Настройка EasyVPN 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

EasyVPN

EasyVPN

EasyVPN построен по схеме клиент-сервер:

- Клиенты EasyVPN
  - Cisco VPN Client
  - Маршрутизаторы Cisco с функционалом EasyVPN Remote
  - Cisco ASA*
- EasyVPN Server
  - Cisco ASA
  - Cisco IOS маршрутизаторы

EasyVPN Server

Платформы, которые могут использоваться как EasyVPN Server

- Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers—Cisco IOS Release 12.2(8)T or later release. Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR, but they are supported in Cisco IOS Release 12.3(7)XR2.
- Cisco 870 series—Cisco IOS Release 12.3(8)YI1.
- Cisco 1700 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 1800 series fixed configuration router—Cisco IOS Release 12.3(8)YI.
- Cisco 1812 router—Cisco IOS Release 12.3(8)YH.
- Cisco 2600 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3620—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3640—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3660—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7100 series VPN routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7200 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7500 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco PIX 500 series—Software Release 6.2 or later release.
- Cisco VPN 3000 series—Software Release 3.11 or later release.

EasyVPN Remote

Платформы, которые могут использоваться как EasyVPN Remote

- A Cisco 800 series router configured as a Cisco Easy VPN remote.
- A Cisco 1700 series router configured as a Cisco Easy VPN remote.
- A Cisco 1800 series fixed configuration router.
- A Cisco uBR905 or Cisco uBR925 cable access router configured as a Cisco Easy VPN remote.

EasyVPN Remote

Режимы работы EasyVPN Remote

- **Client** — В этом режиме на EasyVPN Remote настраивается PAT
- **Network extension** — В этом режиме не используется PAT. Исходные IP-адреса клиентов за EasyVPN Remote будут видны без изменений.
- **Network extension plus (mode network-plus)** — Аналогичен предыдущему режиму, кроме дополнительной возможности запрашивать IP-адрес через mode configuration и настроить его автоматически на loopback-интерфейсе.

Все режимы поддерживают (опционально) настройку **split tunneling,** которая позволяет получать доступ к корпоративным ресурсам за сервером и доступ в Интернет.

Настройки EasyVPN могут выполняться двумя способами:

- Старый вариант через **crypto map**
- Более современный вариант через **VTI**

Все режимы и функционал работают полнофункционально при совпадении способов настройки на Server и Remote.

Ограничения EasyVPN

Ограничения EasyVPN

На Easy VPN Server поддерживается только ISAKMP Policy Group 2

- Unity Protocol поддерживает только те политики ISAKMP, которые используют group 2 (1024-bit Diffie-Hellman) в первой фазе IKE. Поэтому Easy VPN server должен быть настроен соответственно.

Поддерживаемые Transform Set

- Cisco Easy VPN Remote не поддерживает transform set, которые используют шифрование, но не используют аутентификацию (ESP-DES, ESP-3DES) или transform set, которые используют аутентификацию без шифрования (ESP-NULL ESP-SHA-HMAC, ESP-NULL ESP-MD5-HMAC).

Cisco Unity Client Protocol не поддерживает Authentication Header (AH), но поддерживает Encapsulation Security Protocol (ESP).

Аутентификация в EasyVPN

Аутентификация в EasyVPN

EasyVPN Remote поддерживает аутентификацию в два этапа:

1. Group Level Authentication
    - На этом этапе поддерживаются два типа аутенитификации: preshared keys или по сертификатам
2. Xauth (Extended Authentication)
    - На этом этапе удаленный маршрутизатор (или Cisco VPN Client) отправляет серверу EasyVPN имя и пароль пользователя (этот этап опциональный)
    - Для EasyVPN Remote имя и пароль могут быть:
        - сохранены в конфигурации удаленного маршрутизатора
        - введены вручную через web-аутентификацию
        - введены вручную в командной строке маршрутизатора

Настройка Easy VPN

Старый вариант настройки Easy VPN (crypto map)

Базовая настройка EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1

interface Ethernet0/0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 crypto ipsec client ezvpn TEST_EASY inside
```

Базовая настройка EasyVPN Server

