# PKI в Cisco

**Наташа Самойленко**

***Сетевые Дни***

# Настройка CA на маршрутизаторе Cisco

# Настройка CA на маршрутизаторе Cisco

```
hostname kiev2
ip domain name xgu.ru
ip http server

crypto key generate rsa label KievCA
The name for the keys will be: KievCA
Choose the size of the key modulus in the range of 360 to 4096
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...
[OK] (elapsed time was 3 seconds)
```

# Настройка CA на маршрутизаторе Cisco

```
crypto pki server KievCA
 issuer-name cn=KievCA
 lifetime certificate 365
 lifetime ca-certificate 1095
 hash sha256
 no shutdown

%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:

% Certificate Server enabled.
```

# Настройка CA на маршрутизаторе Cisco

```
kiev2#show crypto pki server
Certificate Server KievCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: cn=KievCA
    CA cert fingerprint: 3DE6A0CA 66D97547 F610939B D9B61888
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 11:02:12 UTC Jul 25 2018
    CRL NextUpdate timer: 17:02:12 UTC Jul 26 2015
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage

kiev2#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=KievCA
  Subject:
    cn=KievCA
  Validity Date:
    start date: 11:02:12 UTC Jul 26 2015
    end   date: 11:02:12 UTC Jul 25 2018
  Associated Trustpoints: KievCA
```

# Настройка CA на маршрутизаторе Cisco

```
kiev1#dir nvram:
Directory of nvram:/

   89  -rw-        2078                    <no date>  startup-config
   90  ----        3552                    <no date>  private-config
    1  ----          23                    <no date>  persistent-data
    2  -rw-          17                    <no date>  ecfm_ieee_mib
    3  -rw-          32                    <no date>  KievCA.ser
    4  -rw-         346                    <no date>  KievCA.crl
    5  -rw-         772                    <no date>  KievCA#1CA.cer

98304 bytes total (87502 bytes free)
```

# Получение сертификата от Cisco IOS CA

# Настройка маршрутизатора

```
hostname kiev1
ip domain name xgu.ru

crypto key generate rsa label KeyForCERT
The name for the keys will be: KeyForCERT
Choose the size of the key modulus in the range of 360 to 4096 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...
[OK] (elapsed time was 2 seconds)

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
 hash sha256
```

# Настройка маршрутизатора

```
kiev1#sh crypto pki trustpoints
Trustpoint CERT:

kiev1#sh crypto pki trustpoints status
Trustpoint CERT:
  Issuing CA certificate not configured.
  State:
    Keys generated ............. Yes (General Purpose, non-exportable)
    Issuing CA authenticated ....... No
    Certificate request(s) ..... None
```

# Получение сертификата CA

```
kiev1(config)#crypto pki authenticate CERT
Certificate has the following attributes:
       Fingerprint MD5: 3DE6A0CA 66D97547 F610939B D9B61888
      Fingerprint SHA1: B8C5CBEC 68E280BA 589299CE BC55F96B 9E68C1B9

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

```
kiev1#sh crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=KievCA
  Subject:
    cn=KievCA
  Validity Date:
    start date: 11:02:12 UTC Jul 26 2015
    end   date: 11:02:12 UTC Jul 25 2018
  Associated Trustpoints: CERT
```

# Запрос на получение сертификата для маршрутизатора

```
kiev1(config)#crypto pki enroll CERT
%
% 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: OU=KIEV, O=xgu.ru,
CN=kiev1.xgu.ru
% The subject name in the certificate will include: kiev1.xgu.ru
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CERT' commandwill show the
fingerprint.

