Настройка Site-to-Site VPN на маршрутизаторах Cisco

Наташа Самойленко

Настройка Site-to-Site VPN на маршрутизаторах Cisco

Наташа Самойленко

Содержание:

Использование оборудования

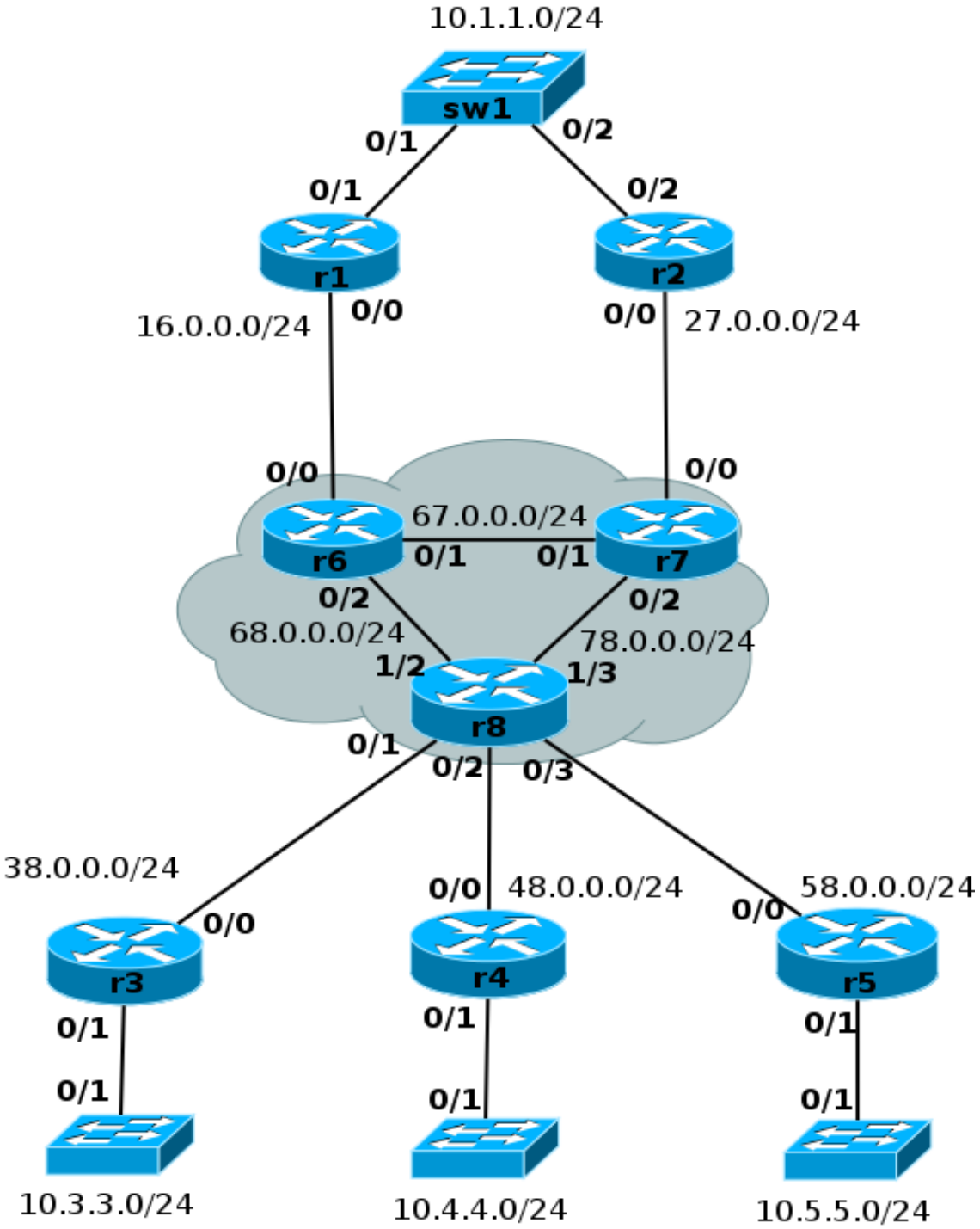
Действие	**Комбинация клавиш**
Переключение между окнами (с 1 по 9 окно)	Ctrl+a номер окна
Переключение между окнами	Ctrl+a ' номер окна
Список всех окон (по нему можно передвигаться и переключиться на другое окно):	Ctrl+a “
Переключиться на следующее окно:	Ctrl+a space или Ctrl+a n
Переключиться на предыдущее окно	Ctrl+a backspace или Ctrl+a p
Прокрутка вверх	Ctrl+a [после нажатия комбинации, передвигаться можно стрелками вверх и вниз

Консольный сервер: 5.9.243.178
Port SSH: 3080X
Пользователь: network
Пароль: netpass

Лабораторная 1. Настройка Site-to-site VPN с аутентификацией по pre-shared key.

Использование crypto-map

Топология



Задание:

Настроить VPN между маршрутизаторами r1 и r3 с аутентификацией по pre-shared key.

1 Подготовка к настройке VPN.
   1.1 Настройка маршрутизации между r1 и r3
   1.2 Проверить доступность внешних интерфейсов
2 Настроить политику IKE (ISAKMP)
3 Настроить pre-shared ключ, который будет использоваться для аутентификации
4 Указать какой трафик между сетями необходимо шифровать. Шифроваться должен трафик между сетями 10.1.1.0/24 и 10.3.3.0/24
5 Настроить политику для защиты передаваемых данных (transform-set)
6 Настроить crypto-map и применить её на внешнем интерфейсе
7 Проверка работы VPN

Пошаговая настройка:

Настроить VPN между маршрутизаторами r1 и r3 с аутентификацией по pre-shared key.

1 Подготовка к настройке VPN.

1.1 Настройка маршрутизации между r1 и r3

Маршрут по умолчанию на r1:

```
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Маршрут по умолчанию на r3:

```
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

1.2 Проверить доступность внешних интерфейсов

Проверка доступности внешнего интерфейса r3 с r1:

```
r1#ping 38.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 38.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
592/598/600 ms
```

2 Настроить политику IKE (ISAKMP)

Политика IKE одинаковая на r1 и r3:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
 hash sha
```

3 Настроить pre-shared ключ, который будет использоваться для аутентификации

Настройка ключа на r1:

```
crypto isakmp key cisco address 38.0.0.3
```

Настройка ключа на r3:

```
crypto isakmp key cisco address 16.0.0.1
```

4 Указать какой трафик между сетями необходимо шифровать. Шифроваться должен трафик между сетями 10.1.1.0/24 и 10.3.3.0/24

Настройка ACL на r1:

```
ip access-list extended MAP_VPN
 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
```

Настройка ACL на r3:

