Настройка Site-to-Site VPN 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
- EasyVPN*
- FlexVPN

Remote VPN:

- EasyVPN*
- SSLVPN

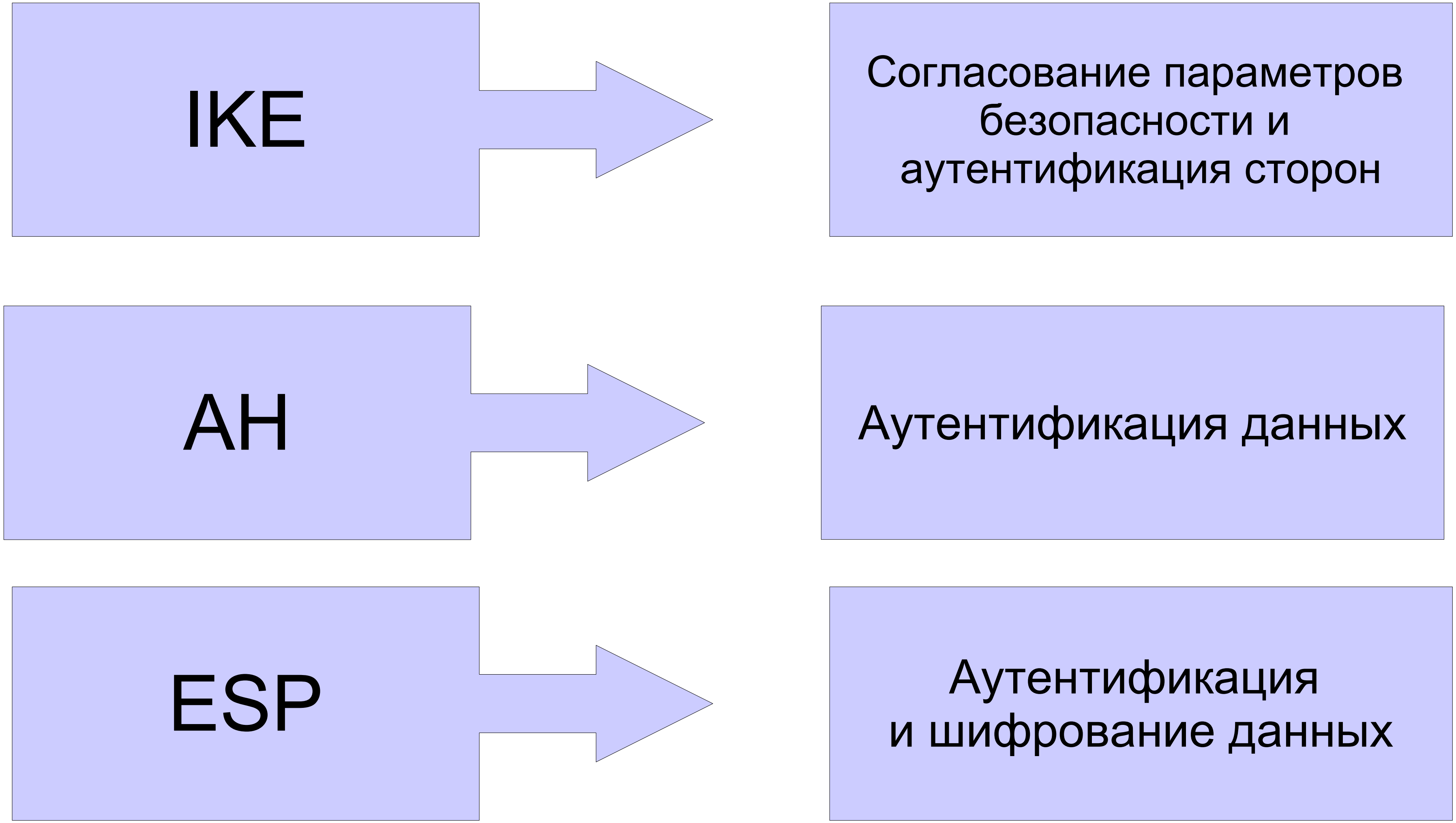
Основы IPsec

IP Security (IPsec)

IPsec – это набор протоколов использующийся для обеспечения сервисов приватности и аутентификации на сетевом уровне модели OSI.

