Настройка FlexVPN на маршрутизаторах Cisco

Наташа Самойленко

Сетевые Дни

Типы VPN в Cisco

Типы VPN в Cisco

Site-to-Site VPN:

- VPN с crypto-map
- Static VTI
- Dynamic VTI
- DMVPN
- **FlexVPN**

Remote VPN:

- EasyVPN*
- SSLVPN

FlexVPN

FlexVPN

FlexVPN объединяет в себе такие технологии:

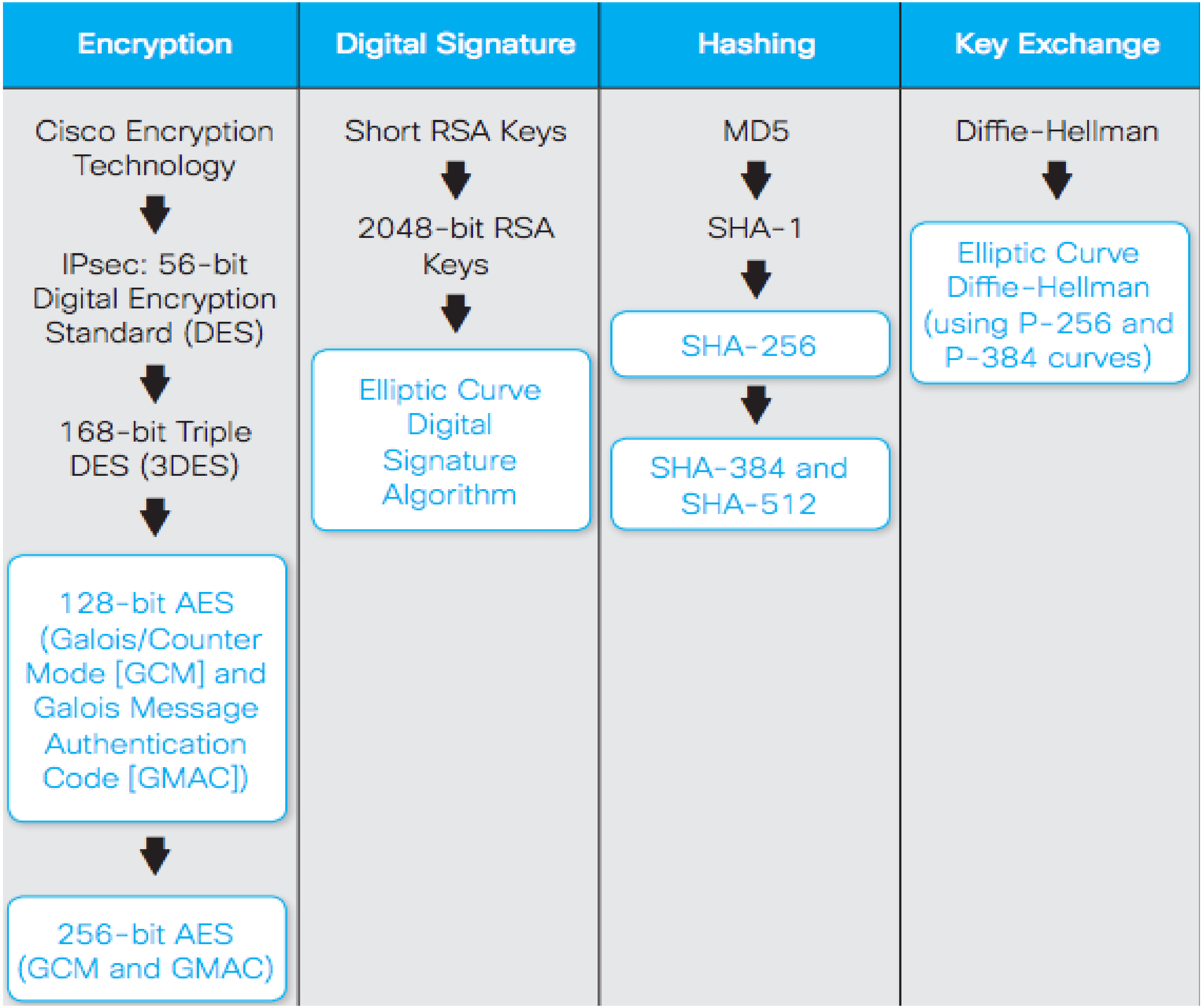
- Site-to-Site VPN
  - Совместимость с crypto-map
  - Совместимость с устройствами других вендоров
  - VTI или GRE туннель
- DMVPN
  - Топология Hub and Spoke (звезда)
  - Spoke-to-Spoke туннели
- Easy VPN
  - Клиент маршрутизатор (или ASA)
  - Клиент AnyConnect
- SSLVPN (ограничено и только на некоторых платформах)

