****Практическая работа № 21****

****Тема:** Настройка туннеля VPN GRE по схеме «точка-точка»**

****Цель:** Организовать L3-VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол GRE.**

****Необходимые ресурсы:****

**ESXI**

**Вирутальный маршрутизатор Eltex**

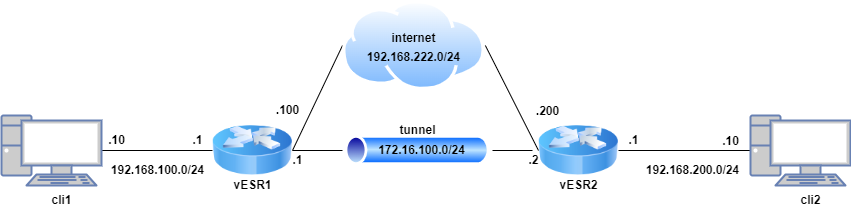
**ОС Альт Линукс Сервер 10**

****Теоретический материал.****

**GRE** (англ. Generic Routing Encapsulation — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты. GRE может использоваться для организации VPN на 3 уровне модели OSI. В маршрутизаторе ESR реализованы статические неуправляемые GRE-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля для каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

**Выполнение работы:**

### Топология:



### Задание 1. Назначаем IP-адреса согласно топологии:

**vESR1**

interface gigabitethernet 1/0/1

description "WAN"

ip address 192.168.222.100/24

exit

ip route 0.0.0.0/0 192.168.222.2

domain name-server 192.168.222.2 # при необходимости

interface gigabitethernet 1/0/2

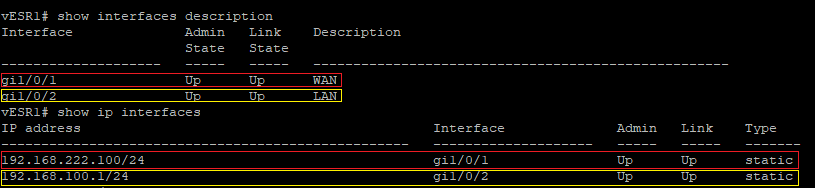
description "LAN"

ip address 192.168.100.1/24

exit

Применяем и проверяем:

do commit



do confirm

**vESR2**

interface gigabitethernet 1/0/1

description "WAN"

ip address 192.168.222.200/24

exit

ip route 0.0.0.0/0 192.168.222.2

domain name-server 192.168.222.2 # при необходимости

interface gigabitethernet 1/0/2

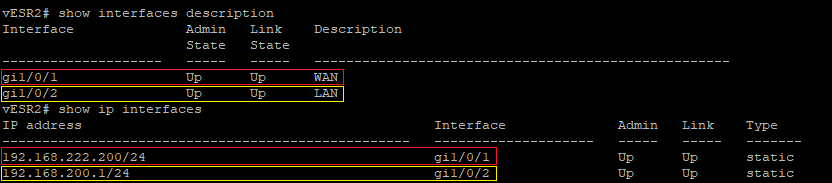
description "LAN"

ip address 192.168.200.1/24

exit

Применяем и проверяем:

do commit



do confirm

### Задание 2. Создаём зоны безопасности и помещаем интерфейсы в соответствующие зоны:

* **trusted** - для внутренней сети (LAN)
* **untrusted** - для внешней сети (WAN)

**vESR1**

security zone trusted

exit

security zone untrusted

exit

interface gigabitethernet 1/0/1

security-zone untrusted

exit

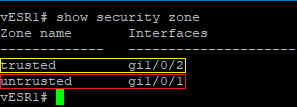
interface gigabitethernet 1/0/2

security-zone trusted

exit

Применяем и проверяем:

do commit



do confirm

**vESR2**

security zone trusted

exit

security zone untrusted

exit

interface gigabitethernet 1/0/1

security-zone untrusted

exit

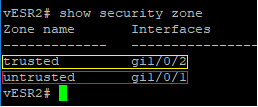
interface gigabitethernet 1/0/2

security-zone trusted

exit

Применяем и проверяем:

do commit



do confirm

### Задание 3. Для удобства и проверки разрешаем ICMP отовсюду:

**vESR1 | vESR2**

* для доступа к маршрутизатору из локальной сети (LAN)

security zone-pair trusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

* для доступа к маршрутизатору из внешней сети сети (WAN)

security zone-pair untrusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

* для проходящего трафика из локальной сети во внешнюю

security zone-pair trusted untrusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

