Университет ИТМО

Факультет программной инженерии и компьютерной техники

Администрирование вычислительных систем

Лабораторная работа № 4

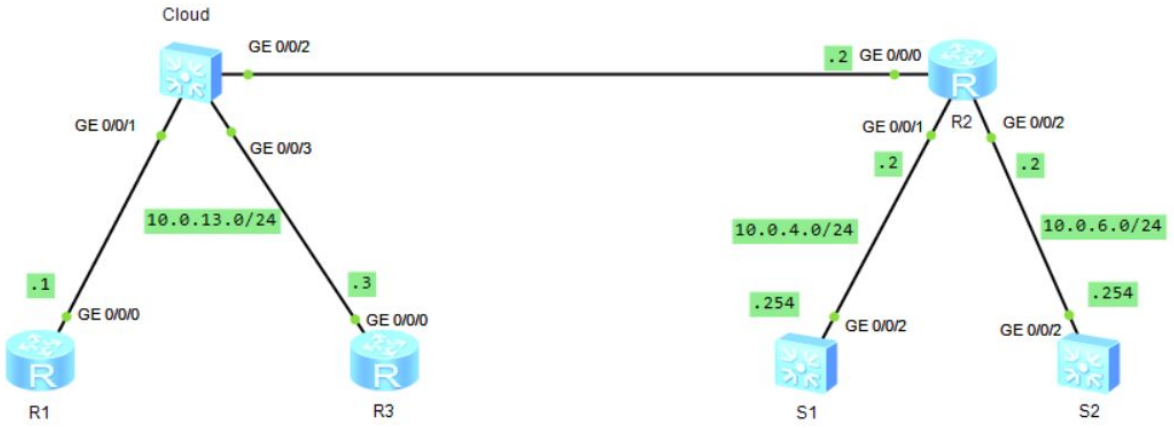
Выполнили:
Дерябин Андрей
Глушков Дима

Группа P3410

Санкт-Петербург, 2020

Оглавление

8.1. Фильтрация корпоративных данных с помощью списков управления доступом



1. Подготовка среды

```
<Huawei>sys
[Huawei]sysname R1

<Huawei>sys
[Huawei]sysname R2

<Huawei>sys
[Huawei]sysname R3

<Huawei>sys
[Huawei]sysname S1
[S1]vlan 4
[S1-vlan4]quit
[S1]int vlanif 4
[S1-Vlanif4]ip addr 10.0.4.254 24

<Huawei>sys
[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]int vlanif 6
[S2-Vlanif6]ip addr 10.0.6.254 24
```

3. Конфигурирование IP-адресации

Конфигурируем адресацию для 10.0.13.0/24

```
[R1]int gi0/0/0
```

```
[R1-GigabitEthernet0/0/0]ip addr 10.0.13.1 24

[R2]int gi0/0/0
[R2-GigabitEthernet0/0/0]ip addr 10.0.13.2 24
[R2-GigabitEthernet0/0/0]int gi0/0/1
[R2-GigabitEthernet0/0/1]ip addr 10.0.4.2 24
[R2-GigabitEthernet0/0/1]int gi0/0/2
[R2-GigabitEthernet0/0/2]ip addr 10.0.6.2 24

[R3]int gi0/0/0
[R3-GigabitEthernet0/0/0]ip addr 10.0.13.3 24
```

Настроим тип соединения порта 0/0/2 на S1. Установим магистрали VLAN на S1 и S2.

```
[S1]int gi0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[S1-GigabitEthernet0/0/2]port trunk pvid vlan 4
[S1-GigabitEthernet0/0/2]quit

[S2]int gi0/0/2
[S2-GigabitEthernet0/0/2]port link-type trunk
[S2-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[S2-GigabitEthernet0/0/2]port trunk pvid vlan 6
[S2-GigabitEthernet0/0/2]quit
```

4. Настройка OSPF для включения межсетевого взаимодействия

Настроим OSPF для R1, R2, R3. Убедимся, что они являются частью одной и той же области OSPF.

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.4.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.6.0 0.0.0.255

[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
```

Настроим статический маршрут на S1, S2. Установим nexthop в качестве шлюза частной сети.

```
[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.2
[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.2
```

Убедимся, что существует маршрут от R1 и R3 до S1 и S2.

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=254 time=80 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=70 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=80 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=70 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=80 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 70/76/80 ms


<R1>ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=254 time=40 ms
    Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=254 time=50 ms

  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/48/70 ms


<R3>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=60 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=50 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/54/70 ms



<R3>ping 10.0.6.254
```

```
PING 10.0.6.254: 56  data bytes, press CTRL_C to break
  Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=254 time=50 ms
  Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=254 time=60 ms
  Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=254 time=60 ms
  Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=254 time=60 ms
  Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=254 time=50 ms

--- 10.0.6.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 50/56/60 ms
```

5. Настройка фильтров с использованием списков управления доступом

Настроим S1 в качестве сервера telnet.

```
[S1]telnet server enable
[S1]user-interface vty 0 4
[S1-ui-vty0-4]protocol inbound all
[S1-ui-vty0-4]authentication-mode password
[S1-ui-vty0-4]set authentication password cipher huawei123
```