Особенности FlexVPN

- **Работает только с IKEv2**
- Во FlexVPN используется новый синтаксис настройки, в котором объединены все варианты конфигурации
- Вместо X-AUTH используется EAP
- IKEv2 Smart defaults

Suite B

Suite B



Encryption

Cisco Encryption Technology

IPsec: 56-bit Digital Encryption Standard (DES)

168-bit Triple DES (3DES)

128-bit AES (Galois/Counter Mode [GCM] and Galois Message Authentication Code [GMAC])

256-bit AES (GCM and GMAC)

Digital Signature

Short RSA Keys

2048-bit RSA Keys

Elliptic Curve Digital Signature Algorithm

Hashing

MD5

SHA-1

SHA-256

SHA-384 and SHA-512

Key Exchange

Diffie-Hellman

Elliptic Curve Diffie-Hellman (using P-256 and P-384 curves)

IKEv2 Smart Defaults

IKEv2 Smart Defaults

```
r1#sh crypto ikev2 proposal
 IKEv2 proposal: default
     Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
     Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
     PRF        : SHA512 SHA384 SHA256 SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

```
r1#sh crypto ikev2 policy

 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
```

```
r1#sh crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

```
r1#sh crypto ipsec profile
IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

IKEv2 Smart Defaults

```
r1#sh run all | s crypto .* default

crypto ikev2 authorization policy default
 route set interface
 route accept any

crypto ikev2 proposal default
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1 md5
 group 5 2

crypto ikev2 policy default
 match fvrf any
 proposal default

crypto ipsec transform-set default esp-aes esp-sha-hmac
 mode tunnel

crypto ipsec profile default
```

IKEv2 Smart Defaults

Значения по умолчанию можно менять:

```
crypto ipsec transform-set default esp-aes 256 esp-
sha256-hmac
```

Восстановить значения в состояние по умолчанию (или восстановить удаленные объекты)

```
default crypto ipsec transform-set
```

Удалить объект:

```
no crypto ipsec transform-set default
```

Настройка Site-to-Site FlexVPN

Базовые настройки для R1

```
hostname kiev1
!
ip domain name xgu.ru
!
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 keyring KIEV-FIL_key
 peer LVV
  address 38.0.0.3
  pre-shared-key local FlexKeyForLVV
  pre-shared-key remote FlexKeyForKIEV
 !
 peer ODE
  address 48.0.0.4
  pre-shared-key local FlexKeyForODE
  pre-shared-key remote FlexKeyForKIEV

crypto ikev2 profile FIL_PROFILE
 match identity remote fqdn domain xgu.ru
 identity local fqdn kiev1.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV-FIL_key

crypto ipsec transform-set default esp-aes esp-sha-hmac
 mode transport

crypto ipsec profile FIL_VPN
 set ikev2-profile FIL_PROFILE
```

Настройки туннелей на R1

```
interface Tunnel3
 description IPsec p2p VPN to LVV
 ip address 10.0.3.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile FIL_VPN

interface Tunnel4
 description IPsec p2p VPN to ODE
 ip address 10.0.4.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 48.0.0.4
 tunnel protection ipsec profile FIL_VPN
```

Базовые настройки для R3