* для прохождения трафика с внешней сети в локальную

security zone-pair untrusted trusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

### Задание 4. Создадим туннель GRE 1

**vESR1**

tunnel gre 1

ttl 64

security-zone untrusted

local address 192.168.222.100

remote address 192.168.222.200

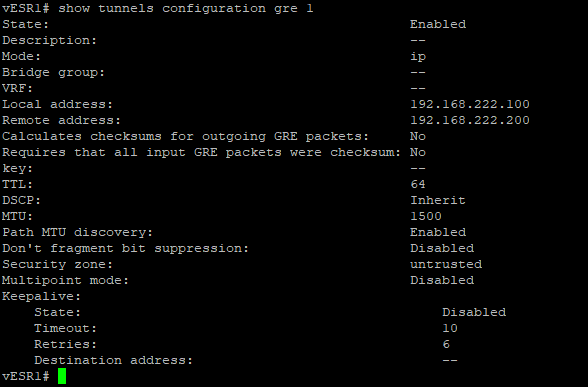
ip address 172.16.100.1/24

enable

exit

Применяем и проверяем:

do commit



do confirm

**vESR2**

tunnel gre 1

ttl 64

security-zone untrusted

local address 192.168.222.200

remote address 192.168.222.100

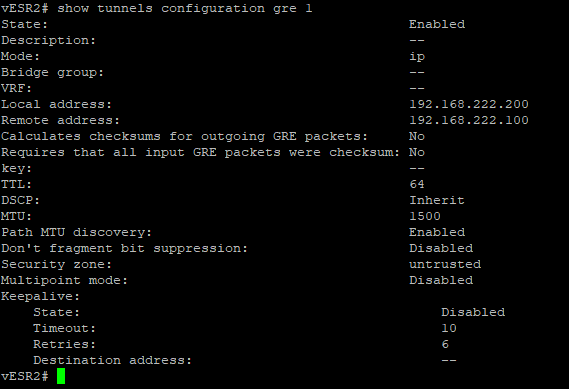
ip address 172.16.100.2/24

enable

exit

Применяем и проверяем:

do commit



do confirm

### Задание 5. Разрешаем получение пакетов GRE:

**vESR1 | vESR2**

security zone-pair untrusted self

rule 2

description "GRE"

action permit

match protocol gre

enable

exit

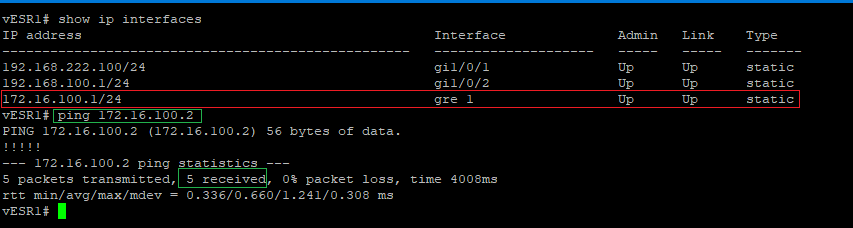
exit

Применяем и проверяем связность по туннелю:

