Настройка Site-to-Site VPN на Cisco ASA

Наташа Самойленко

Сетевые Дни

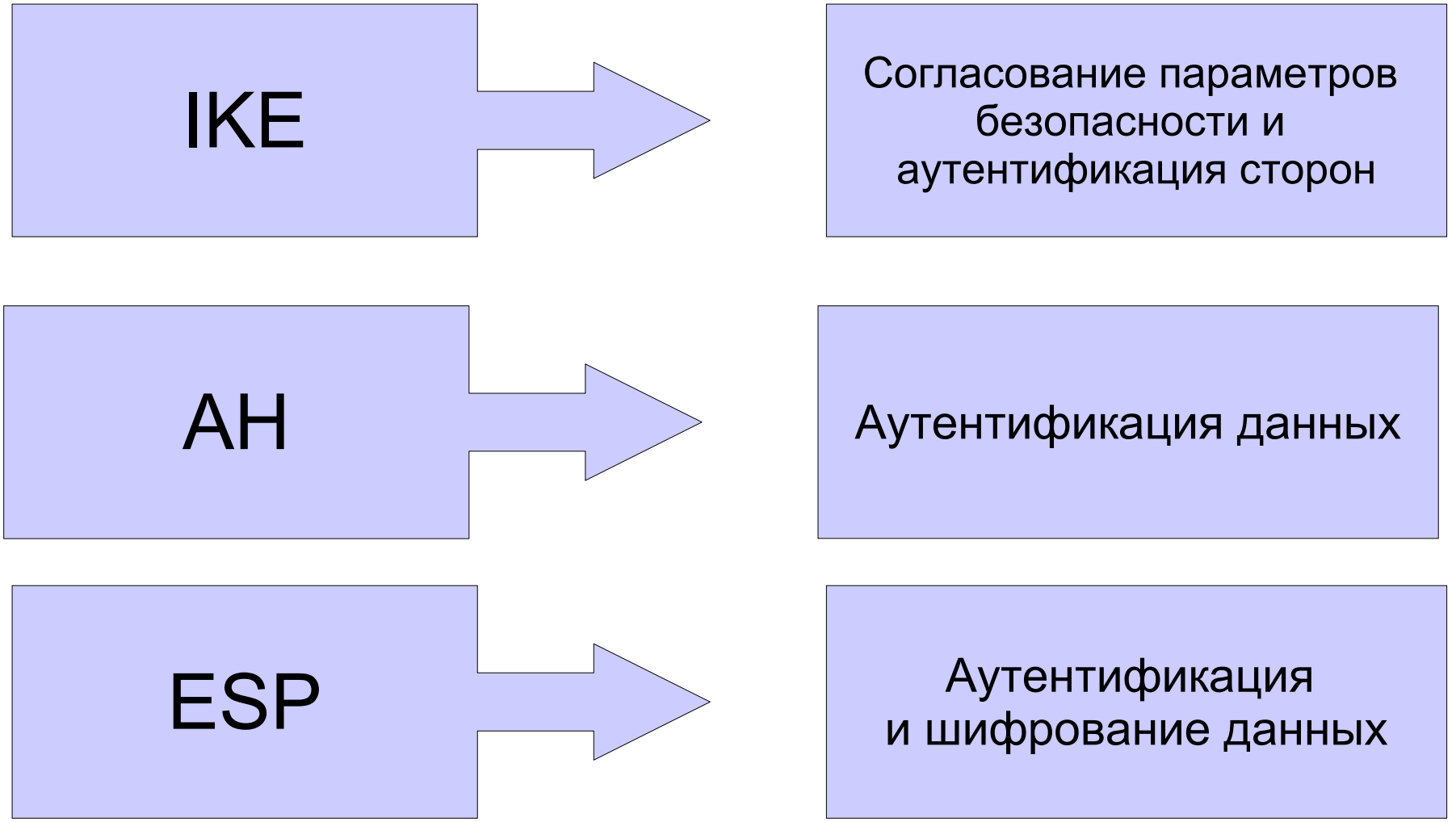
Основы IPsec

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)



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.

