наличии трафика между локальными сетями маршрутизаторов **R1** и **R2**. Весь остальной трафик, передаваемый из этих локальных сетей, шифроваться не будет. Помните о действии неявного запрета «deny any» и о том, что добавление данного правила в список не требуется.

```
R1(config)# access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0
0.0.3.255
```

b. Повторите шаг 1a, чтобы настроить ACL-список 103 для определения трафика в локальной сети маршрутизатора R3 как интересующего.

Шаг 2: Настройте параметры 1 фазы ISAKMP на маршрутизаторе R1.

a. Настройте на маршрутизаторе **R1** свойства криптографической политики ISAKMP **102**, а также общий ключ шифрования **cisco**. Значения по умолчанию настраивать не нужно, поэтому требуется настроить только шифрование, способ обмена ключами и метод DH.

```
R1(config)# crypto isakmp policy 102
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 64.100.13.2
```

b. Повторите шаг 2a, чтобы настроить политику 103. При необходимости измените параметры адресации IP.

Шаг 3: Настройте параметры 2 фазы ISAKMP на маршрутизаторе R1.

a. Создайте набор преобразований (transform-set) **VPN-SET** для использования **esp-aes** и **esp-sha-hmac**. Затем создайте криптографическое сопоставление (crypto map) **VPN-MAP**, которое связывает вместе все параметры 2 фазы. Используйте порядковый номер **10** и определите его в качестве сопоставления **ipsec-isakmp**.

```
R1(config)# crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R1(config-crypto-map)# set peer 64.100.13.2
R1(config-crypto-map)# set transform-set R1_R2_Set
R1(config-crypto-map)# match address 102
R1(config-crypto-map)# exit
```

b. Повторите шаг 3a для настройки R1_R3_Set и R1_R3_Map. При необходимости измените параметры адресации.

Шаг 4: Настройте криптографическое сопоставление для исходящего интерфейса.

Наконец, привяжите криптографические сопоставления **R1_R2_Map** и **R1_R3_Map** к исходящему интерфейсу Serial 0/0/0. **Примечание**. Данный этап не оценивается.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map R1_R2_Map
R1(config-if)# crypto map R1_R3_Map
```

Шаг 5: Настройка параметров IPsec на маршрутизаторах R2 и R3

Повторите шаги 1-5 на маршрутизаторах **R2** и **R3**. Используйте те же имена списков контроля доступа, наборов и сопоставлений, что и для маршрутизатора **R1**. Обратите внимание, что каждому маршрутизатору требуется только одно зашифрованное подключение к маршрутизатору **R1**. Зашифрованное подключение между маршрутизаторами **R2** и **R3** отсутствует.

Часть 4: Настройка туннелей GRE поверх IPsec

Шаг 1: Настройте интерфейсы туннеля на маршрутизаторе R1.

a. Войдите в режим настройки туннеля 0 на маршрутизаторе **R1**.

```
R1(config)# interface tunnel 0
```

b. Настройте IP-адрес согласно таблице адресации.

```
R1(config-if)# ip address 192.168.0.1 255.255.255.252
```

c. Настройте источник и назначение для конечных точек туннеля 0.

```
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 64.100.13.2
```

d. Настройте туннель 0 для передачи трафика IP по GRE.

```
R1(config-if)# tunnel mode gre ip
```

e. Интерфейс туннеля 0 должен быть уже включен. Если это не так, работайте с ним как с любым другим интерфейсом.

f. Повторите шаги 1a-1f для создания интерфейса Tunnel 1 на маршрутизаторе R3. При необходимости измените параметры адресации.

Шаг 2: Настройка интерфейса туннеля 0 на маршрутизаторах R2 и R3.

a. Повторите шаги 1a-1e для маршрутизатора **R2**. Обязательно измените параметры адресации IP.

b. Повторите шаги 1a-1e для маршрутизатора **R3**. Обязательно измените параметры адресации IP.

Шаг 3: Настройка маршрута для частного трафика IP.

a. Определите маршрут от маршрутизатора **R1** до сетей 172.16.0.0 и 172.16.4.0, используя в качестве адреса следующего перехода адрес интерфейса туннеля.

b. Определите маршрут от маршрутизаторов **R2** и **R3** до сети 10.0.0.0, используя в качестве адреса следующего перехода адрес интерфейса туннеля.

Часть 5: Проверьте связь

Шаг 1: Отправьте эхо-запрос на сервер Сервер 1 от L2 и ПК 3.

a. Попытайтесь отправить от **L2** и **ПК 3** эхо-запрос на IP-адрес **Сервера 1**. Эхо-запрос должен быть успешным.

b. Попытайтесь отправить с компьютера **ПК 3** эхо-запрос на IP-адрес **L2**. Выполнение эхо-запроса должно закончиться неудачей из-за отсутствия туннеля между двумя сетями.