CRYPTO_PKI:  Certificate Request Fingerprint MD5: 75D67718 40DC49A2
34CF6016 F51CBDEF
CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 490155D0 4DF06449
C6D6BA54 6FF38E03 1D92F7EC
```

# Выдача сертификата на CA

```
kiev2#sh crypto pki server KievCA requests
Enrollment Request Database:

Router certificates requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
1      pending    75D6771840DC49A234CF6016F51CBDEF
hostname=kiev1.xgu.ru,ou=KIEV,o=xgu.ru,cn=kiev1.xgu.ru

kiev2#crypto pki server KievCA grant 1

kiev2#sh crypto pki server KievCA requests
Enrollment Request Database:

Router certificates requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
1      granted    75D6771840DC49A234CF6016F51CBDEF
hostname=kiev1.xgu.ru,ou=KIEV,o=xgu.ru,cn=kiev1.xgu.ru
```

# Выдача сертификата на CA

```
kiev1#
*Jul 26 11:54:28.499: %PKI-6-CERTRET: Certificate received from
Certificate Authority


kiev1#show crypto pki certificate
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=KievCA
  Subject:
    Name: kiev1.xgu.ru
    hostname=kiev1.xgu.ru
    ou=KIEV
    o=xgu.ru
    cn=kiev1.xgu.ru
  Validity Date:
    start date: 11:54:13 UTC Jul 26 2015
    end   date: 11:54:13 UTC Jul 25 2016
  Associated Trustpoints: CERT
```

# Аутентификация по сертификатам

# Базовая аутентификация по сертификатам с IKEv1 (ISAKMP)

# Crypto map

# IKEv1 и crypto map

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 19
 authentication rsa-sig

ip access-list extended VPN1
 permit ip 10.3.0.0 0.0.255.255 10.4.0.0 0.0.255.255

crypto ipsec transform-set Suite-B_VPN esp-gcm
 mode tunnel

crypto map VPN 1 ipsec-isakmp
 set peer 48.0.0.4
 set transform-set Suite-B_VPN
 set pfs group19
 match address VPN1

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto map VPN
```

# IKEv1 и crypto map

```
ode4#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 Cap.

1003 48.0.0.4  38.0.0.3        ACTIVE aes  sha256 rsig 19 23:59:18
       Engine-id:Conn-id =  SW:3
```

# IKEv1 и crypto map (debug initiator)

```
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash SHA256
ISAKMP:      default group 19
ISAKMP:      auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80


ISAKMP:(1001): peer wants cert issued by cn=KievCA
 Choosing trustpoint CERT as issuer

ISAKMP:(1001):My ID configured as IPv4 Addr, but Addr not in Cert!
ISAKMP:(1001):Using FQDN as My ID
ISAKMP:(1001):SA is doing RSA signature authentication using id type
ID_FQDN
ISAKMP (1001): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : ode4.xgu.ru
        protocol     : 17
        port         : 500
        length       : 19
```

# IKEv1 и crypto map (debug initiator)

```
ISAKMP:(1001):Total payload length: 19
ISAKMP:(1001): IKE->PKI Get CertificateChain to be sent to peer state
(I) MM_KEY_EXCH (peer 38.0.0.3)
ISAKMP:(1001): PKI->IKE Got CertificateChain to be sent to peer state
(I) MM_KEY_EXCH (peer 38.0.0.3)
ISAKMP (1001): constructing CERT payload for
hostname=ode4.xgu.ru,ou=ODE,o=xgu.ru,cn=ode4.xgu.ru
ISAKMP:(1001): using the CERT trustpoint's keypair to sign
ISKAMP: growing send buffer from 1024 to 3072
ISAKMP:(1001): sending packet to 38.0.0.3 my_port 500 peer_port 500 (I)
MM_KEY_EXCH
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1001):Old State = IKE_I_MM4  New State = IKE_I_MM5

ISAKMP (1001): received packet from 38.0.0.3 dport 500 sport 500 Global
(I) MM_KEY_EXCH
ISAKMP:(1001): processing ID payload. message ID = 0
ISAKMP (1001): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : lvv3.xgu.ru
        protocol     : 17
        port         : 500
        length       : 19
```