```
crypto isakmp policy 1
 authentication pre-share
 group 2
 hash sha

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL
```

Базовая настройка EasyVPN Server

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

aaa attribute list VPNaccess
 attribute type service-type noopt service shell mandatory

username cisco password 0 cisco
username cisco aaa attribute list VPNaccess

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

crypto dynamic-map EASY 1
 set transform-set 3DESSHA
 reverse-route

crypto map VPN client authentication list USER
crypto map VPN isakmp authorization list GROUP
crypto map VPN client configuration address respond
crypto map VPN 1 ipsec-isakmp dynamic EASY

interface Ethernet0/0
 crypto map VPN
```

Проверка EasyVPN Remote

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: CONNECT
Address: 192.168.1.4 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 10.1.1.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 16.0.0.1
```

Проверка EasyVPN Remote

lvv3#sh ip nat statistics

```
lvv3#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 01:45:10 ago
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 2056  Misses: 0
CEF Translated packets: 2030, CEF Punted packets: 6
Expired translations: 7
Dynamic mappings:
-- Inside Source
[Id: 7] access-list TEST_EASY_internet-list interface Ethernet0/0
refcount 0
[Id: 6] access-list TEST_EASY_enterprise-list pool TEST_EASY refcount 0
 pool TEST_EASY: netmask 255.255.255.0
        start 192.168.1.4 end 192.168.1.4
        type generic, total addresses 1, allocated 0 (0%), misses 0
```

lvv3#sh access-lists TEST_EASY_enterprise-list

```
Extended IP access list TEST_EASY_enterprise-list
    10 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 (2 matches)
```

lvv3#sh access-lists TEST_EASY_internet-list

```
Extended IP access list TEST_EASY_internet-list
    10 deny ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 (2 matches)
    20 permit ip 10.3.3.0 0.0.0.255 any (1 match)
```

Проверка EasyVPN Remote (split-tunneling)

```
lvv3#ping 67.0.0.6 source 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 67.0.0.6, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms

lvv3#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside
global
icmp 38.0.0.3:2        10.3.3.3:2         67.0.0.6:2         67.0.0.6:2
```

```
lvv3#ping 10.1.1.1 source 10.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms

lvv3#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside
global
icmp 38.0.0.3:2        10.3.3.3:2         67.0.0.6:2         67.0.0.6:2
icmp 192.168.1.4:3     10.3.3.3:3         10.1.1.1:3         10.1.1.1:3
```

Проверка EasyVPN Server

```
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: Ethernet0/0
Username: cisco
Group: LVV_GROUP
Assigned address: 192.168.1.4
Uptime: 00:08:14
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: LVV_GROUP
      Desc: (none)
  IKEv1 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:CX connid:1011 lifetime:23:51:32
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.1.4
        Active SAs: 2, origin: dynamic crypto map
        Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 4232884/2146988
        Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4232884/2146988
```

Проверка EasyVPN Server

```
kiev1#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.

1010  16.0.0.1  38.0.0.3   ACTIVE des  sha         2  23:41:17 CX
       Engine-id:Conn-id =  SW:10
```

Проверка EasyVPN Server

kiev1#sh ip route

```
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, 4 subnets, 2 masks
C        10.0.0.1/32 is directly connected, Loopback1
D        10.0.0.2/32 [90/409600] via 10.1.1.2, 00:54:48, Ethernet0/1
C        10.1.1.0/24 is directly connected, Ethernet0/1
L        10.1.1.1/32 is directly connected, Ethernet0/1
      16.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        16.0.0.0/24 is directly connected, Ethernet0/0
L        16.0.0.1/32 is directly connected, Ethernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
S        192.168.1.3 [1/0] via 38.0.0.3
```

kiev1#sh ip local pool

```
 Pool          Begin           End             Free  In use   Blocked
 POOL_LVV      192.168.1.1     192.168.1.10       9       1         0
```

Проверка EasyVPN Server

```
kiev1#sh crypto map
Crypto Map IPv4 "VPN" 1 ipsec-isakmp
        Dynamic map template tag: EASY