Настроим S2 в качестве сервера FTP.

```
[S2]ftp server enable
[S2]aaa
[S2-aaa]local-user huawei password cipher huawei123
Info: Add a new user.
[S2-aaa]local-user huawei privilege level 3
[S2-aaa]local-user huawei service-type ftp
[S2-aaa]local-user huawei ftp-directory flash:/
```

Настроим список управления доступом на R2, чтобы разрешить R1 доступ к telnet-серверу, а R3 - к FTP-серверу.

```
[R2]acl 3000
[R2-acl-adv-3000]rule 5 permit tcp source 10.0.13.1 0.0.0.0 destination 10.0.4.2
54 0.0.0.0 destination-port eq 23
[R2-acl-adv-3000]rule 10 permit tcp source 10.0.13.3 0.0.0.0 destination 10.0.6.
254 0.0.0.0 destination-port range 20 21
[R2-acl-adv-3000]rule 15 permit ospf
[R2-acl-adv-3000]rule 20 deny ip source any
[R2-acl-adv-3000]quit
```

Применим ACL к интерфейсу 0/0/0 на R2.

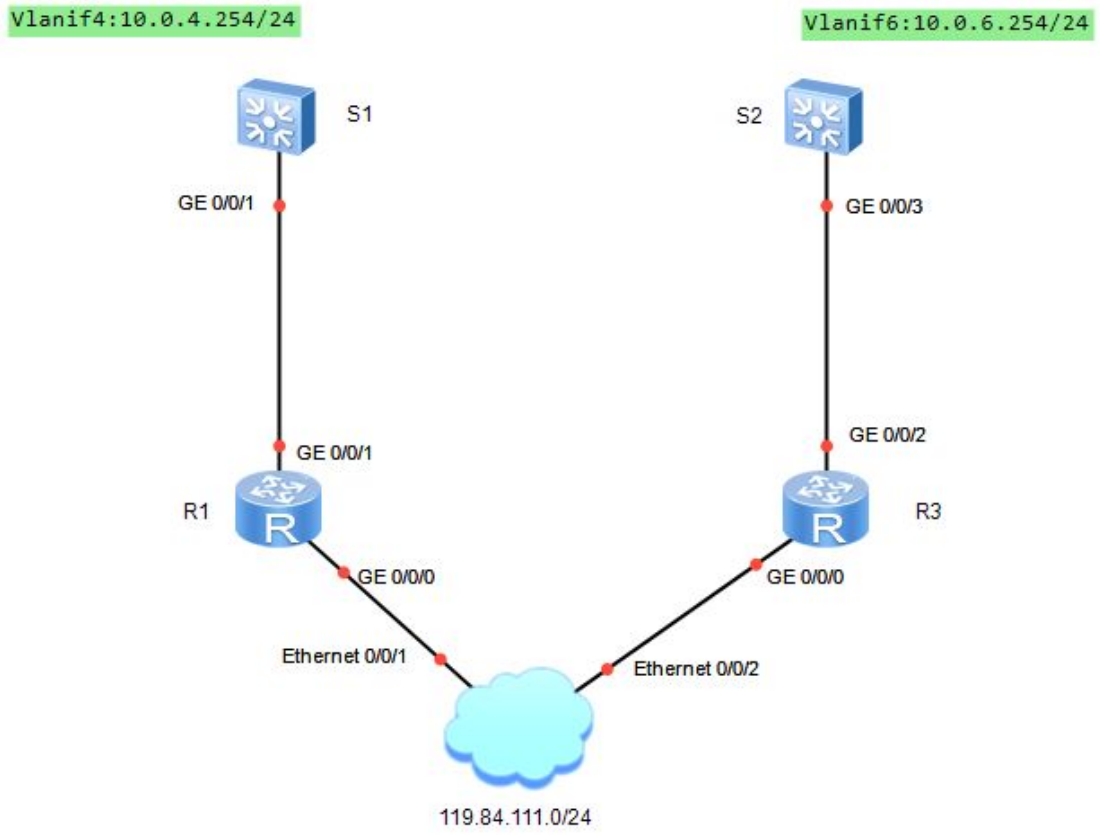
```
[R2]int gi0/0/0
[R2-GigabitEthernet0/0/0]traffic-filter inbound acl 3000
```

Проверим результаты списка управления доступом в сети.

```
<R1>telnet 10.0.4.254
  Press CTRL_] to quit telnet mode
  Trying 10.0.4.254 ...
  Connected to 10.0.4.254 ...
Login authentication
Password:
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
      The current login time is 2020-11-19 20:42:23.
<S1>quit

<R1>ftp 10.0.6.254
Trying 10.0.6.254 ...
Press CTRL+K to abort
Error: Failed to connect to the remote host.

<R3>telnet 10.0.4.254
  Press CTRL_] to quit telnet mode
  Trying 10.0.4.254 ...
  Error: Can't connect to the remote host

<R3>ftp 10.0.6.254
Trying 10.0.6.254 ...

Press CTRL+K to abort
Connected to 10.0.6.254.
220 FTP service ready.
User(10.0.6.254:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[R3-ftp]bye
221 Server closing.
```

8.2 Преобразование сетевых адресов

Реализованная топология



1. Подготовка среды

```
<Huawei>sys
[Huawei]sysname R1
[R1]inter GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24
      [R1]inter GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24

<Huawei>sys
[Huawei]sysname R3
[R3]inter GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24
      [R3]inter GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24

[Huawei]sysname S1
```

```
[S1]vlan 4
[S1-vlan4]quit
[S1]inter vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24
[S1-Vlanif4]quit

[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]inter vlanif6
[S2-Vlanif6]ip address 10.0.6.254 24
[S2-Vlanif6]quit
```