```
ip access-list extended MAP_VPN
 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
```

5 Настроить политику для защиты передаваемых данных (transform-set)

Политика должна быть одинаковой на r1 и r3:

```
crypto ipsec transform-set MAP_set esp-aes esp-sha-hmac
```

6 Настроить crypto map и применить её на внешнем интерфейсе

crypto map это объект в котором собираются все предыдущие настройки.

Настройка crypto map на r1 и применение на интерфейса f0/0:

```
crypto map MAP1 10 ipsec-isakmp
 set peer 38.0.0.3
 set transform-set MAP_set
 match address MAP_VPN

interface FastEthernet0/0
 crypto map MAP1
```

Настройка crypto map на r3:

```
crypto map MAP1 10 ipsec-isakmp
 set peer 16.0.0.1
 set transform-set MAP_set
 match address MAP_VPN

interface FastEthernet0/0
 crypto map MAP1
```

7 Проверка работы VPN

До генерации трафика:

```
r1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

Генерация трафика, который должен попадать в шифрованный туннель:

```
r2#ping 10.0.20.5 source lo0 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.0.20.5, timeout is 2 seconds:
Packet sent with a source address of 10.0.10.4
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max =
592/915/1200 ms
```

Установленные SA первой фазы:

```
r1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
38.0.0.3     16.0.0.1     QM_IDLE           1001 ACTIVE
```

Установленные SA второй фазы:

```
r1#sh crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: MAP1, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
   current_peer 38.0.0.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 10, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 38.0.0.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xAE0DDDFE(2920144382)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xFB87E64D(4219987533)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80000046, crypto map: MAP1
        sa timing: remaining key lifetime (k/sec): (4538368/2751)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xAE0DDDFE(2920144382)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, sibling_flags 80000046, crypto map: MAP1
        sa timing: remaining key lifetime (k/sec): (4538368/2751)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Просмотр crypto-map:

```
r3#sh crypto map
Crypto Map "MAP1" 10 ipsec-isakmp
        Peer = 16.0.0.1
        Extended IP access list MAP_VPN
            access-list MAP_VPN permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255

Current peer: 16.0.0.1
```

```
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                MAP_set:  { esp-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map MAP1:
                FastEthernet0/0
```

Просмотр информации:

```
r1#sh crypto session brief
Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N -
Negotiating
        K - No IKE
ivrf = (none)
           Peer     I/F   Username     Group/Phase1_id   Uptime Status
    38.0.0.3   Fa2/0                    38.0.0.3 00:17:57    UA
```

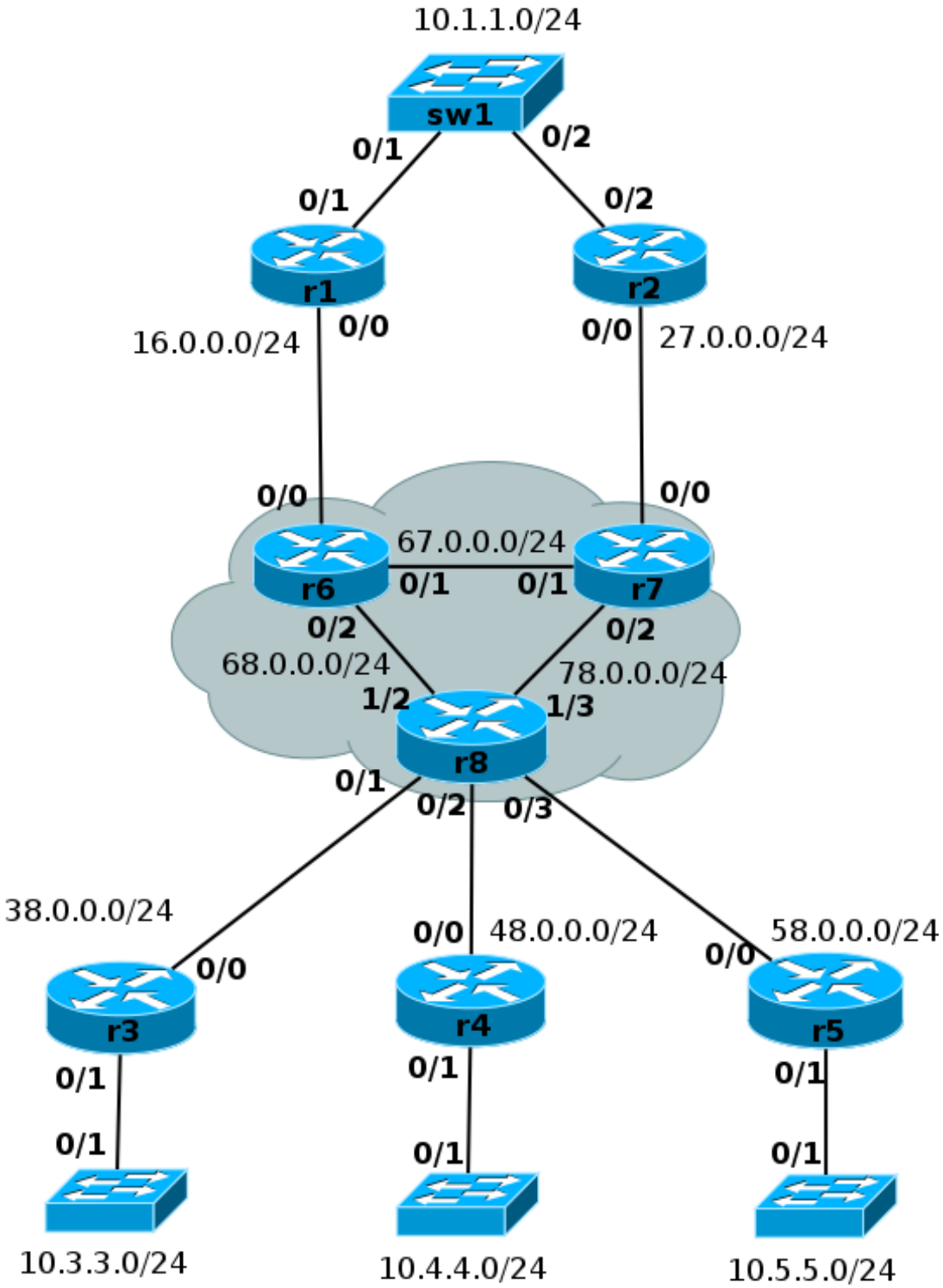
```
r1#sh crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 10.3.3.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

```
r1#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet0/0
Uptime: 00:19:21
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 38.0.0.3
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1001 lifetime:23:40:23
  IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 10.3.3.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 4538368/2438
        Outbound: #pkts enc'ed 10 drop 10 life (KB/Sec) 4538368/2438
```

```
r1#sh crypto ruleset
FastEthernet0/0:
 IP 10.1.1.0/24 10.3.3.0/24 IPSec SA
 IP 10.1.1.0/24 10.3.3.0/24 IPSec Cryptomap
```

Лабораторная 2. Настройка Site-to-site VPN с аутентификацией по pre-shared key. Использование VTI

Топология



Задание:

Настроить VPN между маршрутизаторами r1 и r3 с аутентификацией по pre-shared key.