```
hostname lvv3
!
ip domain name xgu.ru
!
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 keyring KIEV_key
 peer KIEV
  address 16.0.0.1
  pre-shared-key local FlexKeyForKIEV
  pre-shared-key remote FlexKeyForLVV

crypto ikev2 profile KIEV_PROFILE
 match identity remote fqdn kiev1.xgu.ru
 identity local fqdn lvv3.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV_key

crypto ipsec transform-set default esp-aes esp-sha-hmac
 mode transport

crypto ipsec profile KIEV_VPN
 set ikev2-profile KIEV_PROFILE
```

Настройки туннеля на R3

```
interface Tunnel3
 description IPsec p2p VPN to KIEV
 ip address 10.0.3.3 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

Базовые настройки для R4

```
hostname ode4
!
ip domain name xgu.ru
!
interface FastEthernet0/0
 ip address 48.0.0.4 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.4.4.4 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 48.0.0.8
```

Настройки IPsec и IKEv2 для R4

```
crypto ikev2 keyring KIEV_key
 peer KIEV
  address 16.0.0.1
  pre-shared-key local FlexKeyForKIEV
  pre-shared-key remote FlexKeyForODE

crypto ikev2 profile KIEV_PROFILE
 match identity remote fqdn kiev1.xgu.ru
 identity local fqdn ode4.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV_key

crypto ipsec transform-set default esp-aes esp-sha-hmac
 mode transport

crypto ipsec profile KIEV_VPN
 set ikev2-profile KIEV_PROFILE
```

Настройки туннеля на R4

```
interface Tunnel3
 description IPsec p2p VPN to KIEV
 ip address 10.0.4.4 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

Проверка Site-to-Site FlexVPN

Проверка настроек на R1

```
kiev1#sh interfaces tunnel 3

Tunnel3 is up, line protocol is up
  Hardware is Tunnel
  Description: IPsec p2p VPN to LVV
  Internet address is 10.0.3.1/24
  MTU 17874 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 16.0.0.1 (Ethernet0/0), destination 38.0.0.3
   Tunnel Subblocks:
      src-track:
         Tunnel3 source tracking subblock associated with
FastEthernet0/0
          Set of tunnels with source FastEthernet0/0, 2 members
(includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "FIL_VPN")
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters 00:22:39
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 profile
```

```
IKEv2 profile: FIL_PROFILE
 Ref Count: 6
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn domain xgu.ru
  Certificate maps: none
 Local identity: fqdn kiev1.xgu.ru
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KIEV-FIL_key
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none
```

Проверка настроек на R1

```
kiev1#sh crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },


kiev1#sh crypto ipsec profile
IPSEC profile FIL_VPN
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf   Status
3         16.0.0.1/500          38.0.0.3/500          none/none   READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1443 sec

Tunnel-id Local                 Remote                fvrf/ivrf   Status
1         16.0.0.1/500          48.0.0.4/500          none/none   READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1442 sec
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 session
 IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local          Remote         fvrf/ivrf    Status
3         16.0.0.1/500   38.0.0.3/500   none/none    READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1446 sec
Child sa: local selector  16.0.0.1/0 - 16.0.0.1/65535
          remote selector 38.0.0.3/0 - 38.0.0.3/65535
          ESP spi in/out: 0x5ACB031C/0xCF694209

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local          Remote         fvrf/ivrf    Status
1         16.0.0.1/500   48.0.0.4/500   none/none    READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1445 sec
Child sa: local selector  16.0.0.1/0 - 16.0.0.1/65535
          remote selector 48.0.0.4/0 - 48.0.0.4/65535
          ESP spi in/out: 0x15B854A2/0x9144E2E2
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 session detailed
 IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
3         16.0.0.1/500          38.0.0.3/500          none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/1656 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 4A147BFD78D11999       Remote spi: 2507A27E9F40E957
      Local id: kiev1.xgu.ru
      Remote id: lvv3.xgu.ru
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  16.0.0.1/0 - 16.0.0.1/65535
          remote selector 38.0.0.3/0 - 38.0.0.3/65535
          ESP spi in/out: 0x5ACB031C/0xCF694209
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode transport
```

Проверка настроек на R1

```
kiev1#sh crypto session
Crypto session current status

Interface: Tunnel3
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map

Interface: Tunnel4
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map
```

Проверка настроек на R1