Crypto Map IPv4 "VPN" 65536 ipsec-isakmp
        Peer = 38.0.0.3
        Extended IP access list
            access-list  permit ip any host 192.168.1.4
            dynamic (created from dynamic map EASY/1)
        Current peer: 38.0.0.3
        Security association lifetime: 4608000
kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                3DESSHA:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map VPN:
                Ethernet0/0
```

Проверка EasyVPN Server

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

Interface: Ethernet0/0
Username: cisco
Group: LVV_GROUP
Assigned address: 192.168.1.4
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv1 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 host 192.168.1.4
        Active SAs: 2, origin: dynamic crypto map
```

Настройка Easy VPN с VTI

Настройка Easy VPN Server с VTI

Базовая настройка EasyVPN Server с VTI

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

aaa attribute list VPNaccess
 attribute type service-type noopt service shell mandatory

username cisco password 0 cisco
username cisco aaa attribute list VPNaccess

crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any
```

Базовая настройка EasyVPN Server с VTI

```
crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

interface Loopback1
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 16.0.0.1 255.255.255.0

interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0

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

Проверка EasyVPN Server с VTI

```
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: Virtual-Access1
Profile: EASY_VPN
Group: LVV_GROUP
Assigned address: 192.168.1.2
Uptime: 01:16:52
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: LVV_GROUP
      Desc: (none)
  IKEv1 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:C connid:1036 lifetime:22:43:07
  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 10 drop 0 life (KB/Sec) 4244377/2404
        Outbound: #pkts enc'ed 1005 drop 0 life (KB/Sec) 4244349/2404
```

Проверка EasyVPN Server с VTI

kiev1#sh crypto isakmp peers config

```
Client-Public-Addr=38.0.0.3:500;
Client-Assigned-Addr=192.168.1.2;
Client-OS=Cisco IOS Software, Linux Software (I86BI_LINUX-A;
Client-Group=LVV_GROUP;
Client-User=cisco;
Client-Hostname=lvv3.xgu.ru;
Client-Platform=Linux Unix;
Client-Serial=2052199;
Client-Memory=132000208;
Client-Free-Memory=76494984;
Client-Image=unix:./images/i86bi_linux-adventerprisek9-ms;
```

Настройка Easy VPN Remote с VTI

Базовая настройка EasyVPN Remote с VTI

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 virtual-interface
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside
```

Настройка EasyVPN Remote с созданием Virtual Template

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 Virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

Проверка EasyVPN Remote с VTI

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 192.168.1.2 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Disallowed
Split Tunnel List: 1
        Address    : 10.1.1.0
        Mask       : 255.255.255.0
        Protocol   : 0x0
        Source Port: 0
        Dest Port  : 0
Current EzVPN Peer: 16.0.0.1
```

Проверка EasyVPN Remote с VTI

```
lvv3#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 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.3/32 is directly connected, Loopback3
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C        10.3.3.0/24 is directly connected, Ethernet0/1
L        10.3.3.3/32 is directly connected, Ethernet0/1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        38.0.0.0/24 is directly connected, Ethernet0/0
L        38.0.0.3/32 is directly connected, Ethernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.7 is directly connected, Loopback10000
```

Проверка EasyVPN Remote с VTI

```
lvv3#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  } ,
        }

IPSEC profile ezvpn-profile
   Security association lifetime: 4608000 kilobytes/2147483 seconds
   Responder-Only (Y/N): N
   PFS (Y/N): N
   DH group:  group2
   Transform sets={
     ezvpn-profile-autoconfig-transform-0:  { esp-aes esp-sha-hmac  } ,
     ezvpn-profile-autoconfig-transform-1:  { esp-aes esp-md5-hmac  } ,
     ezvpn-profile-autoconfig-transform-2:  { esp-aes esp-sha-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-3:  { esp-aes esp-md5-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-4:  { esp-192-aes esp-sha-hmac  } ,
     ezvpn-profile-autoconfig-transform-5:  { esp-192-aes esp-md5-hmac  } ,
     ezvpn-profile-autoconfig-transform-6:  { esp-256-aes esp-sha-hmac  } ,
     ezvpn-profile-autoconfig-transform-7:  { esp-256-aes esp-md5-hmac  } ,
     ezvpn-profile-autoconfig-transform-8:  { esp-256-aes esp-sha-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-9:  { esp-256-aes esp-md5-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-10:  { esp-3des esp-sha-hmac  } ,
     ezvpn-profile-autoconfig-transform-11:  { esp-3des esp-md5-hmac  } ,
     ezvpn-profile-autoconfig-transform-12:  { esp-3des esp-sha-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-13:  { esp-3des esp-md5-hmac  } , { comp-lzs  } ,
     ezvpn-profile-autoconfig-transform-14:  { esp-des esp-sha-hmac  } ,
     ezvpn-profile-autoconfig-transform-15:  { esp-des esp-md5-hmac  } ,
        }
```