1 Подготовка к настройке VPN.
   1.1 Настроить маршрутизацию между r1 и r3
   1.2 Проверить доступность внешних интерфейсов
   1.3 Настроить динамическую маршрутизацию на r1, r3, sw1, sw2
2 Настроить политику IKE (ISAKMP)
3 Настроить pre-shared ключ, который будет использоваться для аутентификации
4 Настроить политику для защиты передаваемых данных (transform-set)
5 Настроить IPsec profile
6 Настроить туннельный интерфейс и применить к нему IPsec profile
7 Проверить работу VPN

Пошаговая настройка:

Настроить VPN между маршрутизаторами r1 и r3 с аутентификацией по pre-shared key.

1 Подготовка к настройке VPN.

1.1 Настроить маршрутизацию между r1 и r3

Маршрут по умолчанию на r1:

```
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Маршрут по умолчанию на r3:

```
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

1.2 Проверить доступность внешних интерфейсов

```
r3#ping 16.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/105/156 ms
```

1.3 Настроить динамическую маршрутизацию на r1, r3, sw1, sw2

Настройка OSPF на r1, r3, sw1, sw2:

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

2 Настроить политику IKE (ISAKMP)

Политика IKE одинаковая на r1 и r3:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
 hash sha
```

3 Настроить pre-shared ключ, который будет использоваться для аутентификации

Настройка ключа на r1:

```
crypto isakmp key ciscoVTI address 38.0.0.3
```

Настройка ключа на r3:

```
crypto isakmp key ciscoVTI address 16.0.0.1
```

4 Настроить политику для защиты передаваемых данных (transform-set)

Политика должна быть одинаковой на r1 и r3:

```
crypto ipsec transform-set MAP_set esp-aes esp-sha-hmac
```

5 Настроить IPsec profile

На r1 и r3 будет одинаковый IPsec profile:

```
crypto ipsec profile VTI_prof
 set transform-set MAP_set
```

6 Настроить туннельный интерфейс и применить к нему IPsec profile

Настройка интерфейса на r1:

```
interface Tunnel0
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile VTI_prof
```

Настройка интерфейса на r3:

```
interface Tunnel0
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile VTI_prof
```

Для удобства, на туннели можно назначить IP-адреса из приватного диапазона.
На r1:

```
interface Tunnel0
 ip address 10.0.13.1 255.255.255.0
```

На r3:

```
interface Tunnel0
 ip address 10.0.13.3 255.255.255.0
```

7 Проверить работу VPN

Проверка связи:

```
r3#ping 10.1.1.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 504/578/600 ms
```

Маршруты полученные по OSPF на r3:

```
r3#sh ip route ospf
...
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O        10.1.1.0/24 [110/1001] via 10.0.13.1, 00:08:36, Tunnel0
```

SA первой фазы на r1 (второе SA для туннеля с crypto map):

```
r1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
38.0.0.3        16.0.0.1        QM_IDLE           1002 ACTIVE

```

SA первой фазы на r3:

```
r3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
38.0.0.3     16.0.0.1           QM_IDLE           1001 ACTIVE
```

SA второй фазы на r1:

```
r1#sh crypto ipsec sa peer 38.0.0.3

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 38.0.0.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 177, #pkts encrypt: 177, #pkts digest: 177
    #pkts decaps: 153, #pkts decrypt: 153, #pkts verify: 153
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 38.0.0.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x8A11BB04(2316417796)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xAB417D2E(2873195822)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 7, flow_id: SW:7, sibling_flags 80000046, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4499730/2333)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x8A11BB04(2316417796)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 8, flow_id: SW:8, sibling_flags 80000046, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4499726/2333)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

```
     outbound ah sas:

     outbound pcp sas:
```

Автоматически созданные crypto map на r3:

```
r3#sh crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
        Profile name: VTI_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                MAP_set:  { esp-aes esp-sha-hmac  } ,
        }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 16.0.0.1
        Extended IP access list
            access-list  permit ip any any
        Current peer: 16.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                MAP_set:  { esp-aes esp-sha-hmac  } ,
        }
        Always create SAs
        Interfaces using crypto map Tunnel0-head-0:
                Tunnel0
```

```
r3#sh crypto session brief
Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N -
Negotiating
        K - No IKE
ivrf = (none)
           Peer     I/F   Username     Group/Phase1_id   Uptime Status
           16.0.0.1 Tu0                       16.0.0.1  00:28:30    UA
```

```
r3#sh crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKE SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