3. Реализация конфигурирования VLAN для S1 и S2

```
[S1]inter GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk pvid vlan 4
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[S1-GigabitEthernet0/0/1]quit

S2]inter GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type trunk
[S2-GigabitEthernet0/0/3]port trunk
[S2-GigabitEthernet0/0/3]port trunk pvid vlan 6
```

Убедимся в доступности R1 к S1 и R3

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=255 time=60 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/32/60 ms

<R1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms
```

```
--- 119.84.111.3 ping statistics ---
  5 packet(s) transmitted
        5 packet(s) received
        0.00% packet loss
        round-trip min/avg/max = 10/24/50 ms
```

4. Настройка списков управления доступом для R1 и R3

На R1 сконфигурируем расширенный ACL и выберем поток данных с источником S1 и назначение R3 для сервисного порта telnet.

```
[R1]acl 3000
[R1-acl-adv-3000]rule 5 permit tcp source 10.0.4.254 0.0.0.0 destination 119.84.111.3
0.0.0.0 destination-port eq 23
[R1-acl-adv-3000]rule 10 permit ip source 10.0.4.0 0.0.0.255 destination any
[R1-acl-adv-3000]rule 15 deny ip
```

На R3 сконфигурируем стандартный ACL и выберем поток адрес источника, которого 10.0.6.0/24

```
[R3]acl 2000
[R3-acl-basic-2000]rule permit source 10.0.6.0 0.0.0.255
```

5. Конфигурирование динамического NAT

Настроим статические маршруты на S1 и S2, установив nexthop – адрес шлюза частной сети.

```
[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.1
[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.3
```

Настроим на интерфейсе 0/0/0 R1 динамический NAT.

```
[R1]nat address-group 1 119.84.111.240 119.84.111.243
[R1]inter GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]nat outbound 3000 address-group 1
```

Убедимся, что группа адресов настроена правильно

```
<R1>displ nat address-group

 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address           End-address
 --------------------------------------
```

```
 1        119.84.111.240   119.84.111.243
 --------------------------------------
Total : 1
```

Настроим R3 в качестве сервера telnet (для возможности просмотра преобразования сеанса NAT)

```
[R3]telnet server enable
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode password
Please configure the login password (maximum length 16):huawei123
[R3-ui-vty0-4]set authentication password cipher huawei123
[R3-ui-vty0-4]quit
```

Проверим подключение S1 (узла внутренней сети) со шлюзом удаленного однорангового узла.

```
 <S1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=254 time=90 ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=254 time=10 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=254 time=50 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=254 time=50 ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
          round-trip min/avg/max = 10/46/90 ms
```

Установим соединение telnet с S1 с адресом удаленного однорангового узла и посмотрим результаты преобразования сеансов ACL и NAT.

```
<S1>telnet 119.84.111.3
Trying 119.84.111.3 ...
Press CTRL+K to abort
Connected to 119.84.111.3 ...

Login authentication
Password:

[R1]display acl 3000
Advanced ACL 3000, 3 rules
Acl's step is 5
 rule 5 permit tcp source 10.0.4.254 0 destination 119.84.111.3 0 destination-po
rt eq telnet
 rule 10 permit ip source 10.0.4.0 0.0.0.255
 rule 15 deny ip
```

```
[R1]firewall-nat session icmp aging-time 300
[R1]displ nat session all
  NAT Session Table Information:

    Protocol               : TCP(6)
    SrcAddr  Port Vpn : 10.0.4.254     4581
    DestAddr Port Vpn : 119.84.111.3    5888
    NAT-Info
      New SrcAddr      : 119.84.111.242
      New SrcPort      : 10242
      New DestAddr     : ----
      New DestPort     : ----

Total : 1
```

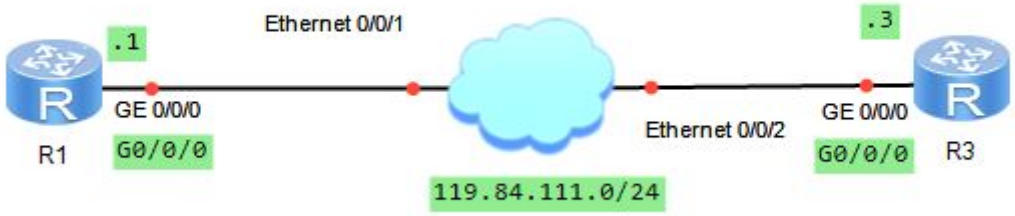
Сконфигурируем easyIP на интерфейсе GE 0/0/0 R3, связав конфигурацию с ACL 2000.

```
[R3]inter GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]nat outbound 2000
```

Проверим конфигурации acl, nat также подключение S2 к R1 через R3.