Протоколы можно разделить на два класса – протоколы защиты передаваемых данных (AH, ESP) и протоколы обмена ключами (IKE).

IP Security (IPsec)



IKE → Согласование параметров безопасности и аутентификация сторон

AH → Аутентификация данных

ESP → Аутентификация и шифрование данных

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) – протокол использующийся для автоматического создания, установления, изменения и удаления Security Associations (SA) между двумя хостами в сети.

SA содержат информацию для установки безопасного соединения между участниками предопределенным способом.

IKE основан на протоколах:

- ISAKMP
- Oakley
- SKEME

Internet Key Exchange (IKE)

ISAKMP

определяет концепцию управления и обмена ключами, управления и установления SA.

Работа ISAKMP разбивается на две отдельные фазы.

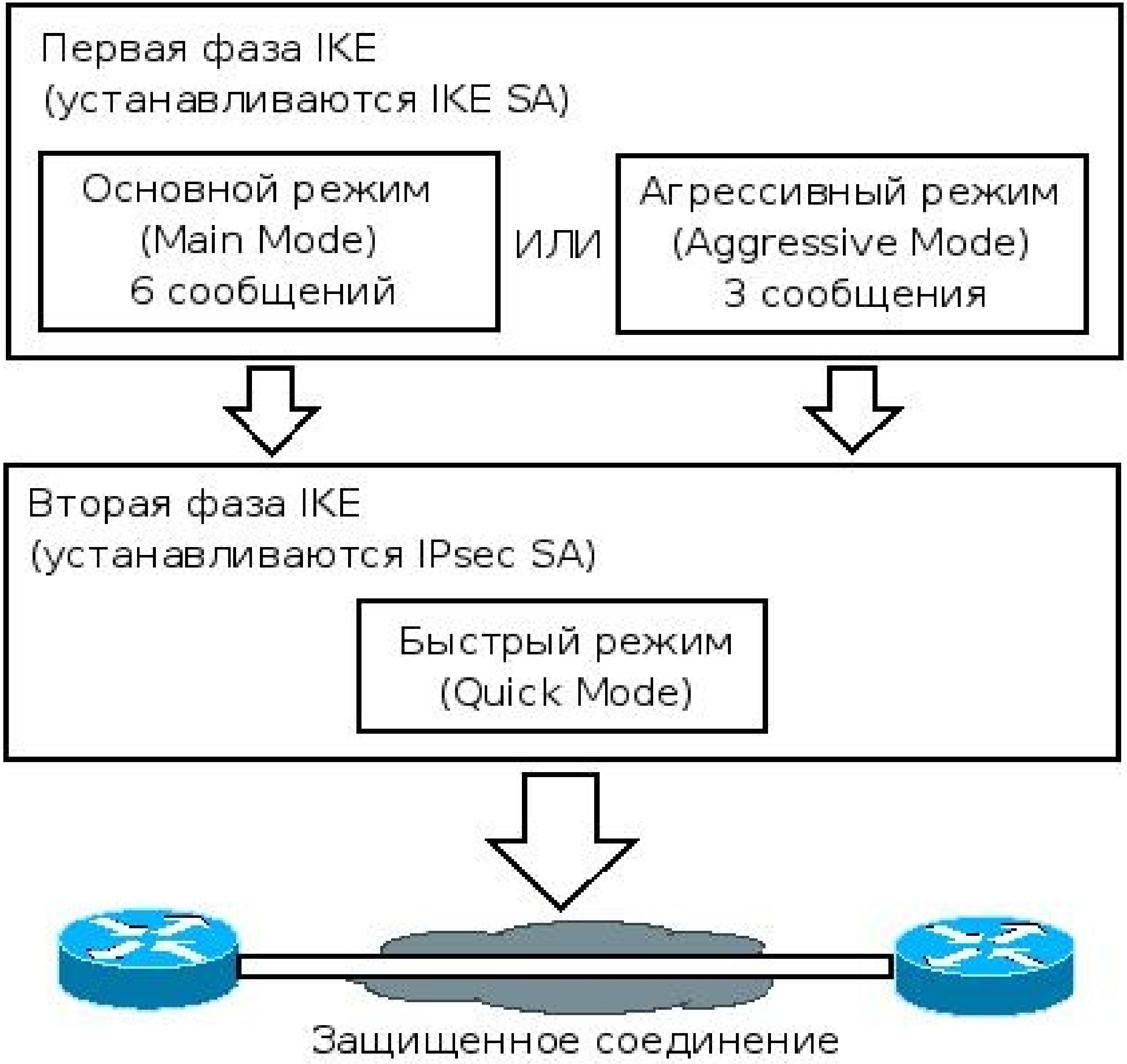
Oakley

Протокол Oakley описывает серии обмена ключами, называемые режимами (modes), и детализирует сервисы предоставляемые каждым режимом.