# IKEv1 и crypto map (debug initiator)

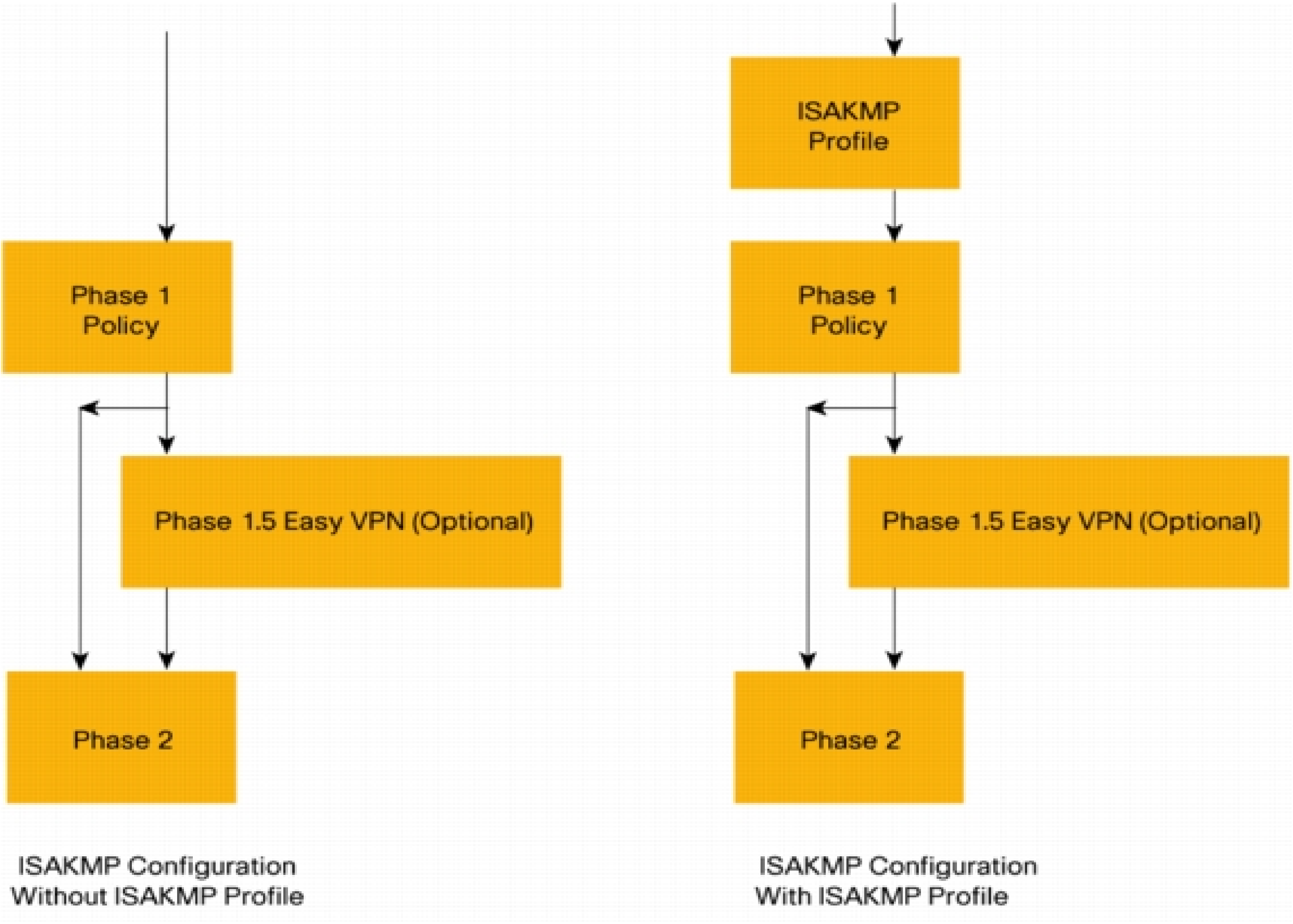
```
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1001): processing CERT payload. message ID = 0
ISAKMP:(1001): processing a CT_X509_SIGNATURE cert
ISAKMP:(1001): IKE->PKI Add peer's certificate state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): PKI->IKE Added peer's certificate state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): IKE->PKI Get PeerCertificateChain state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): PKI->IKE Got PeerCertificateChain state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): peer's pubkey isn't cached
ISAKMP:(1001): IKE->PKI Validate certificate chain state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): PKI->IKE Validate certificate chain state (I) MM_KEY_EXCH
(peer 38.0.0.3)
ISAKMP:(1001): OU = LVV


ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1001): processing SIG payload. message ID = 0
ISAKMP:(1001):SA authentication status:
        authenticated
ISAKMP:(1001):SA has been authenticated with 38.0.0.3
ISAKMP: Trying to insert a peer 48.0.0.4/38.0.0.3/500/,  and inserted
successfully F2671888.
```

