# IKEv2

**Наташа Самойленко**

***Сетевые Дни***

# 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
```

# IKEv2 Pre-shared

# 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 Ethernet0/0
 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 Ethernet0/0
 tunnel destination 48.0.0.4
 tunnel protection ipsec profile FIL_VPN
```

# Проверка Site-to-Site FlexVPN

# 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 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
```

# IKEv2 (pre-shared)
# Site-to-Site FlexVPN c dVTI

# Настройки Ipsec и IKEv2 для R1 (dVTI)

```
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 (dVTI)

```
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 (dVTI)

```
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
 mode transport

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 Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FIL_VPN
```

# Настройки Ipsec и IKEv2 для R3 (VTI)

```
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 (VTI)

```
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 pfs group19
 set ikev2-profile KIEV_PROFILE

interface Tunnel3
 ip unnumbered Loopback3
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile KIEV_VPN
```

# Настройки Ipsec и IKEv2 для R5 (crypto map)

```
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 map)

```
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
 mode transport

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 Ethernet0/0
 ip address 58.0.0.5 255.255.255.0
 crypto map KIEV
```

# IKEv2 (pre-shared)
# Проверка Site-to-Site FlexVPN с dVTI

# 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 Ethernet0/0
 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 
Ethernet0/0
          Set of tunnels with source Ethernet0/0, 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
```

# Аутентификация по сертификатам с IKEv2

# IKEv2 (аутентификация по сертификатам)

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

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

crypto ipsec profile VPN_CERT
 set ikev2-profile IKEv2_CERT

interface Tunnel1
 ip address 10.255.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile VPN_CERT
```

# IKEv2 (аутентификация по сертификатам)

```
kiev1#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: Tunnel1
Uptime: 00:00:00
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: hostname=lvv3.xgu.ru,ou=LVV,o=xgu.ru,cn=lvv3.xgu.ru
      Desc: (none)
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:2 lifetime:23:59:31
  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 13 drop 0 life (KB/Sec)
4239189/4294967267
        Outbound: #pkts enc'ed 13 drop 0 life (KB/Sec)
4239189/4294967267
```

# IKEv2 (аутентификация по сертификатам)

```
kiev1#sh crypto ikev2 profile

IKEv2 profile: IKEv2_CERT
 Ref Count: 5
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities: none
  Certificate maps:
   LVV
 Local identity: DN
 Remote identity: none
 Local authentication method: rsa-sig
 Remote authentication method(s): rsa-sig
 EAP options: none
 Keyring: none
 Trustpoint(s):
  CERT
 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
```

# IKEv2 (аутентификация по сертификатам)

```
lvv3#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         38.0.0.3/500  16.0.0.1/500   none/none   READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign:
RSA, Auth verify: RSA
      Life/Active Time: 86400/132 sec
      CE id: 1002, Session-id: 1
      Status Description: Negotiation done
      Local spi: 6EF1E066801E882A       Remote spi: A1AFFF5D7623F3F8
      Local id: hostname=lvv3.xgu.ru,ou=LVV,o=xgu.ru,cn=lvv3.xgu.ru
      Remote id: hostname=kiev1.xgu.ru,ou=KIEV,o=xgu.ru,cn=kiev1.xgu.ru
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      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 : Yes
      ...
```

# IKEv2

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