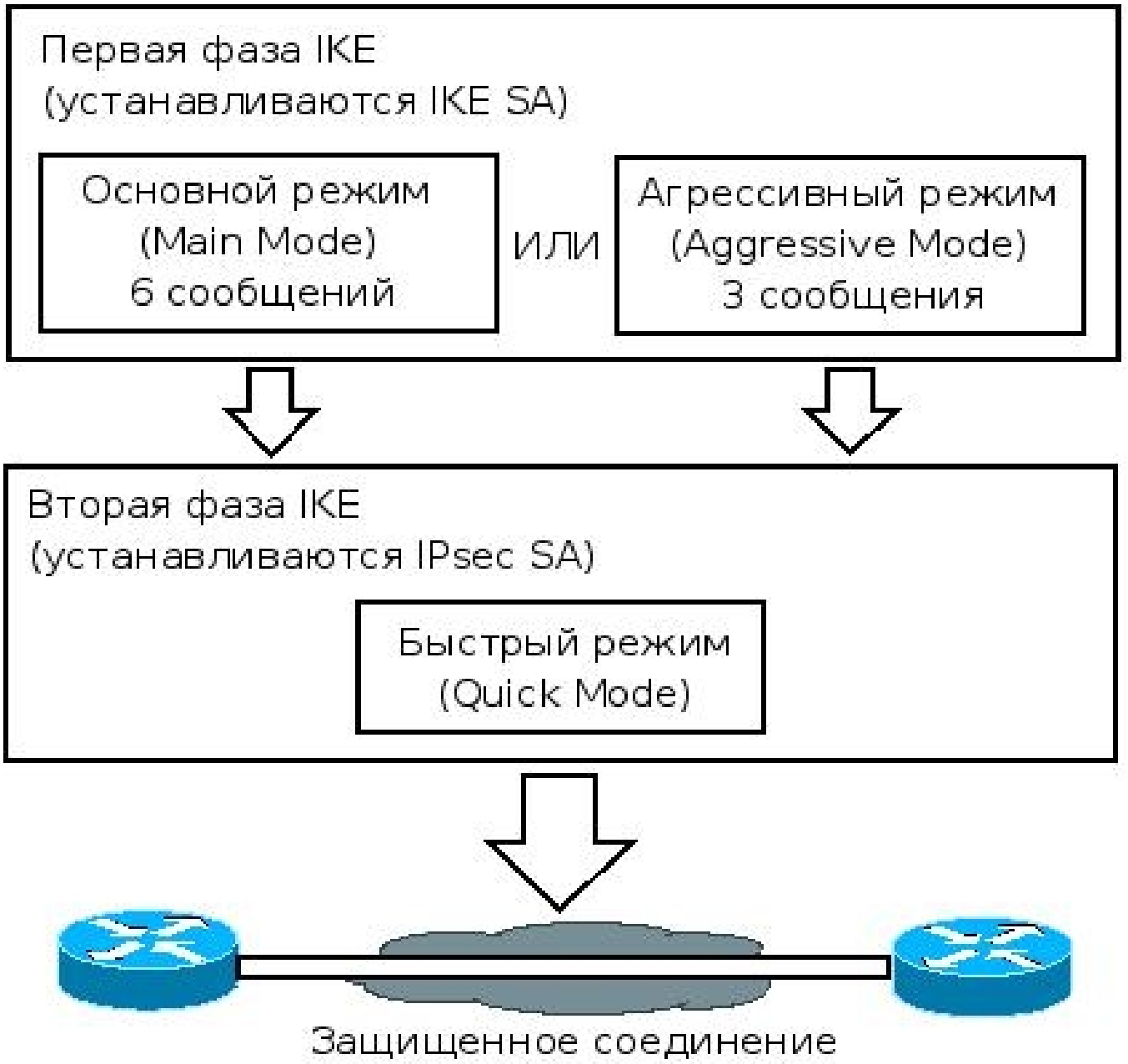
Oakley

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)



Протоколы и технологии

Transport mode

Tunnel mode

DES

3DES

AES

DH

Hash

SHA

MD5

HMAC

PFS

RSA

Transform

Crypto map

CA

Certificate

CRL

Site-to-Site VPN на Cisco ASA

Политика IKE

В документации Cisco термины IKE и ISAKMP, как правило, взаимозаменяемы.

Политика IKE указывает параметры первой фазы:

- Метод аутентификации (пароль, сертификаты)
- Протокол шифрования (DES, 3DES, AES)
- Алгоритм хеширования (MD5, SHA)
- Группа DH
- Время жизни SA

В Cisco ASA, кроме настройки политики IKE, необходимо также включить IKE на интерфейсе.

Tunnel-group

Tunnel-group это объект, в котором при настройке site-to-site VPN, указываются параметры для аутентификации на первой фазе IPsec.