SKEME

Определяет обмен ключами, который обеспечивает анонимность и быстрое обновление ключей.

Internet Key Exchange (IKE)



Первая фаза IKE
(устанавливаются IKE SA)

Основной режим
(Main Mode)
6 сообщений

или

Агрессивный режим
(Aggressive Mode)
3 сообщения

Вторая фаза IKE
(устанавливаются IPsec SA)

Быстрый режим
(Quick Mode)

Защищенное соединение

Протоколы и технологии

Transport mode

Tunnel mode

DES

3DES

AES

DH

Hash

SHA

MD5

HMAC

PFS

RSA

Transform

Crypto map

CA

Certificate

CRL

Настройка IPsec

Настройка IPsec

1. Подготовка к настройке
    - Проверка доступности
    - Разрешить VPN-трафик
    - Выбор политик
2. Настройка первой фазы
    - Политика isakmp
    - Ключи или сертификаты
3. Настройка второй фазы
    - Crypto map
        - ACL -> что защищать
        - Transform-set -> как защищать
    - IPsec profile
        - Routing -> что защищать
        - Transform-set -> как защищать
4. Применить
    - Crypto map -> внешний интерфейс
    - IPsec profile -> туннельный интерфейс

1. Подготовка к настройке

1. Подготовка к настройке

Проверка доступности

Разрешить VPN-трафик

ISAKMP	UDP 500
AH	IP 51
ESP	IP 50
NAT-T	UDP 4500

Выбор политик

AES > 3DES > DES

SHA > MD5

DH 16 > ... DH 5 > DH 2 > DH 1

Сертификаты > pre-shared key

2. Настройка первой фазы

2. Настройка первой фазы

Политика isakmp

```
r1#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES (128 bit keys)
        hash algorithm:         Secure Hash Standard
        authentication method:  RSA Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 sec, no volume limit
```

Ключи

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

Сертификаты

CA

Получить сертификат

Политики IKE по умолчанию

```
crypto isakmp policy 65507
 encr aes
 hash sha
 group 5
 auth rsa-sig
 lifetime 86400

crypto isakmp policy 65508
 encr aes
 hash sha
 group 5
 auth pre-shared
 lifetime 86400

crypto isakmp policy 65509
 encr aes
 hash md5
 group 5
 auth rsa-sig
 lifetime 86400

crypto isakmp policy 65510
 encr aes
 hash md5
 group 5
 auth pre-shared
 lifetime 86400
```

```
crypto isakmp policy 65511
 encr 3des
 hash sha
 group 2
 auth rsa-sig
 lifetime 86400

crypto isakmp policy 65512
 encr 3des
 hash sha
 group 2
 auth pre-shared
 lifetime 86400

crypto isakmp policy 65513
 encr 3des
 hash md5
 group 2
 auth rsa-sig
 lifetime 86400

crypto isakmp policy 65514
 encr 3des
 hash md5
 group 2
 auth pre-shared
 lifetime 86400
```

3. Настройка второй фазы

3. Настройка второй фазы
    - Crypto map
        - ACL -> что защищать
            - Permit -> шифровать
            - Deny -> не шифровать
        - Transform-set -> как защищать

          ```
          ah-md5-hmac
          ah-sha-hmac
          esp-3des
          esp-aes
          esp-des
          esp-md5-hmac
          esp-sha-hmac
          ```
    - IPsec profile
        - Transform-set -> как защищать

4. Применить правила

4. Применить правила

Crypto map -> внешний интерфейс

```
crypto map MAP1 10 ipsec-isakmp
  set peer 38.0.0.3
  set transform-set MAP_set
  match address MAP_VPN
interface fa0/0
  crypto map MAP1
```