```
[R3-GigabitEthernet0/0/0]displ acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 permit source 10.0.6.0 0.0.0.255

<R3>displ nat outbound acl 2000
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                Acl      Address-group/IP/Interface    Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/0          2000             119.84.111.3   easyip
 --------------------------------------------------------------------------
  Total : 1
<R3>ping 119.84.111.1
  PING 119.84.111.1: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.1: bytes=56 Sequence=1 ttl=255 time=30 ms
    Reply from 119.84.111.1: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 119.84.111.1: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 119.84.111.1: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 119.84.111.1: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 119.84.111.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
          round-trip min/avg/max = 10/22/30 ms
```

8.3. Установка решений локального AAA.



1. Подготовка среды

```
[Huawei]sysname R1
[R1]interface GigabitEthernet0/0/0
[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24
[Huawei]sysname R3
[R3]inter GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24
```

2. Проверка связи между R1 и R3

```
<R1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
        Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=90 ms
        Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=20 ms
        Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=20 ms
        Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=20 ms
        Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 119.84.111.3 ping statistics ---
        5 packet(s) transmitted
        5 packet(s) received
        0.00% packet loss
        round-trip min/avg/max = 20/34/90 ms
```

Шаг 3. Выполнение конфигурации AAA на R1

Настроем схему аутентификации и схему авторизации на R1.

```
[R1]aaa
[R1-aaa]authentication-scheme auth1
Info: Create a new authentication scheme.
[R1-aaa-authen-auth1]authentication-mode local
[R1-aaa-authen-auth1]quit
[R1-aaa]authorization-scheme auth2
Info: Create a new authorization scheme.
[R1-aaa-author-auth2]authorization-mode local
[R1-aaa-author-auth2]quit
```

Сконфигурируем домен huawei на R1, затем создадим пользователя и применим для него этот домен.

```
[R1]telnet server enable
[R1]aaa
[R1-aaa]domain huawei
[R1-aaa-domain-huawei]authentication-scheme auth1
[R1-aaa-domain-huawei]authorization-scheme auth2
[R1-aaa-domain-huawei]quit
[R1-aaa]local-user user1@huawei password cipher huawei123
[R1-aaa]local-user user1@huawei service-type telnet
[R1-aaa]local-user user1@huawei privilege level 0
```

Настроим R1 в качестве сервера telnet, используя режим аутентификации AAA.

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
```

Убедимся, что служба telnet на R1 была успешно установлена.

```
<R3>telnet 119.84.111.1
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.1 ...
  Connected to 119.84.111.1 ...

Login authentication

Username:user1@huawei
```

```
Password:
<R1>sys
          ^
Error: Unrecognized command found at '^' position.
<R1>q

  Configuration console exit, please retry to log on

  The connection was closed by the remote host
```

Операции ограничены, поскольку привилегии пользователя ограничены уровнем привилегий 0 для user1@huawei.

4. Выполнение конфигурации AAA на R3

Сконфигурируем режим аутентификации local на R3, а также режим авторизации local.

```
[R3]aaa
[R3-aaa]authentication-scheme auth1Info: Create a new authentication scheme.
[R3-aaa-authen-auth1]authentication-mode local
[R3-aaa-authen-auth1]quit
[R3-aaa]authorization-scheme auth2Info: Create a new authorization scheme.
[R3-aaa-author-auth2]authorization-mode local
[R3-aaa-author-auth2]quit
```

Сконфигурируем домен huawei на R3, затем создадим пользователя и применим для него этот домен.

```
[R3]telnet server enable
[R3]aaa
[R3-aaa]domain huawei
[R3-aaa-domain-huawei]authentication-scheme auth1
[R3-aaa-domain-huawei]authorization-scheme auth2
[R3-aaa-domain-huawei]quit
[R3-aaa]local-user user3@huawei password cipher huawei123
[R3-aaa]local-user user3@huawei service-type telnet
[R3-aaa]local-user user3@huawei privilege level 0
```

Настроим службу telnet на R3 для использования режима аутентификации AAA.

```
[R3]user-interface vty 0 4
```

```
[R3-ui-vty0-4]authentication-mode aaa
```

Проверим результаты реализации AAA на интерфейсе vty.

```
<R1>telnet 119.84.111.3
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.3 ...
  Connected to 119.84.111.3 ...

Login authentication

Username:user3@huawei
Password:
<R3>sys
          ^
Error: Unrecognized command found at '^' position.
```

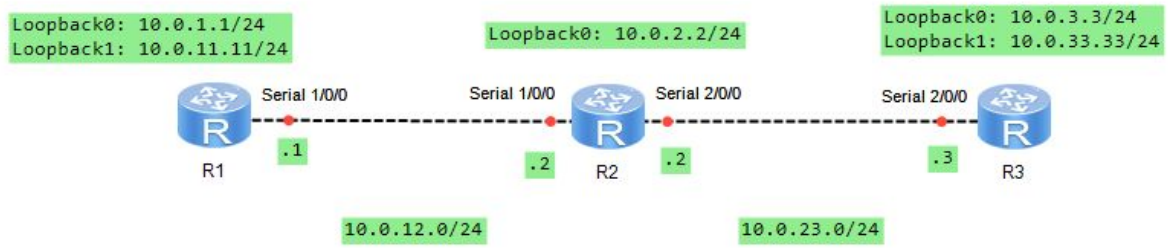
Операции ограничены, поскольку для привилегий пользователя установлено значение уровня привилегий 0 для user3@huawei.

