Университет ИТМО

Администрирование вычислительных систем

Лабораторная работа №4

“Фильтрация корпоративных данных с помощью списков управления доступом”
“Преобразование сетевых адресов”
“Установка решений локального AAA”
“Защита трафика с IPSec VPN”
“Поддержка динамической маршрутизации с GRE”

Выполнили: Калугина Марина
Саржевский Иван
Группа: P3402
Проверил: Афанасьев Дмитрий Борисович

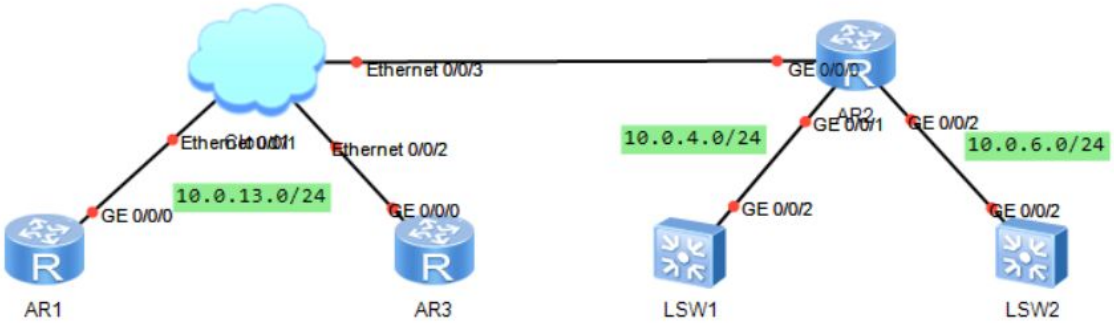
г. Санкт-Петербург

2020 г.

Содержание

Фильтрация корпоративных данных с помощью списков управления доступом

Топология



Подготовка среды

```
[Huawei]sysname R1
2020-05-13 Huawei confidential. No spreading without permission.
Стр 52
[Huawei]sysname R2
[Huawei]sysname R3
```

```
[Huawei]sysname S1
[S1]vlan 4
[S1-vlan4]quit
[S1]interface vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24
```

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

Конфигурирование IP-адресации

Сконфигурируем адресацию для 10.0.13.0/24.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 10.0.13.1 24
```

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 10.0.13.2 24
```

```
[R2-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.4.2 24
[R2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.6.2 24
```

```
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 10.0.13.3 24
```

Установим магистрали VLAN на S1 и S2. Для интерфейса GigabitEthernet 0/0/2 на S1 должен быть предварительно настроен тип соединения порта.

```
[S1]interface GigabitEthernet 0/0/2
[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]interface GigabitEthernet 0/0/2
[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
```

Настройка OSPF для включения межсетевого взаимодействия

Настроим OSPF для R1, R2 и R3. Убедимся, что все они являются частью одной и той же области OSPF, и объявим о созданных сетях.

```
[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 и 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
    Request time out
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 30/32/40 ms

[R1]ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=254 time=50 ms
    Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=254 time=40 ms

  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 30/42/50 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=60 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=110
ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/54/110 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=70 ms
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=254 time=50 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=70 ms

  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/56/70 ms
```

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
[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 серверу telnet, а R3 — доступ к FTP-серверу.

```
[R2]acl 3000
[R2-acl-adv-3000]rule 5 permit tcp source 10.0.13.1 0.0.0.0
destination 10.0.4.254 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 Gigabit Ethernet 0/0/0 маршрутизатора R2.