IPsec profile -> туннельный интерфейс

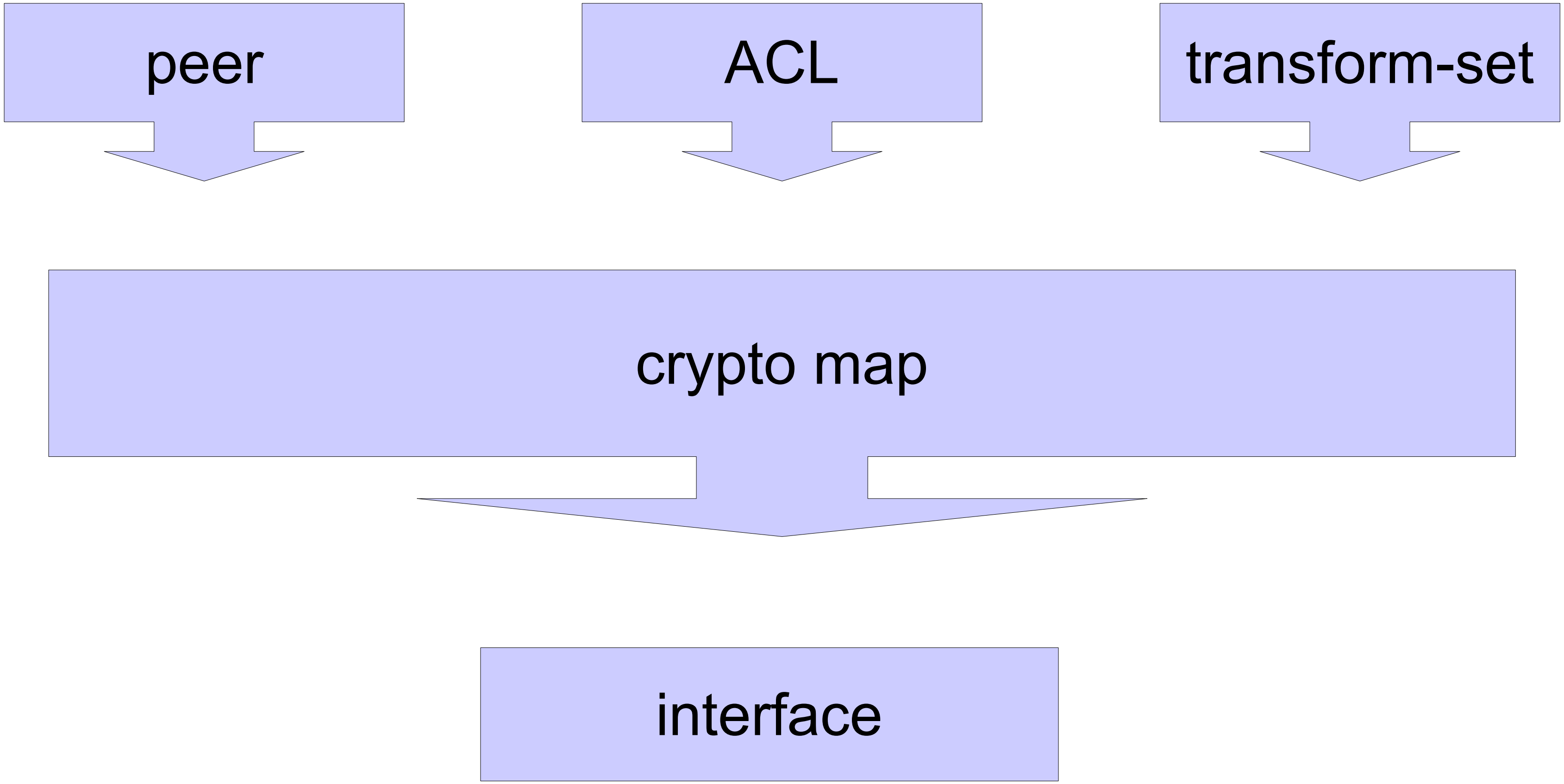
```
crypto ipsec profile DYNS
  set transform-set DVTI
interface tunnel 100
  tunnel protection ipsec profile DYNS
```

Настройка IPsec

1. Подготовка к настройке
    - Проверка доступности
    - Выбор политик
2. Настройка первой фазы
    - Политика isakmp
    - Ключи или сертификаты
3. Настройка второй фазы
    - Crypto map
        - ACL -> что защищать
        - Transform-set -> как защищать
    - IPsec profile
        - Routing -> что защищать
        - Transform-set -> как защищать
4. Применить
    - Crypto map -> внешний интерфейс
    - IPsec profile -> туннельный интерфейс

Использование crypto map и аутентификация по pre-shared key

Настройка VPN с использованием crypto map



Настройка VPN на r1

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

crypto isakmp key cisco address 38.0.0.3

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

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

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 VPN на r3

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

crypto isakmp key cisco address 16.0.0.1

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

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

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
```

Полезные команды debug и show

Установленные SA первой фазы

```
r3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
16.0.0.1        38.0.0.3        QM_IDLE           1009 ACTIVE
```

```
r3#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          Status Encr Hash Auth DH Lifetime Cap.