- При аутентификации по паролю -- пароль, а при аутентификации по сертификатам -- соответствующая trustpoint.
- Для site-to-site VPN вместо имени tunnel-group указывается IP-адрес удаленной стороны туннеля

Tunnel-group DefaultL2LGroup

В конфигурации существует **tunnel-group DefaultL2LGroup** из которой наследуются все настройки, которые не были заданы явно в созданных tunnel-group. Её можно изменять.
По умолчанию она выглядит так:

```
sh run all tunnel-group DefaultL2LGroup

tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 10 retry 2
```

Tunnel-group DefaultL2LGroup удобно использовать в тех случаях, когда, например, на Cisco ASA терминируется много туннелей VPN с одинаковыми настройками. Можно задать, например, trustpoint, которую используют большинство туннелей, а для тех, которые используют другие, или pre-shared пароль, можно задать параметр в соответствующей tunnel-group.

Transform-set (ipsec-proposal)

Transform-set (ipsec-proposal в IKEv2) это объект, который описывает параметры второй фазы.

В Cisco ASA не поддерживается протокол AH, есть только ESP.

В transform-set указывается:

- Протокол ESP
- Протокол шифрования (DES, 3DES, AES)
- Алгоритм хеширования (MD5, SHA)

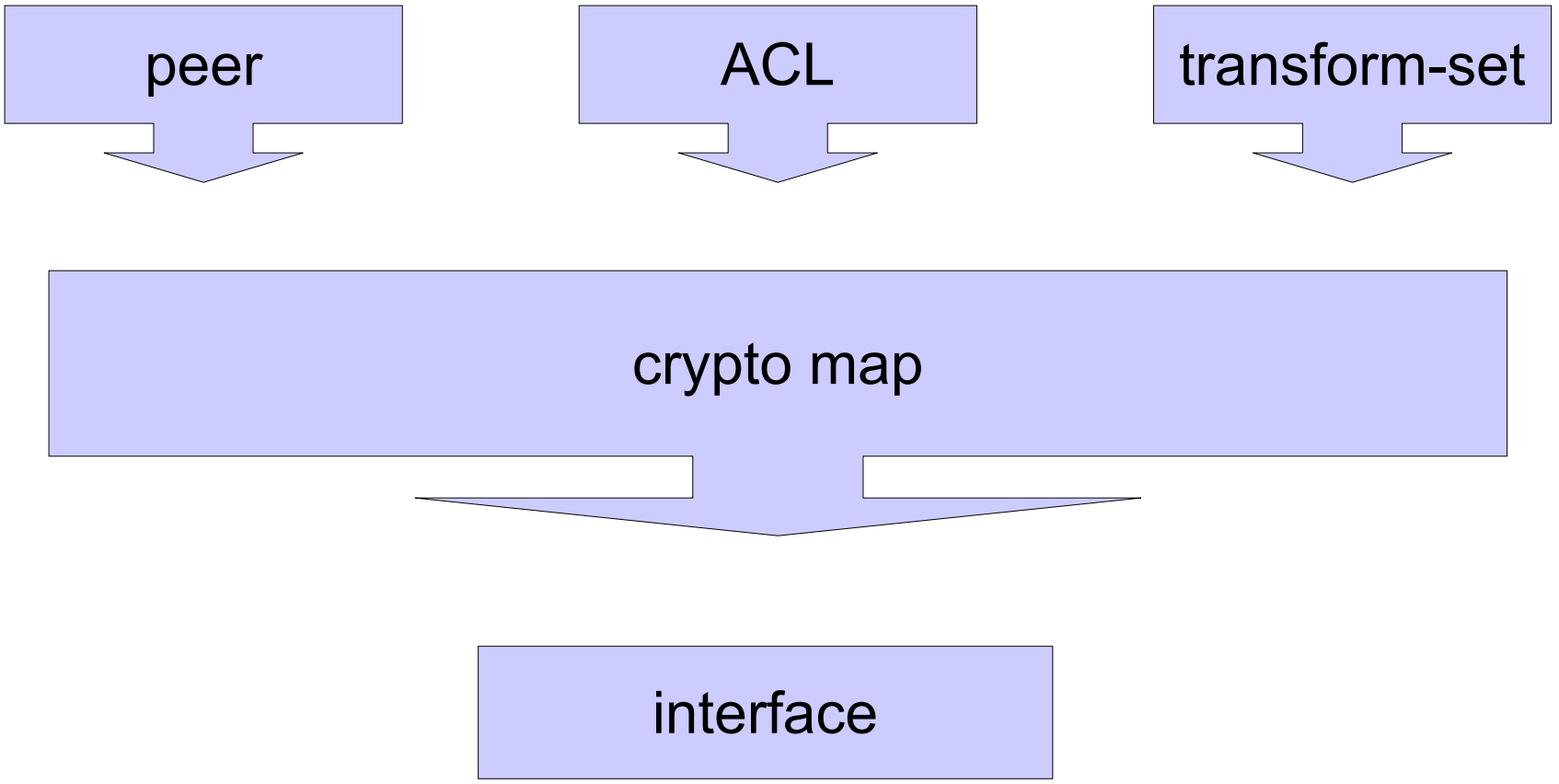
Crypto map

Crypto map это объект, в котором находятся наборы правил, относящиеся к разным туннелям IPsec. Так как к интерфейсу может быть применена только одна crypto map, то описать все туннели необходимо в одной и той же crypto map.
Для того чтобы отличать правила относящиеся в разным туннелям, правила группируются в наборы, которые объединяет общий порядковый номер правила в crypto map.

В каждом наборе правил crypto map можно указать такие параметры:

- Адрес удаленной стороны туннеля (peer)
- ACL, который указывает какие данные попадут в туннель
- Transform-set
- Группа DH для включения PFS
- Вставка обратного маршрута (RRI)

Настройка VPN с использованием crypto map



Аутентификация по PSK

Пример настройки (старый вариант)

```
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-shared
 encryption 3des
 hash sha
 group 2
 lifetime 86400

tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 pre-shared-key cisco

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0
10.0.2.0 255.255.255.0

crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac

crypto map VPN_MAP 10 match address L2LACL
crypto map VPN_MAP 10 set peer 80.1.1.1
crypto map VPN_MAP 10 set transform-set 3DES_SHA
crypto map VPN_MAP 10 set reverse-route

crypto map VPN_MAP interface outside
```

Пример настройки IKEv1

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400

tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 ikev1 pre-shared-key *****

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.255.255.0

crypto ipsec ikev1 transform-set 3DES_SHA esp-3des esp-sha-hmac

crypto map IKEv1_MAP 10 match address L2LACL
crypto map IKEv1_MAP 10 set peer 80.1.1.1
crypto map IKEv1_MAP 10 set ikev1 transform-set 3DES_SHA
crypto map IKEv1_MAP 10 set reverse-route

crypto map IKEv1_MAP interface outside
```

Пример настройки IKEv2

```
crypto ikev2 enable outside
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 5
 prf sha512
 lifetime seconds 86400

tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes-256
 protocol esp integrity sha-1

crypto map IKEv2_MAP 10 match address L2LACL
crypto map IKEv2_MAP 10 set peer 80.1.1.1
crypto map IKEv2_MAP 10 set ikev2 ipsec-proposal AES
crypto map IKEv2_MAP 10 set reverse-route

crypto map IKEv2_MAP interface outside
```

Отличия IKEv1 и IKEv2

Политика IKE

```
crypto ikev1 enable outside

crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
```

```
crypto ikev2 enable outside

crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 5
 prf sha512
 lifetime seconds 86400
```

Tunnel-group

```
tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 ikev1 pre-shared-key *****
```

```
tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

Transform-set / IPsec-proposal

```
crypto ipsec ikev1 transform-set AES esp-aes esp-sha-hmac
```

```
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1
```

Crypto map

```
crypto map IKEv1_MAP 10 match address L2LACL
crypto map IKEv1_MAP 10 set peer 80.1.1.1
crypto map IKEv1_MAP 10 set ikev1 transform-set AES
crypto map IKEv1_MAP 10 set reverse-route

crypto map IKEv1_MAP interface outside
```

```
crypto map IKEv2_MAP 10 match address L2LACL
crypto map IKEv2_MAP 10 set peer 80.1.1.1
crypto map IKEv2_MAP 10 set ikev2 ipsec-proposal AES
crypto map IKEv2_MAP 10 set reverse-route

crypto map IKEv2_MAP interface outside
```

Аутентификация по сертификатам

Получение сертификата

```
crypto ca trustpoint IOS_CA
 enrollment url http://192.168.1.1:80
 subject-name CN=ASA1
```

```
ASA1(config)# crypto ca authenticate IOS_CA

INFO: Certificate has the following attributes:
Fingerprint:     3c6bd334 a8173e1b 28bd4d41 83a02f3a
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

ASA1(config)# crypto ca enroll IOS_CA noconfirm
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=ASA1

% The fully-qualified domain name in the certificate will be:
ASA1.unix.nt
% Certificate request sent to Certificate Authority
ASA1(config)# The certificate has been granted by CA!
```