Дополнительный функционал Easy VPN Remote

Режимы работы Easy VPN Remote

EasyVPN Server (не меняется)

```
aaa authentication login USER local
aaa authorization network GROUP local

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

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

router eigrp 1
 network 10.0.0.0
 redistribute static
```

Client Mode

EasyVPN Remote Client mode

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

Проверка EasyVPN Remote Client mode

```
kiev1#sh ip route
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, 4 subnets, 2 masks
D        10.0.0.2/32 [90/409600] via 10.1.1.2, 1d05h,
Ethernet0/1
      16.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
      192.168.1.0/32 is subnetted, 1 subnets
S        192.168.1.9 [1/0] via 0.0.0.0, Virtual-Access1

lvv3#sh ip route
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.9 is directly connected, Loopback10000
```

Проверка EasyVPN Remote Client mode

```
lvv3#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Ethernet0/0, Virtual-Access1
Inside interfaces:
  Ethernet0/1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list TEST_EASY_internet-list interface Ethernet0/0
refcount 0
[Id: 1] access-list TEST_EASY_enterprise-list pool TEST_EASY refcount 0
 pool TEST_EASY: netmask 255.255.255.0
        start 192.168.1.1 end 192.168.1.1
        type generic, total addresses 1, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Проверка EasyVPN Remote Client mode

```
lvv3#sh ip nat translations
Pro Inside global      Inside local    Outside local      Outside global
icmp 192.168.1.1:17    10.3.3.12:17    10.1.1.1:17        10.1.1.1:17
icmp 38.0.0.3:18       10.3.3.12:18    67.0.0.6:18        67.0.0.6:18

lvv3#sh access-lists TEST_EASY_internet-list
Extended IP access list TEST_EASY_internet-list
    10 deny ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 (2 matches)
    20 permit ip 10.3.3.0 0.0.0.255 any (2 matches)

lvv3#sh access-lists TEST_EASY_enterprise-list
Extended IP access list TEST_EASY_enterprise-list
    10 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 (2 matches)
```

Network Extension Mode

EasyVPN Remote Network extension mode

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode network-extension
 peer 16.0.0.1
 virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

Проверка EasyVPN Remote Network extension mode

```
kiev1#sh ip route
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, 5 subnets, 2 masks
D        10.0.0.2/32 [90/409600] via 10.1.1.2, 1d05h, Ether0/1
S        10.3.3.0/24 [1/0] via 0.0.0.0, Virtual-Access1

lvv3#sh ip route
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.3/32 is directly connected, Loopback3
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C        10.3.3.0/24 is directly connected, Ethernet0/1
L        10.3.3.3/32 is directly connected, Ethernet0/1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        38.0.0.0/24 is directly connected, Ethernet0/0
L        38.0.0.3/32 is directly connected, Ethernet0/0
```

Проверка EasyVPN Remote Network extension mode

```
lvv3#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 4, occurred 00:03:01 ago
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 40  Misses: 0
CEF Translated packets: 40, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 5] access-list TEST_EASY_internet-list interface Ethernet0/0
refcount 0

lvv3#sh access-lists TEST_EASY_internet-list
Extended IP access list TEST_EASY_internet-list
    10 deny ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
    20 permit ip 10.3.3.0 0.0.0.255 any
```

Network Extension Plus Mode

EasyVPN Remote Network extension plus mode

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode network-plus
 peer 16.0.0.1
 virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

Проверка EasyVPN Remote Network extension plus mode