# IKEv1 аутентификация по сертификатам с ISAKMP profile

# Crypto map

# ISAKMP (IKEv1) profile



ISAKMP Configuration Without ISAKMP Profile

ISAKMP Configuration With ISAKMP Profile

# IKEv1 и crypto map

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

crypto isakmp profile CERT_ODE
   ca trust-point CERT
   match identity host domain xgu.ru
   match certificate ODE

crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 19
 authentication rsa-sig

ip access-list extended VPN1
 permit ip 10.3.0.0 0.0.255.255 10.4.0.0 0.0.255.255

crypto map VPN 1 ipsec-isakmp
 set peer 48.0.0.4
 set transform-set Suite-B_VPN
 set pfs group19
 set isakmp-profile CERT_ODE
 match address VPN1

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto map VPN
```

# IKEv1 и crypto map

```
lvv3#sh crypto isakmp profile

IKEv1 PROFILE CERT_ODE
Ref Count = 3
   Identities matched are:
    domain xgu.ru
   Certificate maps matched are:
      ODE
   keyring(s): <none>
   trustpoint(s): CERT
```

```
lvv3#sh crypto map
Crypto Map IPv4 "VPN" 1 ipsec-isakmp
        Peer = 48.0.0.4
        ISAKMP Profile: CERT_ODE
        Extended IP access list VPN1
            access-list VPN1 permit ip 10.3.0.0 0.0.255.255 10.4.0.0
0.0.255.255
        Current peer: 48.0.0.4
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group19
        Transform sets={
                Suite-B_VPN:  { esp-gcm  } ,
        }
        Interfaces using crypto map VPN:
                Ethernet0/0
```

# Базовая аутентификация по сертификатам с IKEv1 (ISAKMP)

# VTI tunnel

# IKEv1 и VTI tunnel

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 19
 authentication rsa-sig

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

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

interface Tunnel3
 ip address 10.255.0.3 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 48.0.0.4
 tunnel protection ipsec profile KIEV_VPN
```

# IKEv1 аутентификация по сертификатам с ISAKMP profile

# VTI tunnel

# IKEv1 и VTI tunnel

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

crypto isakmp profile CERT_ODE
   ca trust-point CERT
   match identity host domain xgu.ru
   match certificate ODE

crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 19
 authentication rsa-sig

crypto ipsec profile KIEV_VPN
 set transform-set Suite-B
 set pfs group19
 set isakmp-profile CERT_ODE

interface Tunnel3
 ip address 10.255.0.3 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 48.0.0.4
 tunnel protection ipsec profile KIEV_VPN
```

# IKEv1 и VTI tunnel

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

Interface: Tunnel3
Profile: CERT_ODE
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv1 SA: local 38.0.0.3/500 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: 4, origin: crypto map
```

# Аутентификация по сертификатам с IKEv2

# IKEv2 и VTI tunnel

```
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 и VTI tunnel

```
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 и VTI tunnel

```
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 и VTI tunnel

```
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
      ...
```

# PKI в Cisco

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

*Сетевые Дни*