1007  38.0.0.3        16.0.0.1        ACTIVE aes  sha  rsig 5  11:47:36
       Engine-id:Conn-id =  SW:7
```

Установленные SA второй фазы

```
r1#sh crypto ipsec sa

interface: FastEthernet2/0
    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
...
```

Установленные SA второй фазы

```
r1#sh crypto ipsec sa
...
     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
...

     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
….
```

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 kbytes/3600 sec
        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
```

Сессии VPN

```
r1#sh crypto session brief
Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N -
Negotiating
        K - No IKE

   Peer        I/F    Username     Group/Phase1_id   Uptime Status
   38.0.0.3    Fa0/0                     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
```

Сессии VPN

```
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
```

Команды debug

```
r1# debug crypto isakmp
r1# debug crypto ipsec

r1# debug crypto condition ?
```

```
  connid     IKE/IPsec connection-id filter
  isakmp     Isakmp profile filter
  local      IKE local address filter
  peer       IKE peer filter
  reset      Delete all debug filters and turn off cond. debug
  spi        SPI (Security Policy Index) filter
  username   Xauth or Pki-aaa username filter
```

Использование GRE-туннелей

Настройка GRE-туннелей

На r1:

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source 16.0.0.1
 tunnel destination 38.0.0.3
```

На r3:

```
interface Tunnel3
 ip address 10.0.0.3 255.255.255.0
 tunnel source 38.0.0.3
 tunnel destination 16.0.0.1
```

Настройка IPsec с ipsec profile

На r1:

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

crypto isakmp key cisco address 38.0.0.3

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

crypto ipsec profile GRE_prof
 set transform-set AESSHA

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source 16.0.0.1
 tunnel destination 38.0.0.3
 tunnel protection ipsec profile GRE_prof
```

Настройка IPsec с ipsec profile

На r1:

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

crypto isakmp key cisco address 16.0.0.1

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

crypto ipsec profile GRE_prof
 set transform-set AESSHA

interface Tunnel1
 ip address 10.0.0.3 255.255.255.0
 tunnel source 38.0.0.3
 tunnel destination 16.0.0.1
 tunnel protection ipsec profile GRE_prof
```

Настройка IPsec 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: dyn3
      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
```

Настройка IPsec с crypto map на r1

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source 16.0.0.1
 tunnel destination 38.0.0.3
```

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
```

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 IPsec с crypto map на r3

```
interface Tunnel3
 ip address 10.0.0.3 255.255.255.0
 tunnel source 38.0.0.3
 tunnel destination 16.0.0.1
```

ACL с указанием какой трафик необходимо шифровать на dyn3:

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

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
```

Настройка IPsec с crypto map

```
r3#sh crypto session detail

Crypto session current status

Interface: FastEthernet1/0
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
```

Использование VTI-интерфейсов

Настройка VPN на r1

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

crypto isakmp key ciscoVTI address 38.0.0.3

crypto ipsec transform-set AESSHA esp-aes esp-sha-hmac

crypto ipsec profile VTI_prof
 set transform-set AESSHA

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 VPN на r3

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

crypto isakmp key ciscoVTI address 16.0.0.1

crypto ipsec transform-set AESSHA esp-aes esp-sha-hmac

crypto ipsec profile VTI_prof
 set transform-set AESSHA

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
```

Автоматически созданные crypto map

```
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
```

Сессии VPN

```
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
```

Использование динамических VTI-интерфейсов

Настройка DVTI на r1

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

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

crypto ipsec transform-set DVTI esp-aes esp-sha-hmac

crypto ipsec profile DYN_prof
 set transform-set DVTI

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

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
```

Настройка SVTI на r3

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

crypto isakmp key r1-3 address 16.0.0.1

crypto ipsec transform-set DVTI esp-aes esp-sha-hmac

crypto ipsec profile DYN_prof
 set transform-set DVTI

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 DYN_prof
```