```
kiev1#sh ip route
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, 5 subnets, 2 masks
S        10.3.3.0/24 [1/0] via 0.0.0.0, Virtual-Access1
      192.168.1.0/32 is subnetted, 1 subnets
S        192.168.1.10 [1/0] via 0.0.0.0, Virtual-Access1

lvv3#sh ip route
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.3/32 is directly connected, Loopback3
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C        10.3.3.0/24 is directly connected, Ethernet0/1
L        10.3.3.3/32 is directly connected, Ethernet0/1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        38.0.0.0/24 is directly connected, Ethernet0/0
L        38.0.0.3/32 is directly connected, Ethernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.10 is directly connected, Loopback10000
```

Настройка аутентификации в EasyVPN

Аутентификация в EasyVPN

EasyVPN Remote поддерживает аутентификацию в два этапа:

1. **Group Level Authentication**
   - preshared keys
   - сертификаты
2. **Xauth (Extended Authentication)**
   - На этом этапе удаленный маршрутизатор (или Cisco VPN Client) отправляет серверу EasyVPN имя и пароль пользователя (этот этап опциональный)
   - Логин и пароль могут проверяться:
     - Локально
     - На RADIUS
   - Для EasyVPN Remote имя и пароль могут быть:
     - сохранены в конфигурации удаленного маршрутизатора
     - введены вручную через web-аутентификацию
     - введены вручную в командной строке маршрутизатора

Group Level Authentication

Group Level Authentication

Pre-shared Аутентификация

Pre-shared Аутентификация EasyVPN Server

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

username cisco password 0 cisco

crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any
```

Pre-shared Аутентификация EasyVPN Server

```
crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

interface Loopback1
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 16.0.0.1 255.255.255.0

interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0

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

Pre-shared Аутентификация EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 Virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

Group Level Authentication
Аутентификация по сертификатам

Аутентификация по сертификатам EasyVPN Server

```
hostname kiev1
ip domain name xgu.ru

crypto key generate rsa label KeyForCERT

crypto pki trustpoint CERT
 enrollment url http://10.1.1.2:80
 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

crypto isakmp policy 1
 group 2
 authentication rsa-sig
```

Аутентификация по сертификатам EasyVPN Server

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

username cisco password 0 cisco

crypto isakmp client configuration group LVV_GROUP
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any
```

Аутентификация по сертификатам EasyVPN Server

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

crypto isakmp profile EASY_VPN
   ca trust-point CERT
   match certificate LVV
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

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

Аутентификация по сертификатам EasyVPN Remote

```
hostname lvv3
ip domain name xgu.ru

crypto key generate rsa label KeyForCERT

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

crypto pki authenticate CERT
crypto pki enroll CERT
```

Аутентификация по сертификатам EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 mode network-extension
 peer 16.0.0.1
 virtual-interface 3
 username cisco password cisco
 xauth userid mode local

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4
```

XAUTH

XAUTH

Xauth (Extended Authentication) – это опциональный этап аутентификации, который следует за групповой аутентификацией (по pre-shared паролям или по сертификатам)

- На этом этапе удаленный маршрутизатор (или Cisco VPN Client) отправляет серверу EasyVPN имя и пароль пользователя
- Для EasyVPN Remote имя и пароль могут быть:
  - сохранены в конфигурации удаленного маршрутизатора
  - введены вручную через web-аутентификацию
  - введены вручную в командной строке маршрутизатора
- XAUTH может выполняться локально на сервере, а может проверять пользователей на RADIUS*

* Для EasyVPN Remote, как правило, нет смысла выполнять аутентификацию удаленно и достаточно настроить локальную аутентификацию

Введение логина и пароля в командной строке

EasyVPN Server

```
crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL
```

EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode network-plus
 peer 16.0.0.1
 virtual-interface 3
 xauth userid mode interactive
```

Введение логина и пароля в командной строке

По умолчанию политика сервера не разрешает сохранять пароль на EasyVPN Remote и при каждом соединении, надо вводить пароль вручную в командной строке:

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Address: 192.168.1.10 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Disallowed
Split Tunnel List: 1
...