```
r3#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:29:20
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 16.0.0.1
```

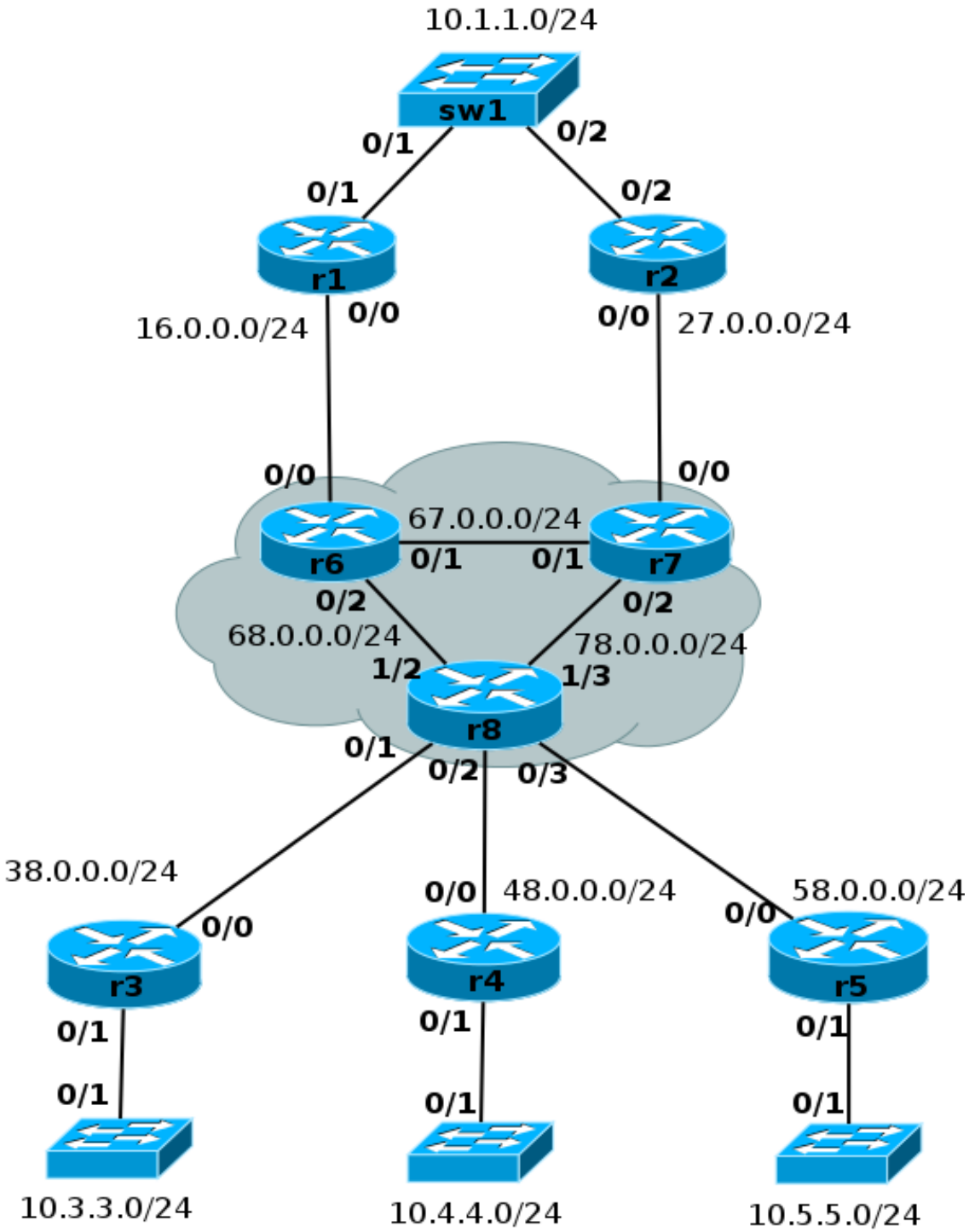
```
      Desc: (none)
  IKE SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
          Capabilities:(none) connid:1001 lifetime:23:30:37
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 229 drop 0 life (KB/Sec) 4383756/1839
        Outbound: #pkts enc'ed 205 drop 0 life (KB/Sec) 4383760/1839
```

```
r3#sh crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKE SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit ip 10.3.3.0/255.255.255.0 10.1.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

```
r3#sh crypto ruleset
FastEthernet0/0:
 IP 10.3.3.0/24 10.1.1.0/24 IPSec SA
 IP 10.3.3.0/24 10.1.1.0/24 IPSec Cryptomap
Tunnel0:
 IP ANY ANY IPSec SA
 IP ANY ANY IPSec Cryptomap
```

Лабораторная 3. Настройка Site-to-site VPN с аутентификацией по pre-shared key. Использование динамических VTI

Топология



Задание:

Настроить VPN между маршрутизаторами r1, r3 и r4 с аутентификацией по pre-shared key. Использовать динамические VTI на r1.

1 Подготовка к настройке VPN.

   1.1 Настроить маршрутизацию между r1, r3 и r4

   1.2 Проверить доступность внешних интерфейсов

2 Политика IKE (ISAKMP) остается из прошлых лабораторных

3 Настроить pre-shared ключи, которые будут использоваться для аутентификации

4 Настроить политику для защиты передаваемых данных (transform-set)

5 Настроить IPsec profile на r1, r3, r4

6 На r1 настроить шаблонный интерфейс (Virtual-Template) для создания динамических VTI и применить к нему IPsec profile. Включить OSPF на этом интерфейсе

7 На r3 и r4 настроить статические VTI и применить к ним IPsec profile

8 Настроить crypto isakmp profile, указать в каких случаях он будет срабатывать и связать его с созданным шаблонным интерфейсом

9 Проверить работу VPN

Пошаговая настройка:

Настроить VPN между маршрутизаторами r1, r3 и r3 с аутентификацией по pre-shared key. Использовать динамические VTI на r3 и r3.

1 Подготовка к настройке VPN.

1.1 Проверить доступность внешних интерфейсов

```
r3#ping 16.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 160/322/564 ms
r4#ping 16.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 592/597/600 ms
```

2 Политика IKE (ISAKMP) остается из прошлых лабораторных

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
 hash sha
```

3 Настроить pre-shared ключи, которые будут использоваться для аутентификации

Настройка ключей на r1:

```
crypto keyring DYNS
  pre-shared-key address 38.0.0.0 255.255.255.0 key r1-3
  pre-shared-key address 48.0.0.0 255.255.255.0 key r1-4
```

Просмотр ключей:

```
r1#sh crypto isakmp key
Keyring      Hostname/Address                              Preshared Key

default      38.0.0.3                                    cisco

DYNS         38.0.0.0    [255.255.255.0  ]               r1-3
             48.0.0.0    [255.255.255.0  ]               r1-4
```

Настройка ключей на r3:

```
crypto isakmp key r1-3 address 16.0.0.1
```

Настройка ключей на r3:

```
crypto isakmp key r1-4 address 16.0.0.1
```

4 Настроить политику для защиты передаваемых данных (transform-set)

```
crypto ipsec transform-set DVTI esp-3des esp-sha-hmac
```

5 Настроить IPsec profile на r1, r3, r3

```
crypto ipsec profile DYNS_prof
 set transform-set DVTI
```

6 На r1 настроить шаблонный интерфейс (Virtual-Template) для создания динамических VTI и применить к нему IPsec profile

```
interface Virtual-Template100 type tunnel
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile DYNS_prof
```

7 На r3 и r4 настроить статические VTI и применить к ним IPsec profile

Настройка на r3:

```
interface Tunnel 100
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile DYNS_prof
```

Настройка на r4:

```
interface Tunnel100
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile DYNS_prof
```

8 Настроить crypto isakmp profile на r1, указать в каких случаях он будет срабатывать и связать его с созданным шаблонным интерфейсом

```
crypto isakmp profile IKE_prof
   keyring DYNS
   match identity address 38.0.0.0 255.255.255.0
   match identity address 48.0.0.0 255.255.255.0
   virtual-template 100
```

```
r1#sh crypto isakmp profile

ISAKMP PROFILE IKE_prof

Ref Count = 3
   Identities matched are:
    ip-address 38.0.0.0 255.255.255.0
    ip-address 48.0.0.0 255.255.255.0
   Certificate maps matched are:
   keyring(s): DYNS
   trustpoint(s): <all>
   virtual-template: 100
```

9 Проверить работу VPN

Для r3 и r4 автоматически созданы 2 виртуальных интерфейса

```
r1#sh ip int br
Interface                  IP-Address      OK? Method Status       Protocol
FastEthernet0/1            10.1.1.1        YES NVRAM  up           up
FastEthernet0/0            16.0.0.1        YES NVRAM  up           up
Tunnel0                    unassigned      YES NVRAM  up           down
Virtual-Access1            unassigned      YES unset  down         down
Virtual-Access2            16.0.0.1        YES unset  up           up
Virtual-Access3            16.0.0.1        YES unset  up           up
Virtual-Template100        16.0.0.1        YES unset  up           down
```

(хотя они отображаются в текущей конфигурации в стартовую они не попадут), посмотреть на их конфигурацию можно только командой sh run interface Virtual-Access <number>:

```
r1#sh run interface Virtual-Access 2
Building configuration...