```
kiev1#sh crypto session detail
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: Tunnel3
Uptime: 00:29:55
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: lvv3.xgu.ru
      Desc: (none)
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:3 lifetime:23:30:05
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 395 drop 0 life (KB/Sec) 4252064/4294965502
        Outbound: #pkts enc'ed 396 drop 0 life (KB/Sec) 4252064/4294965502

Interface: Tunnel4
Uptime: 00:29:54
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: ode4.xgu.ru
      Desc: (none)
  IKEv2 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:1 lifetime:23:30:06
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 397 drop 0 life (KB/Sec) 4233738/1806
        Outbound: #pkts enc'ed 397 drop 0 life (KB/Sec) 4233738/1806
```

FlexVPN с dVTI
Базовая схема Hub-and-Spoke

Базовые настройки для R1

```
hostname kiev1
!
ip domain name xgu.ru
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy FIL
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 keyring KIEV-FIL_key
 peer LVV
  address 38.0.0.3
  pre-shared-key local FlexKeyForLVV
  pre-shared-key remote FlexKeyForKIEV

 peer ODE
  address 48.0.0.4
  pre-shared-key local FlexKeyForODE
  pre-shared-key remote FlexKeyForKIEV

 peer DNE
  address 58.0.0.5
  pre-shared-key local FlexKeyForDNE
  pre-shared-key remote FlexKeyForKIEV
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 profile FIL_PROFILE
 match identity remote fqdn domain xgu.ru
 identity local fqdn kiev1.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV-FIL_key
 virtual-template 1

crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile FIL_VPN
 set transform-set Suite-B
 set pfs group19
 set ikev2-profile FIL_PROFILE

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FIL_VPN
```

Базовые настройки для R3

```
hostname lvv3
!
ip domain name xgu.ru
!
interface Loopback3
 ip address 10.0.0.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy KIEV
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto ikev2 keyring KIEV_key
 peer KIEV
  address 16.0.0.1
  pre-shared-key local FlexKeyForKIEV
  pre-shared-key remote FlexKeyForLVV
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 profile KIEV_PROFILE
 match identity remote fqdn kiev1.xgu.ru
 identity local fqdn lvv3.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV_key

crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile KIEV_VPN
 set transform-set Suite-B
 set pfs group19
 set ikev2-profile KIEV_PROFILE

interface Tunnel3
 ip unnumbered Loopback3
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

Базовые настройки для R5

```
hostname dne5
!
ip domain name xgu.ru
!
interface FastEthernet0/0
 ip address 58.0.0.5 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.5.5.5 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 58.0.0.8
```

Настройки IPsec и IKEv2 для R5

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy KIEV
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto ikev2 keyring KIEV_key
 peer KIEV
  address 16.0.0.1
  pre-shared-key local FlexKeyForKIEV
  pre-shared-key remote FlexKeyForDNE
```

Настройки IPsec и IKEv2 для R5

```
crypto ikev2 profile KIEV_PROFILE
 match identity remote fqdn kiev1.xgu.ru
 identity local fqdn dne5.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV_key

crypto ipsec transform-set Suite-B esp-gcm

ip access-list extended KIEV_VPN
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255

crypto map KIEV 1 ipsec-isakmp
 set peer 16.0.0.1
 set transform-set Suite-B
 set pfs group19
 set ikev2-profile KIEV_PROFILE
 match address KIEV_VPN

interface FastEthernet0/0
 ip address 58.0.0.5 255.255.255.0
 crypto map KIEV
```

FlexVPN с dVTI

Проверка работы базовой схемы Hub-and-Spoke

Проверка настроек на R1

```
kiev1#sh interfaces virtual-template 1
Virtual-Template1 is up, line protocol is down
  Hardware is Virtual Template interface
  Interface is unnumbered. Using address of Loopback1 (10.0.0.1)
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 16.0.0.1 (Ethernet0/0)
   Tunnel Subblocks:
      src-track:
         Virtual-Template1 source tracking subblock associated with
FastEthernet0/0
          Set of tunnels with source FastEthernet0/0, 4 members
(includes iterators), on interface <OK>
  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 "FIL_VPN")
  Last input never, output never, output hang never
  ...
```

Проверка настроек на R1