Пример настройки (старый вариант)

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

tunnel-group 192.168.2.2 type ipsec-l2l
tunnel-group 192.168.2.2 ipsec-attributes
 trust-point IOS_CA

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.255.255.0

crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac

crypto map TEST_MAP 10 match address L2LACL
crypto map TEST_MAP 10 set peer 192.168.2.2
crypto map TEST_MAP 10 set transform-set 3DES_SHA
crypto map TEST_MAP 10 set reverse-route

crypto map TEST_MAP interface outside

crypto ca certificate map L2L 10
 subject-name attr cn eq asa2

tunnel-group-map enable rules
tunnel-group-map L2L 10 192.168.2.2
```

Пример настройки IKEv2

```
crypto ikev2 enable outside
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 5
 prf sha512
 lifetime seconds 86400

tunnel-group 80.1.1.1 type ipsec-l2l
tunnel-group 80.1.1.1 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate IOS_CA

access-list L2LACL extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.255.255.0

crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes-256
 protocol esp integrity sha-1

crypto map IKEv2_MAP 10 match address L2LACL
crypto map IKEv2_MAP 10 set peer 80.1.1.1
crypto map IKEv2_MAP 10 set ikev2 ipsec-proposal AES
crypto map IKEv2_MAP 10 set reverse-route
crypto map IKEv2_MAP 10 set trustpoint IOS_CA chain

crypto map IKEv2_MAP interface outside
```

Проверка VPN

Проверка VPN

```
asa1# sh vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection   : 192.168.2.2
Index        : 2                        IP Addr      : 172.16.1.0
Protocol     : IKE IPsec
Encryption   : DES                      Hashing      : SHA1
Bytes Tx     : 22140                    Bytes Rx     : 22140
Login Time   : 12:22:24 UTC Fri Apr 8 2011
Duration     : 0h:06m:14s
```

Проверка VPN

```
asa1# sh vpn-sessiondb detail l2l

Session Type: LAN-to-LAN Detailed

Connection   : 192.168.2.2
Index        : 2                        IP Addr      : 172.16.1.0
Protocol     : IKE IPsec
Encryption   : DES                      Hashing      : SHA1
Bytes Tx     : 22140                    Bytes Rx     : 22140
Login Time   : 12:22:24 UTC Fri Apr 8 2011
Duration     : 0h:06m:14s
IKE Tunnels: 1
IPsec Tunnels: 1

IKE:
  Tunnel ID    : 2.1
  UDP Src Port : 500                      UDP Dst Port : 500
  IKE Neg Mode : Main                     Auth Mode    : preSharedKeys
  Encryption   : DES                      Hashing      : SHA1
  Rekey Int (T): 86400 Seconds            Rekey Left(T): 86027 Seconds
  D/H Group    : 5
  Filter Name  :
```

Проверка VPN (продолжение)

```
IPsec:
  Tunnel ID     : 2.2
  Local Addr    : 10.0.1.0/255.255.255.0/0/0
  Remote Addr   : 172.16.1.0/255.255.255.0/0/0
  Encryption    : DES                  Hashing       : SHA1
  Encapsulation: Tunnel                PFS Group     : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28427 Seconds
  Rekey Int (D): 3825000 K-Bytes       Rekey Left(D): 3824979 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left  : 30 Minutes
  Bytes Tx      : 22140                Bytes Rx      : 22140
  Pkts Tx       : 369                  Pkts Rx       : 369

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)    : 0 Seconds            EoU Age(T)    : 373 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Подсказка по настройке VPN

Подсказка по настройке VPN

```
asa1(config)# vpnsetup site-to-site steps

Steps to configure a simple site-to-site IKE/IPSec connection with examples:

1. Configure Interfaces

        interface GigabitEthernet0/0
         ip address 10.10.4.200 255.255.255.0
         nameif outside
         no shutdown

        interface GigabitEthernet0/1
         ip address 192.168.0.20 255.255.255.0
         nameif inside
         no shutdown

2. Configure ISAKMP policy

        crypto isakmp policy 10
         authentication pre-share
         encryption 3des
         hash sha

3. Configure transform-set

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

Подсказка по настройке VPN

4. Configure ACL