do commit

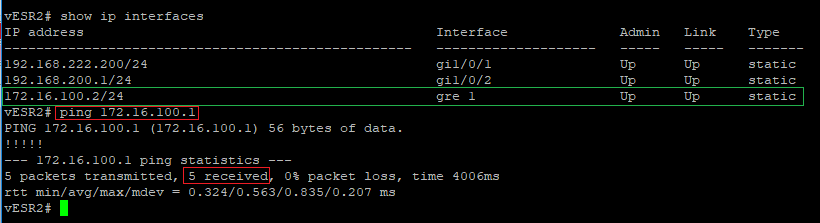
**vESR1**

* **vESR1 -> vESR2**

****

**vESR2**

* **vESR2 -> vESR1**



do confirm

### Задание 6. Настраиваем динамическую маршрутизацию для связи локальных сетей через туннельный интерфейс:

**vESR1 | vESR2**

* Создадим OSPF-процесс с идентификатором 1 и перейдём в режим конфигурирования протокола OSPF
* Создадим и включим требуемую область
* Включим OSPF-процесс

router ospf 1

area 0.0.0.0

enable

exit

enable

exit

* Для установления соседства с другими маршрутизаторами привяжем их к OSPF-процессу и области.
* Далее включим на интерфейсе маршрутизацию по протоколу OSPF:
  + интерфейс gre 1 - для установления соседства
  + интерфейс gi1/0/2 - для обявления локальных сетей

interface gigabitethernet 1/0/2

ip ospf instance 1

ip ospf

exit

tunnel gre 1

ip ospf instance 1

ip ospf

exit

* Разрешаем трафик OSPF:

security zone-pair untrusted self

rule 3

description "OSPF"

action permit

match protocol ospf

enable

exit

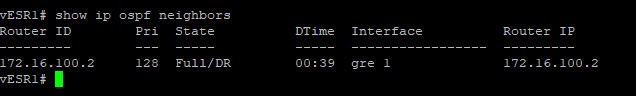
exit

Применяем и проверяем:

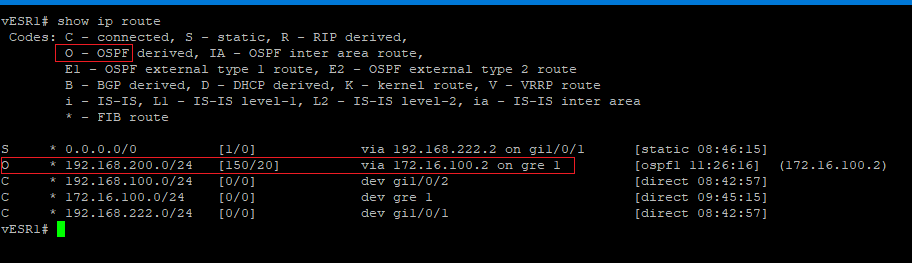
do commit

**vESR1**

* Проверяем установление соседства:



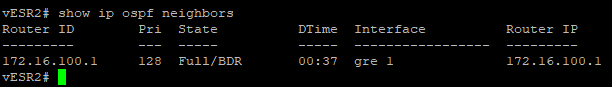
* Проверяем таблицу маршрутизации:



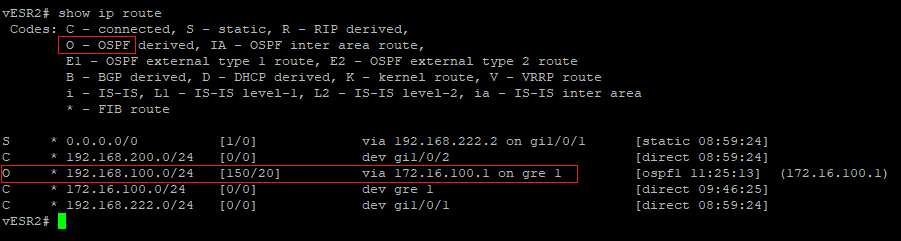
do confirm

**vESR2**

* Проверяем установление соседства:



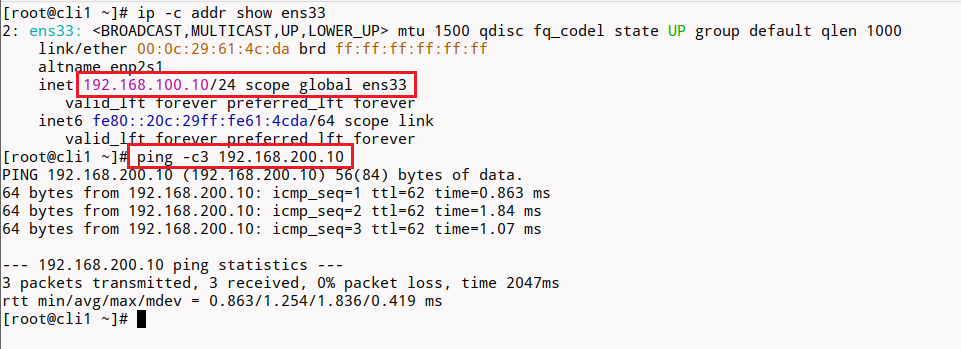
* Проверяем таблицу маршрутизации:



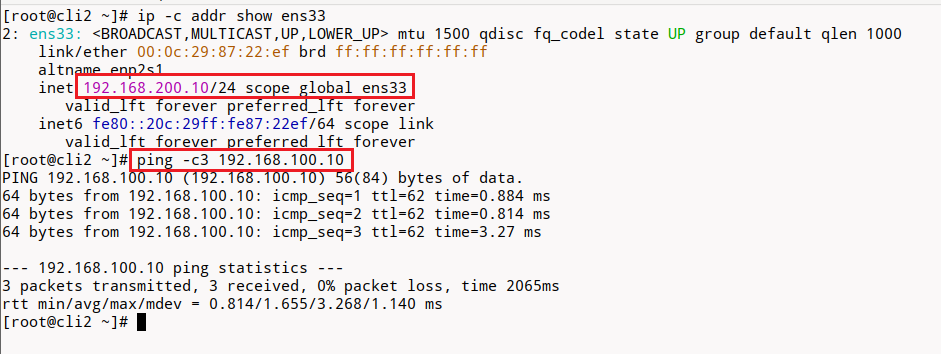
do confirm

### Задание 7. Проверяем связность с клиентов:

* **cli1 -> cli2**:

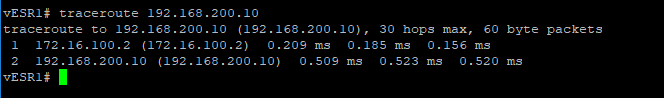


* **cli2 -> cli1**:

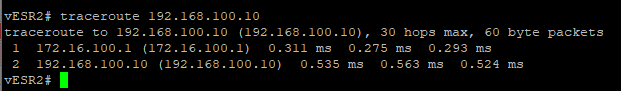


### Задание 8. При добавлении необходимых правил можно разрешить и ****traceroute****:

* **vESR1 -> cli2**:



* **vESR2 -> cli1**:



Конфигурация устройств получилась следующая:

vESR1# show running-config

hostname vESR1

object-group service TRACEROUTE

description "TRACEROUTE"

port-range 33434-33529

port-range 15121

exit

object-group service SSH

description "SSH"

port-range 22

exit

syslog max-files 3

syslog file-size 512

syslog file tmpsys:syslog/default

severity info

exit

username admin

password encrypted $6$83u7ZpzpElZuWbL9$bdFyffbPozW18xVkVCWHROwUZOsxcdEKFy2rRSgj2Z8ep4XsjGcKlu/.0XMOSGDsyU9cxX5Tsoz0bA.iyGTcT/

exit

username sshuser

password encrypted $6$ZeBDVMWrDP8uqj5c$zx6lhKy8NKSVIpwpk3BJAf5Vdm.v9Il4CQ5DrOPtwdXu2qWloNNJEMymAfh0Ca67eb5qB2B0ra/pfhe9CHL0U/

privilege 15

exit

domain lookup enable

domain name-server 192.168.222.2

security zone trusted

exit

security zone untrusted

exit

router ospf 1

area 0.0.0.0

enable

exit

enable

exit

interface gigabitethernet 1/0/1

description "WAN"