```
[R2]interface GigabitEthernet0/0/0
[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 2020-11-16 22:49:18.
<S1>

<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]
```

Окончательная конфигурация

```
<R1>display current-configuration
[V200R003C00]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.1 255.255.255.0
#
```

```
ospf 1
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
return
```

```
<R2>display current-configuration
[V200R003C00]
#
 sysname R2
#
acl number 3000
 rule 5 permit tcp source 10.0.13.1 0 destination 10.0.4.254 0
destination-port
eq telnet
 rule 10 permit tcp source 10.0.13.3 0 destination 10.0.6.254 0
destination-port
 range ftp-data ftp
 rule 15 permit ospf
 rule 20 deny ip
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.2 255.255.255.0
 traffic-filter inbound acl 3000
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.4.0 0.0.0.255
  network 10.0.6.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
#
return
```

```
<R3>display current-configuration
[V200R003C00]
#
 sysname R3
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.3 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
return
```

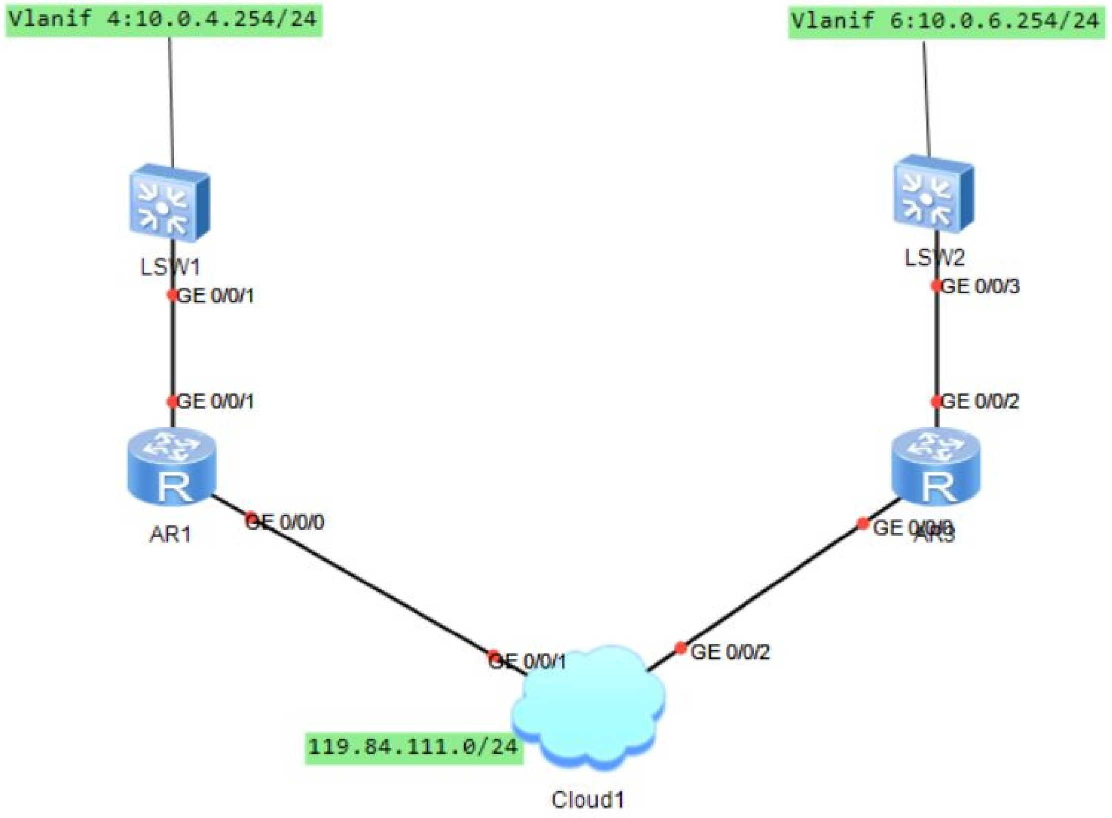
```
<S1>display current-configuration
#
sysname S1
#
vlan batch 4
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.2
#
user-interface con 0
user-interface vty 0 4
 set authentication password cipher .Vq8X~\X1/,vs=Hws)!Ww^,#
 protocol inbound all
#
return
```

```
<S2>display current-configuration
```

```
#
sysname S2
#
FTP server enable
#
vlan batch 6
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
 local-user huawei password cipher -J&7(SW'E2AI>,Z,88J\:Q!!
 local-user huawei privilege level 3
 local-user huawei ftp-directory flash:/
 local-user huawei service-type ftp
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.6.2
#
return
```

Преобразование сетевых адресов

Топология



Подготовка среды