```
kiev1#sh ip int brief
Interface                  IP-Address      OK? Method Status        Protocol
Ethernet0/0                16.0.0.1        YES NVRAM  up            up
Ethernet0/1                10.1.1.1        YES NVRAM  up            up
Loopback1                  10.0.0.1        YES NVRAM  up            up
Virtual-Access1            10.0.0.1        YES unset  up            up
Virtual-Access2            10.0.0.1        YES unset  up            up
Virtual-Access3            10.0.0.1        YES unset  up            up
Virtual-Template1          10.0.0.1        YES unset  up            down
```

```
kiev1#sh interfaces virtual-access 1 configuration
Virtual-Access1 is in use, but purpose is unknown

Derived configuration : 179 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback1
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile FIL_VPN
```

Проверка настроек на R1

```
Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (10.0.0.1)
  MTU 17886 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x0, loopback not set
  Keepalive not set
  Tunnel source 16.0.0.1 (Ethernet0/0), destination 38.0.0.3
   Tunnel Subblocks:
      src-track:
         Virtual-Access1 source tracking subblock associated with
FastEthernet0/0
          Set of tunnels with source FastEthernet0/0, 4 members
(includes iterators), on interface <OK>
  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 "FIL_VPN")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 02:21:19
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 profile
```

```
IKEv2 profile: FIL_PROFILE
 Ref Count: 9
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn domain xgu.ru
  Certificate maps: none
 Local identity: fqdn kiev1.xgu.ru
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KIEV-FIL_key
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: 1
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none
```

Проверка настроек на R1

```
kiev1#sh crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set Suite-B: { esp-gcm  }
   will negotiate = { Transport,  },

kiev1#sh crypto ipsec profile
IPSEC profile FIL_VPN
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group19
        Transform sets={
                Suite-B:  { esp-gcm  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote          fvrf/ivrf  Status
1         16.0.0.1/500    38.0.0.3/500  none/none  READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/8686 sec

Tunnel-id Local           Remote          fvrf/ivrf  Status
2         16.0.0.1/500    48.0.0.4/500  none/none  READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/8678 sec

Tunnel-id Local           Remote          fvrf/ivrf  Status
3         16.0.0.1/500    58.0.0.5/500  none/none  READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/7497 sec
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 session
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         16.0.0.1/500          38.0.0.3/500          none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/9691 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xF4D834B7/0x97798146

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                 Remote                fvrf/ivrf            Status
2         16.0.0.1/500          48.0.0.4/500          none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/9683 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x6B52EC0A/0xE1C429C8

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                 Remote                fvrf/ivrf            Status
3         16.0.0.1/500          58.0.0.5/500          none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/8502 sec
Child sa: local selector  10.0.0.0/0 - 10.255.255.255/65535
          remote selector 10.0.0.0/0 - 10.255.255.255/65535
          ESP spi in/out: 0xC5441582/0xD845A644
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 session detailed
 IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         16.0.0.1/500          38.0.0.3/500          none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/9886 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 5A47754F0CE14ABE       Remote spi: FE92E46D27CB7DA2
      Local id: kiev1.xgu.ru
      Remote id: lvv3.xgu.ru
      Local req msg id:  4              Remote req msg id:  2
      Local next msg id: 4              Remote next msg id: 2
      Local req queued:  4              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xF4D834B7/0x97798146
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: None
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Проверка настроек на R1

```
kiev1#sh crypto ikev2 session detailed (сосед с crypto map)
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
3         16.0.0.1/500          58.0.0.5/500          none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/8697 sec
      CE id: 1004, Session-id: 4
      Status Description: Negotiation done
      Local spi: AF6F1DDD20483C3D       Remote spi: 42C66272ADABF798
      Local id: kiev1.xgu.ru
      Remote id: dne5.xgu.ru
      Local req msg id:  4              Remote req msg id:  2
      Local next msg id: 4              Remote next msg id: 2
      Local req queued:  4              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  10.0.0.0/0 - 10.255.255.255/65535
          remote selector 10.0.0.0/0 - 10.255.255.255/65535
          ESP spi in/out: 0xC5441582/0xD845A644
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: None
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Проверка настроек на R1