```
        access-list L2LAccessList extended permit ip 192.168.0.0
255.255.255.0 192.168.50.0 255.255.255.0
```

5. Configure Tunnel group

```
        tunnel-group 10.20.20.1 type ipsec-l2l
        tunnel-group 10.20.20.1 ipsec-attributes
         pre-shared-key P@rtn3rNetw0rk
```

6. Configure crypto map and attach to interface

```
        crypto map mymap 10 match address L2LAccessList
        crypto map mymap 10 set peer 10.10.4.108
        crypto map mymap 10 set transform-set myset
        crypto map mymap 10 set reverse-route
        crypto map mymap interface outside
```

7. Enable isakmp on interface

```
        crypto isakmp enable outside
```

Easy VPN на Cisco ASA

Tunnel-group

Tunnel-group это объект, в котором при настройке Easy VPN, указываются такие параметры (перечислены не все доступные параметры, а только примеры):

- **В режиме ipsec-attributes:**
  - Настройки аутентификации устройств:
    - При аутентификации по паролю -- пароль
    - при аутентификации по сертификатам -- соответствующая trustpoint.
  - Настройки аутентификации пользователей (xauth или hybrid):
    - Включается аутентификация xauth и указывается как она будет выполняться
      - по умолчанию xauth включена и аутентификация выполняется по локальной базе пользователей
    - Включается аутентификация hybrid (в Cisco VPN клиенте она называется mutual)
- **В режиме general-attributes:**
  - Привязывается пул адресов, который соответствует этой tunnel-group
  - Привязывается соответствующая групповая политика

Tunnel-group DefaultRAGroup

В конфигурации существует tunnel-group DefaultRAGroup из которой наследуются все настройки, которые не были заданы явно в созданных tunnel-group. Её можно изменять.

По умолчанию она выглядит так (параметры webvpn и ppp удалены):

```
sh run all tunnel-group DefaultRAGroup

tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
```

Групповая политика (group-policy)

После прохождения аутентификации (устройств и пользователей) на клиента назначаются параметры, которые указываются в групповой политике.

В group-policy можно задать, например, такие параметры:

- ACL для фильтрации трафика
- Политику туннелирования трафика и какой трафик попадет в туннель
- DNS-сервер
- и др.

Групповая политика может быть настроена локально или на RADIUS-сервере.

Групповая политика по умолчанию DfltGrpPolicy

В конфигурации существует групповая политика по умолчанию DfltGrpPolicy из которой наследуются все настройки, которые не были заданы явно в созданных групповых политиках. Её можно изменять.

По умолчанию она выглядит так (параметры webvpn удалены):

```
sh run all DfltGrpPolicy

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 2000
 vpn-idle-timeout none
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec webvpn
 password-storage enable
 re-xauth disable
 group-lock none
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
```

Пример настройки

```
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-shared
 encryption 3des
 hash sha
 group 2
 lifetime 86400

crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac

crypto dynamic-map RVPN 10 set transform-set 3DES_SHA
crypto dynamic-map RVPN 10 set reverse-route

crypto map VPN_MAP 65535 ipsec-isakmp dynamic RVPN
crypto map VPN_MAP interface outside
```

Пример настройки

```
ip local pool MANAGER_POOL 172.16.3.3-172.16.3.5 mask 255.255.255.255

access-list RVPN-SPLITT standard permit 10.0.2.0 255.255.255.0

access-list RVPN-ALLOWED extended permit tcp any host 10.0.2.10 eq ftp
access-list RVPN-ALLOWED extended permit tcp any host 10.0.2.10 eq www
access-list RVPN-ALLOWED extended permit tcp any host 10.0.2.11 eq 3389

group-policy MANAGER_GROUP internal
group-policy MANAGER_GROUP attributes
 dns-server value 10.0.2.10
 vpn-filter value RVPN-ALLOWED
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RVPN-SPLITT

username MANAGER1 password FGxPirrtw9DRO2qS encrypted
username MANAGER1 attributes
 vpn-group-policy MANAGER_GROUP
 vpn-filter none
 group-lock value MANAGER_GROUP
 service-type remote-access

tunnel-group MANAGER type remote-access
tunnel-group MANAGER general-attributes
 address-pool MANAGER_POOL
 default-group-policy MANAGER_GROUP

tunnel-group MANAGER ipsec-attributes
 pre-shared-key cisco123
```

Настройка Site-to-Site VPN на Cisco ASA

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

Сетевые Дни