```
[Huawei]sysname R1
[R1]inter GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24
```

```
[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24
```

```
[Huawei]sysname S1
[S1]vlan 4
[S1-vlan3]quit
[S1]interface vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24
[S1-Vlanif4]quit
```

```
[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]interface vlanif 6
```

```
[S2-Vlanif6]ip address 10.0.6.254 24
[S2-Vlanif6]quit
```

Реализация конфигурирования VLAN для S1 и S2

```
[S1]interface 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
```

```
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type trunk
[S2-GigabitEthernet0/0/3]port trunk pvid vlan 6
[S2-GigabitEthernet0/0/3]port trunk allow-pass vlan all
```

```
[R1]interface GigabitEthernet0/0/0
[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24
```

```
[R3]interface GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24
```

Убедимся, что R1 может достичь как S1, так 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=340
ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=255 time=30 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 = 20/88/340 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=140
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=30
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=30
ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/48/140 ms
```

Настройка списков управления доступом для R1 и R3

Сконфигурируем расширенный ACL на R1 и выберем поток данных с источником S1, пунктом назначения 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
```

Сконфигурируем стандартный ACL на R3 и выберем поток данных, IP-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
```

Конфигурирование динамического NAT

Настроим статический маршрут на S1 и S2, установим nexthop в качестве 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
```

Настройте динамический NAT на интерфейсе GigabitEthernet0/0/0 R1.

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

Настроим R3 в качестве сервера telnet.

```
[R3]telnet server enable
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode password
[R3-ui-vty0-4]set authentication password cipher
Warning: The “password” authentication mode is not secure,and it
is strongly recommended to
use ”aaa” authentication mode.
Enter Password(<8-128>):huawei123
Confirm password:huawei123
```

Убедимся, что группа адресов настроена правильно.

```
<R1>display nat address-group

 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
 1      119.84.111.240   119.84.111.243
 --------------------------------------
  Total : 1
```

Увеличим время сеанса ICMP, чтобы он отображался в таблице NAT.

```
[R1]firewall-nat session icmp aging-time 300
```

Проверим подключение к шлюзу удаленного одноранговой узла от внутренней сети.

```
<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=100
ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=254 time=40
ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=254 time=50
ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=254 time=60
ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=254 time=40
ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/58/100 ms
```

Установим соединение telnet с общедоступным адресом удаленного однорангового узла.

```
<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:
<R3>
```

Откроем второе окно сеанса для R1 и просмотрим результаты преобразования сеансов ACL и NAT.

```
<R1>dis 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>display nat session all
 NAT Session Table Information:


     Protocol          : ICMP(1)
     SrcAddr   Vpn     : 10.0.4.254
     DestAddr  Vpn     : 119.84.111.3
     Type Code IcmpId  : 0   8   43982
     NAT-Info
       New SrcAddr     : 119.84.111.242
       New DestAddr    : ----
       New IcmpId      : 10243

     Protocol          : TCP(6)
     SrcAddr  Port Vpn : 10.0.4.254      17098
     DestAddr Port Vpn : 119.84.111.3    5888
     NAT-Info
       New SrcAddr     : 119.84.111.242
       New SrcPort     : 10242
       New DestAddr    : ----
       New DestPort    : ----
```

Сконфигурируем easyIP на интерфейсе Gigabit Ethernet 0/0/0 R3, связав конфигурацию easyIP с ACL 2000, который был настроен ранее.

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

Проверим подключение от S2 к R1 через R3.