5. Просмотр результатов конфигурации AAA

```
<R1>display domain name huawei

  Domain-name                 : huawei
  Domain-state                : Active
  Authentication-scheme-name  : auth1
  Accounting-scheme-name      : default
  Authorization-scheme-name   : auth2
  Service-scheme-name         : -
  RADIUS-server-template      : -
  HWTACACS-server-template    : -
  User-group                  : -

<R1>display local-user username user1@huawei

  The contents of local user(s):
  Password             : **********
  State          : active
  Service-type-mask : T
  Privilege level   : 0
```

```
  Ftp-directory : -
  Access-limit  : -
  Accessed-num        : 0
  Idle-timeout  : -
  User-group          : -

<R3>display domain name huawei

  Domain-name                 : huawei
  Domain-state                : Active
  Authentication-scheme-name  : auth1
  Accounting-scheme-name      : default
  Authorization-scheme-name   : auth2
  Service-scheme-name         : -
  RADIUS-server-template      : -
  HWTACACS-server-template    : -
  User-group                  : -

<R3>display local-user username user3@huawei

  The contents of local user(s):
  Password            : **********
  State          : active
  Service-type-mask : T
  Privilege level   : 0
  Ftp-directory : -
  Access-limit  : -
  Accessed-num        : 0
  Idle-timeout  : -
  User-group          : -
```

8.4. Защита трафика с IPSec VPN.



1. Подготовка среды

Произведем настройку устройств.

```
<Huawei>system-view
[Huawei]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
[Huawei]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
[R2-Serial1/0/0]interface serial 2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24
[R2-Serial2/0/0]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
[Huawei]sysname R3
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
[R3-Serial2/0/0]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

3. Настройка дополнительных логических интерфейсов

```
[R1]interface loopback 1
[R1-LoopBack1]ip address 10.0.11.11 24
```

```
[R3]interface loopback 1
[R3-LoopBack1]ip address 10.0.33.33 24
```

4. Настройка OSPF

Используем IP-адрес Loopback 0 в качестве идентификатора маршрутизатора и процесс OSPF по умолчанию. Также укажем сегменты общедоступной сети 10.0.12.0/24 и 10.0.23.0/24 в качестве часть области 0 OSPF

```
[R1-LoopBack1]ospf router-id 10.0.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.11.0 0.0.0.255

[R2-LoopBack0]ospf router-id 10.0.2.2
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255

[R3-LoopBack1]ospf router-id 10.0.3.3
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 10.0.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 10.0.33.0 0.0.0.255
```

После завершения конвергенции маршрута OSPF проверяем конфигурацию:

```
<R2>display ospf peer brief
    OSPF Process 1 with Router ID 10.0.2.2
            Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                  Neighbor id      State
 0.0.0.0          Serial1/0/0                10.0.1.1         Full
 0.0.0.0          Serial2/0/0                10.0.3.3         Full
 ----------------------------------------------------------------------------

[R1-ospf-1-area-0.0.0.0]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18        Routes : 18
Destination/Mask    Proto   Pre  Cost        Flags NextHop         Interface
```

```
        10.0.1.0/24  Direct  0  0        D   10.0.1.1    LoopBack0
        10.0.1.1/32  Direct  0  0        D   127.0.0.1           LoopBack0
        10.0.1.255/32  Direct  0        0        D   127.0.0.1           LoopBack0
        10.0.2.2/32  OSPF    10   48          D   10.0.12.2           Serial1/0/0
        10.0.3.3/32  OSPF    10   96          D   10.0.12.2           Serial1/0/0
        10.0.11.0/24  Direct  0        0        D   10.0.11.11          LoopBack1
        10.0.11.11/32  Direct  0        0        D   127.0.0.1           LoopBack1
        10.0.11.255/32  Direct  0      0        D   127.0.0.1           LoopBack1
        10.0.12.0/24  Direct  0        0        D   10.0.12.1           Serial1/0/0
        10.0.12.1/32  Direct  0        0        D   127.0.0.1           Serial1/0/0
        10.0.12.2/32  Direct  0        0        D   10.0.12.2           Serial1/0/0
        10.0.12.255/32  Direct  0      0        D   127.0.0.1           Serial1/0/0
        10.0.23.0/24  OSPF    10   96          D   10.0.12.2           Serial1/0/0
        10.0.33.33/32  OSPF  10   96          D   10.0.12.2           Serial1/0/0
        127.0.0.0/8   Direct  0 0        D   127.0.0.1           InLoopBack0
        127.0.0.1/32  Direct  0        0        D   127.0.0.1           InLoopBack0
127.255.255.255/32  Direct  0        0        D   127.0.0.1           InLoopBack0
255.255.255.255/32  Direct  0        0        D   127.0.0.1           InLoopBack0