```
kiev1#sh crypto session
Crypto session current status

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv2 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

Interface: Virtual-Access3
Session status: UP-ACTIVE
Peer: 58.0.0.5 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 58.0.0.5/500 Active
  IPSEC FLOW: permit ip 10.0.0.0/255.0.0.0 10.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 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
```

Особенности взаимодействия FlexVPN dVTI с crypto map

Проверка настроек на R1

```
kiev1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 16.0.0.6 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 16.0.0.6
      10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Virtual-Access3
C        10.0.0.1/32 is directly connected, Loopback1
D        10.0.0.3/32 [90/27008000] via 10.0.0.3, 03:03:39, Virtual-Access1
D        10.0.0.4/32 [90/27008000] via 10.0.0.4, 03:03:37, Virtual-Access2
C        10.1.1.0/24 is directly connected, FastEthernet0/1
L        10.1.1.1/32 is directly connected, FastEthernet0/1
D        10.3.3.0/24 [90/26905600] via 10.0.0.3, 03:03:39, Virtual-Access1
D        10.4.4.0/24 [90/26905600] via 10.0.0.4, 03:03:37, Virtual-Access2
      16.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        16.0.0.0/24 is directly connected, FastEthernet0/0
L        16.0.0.1/32 is directly connected, FastEthernet0/0
```

Проверка настроек на R1

```
kiev1#sh ip route 10.0.0.0 255.0.0.0
Routing entry for 10.0.0.0/8
  Known via "static", distance 1, metric 0 (connected)
  Redistributing via eigrp 1
  Advertised by eigrp 1
  Routing Descriptor Blocks:
  * directly connected, via Virtual-Access3
      Route metric is 0, traffic share count is 1

kiev1#sh crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
10.0.0.0/255.0.0.0 [1/0] via 58.0.0.5 tag 0 count 1 rtid 3
                                on Virtual-Access3 RRI
```

Проверка настроек на R1

```
dne5#sh crypto map
Crypto Map IPv4 "KIEV" 1 ipsec-isakmp
        Peer = 16.0.0.1
        IKEv2 Profile: KIEV_PROFILE
        Extended IP access list KIEV_VPN
            access-list KIEV_VPN permit ip 10.0.0.0
0.255.255.255 10.0.0.0 0.255.255.255
        Current peer: 16.0.0.1
        Security association lifetime: 4608000 kilobytes/3600
seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group19
        Transform sets={
                Suite-B:  { esp-gcm  } ,
        }
        Interfaces using crypto map KIEV:
                FastEthernet0/0
```

Hub-and-Spoke FlexVPN

Аутентификация по сертификатам

Базовые настройки для R1

```
hostname kiev1
!
ip domain name xgu.ru
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy FIL
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto pki trustpoint CERT
 enrollment url http://10.0.0.2:80
 subject-name OU=KIEV, O=xgu.ru, CN=kiev1.xgu.ru
 revocation-check none
 source interface Loopback1
 rsakeypair KeyForCERT

crypto pki authenticate CERT
crypto pki enroll CERT
```

Настройки IPsec и IKEv2 для R1

```
crypto pki certificate map FIL 1
 issuer-name eq cn = kievca
 subject-name co o = xgu.ru

crypto ikev2 profile IKEv2_CERT
 match certificate FIL
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint CERT
 virtual-template 1
```

Настройки IPsec и IKEv2 для R1

```
crypto ipsec transform-set Suite-B esp-gcm
 mode transport

crypto ipsec profile FIL_VPN
 set transform-set Suite-B
 set ikev2-profile IKEv2_CERT

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FIL_VPN
```

Базовые настройки для R3

```
hostname lvv3
!
ip domain name xgu.ru
!
interface Loopback3
 ip address 10.0.0.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy KIEV
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto pki trustpoint CERT
 enrollment url http://10.0.0.2:80
 subject-name OU=KIEV, O=xgu.ru, CN=lvv3.xgu.ru
 revocation-check none
 source interface Loopback1
 rsakeypair KeyForCERT

crypto pki authenticate CERT
crypto pki enroll CERT
```

Настройки IPsec и IKEv2 для R3