Current configuration : 248 bytes
!
interface Virtual-Access2
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source 16.0.0.1
 tunnel mode ipsec ipv4
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile DYNS_prof
 no tunnel protection ipsec initiate
 !
end

r1#sh run interface Virtual-Access 3
Building configuration...

Current configuration : 248 bytes
!
interface Virtual-Access3
 ip unnumbered FastEthernet0/0
 ip ospf 1 area 0
 tunnel source 16.0.0.1
 tunnel mode ipsec ipv4
 tunnel destination 48.0.0.4
 tunnel protection ipsec profile DYNS_prof
 no tunnel protection ipsec initiate
 !
end
```

```
r1#sh interfaces virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of FastEthernet0/0 (16.0.0.1)
  MTU 17886 bytes, BW 100000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  CDMA vaccess, cloned from Virtual-Template100
  Vaccess status 0x4, loopback not set
  Keepalive not set
```

```
  Tunnel source 16.0.0.1, destination 38.0.0.3
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1446 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "DYNS_prof")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:26:04
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     145 packets input, 11776 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     145 packets output, 11800 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

```
r1#sh interfaces virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of FastEthernet0/0 (16.0.0.1)
  MTU 17886 bytes, BW 100000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  CDMA vaccess, cloned from Virtual-Template100
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 16.0.0.1, destination 48.0.0.4
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1446 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "DYNS_prof")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:26:24
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     151 packets input, 12216 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     154 packets output, 12496 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

```
r1#sh interfaces virtual-template 100
Virtual-Template100 is up, line protocol is down
  Hardware is Virtual Template interface
  Interface is unnumbered. Using address of FastEthernet0/0 (16.0.0.1)
  MTU 17940 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source UNKNOWN
  Tunnel protocol/transport IPSEC/IP
```

```
  Tunnel TTL 255
  Tunnel transport MTU 1500 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "DYNS_prof")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

```
r1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
16.0.0.1     48.0.0.4           QM_IDLE           1004 ACTIVE
16.0.0.1     38.0.0.3           QM_IDLE           1003 ACTIVE
```

```
r1#sh crypto ipsec sa

interface: Virtual-Access3
    Crypto map tag: Virtual-Access3-head-0, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 16.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 102, #pkts encrypt: 102, #pkts digest: 102
    #pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 48.0.0.4
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x45D46AA8(1171548840)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x36936087(915628167)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 9, flow_id: SW:9, sibling_flags 80000046, crypto map:
Virtual-Access3-head-0
        sa timing: remaining key lifetime (k/sec): (4421081/2723)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
     inbound pcp sas:

     outbound esp sas:
      spi: 0x45D46AA8(1171548840)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 10, flow_id: SW:10, sibling_flags 80000046, crypto map:
Virtual-Access3-head-0
        sa timing: remaining key lifetime (k/sec): (4421081/2723)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 38.0.0.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 98, #pkts encrypt: 98, #pkts digest: 98
    #pkts decaps: 98, #pkts decrypt: 98, #pkts verify: 98
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 38.0.0.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x6069B058(1617539160)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCFBFAC2E(3485445166)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 11, flow_id: SW:11, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4518238/2732)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6069B058(1617539160)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 12, flow_id: SW:12, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4518238/2732)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

```
r1#sh crypto map

Crypto Map "Virtual-Access2-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }

Crypto Map "Virtual-Access2-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 38.0.0.3
        Extended IP access list
            access-list  permit ip any any
        Current peer: 38.0.0.3
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map Virtual-Access2-head-0:
                Virtual-Access2


Crypto Map "Virtual-Access3-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }

Crypto Map "Virtual-Template100-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }
        Interfaces using crypto map Virtual-Template100-head-0:
                Virtual-Template100
```

```
r1#sh crypto session
Crypto session current status

Interface: Virtual-Access3
Profile: IKE_prof
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKE SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Virtual-Access2
Profile: IKE_prof
```