EZVPN(TEST_EASY): Pending XAuth Request, Please enter the following
command:
EZVPN: crypto ipsec client ezvpn xauth

lvv3#crypto ipsec client ezvpn xauth
Username: cisco
Password:
```

Разрешить сохранять пароль XAUTH

EasyVPN Server

```
crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL
 save-password
```

EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 virtual-interface
 username cisco password cisco
 xauth userid mode local
```

Введение логина и пароля в командной строке

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Address: 192.168.1.2 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Allowed
Split Tunnel List: 1
...
```

Web-аутентификация XAUTH

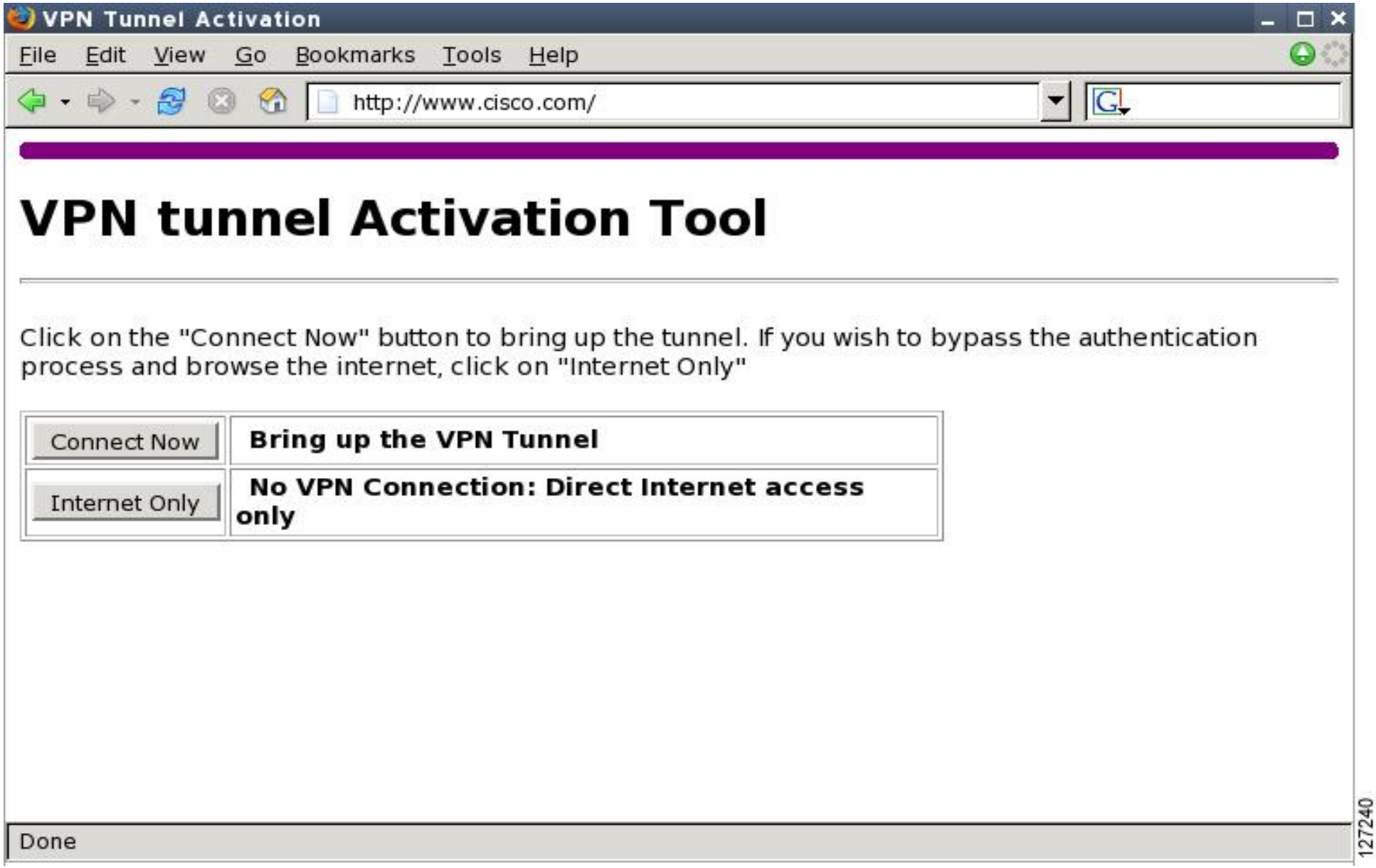
EasyVPN Server