```
crypto pki certificate map KIEV 1
 issuer-name eq cn = kievca
 subject-name co o = xgu.ru

crypto ikev2 profile IKEv2_CERT
 match certificate KIEV
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint CERT

crypto ipsec transform-set Suite-B esp-gcm
 mode transport

crypto ipsec profile KIEV_VPN
 set transform-set Suite-B
 set ikev2-profile KIEV_PROFILE

interface Tunnel3
 ip unnumbered Loopback3
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

Hub-and-Spoke FlexVPN

Spoke-to-spoke туннели FlexVPN

DMVPN Phase 4

Базовые настройки для R1 (Hub)

```
hostname kiev1
!
ip domain name xgu.ru
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Настройки IPsec и IKEv2 для R1 (Hub)

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy FIL
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto ikev2 keyring KEYRING
 peer FLEXVPN
  address 0.0.0.0 0.0.0.0
  identity address 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
```

Настройки IPsec и IKEv2 для R1 (Hub)

```
crypto ikev2 profile IKEV2-PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring KEYRING
 virtual-template 1

crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile FlexVPN
 set transform-set Suite-B
 set pfs group19
 set ikev2-profile IKEV2-PROFILE

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip nhrp network-id 100
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel protection ipsec profile FlexVPN
```

Базовые настройки для R3 (Spoke)

```
hostname lvv3
!
ip domain name xgu.ru
!
interface Loopback3
 ip address 10.0.0.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

Настройки IPsec и IKEv2 для R3 (Spoke)

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy KIEV
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto ikev2 keyring KEYRING
 peer FLEXVPN
  address 0.0.0.0 0.0.0.0
  identity address 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
```

Настройки IPsec и IKEv2 для R3 (Spoke)

```
crypto ikev2 profile IKEV2-PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring KEYRING
 virtual-template 1

crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile FlexVPN
 set transform-set Suite-B
 set pfs group19
 set ikev2-profile IKEV2-PROFILE

interface Tunnel0
 ip unnumbered Loopback3
 ip nhrp network-id 100
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile FlexVPN

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback3
 ip nhrp network-id 100
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel protection ipsec profile FlexVPN
```

Проверка

Spoke-to-spoke туннели FlexVPN

DMVPN Phase 4

Проверка IPsec и IKEv2 на R1 (Hub)

```
kiev1#sh crypto session
Crypto session current status

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map

Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 58.0.0.5 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 58.0.0.5/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 58.0.0.5
        Active SAs: 2, origin: crypto map

Interface: Virtual-Access3
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map
```

Проверка IPsec и IKEv2 на R3 (Spoke)

```
lvv3#sh crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
```

Проверка IPsec и IKEv2 на R3 (Spoke)

```
lvv3#ping 10.4.4.4 source 10.3.3.3 repeat 30
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.3
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (30/30), round-trip min/avg/max = 5/10/23 ms

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.4 (Virtual-Access1) is
up: new adjacency

lvv3#sh crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 48.0.0.4
        Active SAs: 2, origin: crypto map
```

Проверка IPsec и IKEv2 на R3 (Spoke)

```
lvv3#sh ip nhrp shortcut
10.0.0.4/32 via 10.0.0.4
   Virtual-Access1 created 00:01:21, expire 01:58:38
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 48.0.0.4

lvv3#sh ip route eigrp

D       10.0.0.1/32 [90/27008000] via 10.0.0.1, 00:02:47, Tunnel0
D       10.0.0.2/32 [90/27033600] via 10.0.0.1, 00:02:47, Tunnel0
D       10.0.0.4/32 [90/27008000] via 10.0.0.4, 00:02:47, Virtual-Access1
D       10.0.0.5/32 [90/28288000] via 10.0.0.1, 00:02:47, Tunnel0
D       10.1.1.0/24 [90/26905600] via 10.0.0.1, 00:02:47, Tunnel0
D       10.3.10.0/24 [90/409600] via 10.3.3.12, 00:02:47, Ethernet0/1
D       10.3.20.0/24 [90/409600] via 10.3.3.12, 00:02:47, Ethernet0/1
D       10.3.30.0/24 [90/409600] via 10.3.3.12, 00:02:47, Ethernet0/1
D       10.4.4.0/24 [90/26905600] via 10.0.0.4, 00:02:47, Virtual-Access1
D       10.5.5.0/24 [90/28185600] via 10.0.0.1, 00:02:47, Tunnel0

lvv3#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address          Interface        Hold Uptime   SRTT   RTO  Q  Seq
                                      (sec)         (ms)       Cnt Num
2   10.0.0.4         Vi1                11 00:04:03   31  1470  0  9
1   10.0.0.1         Tu0                13 00:04:49   17  1470  0  19
0   10.3.3.12        Et0/1              12 00:04:59    5   100  0  352
```