```
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

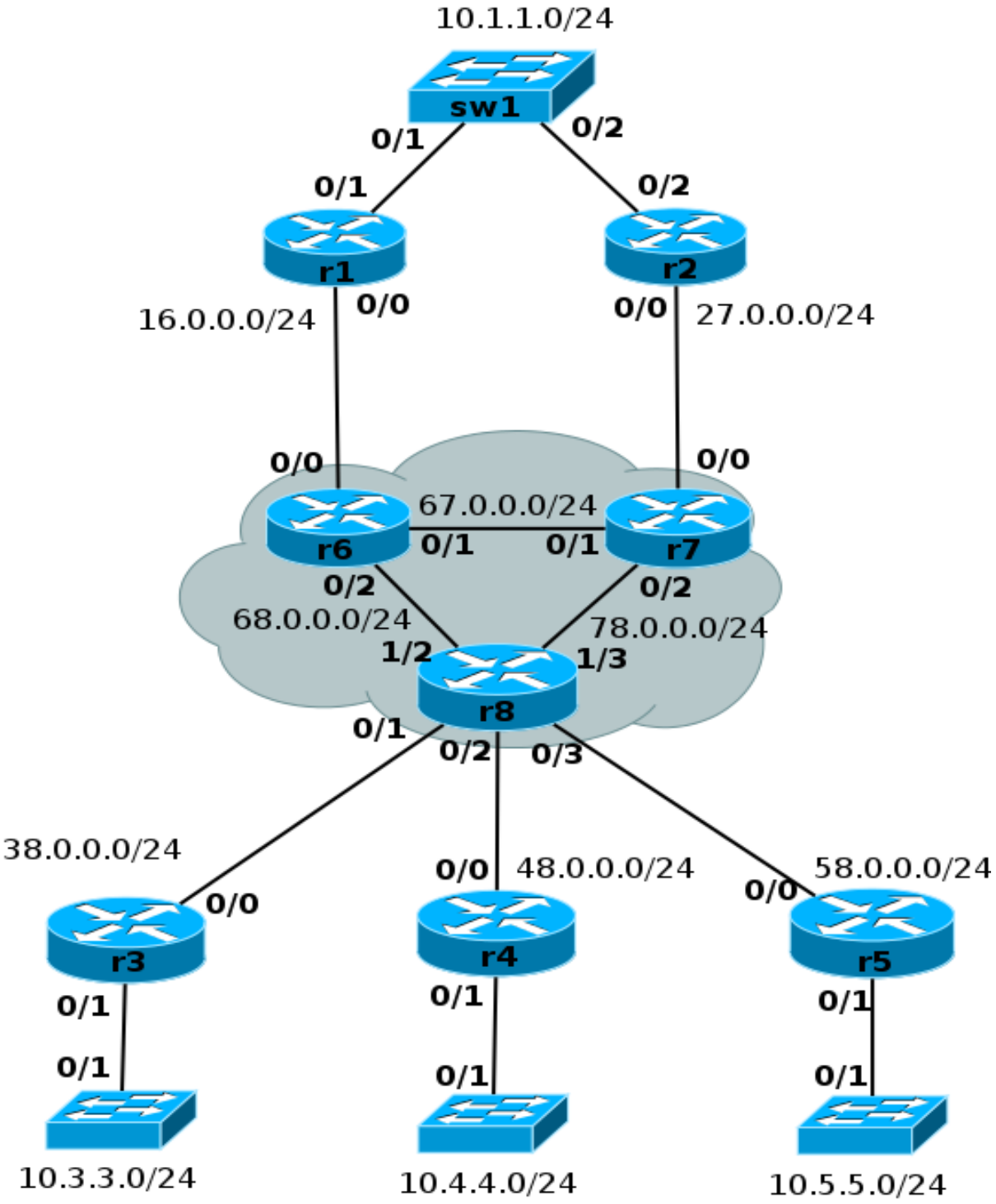
```
r1#sh crypto session detail

Interface: Virtual-Access3
Profile: IKE_prof
Uptime: 00:18:21
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 16.0.0.1
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:1003 lifetime:23:41:35
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 123 drop 0 life (KB/Sec) 4421078/2498
        Outbound: #pkts enc'ed 126 drop 0 life (KB/Sec) 4421078/2498

Interface: Virtual-Access2
Profile: IKE_prof
Uptime: 00:18:11
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 38.0.0.3
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1004 lifetime:23:41:38
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 121 drop 0 life (KB/Sec) 4518235/2508
        Outbound: #pkts enc'ed 122 drop 0 life (KB/Sec) 4518235/2508
```

```
r1#sh crypto ruleset
FastEthernet0/0:
 IP 10.1.1.0/24 10.3.3.0/24 IPSec Cryptomap
Virtual-Template100:
Virtual-Access3:
 IP ANY ANY IPSec SA
 IP ANY ANY IPSec Cryptomap
Virtual-Access2:
 IP ANY ANY IPSec SA
 IP ANY ANY IPSec Cryptomap
```

```
sw2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 600/817/900 ms
sw3#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 196/159/104 ms
```

Лабораторная 4. Настройка Site-to-site VPN с аутентификацией по сертификатам

Топология



Задание:

Настроить аутентификацию по сертификатам для существующих туннелей VPN

1. Проверить время на всех маршрутизаторах, которые будут участвовать в схеме аутентификации по сертификатам
2. Настроить центр сертификатов на маршрутизаторе r2.
   - 2.1 Задать имя домена
   - 2.2 Включить HTTP-сервер
   - 2.3 Сгенерировать пару ключей, которые будет использовать CA
   - 2.4 Включить CA-сервер
3. Выдать сертификаты маршрутизаторам r1, r3, r3 (процедура повторяется для каждого маршрутизатора)
   - 3.1 Проверить доступность CA
   - 3.2 Задать имя домена
   - 3.3 Сгенерировать пару ключей
   - 3.4 Настроить trustpoint
   - 3.5 Запросить сертификат CA
   - 3.6 Запросить сертификат для маршрутизатора
4. На CA r2 выдать сертификаты для r1, r3, r3
5. Выдать сертификат маршрутизатору, который работает как центр сертификатов
6. Настроить VPN для аутентификации по сертификатам
   - 6.1 Настроить политику IKE с аутентификацией по сертификатам
   - 6.2 Настроить certificate map
   - 6.3 Настроить isakmp profile
7. Проверить работу VPN

Пошаговая настройка:

Настроить аутентификацию по сертификатам для существующих туннелей VPN

1 Проверить время на всех маршрутизаторах, которые будут участвовать в схеме аутентификации по сертификатам

```
r1#sh clock
*07:41:54.451 UTC Sun May 15 2011
```

2 Настроить центр сертификатов на маршрутизаторе r2.

2.1 Задать имя домена

```
ip domain-name nt.ua
```

2.2 Включить HTTP-сервер

```
ip http server
```

2.3 Сгенерировать пару ключей, которые будет использовать центр сертификатов

```
crypto key generate rsa general-keys label CA

The name for the keys will be: CA

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
```

2.4 Включить CA-сервер

```
crypto pki server CA
 no shut

%Some server settings cannot be changed after CA certificate
generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.

*May 15 07:57:43.707: %PKI-6-CS_ENABLED: Certificate server now
enabled.
```

```
r2#sh crypto pki server
Certificate Server CA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=CA
    CA cert fingerprint: 358E298C A9F0A050 BAE2C427 565B6D8D
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 07:57:40 UTC May 14 2014
```

```
    CRL NextUpdate timer: 13:57:41 UTC May 15 2011
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

3 Выдать сертификаты маршрутизаторам r1, r3, r4 (процедура повторяется для каждого маршрутизатора)

3.1 Проверить доступность CA

```
r3#p 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 900/958/1192
ms
```

3.2 Сгенерировать пару ключей

```
crypto key generate rsa label VPN

The name for the keys will be: VPN
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
```

3.3 Настроить trustpoint

```
crypto pki trustpoint VPN
 enrollment url http://10.1.1.2
 subject-name CN=r3,OU=VPN,O=NT,C=UA
 rsakeypair VPN
 revocation-check none
```

3.4 Запросить сертификат CA

```
r3(config)#crypto pki authenticate VPN
Certificate has the following attributes:
       Fingerprint MD5: 358E298C A9F0A050 BAE2C427 565B6D8D
      Fingerprint SHA1: BBDC0448 32558328 8571B220 366161FA 644A6AAA

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
r3#sh crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
  Subject:
    cn=CA
  Validity Date:
    start date: 07:57:40 UTC May 15 2011
    end   date: 07:57:40 UTC May 14 2014
```

```
  Associated Trustpoints: VPN
```

3.5 Запросить сертификат для маршрутизатора

```
r3(config)#crypto pki enroll VPN
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the
configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=r3,OU=VPN,O=NT,C=UA
% The subject name in the certificate will include: r3
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose VPN' commandwill show the
fingerprint.