<R3>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18        Routes : 18
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        10.0.1.1/32  OSPF    10   96          D   10.0.23.2           Serial2/0/0
        10.0.2.2/32  OSPF    10   48          D   10.0.23.2           Serial2/0/0
        10.0.3.0/24  Direct  0  0        D   10.0.3.3    LoopBack0
        10.0.3.3/32  Direct  0  0        D   127.0.0.1           LoopBack0
        10.0.3.255/32  Direct  0        0        D   127.0.0.1           LoopBack0
        10.0.11.11/32  OSPF  10   96          D   10.0.23.2           Serial2/0/0
        10.0.12.0/24  OSPF    10   96          D   10.0.23.2           Serial2/0/0
        10.0.23.0/24  Direct  0        0        D   10.0.23.3           Serial2/0/0
        10.0.23.2/32  Direct  0        0        D   10.0.23.2           Serial2/0/0
        10.0.23.3/32  Direct  0        0        D   127.0.0.1           Serial2/0/0
        10.0.23.255/32  Direct  0      0        D   127.0.0.1           Serial2/0/0
        10.0.33.0/24  Direct  0        0        D   10.0.33.33          LoopBack1
        10.0.33.33/32  Direct  0       0        D   127.0.0.1           LoopBack1
        10.0.33.255/32  Direct  0      0        D   127.0.0.1           LoopBack1
        127.0.0.0/8   Direct  0 0        D   127.0.0.1           InLoopBack0
        127.0.0.1/32  Direct  0        0        D   127.0.0.1           InLoopBack0
127.255.255.255/32  Direct  0        0        D   127.0.0.1           InLoopBack0
255.255.255.255/32  Direct  0        0        D   127.0.0.1           InLoopBack0
```

5. Конфигурирование ACL для определения “интересного” трафика

Расширенный ACL создается для определения «интересного» трафика, для которого будет применяться IPSec VPN. Расширенный ACL имеет возможность фильтрования на основе определенных параметров для выборочной фильтрации трафика.

```
[R1]acl 3001
[R1-acl-adv-3001]rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255

[R3]acl 3001
[R3-acl-adv-3001]rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
```

6. Конфигурирование предложения IPSec VPN

Создадим предложение IPSec и войдем в представление предложения IPSec, чтобы указать используемые протоколы безопасности. Также убедимся, что оба узла используют одинаковые протоколы.

```
[R1]ipsecproposaltran1
[R1-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R1-ipsec-proposal-tran1]esp encryption-algorithm 3des

[R3]ipsec proposal tran1
[R3-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R3-ipsec-proposal-tran1]esp encryption-algorithm 3des
```

Проверим конфигурацию:

```
[R1-ipsec-proposal-tran1]display ipsec proposal

Number of proposals  : 1
IPSec proposal name :        tran1
 Encapsulation mode  :       Tunnel
 Transform           :       esp-new
 ESP protocol        :       Authentication SHA1-HMAC-96
Encryption    3DES

[R3-ipsec-proposal-tran1]display ipsec proposal

Number of proposals  : 1
IPSec proposal name :        tran1
 Encapsulation mode  :       Tunnel
 Transform           :       esp-new
 ESP protocol        :       Authentication SHA1-HMAC-96
Encryption    3DES
```

7. Создание политики IPSec

Создадим политику IPSec и определим параметры для установления SA.

```
[R1]ipsec policy P1 10 manual
[R1-ipsec-policy-manual-P1-10]security acl 3001
[R1-ipsec-policy-manual-P1-10]proposal tran1
[R1-ipsec-policy-manual-P1-10]tunnel remote 10.0.23.3
[R1-ipsec-policy-manual-P1-10]tunnel local 10.0.12.1
[R1-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[R1-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[R1-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R1-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei

[R3]ipsec policy P1 10 manual
[R3-ipsec-policy-manual-P1-10]security acl 3001
[R3-ipsec-policy-manual-P1-10]proposal tran1
[R3-ipsec-policy-manual-P1-10]tunnel remote 10.0.12.1
[R3-ipsec-policy-manual-P1-10]tunnel local 10.0.23.3
[R3-ipsec-policy-manual-P1-10]sa spi outbound esp 12345
[R3-ipsec-policy-manual-P1-10]sa spi inbound esp 54321
[R3-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R3-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

Проверим конфигурацию:

```
<R1>display ipsec policy
==========================================
IPSec policy group: "P1"
Using interface:
==========================================
        Sequence number: 10
        Security data flow: 3001
        Tunnel local  address: 10.0.12.1
        Tunnel remote address: 10.0.23.3
        Qos pre-classify: Disable
        Proposal name:tran1
        Inbound AH setting:
        AH SPI:
        AH string-key:
        AH authentication hex key:
        Inbound ESP setting:
        ESP SPI: 12345 (0x3039)
```

ESP string-key: huawei
ESP encryption hex key:
ESP authentication hex key:
Outbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Outbound ESP setting:
ESP SPI: 54321 (0xd431)
ESP string-key: huawei
ESP encryption hex key:
ESP authentication hex key:

<R3>display ipsec policy
==========
IPSec policy group: "P1"
Using interface:
==========
Sequence number: 10
Security data flow: 3001
Tunnel local address: 10.0.23.3
Tunnel remote address: 10.0.12.1
Qos pre-classify: Disable
Proposal name:tran1
Inbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Inbound ESP setting:
ESP SPI: 54321 (0xd431)
ESP string-key: huawei
ESP encryption hex key:
ESP authentication hex key:
Outbound AH setting:
AH SPI:
AH string-key:
AH authentication hex key:
Outbound ESP setting:
ESP SPI: 12345 (0x3039)
ESP string-key: huawei
ESP encryption hex key:
ESP authentication hex key:

8. Применение политик IPSec к интерфейсам

Применим политику к физическому интерфейсу, на котором трафик будет подвергаться обработке IPSec.