FlexVPN Client

Базовые настройки для R1

```
hostname kiev1
!
ip domain name xgu.ru
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

Настройки IPsec и IKEv2 для R1

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy FIL
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto pki trustpoint CERT
 enrollment url http://10.0.0.2:80
 subject-name OU=KIEV, O=xgu.ru, CN=kiev1.xgu.ru
 revocation-check none
 source interface Loopback1
 rsakeypair KeyForCERT
```

Настройки IPsec и IKEv2 для R1

```
aaa new-model
aaa authorization network LOCAL_LIST local

crypto ikev2 name-mangler FIL
 dn organization-unit

crypto ikev2 authorization policy LVV
 pool POOL_LVV

crypto pki certificate map FIL 1
 issuer-name eq cn = kievca
 subject-name co o = xgu.ru

crypto ikev2 profile IKEv2_CERT
 match certificate FIL
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint CERT
 aaa authorization group cert LOCAL_LIST name-mangler FIL
 virtual-template 1

ip local pool POOL_LVV 192.168.1.1 192.168.1.10
```

Настройки IPsec и IKEv2 для R1

```
crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile FIL_VPN
 set transform-set Suite-B
 set ikev2-profile IKEv2_CERT

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FIL_VPN

router eigrp 1
 network 10.0.0.0
```

Базовые настройки для R3

```
hostname lvv3
!
ip domain name xgu.ru
!
interface Loopback3
 ip address 10.0.0.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 proposal Suite-B_proposal1
 encryption aes-cbc-128
 integrity sha256
 group 19

crypto ikev2 proposal Suite-B_proposal2
 encryption aes-cbc-256
 integrity sha384
 group 20

crypto ikev2 policy KIEV
 match fvrf any
 proposal Suite-B_proposal1
 proposal Suite-B_proposal2

crypto pki trustpoint CERT
 enrollment url http://10.1.1.2:80
 subject-name OU=LVV, O=xgu.ru, CN=lvv3.xgu.ru
 revocation-check none
 source interface Ethernet0/1
 rsakeypair KeyForCERT
```

Настройки IPsec и IKEv2 для R3

```
crypto pki certificate map KIEV 1
 subject-name co ou = kiev
 issuer-name eq cn = kievca

crypto ikev2 profile IKEv2_CERT
 match certificate KIEV
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint CERT
 config-mode set

crypto ikev2 client flexvpn FLEX
  peer 1 16.0.0.1
  client connect Tunnel3

crypto ipsec transform-set Suite-B esp-gcm

crypto ipsec profile KIEV_VPN
 set transform-set Suite-B
 set ikev2-profile KIEV_PROFILE

interface Tunnel3
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile VPN
```

Настройки IPsec и IKEv2 для R3

```
crypto ikev2 profile KIEV_PROFILE
 match identity remote fqdn kiev1.xgu.ru
 identity local fqdn lvv3.xgu.ru
 authentication remote pre-share
 authentication local pre-share
 keyring KIEV_key

crypto ipsec transform-set Suite-B esp-gcm
 mode transport

crypto ipsec profile KIEV_VPN
 set transform-set Suite-B
 set ikev2-profile KIEV_PROFILE

interface Tunnel3
 ip unnumbered Loopback3
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

Настройка FlexVPN на маршрутизаторах Cisco

Автор курса: Наташа Самойленко
nataliya.samoylenko@gmail.com

Сетевые Дни