r3(config)#
*May 15 08:12:23.263: CRYPTO_PKI:  Certificate Request Fingerprint MD5:
5EB2051A E399854A 99ECCD40 D5511984
*May 15 08:12:23.275: CRYPTO_PKI:  Certificate Request Fingerprint SHA1:
9C996A46 5D0C3108 84990D54 717EE4B0 DDEFB2DD
r3(config)#
```

4 На CA r2 выдать сертификаты для r1, r3, r4

Проверить пришедшие запросы на CA:

```
r2#sh crypto pki server CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------

RA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------

Router certificates requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
3      pending    E8519FE28A463D706CDF5F4A149D0204
hostname=r1,cn=r1,ou=VPN,o=NT,c=UA
2      pending    04EFFDFD544338C3372ACD145205B446
hostname=r3,cn=r3,ou=VPN,o=NT,c=UA
1      pending    5EB2051AE399854A99ECCD40D5511984
hostname=r3,cn=r4,ou=VPN,o=NT,c=UA
```

Выдать всем сертификаты:

```
r2#crypto pki server CA grant all
```

```
r2#sh crypto pki server CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------------

RA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------------

Router certificates requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------------
3      granted    E8519FE28A463D706CDF5F4A149D0204
hostname=r1,cn=r1,ou=VPN,o=NT,c=UA
2      granted    04EFFDFD544338C3372ACD145205B446
hostname=r3,cn=r3,ou=VPN,o=NT,c=UA
1      granted    5EB2051AE399854A99ECCD40D5511984
hostname=r3,cn=r3,ou=VPN,o=NT,c=UA
```

На маршрутизаторах появится сообщение о том, что пришел сертификат:

```
*May 15 08:19:40.539: %PKI-6-CERTRET: Certificate received from
Certificate Authority
```

Полученный сертификат:

```
r3#sh crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: r3
    hostname=r3
    cn=r3
    ou=VPN
    o=NT
    c=UA
  Validity Date:
    start date: 08:17:26 UTC May 15 2011
    end   date: 08:17:26 UTC May 14 2012
  Associated Trustpoints: VPN

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
  Subject:
    cn=CA
  Validity Date:
```

```
    start date: 07:57:40 UTC May 15 2011
    end   date: 07:57:40 UTC May 14 2014
  Associated Trustpoints: VPN
```

5 Выдать сертификат маршрутизатору, который работает как центр сертификатов

Для того чтбоы выбать сертификат маршрутизатору, на котором находится CA, на нем необходимо сгенерировать ещё одну trustpoint (нельзя использовать автоматически созданную trustpoint):

```
crypto pki trustpoint I_CA
 enrollment url http://10.0.1.4
 subject-name CN=r2,OU=VPN,O=NT,C=UA
 revocation-check none
 rsakeypair I_CA
```

```
crypto pki authenticate I_CA
```

```
crypto pki enroll I_CA
```

6 Настроить VPN для аутентификации по сертификатам

6.1 Настроить политику IKE с аутентификацией по сертификатам

Исправить в существующей политике аутентификацию на сертификаты:

```
crypto isakmp policy 10
  authentication rsa-sig
```

6.2 Настроить certificate map

```
crypto pki certificate map DYNS_cert 10
 subject-name co ou = vpn
```

6.3 Настроить isakmp profile

```
crypto isakmp profile CERT
   match certificate DYNS_cert
   virtual-template 100
```

7 Проверить работу VPN

SA первой фазы (аутентификация по сертификатам):

```
r1#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote      I-VRF Status Encr Hash Auth DH Lifetime

1013  16.0.0.1     38.0.0.3             ACTIVE aes  sha  rsig 5  23:54:16
       Engine-id:Conn-id =  SW:13

1014  16.0.0.1     48.0.0.4             ACTIVE aes  sha  rsig 5  23:54:11
```

```
       Engine-id:Conn-id =  SW:14
```

```
r1#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access2
Profile: CERT
Uptime: 00:07:12
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: r3
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1013 lifetime:23:52:37
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 59 drop 0 life (KB/Sec) 4587198/3167
        Outbound: #pkts enc'ed 63 drop 0 life (KB/Sec) 4587198/3167

Interface: Virtual-Access3
Profile: CERT
Uptime: 00:07:11
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: r3
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:1014 lifetime:23:52:32
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 68 drop 0 life (KB/Sec) 4607077/3168
        Outbound: #pkts enc'ed 70 drop 0 life (KB/Sec) 4607077/3168
```

```
r1#show crypto isakmp profile


ISAKMP PROFILE CERT

Ref Count = 3
   Identities matched are:
   Certificate maps matched are:
      DYNS_cert
   keyring(s): <none>
   trustpoint(s): <all>
   virtual-template: 100
```