```
<S2>
Nov 16 2020 23:32:26-08:00 S2
%%01VOSCPU/4/CPU_USAGE_HIGH(l)[0]:The CPU is overl
oaded(CpuUsage=86%, Threshold=80%), and the tasks with top three
CPU occupancy a
re:
NonDopraTask  total      : 76%
IFPD  total      : 2%
TICK  total      : 2% 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=254 time=30
ms
```

```
    Reply from 119.84.111.1: bytes=56 Sequence=2 ttl=254 time=30
ms
    Reply from 119.84.111.1: bytes=56 Sequence=3 ttl=254 time=50
ms
    Reply from 119.84.111.1: bytes=56 Sequence=4 ttl=254 time=60
ms
    Reply from 119.84.111.1: bytes=56 Sequence=5 ttl=254 time=50
ms

  --- 119.84.111.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/44/60 ms
```

```
<R3>display 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>display 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
```

Окончательная конфигурация

```
<R1>display
current-configuration
[V200R003C00]
#
 sysname R1
#
firewall-nat session icmp
aging-time 300
#
acl number 3000
 rule 5 permit tcp source
```

```
<R3>dis current-configuration
[V200R003C00]
#
 sysname R3
#
acl number 2000
 rule 5 permit source 10.0.6.0
0.0.0.255
#
aaa
 authentication-scheme default
```

```
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
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password
cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%
$
 local-user admin service-type
http
#
 nat address-group 1
119.84.111.240 119.84.111.243
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1
255.255.255.0
 nat outbound 3000
address-group 1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1
255.255.255.0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```

```
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password
cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%
$
 local-user admin service-type
http
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3
255.255.255.0
 nat outbound 2000
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.3
255.255.255.0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode password
 set authentication password
cipher
%$%$u59m3PpE2)3-Z+ArS,DW,#=!fw:
fR4ec'Baz{A9m
s9=B#=$,%$%$
user-interface vty 16 20
#
return
```

```
<S1>dis current-configuration
#
sysname S1
#
vlan batch 3 to 4
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password
simple admin
 local-user admin service-type
```

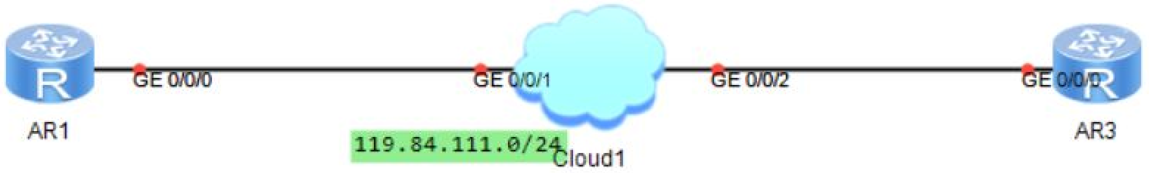
```
<S2>dis current-configuration
#
sysname S2
#
vlan batch 6
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password
simple admin
 local-user admin service-type
```

```
http
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.1
#
user-interface con 0
user-interface vty 0 4
#
return
```

```
http
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.6.3
#
user-interface con 0
user-interface vty 0 4
#
return
```

Установка решений локального AAA

Топология



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
```

Проверка связи между R1 и R3

```
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=80
ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=1
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=1
ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=1
ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/20/80 ms
```

Выполнение конфигурации AAA на R1

Настроим 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
```

Сконфигурируем домен *huawei* на R1, затем создим 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
```

Настройте 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:authentication
Password:

  Configuration console exit, please retry to log on

  The connection was closed by the remote host
<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
<R1>system-view
    ^
Error: Unrecognized command found at '^' position.
<R1>quit

  Configuration console exit, please retry to log on

  The connection was closed by the remote host
```

Операции ограничены, поскольку для привилегий пользователя установлено значение уровня привилегий 0 для user1@huawei.

Выполнение конфигурации AAA на R3

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

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

Сконфигурируем домен *huawei* на R3, затем создим 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:
Error: Local authentication is rejected.

  Logged Fail!