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ipsec policy P1

[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ipsec policy P1
```

9. Проверка связи между IP-сетями

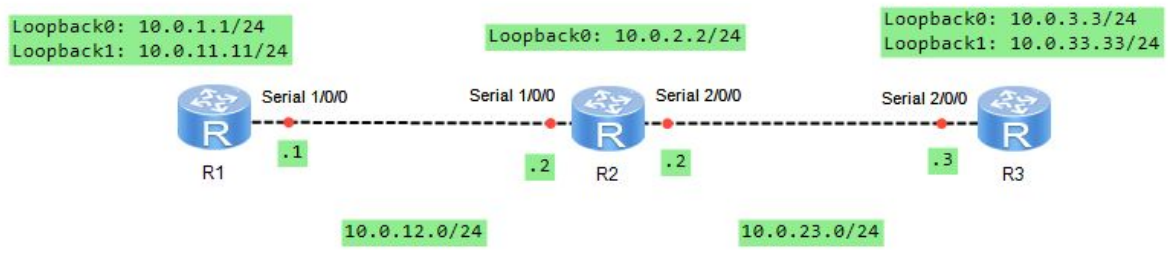
Проверяем, что “неинтересный” трафик обходит обработку IPSec:

```
<R1>ping -a 10.0.11.11 10.0.33.33
  PING 10.0.33.33: 56  data bytes, press CTRL_C to break
        Reply from 10.0.33.33: bytes=56 Sequence=1 ttl=254 time=70 ms
        Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=30 ms
        Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=30 ms
        Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=20 ms
        Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=20 ms
  --- 10.0.33.33 ping statistics ---
        5 packet(s) transmitted
        5 packet(s) received
        0.00% packet loss
        round-trip min/avg/max = 20/34/70 ms

<R1>display ipsec statistics esp
 Inpacket count      : 0
 Inpacket auth count          : 0
 Inpacket decap count         : 0
 Outpacket count              : 0
 Outpacket auth count         : 0
 Outpacket encap count        : 0
 Inpacket drop count          : 0
 Outpacket drop count         : 0
 BadAuthLen count             : 0
 AuthFail count         : 0
 InSAAclCheckFail count       : 0
 PktDuplicateDrop count       : 0
 PktSeqNoTooSmallDrop count: 0
 PktInSAMissDrop count        : 0
```

Проверяем, что IPSec VPN обрабатывает “интересный” трафик:

```
<R1>ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
        Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=30 ms
        Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=30 ms
        Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=30 ms
        Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=30 ms
        Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=30 ms
  --- 10.0.3.3 ping statistics ---
        5 packet(s) transmitted
        5 packet(s) received
        0.00% packet loss
        round-trip min/avg/max = 30/30/30 ms

<R1>display ipsec statistics esp
 Inpacket count      : 5
 Inpacket auth count          : 0
 Inpacket decap count         : 0
 Outpacket count              : 5
 Outpacket auth count         : 0
 Outpacket encap count        : 0
 Inpacket drop count          : 0
 Outpacket drop count         : 0
 BadAuthLen count             : 0
 AuthFail count         : 0
 InSAAclCheckFail count       : 0
 PktDuplicateDrop count       : 0
 PktSeqNoTooSmallDrop count: 0
 PktInSAMissDrop count        : 0
```

8.5. Поддержка динамической маршрутизации с GRE



1. Настройка трафика GRE в качестве “интересного” трафика.

```
[R1]acl 3001
[R1-acl-adv-3001]rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0

[R3]acl 3001
[R3-acl-adv-3001]rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0
```

2. Конфигурирование туннельного интерфейса.

```
[R1]int tunnel 0/0/1
[R1-Tunnel0/0/1]ip addr 100.1.1.1 24
[R1-Tunnel0/0/1]tunnel-protocol gre
[R1-Tunnel0/0/1]source 10.0.12.1
[R1-Tunnel0/0/1]dest 10.0.23.3

[R3]int tunnel 0/0/1
[R3-Tunnel0/0/1]ip addr 100.1.1.2 24
[R3-Tunnel0/0/1]tunnel-protocol gre
[R3-Tunnel0/0/1]source 10.0.23.3
[R3-Tunnel0/0/1]dest 10.0.12.1
```

3. Конфигурирование второго процесса OSPF для маршрутизации туннеля.

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]net 100.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]undo net 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]ospf 2 router-id 10.0.1.1
[R1-ospf-2]area 0
[R1-ospf-2-area-0.0.0.0]net 10.0.12.0 0.0.0.255
[R1]disp int tunnel 0/0/1
```

```
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-20 12:27:13 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2020-11-20 12:27:23-08:00
        300 seconds input rate 0 bits/sec, 0 packets/sec
        300 seconds output rate 0 bits/sec, 0 packets/sec
        0 seconds input rate 0 bits/sec, 0 packets/sec
        0 seconds output rate 0 bits/sec, 0 packets/sec
        0 packets input,  0 bytes
        0 input error
        2 packets output,  176 bytes
        0 output error
        Input bandwidth utilization  : --
        Output bandwidth utilization : --
```

```
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]net 100.1.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]undo net 10.0.23.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]ospf 2 router-id 10.0.3.3
[R3-ospf-2]area 0
[R3-ospf-2-area-0.0.0.0]network 10.0.23.0 0.0.0.255
[R3] disp int tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-20 12:29:11 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.23.3 (Serial2/0/0), destination 10.0.12.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2020-11-20 12:29:22-08:00
        300 seconds input rate 0 bits/sec, 0 packets/sec
        300 seconds output rate 0 bits/sec, 0 packets/sec
        7 seconds input rate 0 bits/sec, 0 packets/sec
```

```
    7 seconds output rate 848 bits/sec, 1 packets/sec
    0 packets input,  0 bytes
    0 input error
    21 packets output,  1856 bytes
    5 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

4. Проверка переноса маршрутов посредством GRE