Настройка SVTI на r4

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

crypto isakmp key r1-4 address 16.0.0.1

crypto ipsec transform-set DVTI esp-aes esp-sha-hmac

crypto ipsec profile DYN_prof
 set transform-set DVTI

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 DYN_prof
```

Автоматически созданные интерфейсы

```
r1#sh ip int br
Interface             IP-Address     OK? Method Status       Protocol
FastEthernet0/0       16.0.0.1       YES NVRAM  up           up
FastEthernet0/1       10.1.1.1       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
```

Автоматически созданные интерфейсы

```
r1#sh run interface Virtual-Access 2
```

```
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 DYN_prof
 no tunnel protection ipsec initiate
```

```
r1#sh run interface Virtual-Access 3
```

```
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 DYN_prof
 no tunnel protection ipsec initiate
```

Установленные сессии

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

Interface: Virtual-Access3
Profile: IKE_prof
Session status: UP-ACTIVE
Peer: 48.0.0.4 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
```

Аутентификация по сертификатам

Настройка CA-сервера

1 Задать имя домена

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

2 Включить HTTP-сервер

```
ip http server
```

3 Сгенерировать пару ключей, которые будет использовать CA

```
crypto key generate rsa general-keys label CA_Cisco modulus 2048

The name for the keys will be: CA_Cisco
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
```

4 Включить CA-сервер

```
crypto pki server CA_Cisco
 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.
```

Опциональные настройки CA-сервера

```
dyn3(config)#crypto pki server CA_Cisco
dyn3(cs-server)#?

CA Server configuration commands:
  auto-rollover  Rollover the CA key and certificate
  cdp-url        CRL Distribution Point to be included in the
issued certs
  crl            server crl
  database       Certificate Server database config parameters
  default        Set a command to its defaults
  grant          Certificate granting options
  hash           Hash algorithm
  issuer-name    Issuer name
  lifetime       Lifetime parameters
  mode           Mode
  redundancy     sync this server to the standby
  show           Show this certificate server configuration
  shutdown       Shutdown the Certificate Server
```

Настройка маршрутизатора для получения сертификата

1 Проверить доступность CA

2 Задать имя домена

3 Сгенерировать пару ключей

```
crypto key generate rsa label VPN_keys
```

4 Настроить trustpoint

```
crypto pki trustpoint VPN_CA
    enrollment url http://10.0.1.4
    subject-name CN=r3,OU=VPN,O=NT,C=UA
    rsakeypair VPN_keys
    revocation-check none
```

5 Запросить сертификат CA

```
r3(config)#crypto pki authenticate VPN_CA
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.
```

6 Запросить сертификат для маршрутизатора

```
r3(config)#crypto pki enroll VPN_CA
```

Выдать сертификаты на CA

```
r4#sh crypto pki server CA_Cisco 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=r4,cn=r4,ou=VPN,o=NT,c=UA
1      pending    5EB2051AE399854A99ECCD40D5511984 hostname=r3,cn=r3,ou=VPN,o=NT,c=UA
```

```
r4#crypto pki server CA_Cisco grant all
```

Просмотр сертификатов

```
r3#sh crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=CA_Cisco
  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

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA_Cisco
  Subject:
    cn=CA_Cisco
  Validity Date:
    start date: 07:57:40 UTC May 15 2011
    end   date: 07:57:40 UTC May 14 2014
  Associated Trustpoints: VPN_CA
```

Настройка DVTI на r1

```
crypto isakmp policy 10
 authentication rsa-sig

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

crypto isakmp profile CERT
   match certificate DYNS_cert
   virtual-template 100

crypto ipsec profile DYNS_prof
 set transform-set DVTI

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

Настройка SVTI на r3

```
crypto isakmp policy 10
 authentication rsa-sig


crypto ipsec profile DYNS_prof
 set transform-set DVTI

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
```

Настройка SVTI на r4

```
crypto isakmp policy 10
 authentication rsa-sig


crypto ipsec profile DYNS_prof
 set transform-set DVTI

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 DYNS_prof
```

Настройка Site-to-Site VPN на маршрутизаторах Cisco

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

Сетевые Дни