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

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

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        : -
```

Окончательная конфигурация

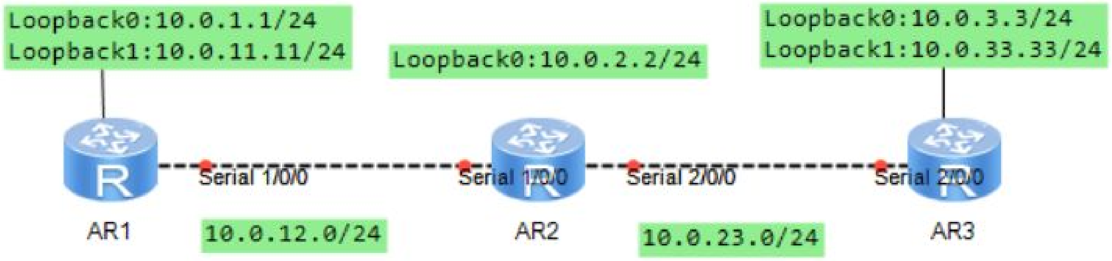
`<R1>display`
`current-configuration`
`[V200R003C00]`
	`<R3>display`
	`current-configuration`
	`[V200R003C00]`

```
#
 sysname R1
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
 local-user user1@huawei password cipher %$%$E*4pUctz1.m)_y(G>[z<;Q*Y%$%$
 local-user user1@huawei privilege level 0
 local-user user1@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1 255.255.255.0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
return
```

```
#
 sysname R3
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
 local-user user3@huawei password cipher %$%$+$6^LcT_%(`.bi!)Rgw>;Z6j%$%$
 local-user user3@huawei privilege level 0
 local-user user3@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3 255.255.255.0
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
return
```

Защита трафика с IPSec VPN

Топология



Подготовка среды

```
<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
```

Настройка дополнительных логических интерфейсов

```
[R1-LoopBack0]interface loopback 1
[R1-LoopBack1]ip address 10.0.11.11 24
[R3-LoopBack0]interface loopback 1
[R3-LoopBack1]ip address 10.0.33.33 24
```

Настройка OSPF

Используем IP-адрес Loopback 0 в качестве идентификатора маршрутизатора, используем процесс OSPF по умолчанию (1) и укажем сегменты общедоступной сети 10.0.12.0/24 и 10.0.23.0/24 в качестве области 0 OSPF.

```
[R1]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]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]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
```

Проверим 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>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
```

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
```

Конфигурирование предложения IPSec VPN

```
[R1]ipsec proposal tran1
[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
```

Выполним команду **display ipsec proposal** для проверки конфигурации.

```
[R1]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]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
```

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
```

Выполним команду display ipsec policy для проверки конфигурации

```
<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:
```

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
```

Проверка связи между IP-сетями

Убедитесь, 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=60 ms
    Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=20 ms
    Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 10.0.33.33 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/38/60 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
```

Обратите внимание , что IPSec VPN будет защищать только « 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=40 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=20 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 = 20/30/40 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
```

Окончательная конфигурация

```
<R1>dis current-configuration
[V200R003C00]
#
 sysname R1
#
 board add 0/1 2SA
#
acl number 3001
 rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0
0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
#
interface Serial1/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```

```
<R2>dis current-configuration
[V200R003C00]
#
 sysname R2
#
 board add 0/1 2SA
 board add 0/2 2SA
#
aaa
```

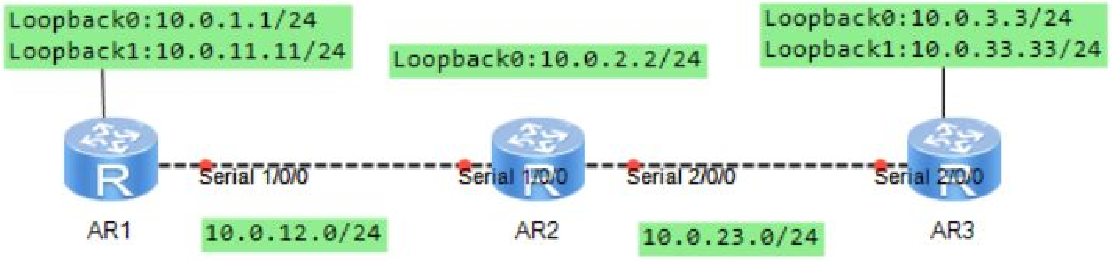
```
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
#
interface Serial1/0/1
 link-protocol ppp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.2 255.255.255.0
#
interface Serial2/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```

```
<R3>dis current-configuration
[V200R003C00]
#
 sysname R3
#
 board add 0/2 2SA
#
acl number 3001
 rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0
0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
```