```
[R1]disp ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 21        Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  Direct  0  0           D   10.0.1.1    LoopBack0
        10.0.1.1/32  Direct  0  0           D   127.0.0.1           LoopBack0
        10.0.1.255/32  Direct  0    0           D   127.0.0.1           LoopBack0
        10.0.2.2/32  OSPF    10   48          D   10.0.12.2           Serial1/0/0
        10.0.3.3/32  OSPF    10   1562        D   100.1.1.2           Tunnel0/0/1
        10.0.11.0/24  Direct  0    0           D   10.0.11.11          LoopBack1
        10.0.11.11/32  Direct  0    0           D   127.0.0.1           LoopBack1
        10.0.11.255/32  Direct  0    0           D   127.0.0.1           LoopBack1
        10.0.12.0/24  Direct  0    0           D   10.0.12.1           Serial1/0/0
        10.0.12.1/32  Direct  0    0           D   127.0.0.1           Serial1/0/0
        10.0.12.2/32  Direct  0    0           D   10.0.12.2           Serial1/0/0
        10.0.12.255/32  Direct  0    0           D   127.0.0.1           Serial1/0/0
        10.0.23.0/24  OSPF    10   96          D   10.0.12.2           Serial1/0/0
        10.0.33.33/32  OSPF  10   1562        D   100.1.1.2           Tunnel0/0/1
        100.1.1.0/24  Direct  0    0           D   100.1.1.1           Tunnel0/0/1
        100.1.1.1/32  Direct  0    0           D   127.0.0.1           Tunnel0/0/1
        100.1.1.255/32  Direct  0    0           D   127.0.0.1           Tunnel0/0/1
        127.0.0.0/8   Direct  0  0           D   127.0.0.1           InLoopBack0
        127.0.0.1/32  Direct  0    0           D   127.0.0.1           InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1           InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1           InLoopBack0
```

```
[R3]disp ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 21        Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```

```
      10.0.1.1/32  OSPF    10   1562       D   100.1.1.1       Tunnel0/0/1
      10.0.2.2/32  OSPF    10   48         D   10.0.23.2       Serial2/0/0
      10.0.3.0/24  Direct  0  0          D   10.0.3.3    LoopBack0
      10.0.3.3/32  Direct  0  0          D   127.0.0.1       LoopBack0
      10.0.3.255/32  Direct  0    0        D   127.0.0.1       LoopBack0
      10.0.11.11/32  OSPF  10   1562       D   100.1.1.1       Tunnel0/0/1
      10.0.12.0/24  OSPF   10   96         D   10.0.23.2       Serial2/0/0
      10.0.23.0/24  Direct  0    0        D   10.0.23.3       Serial2/0/0
      10.0.23.2/32  Direct  0    0        D   10.0.23.2       Serial2/0/0
      10.0.23.3/32  Direct  0    0        D   127.0.0.1       Serial2/0/0
      10.0.23.255/32  Direct  0    0      D   127.0.0.1       Serial2/0/0
      10.0.33.0/24  Direct  0    0        D   10.0.33.33      LoopBack1
      10.0.33.33/32  Direct  0    0       D   127.0.0.1       LoopBack1
      10.0.33.255/32  Direct  0    0      D   127.0.0.1       LoopBack1
      100.1.1.0/24  Direct  0    0        D   100.1.1.2       Tunnel0/0/1
      100.1.1.2/32  Direct  0    0        D   127.0.0.1       Tunnel0/0/1
      100.1.1.255/32  Direct  0    0      D   127.0.0.1       Tunnel0/0/1
      127.0.0.0/8   Direct  0  0          D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0        D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0        D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0        D   127.0.0.1       InLoopBack0
```

```
<R1>reset ipsec statistics esp
[R1]ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=30 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=40 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/30/40 ms
[R1]disp ipsec statistics esp
 Inpacket count         : 8
 Inpacket auth count            : 0
 Inpacket decap count           : 0
 Outpacket count        : 8
 Outpacket auth count           : 0
 Outpacket encap count          : 0
 Inpacket drop count            : 0
 Outpacket drop count           : 0
 BadAuthLen count               : 0
 AuthFail count         : 0
```

```
InSAAclCheckFail count       : 0
PktDuplicateDrop count       : 0
PktSeqNoTooSmallDrop count: 0
PktInSAMissDrop count        : 0
```

5. Реализация функции keepalive в туннеле GRE.

```
[R1]inter tunnel 0/0/1
[R1-Tunnel0/0/1]keepalive period 3
<R1>disp inter tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-20 12:27:13 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 3 retry-times 3
Checksumming of packets disabled
Current system time: 2020-11-20 12:39:44-08:00
        300 seconds input rate 0 bits/sec, 0 packets/sec
        300 seconds output rate 64 bits/sec, 0 packets/sec
        0 seconds input rate 0 bits/sec, 0 packets/sec
        0 seconds output rate 0 bits/sec, 0 packets/sec
        0 packets input,  0 bytes
        0 input error
        100 packets output,  9136 bytes
        0 output error
        Input bandwidth utilization  : --
        Output bandwidth utilization : --
```