```
crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL
```

EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 virtual-interface
 xauth userid mode http-intercept
```

Xauth через Web в EasyVPN Remote



XAUTH + RADIUS

XAUTH аутентификация на RADIUS сервере

```
aaa new-model
aaa authentication login USER group radius local
aaa authorization network GROUP group radius local

username cisco password 0 cisco

crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any

radius server radius
 address ipv4 10.1.1.100 auth-port 1645 acct-port 1646
 key 11111
```

XAUTH аутентификация на RADIUS сервере

```
crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

interface Loopback1
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 16.0.0.1 255.255.255.0

interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0

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

Split Tunneling

Split tunneling

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

username cisco password 0 cisco

crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any
 permit ip 10.1.10.0 0.0.0.255 any
```

Split tunneling

```
crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

interface Loopback1
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 16.0.0.1 255.255.255.0

interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0

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

Split tunneling

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 192.168.1.3 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Allowed
Split Tunnel List: 1
       Address    : 10.1.1.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Split Tunnel List: 2
       Address    : 10.1.10.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 16.0.0.1
```

Split tunneling

```
lvv3#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 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.0.0.3/32 is directly connected, Loopback3
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
S        10.1.10.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C        10.3.3.0/24 is directly connected, Ethernet0/1
L        10.3.3.3/32 is directly connected, Ethernet0/1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        38.0.0.0/24 is directly connected, Ethernet0/0
L        38.0.0.3/32 is directly connected, Ethernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.3 is directly connected, Loopback10000
```

Split tunneling

```
lvv3#sh ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:17 ago
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 10  Misses: 0
CEF Translated packets: 10, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list TEST_EASY_internet-list interface Ethernet0/0 refcount 1

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

```
lvv3#sh access-lists TEST_EASY_internet-list
Extended IP access list TEST_EASY_internet-list
    10 deny ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
    20 deny ip 10.3.3.0 0.0.0.255 10.1.10.0 0.0.0.255
    30 permit ip 10.3.3.0 0.0.0.255 any (1 match)
```

```
lvv3#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 38.0.0.3:11       10.3.3.12:11       16.0.0.6:11        16.0.0.6:11
```

Поддержка нескольких локальных подсетей за EasyVPN Remote

Подержка нескольких подсетей

- Не поддерживается в режиме client
- Работает только на маршрутизаторах
- Настраивается на EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 acl PROTECTED


ip access-list extended PROTECTED
 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.10.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.20.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.30.0 0.0.0.255 10.1.1.0 0.0.0.255
```

Настройка EasyVPN Server (не меняется)

```
aaa new-model
aaa authentication login USER local
aaa authorization network GROUP local

username cisco password 0 cisco

crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp client configuration group LVV_GROUP
 key lvvpass
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL ---> используется для Split Tunneling

ip local pool POOL_LVV 192.168.1.1 192.168.1.10

ip access-list extended EASY_VPN_ACL
 permit ip 10.1.1.0 0.0.0.255 any
```