```
r1#sh crypto ipsec sa

interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 38.0.0.3 port 500
```

```
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 79, #pkts encrypt: 79, #pkts digest: 79
    #pkts decaps: 75, #pkts decrypt: 75, #pkts verify: 75
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 38.0.0.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xB2AA30A6(2997498022)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8093F349(2157179721)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4587196/3016)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB2AA30A6(2997498022)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4587196/3016)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Virtual-Access3
    Crypto map tag: Virtual-Access3-head-0, local addr 16.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 16.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 86, #pkts encrypt: 86, #pkts digest: 86
    #pkts decaps: 84, #pkts decrypt: 84, #pkts verify: 84
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 16.0.0.1, remote crypto endpt.: 16.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xE4A7D79(239762809)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xB607C1C9(3053961673)
        transform: esp-3des esp-sha-hmac ,
```

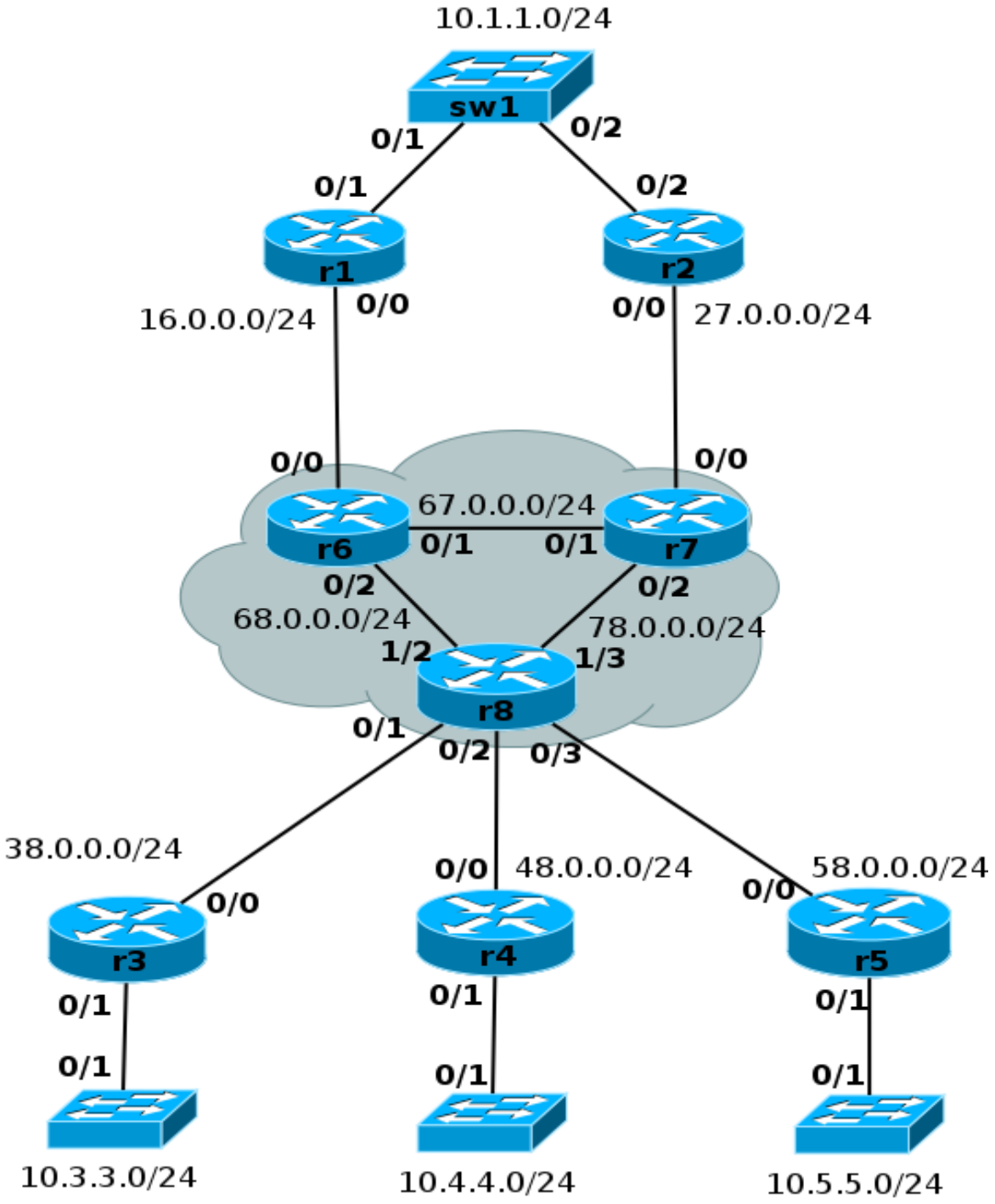
```
        in use settings ={Tunnel, }
        conn id: 19, flow_id: SW:19, sibling_flags 80000046, crypto map:
Virtual-Access3-head-0
        sa timing: remaining key lifetime (k/sec): (4607075/3016)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xE4A7D79(239762809)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 20, flow_id: SW:20, sibling_flags 80000046, crypto map:
Virtual-Access3-head-0
        sa timing: remaining key lifetime (k/sec): (4607075/3016)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

```
r1#sh crypto map

Crypto Map "Virtual-Access2-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }

Crypto Map "Virtual-Access2-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 38.0.0.3
        Extended IP access list
            access-list  permit ip any any
        Current peer: 38.0.0.3
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map Virtual-Access2-head-0:
                Virtual-Access2


Crypto Map "Virtual-Access3-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }

Crypto Map "Virtual-Access3-head-0" 65537 ipsec-isakmp
```

```
        Map is a PROFILE INSTANCE.
        Peer = 48.0.0.4
        Extended IP access list
            access-list  permit ip any any
        Current peer: 48.0.0.4
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map Virtual-Access3-head-0:
                Virtual-Access3


Crypto Map "Virtual-Template100-head-0" 65536 ipsec-isakmp
        Profile name: DYNS_prof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                DVTI:  { esp-3des esp-sha-hmac  } ,
        }
        Interfaces using crypto map Virtual-Template100-head-0:
                Virtual-Template100
```

Лабораторная 5. Настройка Site-to-site VPN с аутентификацией по сертификатам. Использование GRE-туннелей

Топология



Задание:

1 Настроить GRE-туннели

2 Настроить шифрование данных (два варианта)

2.1 Настроить и применить ipsec profile

2.2 Настроить и применить crypto map

3 Проверить работу VPN

3.1 С ipsec profile

3.2 С crypto map

Пошаговая настройка:

1 Настроить GRE-туннели

На r1:

```
interface Tunnel1
 ip address 10.0.13.1 255.255.255.0
 tunnel source 16.0.0.1
 tunnel destination 38.0.0.3
```

На r3:

```
interface Tunnel3
 ip address 10.0.13.3 255.255.255.0
 tunnel source 38.0.0.3
 tunnel destination 16.0.0.1
```

```
r3#sh interfaces tunnel 3
Tunnel23 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.13.3/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 38.0.0.3, destination 16.0.0.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:02, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     56 packets input, 6300 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     61 packets output, 6848 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

2 Настроить шифрование данных (два варианта)

2.1 Настроить и применить ipsec profile

Настройка ipsec profile (используется существующий transform-set) на r3 и r3:

```
crypto ipsec profile GRE_prof
 set transform-set DVTI
```

Применить ipsec profile к туннельному интерфейсу:

```
interface Tunnel3
 tunnel protection ipsec profile GRE_prof
```

2.2 Настроить и применить crypto map

ACL с указанием какой трафик необходимо шифровать на r1:

```
ip access-list extended GRE
 permit gre host 16.0.0.1 host 38.0.0.3
```

Зеркальный ACL на r3:

```
ip access-list extended GRE
  permit gre host 38.0.0.3 host 16.0.0.1
```

Настройка и применение crypto map на r1:

```
crypto map GRE 10 ipsec-isakmp
 set peer 38.0.0.3
 set transform-set DVTI
 match address GRE

interface fa0/0
 crypto map GRE
```

Настройка и применение crypto map на r3:

```
crypto map GRE 10 ipsec-isakmp
 set peer 16.0.0.1
 set transform-set DVTI
 match address GRE

interface fa0/0
 crypto map GRE
```

3 Проверить работу VPN

3.1 С ipsec profile

```
r1#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel23
Uptime: 00:10:30
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: r3
      Desc: (none)
  IKE SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1010 lifetime:23:49:18
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 68 drop 0 life (KB/Sec) 4476988/2969
        Outbound: #pkts enc'ed 68 drop 1 life (KB/Sec) 4476988/2969
```

3.2 С crypto map

```
r3#sh crypto session detail
```

```
Crypto session current status

Interface: FastEthernet0/0
Uptime: 00:01:48
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: r3
      Desc: (none)
  IKE SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
          Capabilities:(none) connid:1009 lifetime:23:56:35
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 23 drop 0 life (KB/Sec) 4383006/3491
        Outbound: #pkts enc'ed 21 drop 2 life (KB/Sec) 4383006/3491
```

Полная топология лабораторных работ