```
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
interface Serial2/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
 ip address 10.0.33.33 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```

Поддержка динамической маршрутизации с GRE

Топология



Настройка трафика GRE в качестве «интересного» трафика

Перенастроим список управления доступом и установим инкапсуляцию GRE по IPSec.

```
[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
```

Конфигурирование туннельного интерфейса

Создадим туннельный интерфейс и укажем GRE в качестве типа инкапсуляции. Установим адрес источника туннеля или интерфейс источника и адрес назначения туннеля.

```
[R1]interface Tunnel 0/0/1
[R1-Tunnel0/0/1]ip address 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]destination 10.0.23.3
```

```
[R3]interface Tunnel 0/0/1
[R3-Tunnel0/0/1]ip address 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]destination 10.0.12.1
```

Конфигурирование второго процесса OSPF для маршрутизации туннеля

Добавим сеть с туннельным интерфейсом к процессу OSPF 1 и создим второй экземпляр OSPF базы данных состояний каналов (процесс 2) для сетей 10.0.12.0 и 10.0.23.0, удалим эти сети из OSPF 1.

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]undo network 10.0.12.0 0.0.0.255
[R1]ospf 2 router-id 10.0.1.1
[R1-ospf-2]area 0
[R1-ospf-2-area-0.0.0.0]network 10.0.12.0 0.0.0.255
```

```
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]undo network 10.0.23.0 0.0.0.255
[R3]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
```

OSPF LSDB важны только для локального маршрутизатора, поэтому маршруты от OSPF LSDB 2 R1 и R3 достигают OSPF LSDB 1 R2.

Выполним команду **display interface Tunnel 0/0/1** для проверки конфигурации

```
<R1>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-17 23:09:46 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: 2020-11-17 23:10:58-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    9 seconds input rate 0 bits/sec, 0 packets/sec
    9 seconds output rate 80 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    30 packets output,  3264 bytes
    0 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

```
<R3>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-17 23:10:41 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: 2020-11-17 23:15:29-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 88 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
    50 packets output,  4604 bytes
    5 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Проверка переноса маршрутов посредством GRE

Выполним команду **display ip routing-table** для проверки таблицы маршрутизации IPv4.

```
<R1>display 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>display 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
```

После настройки туннеля GRE маршрутизатор может обмениваться пакетами OSPF через туннель GRE. Удалим статистику IPSec и протестируйте соединение.

```
<R1>reset ipsec statistics esp
<R1>sys
Enter system view, return user view with Ctrl+Z.
[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=50 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=20 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 = 20/32/50 ms
```

```
<R1>display ipsec statistics esp
 Inpacket count            : 9
 Inpacket auth count       : 0
 Inpacket decap count      : 0
 Outpacket count           : 9
 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
```

Реализация функции keepalive в туннеле GRE

```
[R1]interface Tunnel 0/0/1
[R1-Tunnel0/0/1]keepalive period 3
```

Убедимся, что на интерфейсе туннеля включена функция keepalive.

```
<R1>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-11-17 23:09:46 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: 2020-11-17 23:20:46-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 72 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
    95 packets output,  9236 bytes
    0 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Окончательная конфигурация

```
<R1>dis current-configuration
[V200R003C00]
#
 sysname R1
#
 board add 0/1 2SA
#
acl number 3001
 rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
```

```
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
#
interface Serial1/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 3
 source 10.0.12.1
 destination 10.0.23.3
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
```

```
#
return
```

```
<R2>dis current-configuration
[V200R003C00]
#
 sysname R2
#
 board add 0/1 2SA
 board add 0/2 2SA
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
#
interface Serial1/0/1
 link-protocol ppp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.2 255.255.255.0
#
interface Serial2/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```

```
<R3>dis current-configuration
[V200R003C00]
```

```
#
 sysname R3
#
 board add 0/2 2SA
#
acl number 3001
 rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
interface Serial2/0/1
 link-protocol ppp
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
 ip address 10.0.33.33 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.0.23.3
 destination 10.0.12.1
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
return
```