security-zone untrusted

ip address 192.168.222.100/24

exit

interface gigabitethernet 1/0/2

description "LAN"

security-zone trusted

ip address 192.168.100.1/24

ip ospf instance 1

ip ospf

exit

tunnel gre 1

ttl 64

security-zone untrusted

local address 192.168.222.100

remote address 192.168.222.200

ip address 172.16.100.1/24

ip ospf instance 1

ip ospf

enable

exit

security zone-pair trusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

security zone-pair untrusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "GRE"

action permit

match protocol gre

enable

exit

rule 3

description "OSPF"

action permit

match protocol ospf

enable

exit

rule 22

description "SSH"

action permit

match protocol tcp

match destination-port SSH

enable

exit

exit

security zone-pair trusted untrusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "TRACEROUTE"

action permit

match protocol udp

match destination-port TRACEROUTE

enable

exit

exit

security zone-pair untrusted trusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "TRACEROUTE"

action permit

match protocol udp

match destination-port TRACEROUTE

enable

exit

exit

security passwords default-expired

ip route 0.0.0.0/0 192.168.222.2

ip ssh server

ntp enable

ntp broadcast-client enable

licence-manager

host address elm.eltex-co.ru

exit

vESR2# show running-config

hostname vESR2

object-group service TRACEROUTE

description "TRACEROUTE"

port-range 33434-33529

port-range 15121

exit

object-group service SSH

description "SSH"

port-range 22

exit

syslog max-files 3

syslog file-size 512

syslog file tmpsys:syslog/default

severity info

exit

username admin

password encrypted $6$DJXxBotgkalhpvdS$M4X3JJZLIYAo.H2NACe4iBNthGcrQ7FpIuxwTSG8PZFmJGw8oqdyrNMoy1b8CM7aKxfmoxC4jyZpXHHKDtWBc0

exit

username sshuser

password encrypted $6$QwpWsLDV.GfE04QE$j1WSJOYdIY806fNiyC5YIthELjRBGmE32L0RQHzrp4l1kf1NHvul9edbOF/pvQXmCWK58etaTiZBhDj5rAHzZ/

privilege 15

exit

domain lookup enable

domain name-server 192.168.222.2

security zone trusted

exit

security zone untrusted

exit

router ospf 1

area 0.0.0.0

enable

exit

enable

exit

interface gigabitethernet 1/0/1

description "WAN"

security-zone untrusted

ip address 192.168.222.200/24

exit

interface gigabitethernet 1/0/2

description "LAN"

security-zone trusted

ip address 192.168.200.1/24

ip ospf instance 1

ip ospf

exit

tunnel gre 1

ttl 64

security-zone untrusted

local address 192.168.222.200

remote address 192.168.222.100

ip address 172.16.100.2/24

ip ospf instance 1

ip ospf

enable

exit

security zone-pair trusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

exit

security zone-pair untrusted self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "GRE"

action permit

match protocol gre

enable

exit

rule 3

description "OSPF"

action permit

match protocol ospf

enable

exit

rule 22

description "SSH"

action permit

match protocol tcp

match destination-port SSH

enable

exit

exit

security zone-pair trusted untrusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "TRACEROUTE"

action permit

match protocol udp

match destination-port TRACEROUTE

enable

exit

exit

security zone-pair untrusted trusted

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "TRACEROUTE"

action permit

match protocol udp

match destination-port TRACEROUTE

enable

exit

exit

security passwords default-expired

ip route 0.0.0.0/0 192.168.222.2

ip ssh server

ntp enable

ntp broadcast-client enable

licence-manager

host address elm.eltex-co.ru

exit

Результат выполнения практической работы оформить в виде отчета.

**Контрольные вопросы:**

Какие еще конфигурации необходимы для создания защищенного GRE-туннеля?

Какой используется протокол туннелирования?

Какие IP-адреса источника и назначения туннеля связаны с GRE tunnel на каждом маршрутизаторе?