Настройка EasyVPN Server (не меняется)

```
crypto isakmp profile EASY_VPN
   match identity group LVV_GROUP
   client authentication list USER
   isakmp authorization list GROUP
   client configuration address respond
   client configuration group LVV_GROUP
   virtual-template 1

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

crypto ipsec profile EASY_PROFILE
 set transform-set 3DESSHA
 set isakmp-profile EASY_VPN

interface Loopback1
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 16.0.0.1 255.255.255.0

interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0

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

Несколько локальных сетей за EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode client
 peer 16.0.0.1
 acl PROTECTED ---> Указывает какие локальные сети шифруются
 virtual-interface 3
 xauth userid mode interactive

interface Ethernet0/0
 ip address 38.0.0.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY

interface Ethernet0/1
 ip address 10.3.3.3 255.255.255.0
 crypto ipsec client ezvpn TEST_EASY inside

interface Virtual-Template3 type tunnel
 tunnel mode ipsec ipv4

ip access-list extended PROTECTED
 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.10.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.20.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ip 10.3.30.0 0.0.0.255 10.1.1.0 0.0.0.255
```

Несколько локальных сетей за EasyVPN Remote

```
kiev1#sh ip route
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, 2 masks
C        10.0.0.1/32 is directly connected, Loopback1
D        10.0.0.2/32 [90/409600] via 10.1.1.2, 00:08:25, Ethernet0/1
C        10.1.1.0/24 is directly connected, Ethernet0/1
L        10.1.1.1/32 is directly connected, Ethernet0/1
S        10.3.3.0/24 [1/0] via 0.0.0.0, Virtual-Access1
S        10.3.10.0/24 [1/0] via 0.0.0.0, Virtual-Access1
S        10.3.20.0/24 [1/0] via 0.0.0.0, Virtual-Access1
S        10.3.30.0/24 [1/0] via 0.0.0.0, Virtual-Access1

lvv3#sh ip route
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C        10.0.0.3/32 is directly connected, Loopback3
S        10.1.1.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C        10.3.3.0/24 is directly connected, Ethernet0/1
L        10.3.3.3/32 is directly connected, Ethernet0/1
D        10.3.10.0/24 [90/409600] via 10.3.3.12, 00:07:58, Ethernet0/1
D        10.3.20.0/24 [90/409600] via 10.3.3.12, 00:07:58, Ethernet0/1
D        10.3.30.0/24 [90/409600] via 10.3.3.12, 00:07:58, Ethernet0/1
      16.0.0.0/32 is subnetted, 1 subnets
S        16.0.0.1 [1/0] via 38.0.0.8
      38.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        38.0.0.0/24 is directly connected, Ethernet0/0
L        38.0.0.3/32 is directly connected, Ethernet0/0
```

Варианты активации туннеля

Варианты активации туннеля

- Варианты настройки
  - Auto (автоматический)
  - Manual (вручную)
  - Traffic-triggered
- Настраивается на EasyVPN Remote

Automatic activation

```
crypto ipsec client ezvpn TEST_EASY
 connect auto
 group LVV_GROUP key lvvpass
 mode network-plus
 peer 16.0.0.1
 virtual-interface 3
 username cisco password cisco
 xauth userid mode local
```

- Automatic activation это режим по умолчанию
- В этом режиме туннель будет автоматически создаваться, если существуют настройки EasyVPN Remote

Manual activation

```
crypto ipsec client ezvpn TEST_EASY
 connect manual
 group LVV_GROUP key lvvpass
 mode network-plus
 peer 16.0.0.1
 virtual-interface 3
 username cisco password cisco
 xauth userid mode local
```

- Туннель создается только после того как на EasyVPN Remote выполнена команда:

  crypto ipsec client ezvpn connect

- Выключить туннель можно командой:

  clear crypto ipsec client ezvpn

Manual activation

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: CONNECT_REQUIRED
Last Event: CONN_DOWN
Save Password: Allowed
Current EzVPN Peer: 16.0.0.1

lvv3#crypto ipsec client ezvpn connect

lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Address: 192.168.1.7 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Allowed
Current EzVPN Peer: 16.0.0.1
```

Traffic-Triggered activation

```
crypto ipsec client ezvpn TEST_EASY
 connect acl CONNECT_EASY
 group LVV_GROUP key lvvpass
 mode network-plus
 peer 16.0.0.1
 virtual-interface 3
 username cisco password cisco
 xauth userid mode local

ip access-list extended CONNECT_EASY
 permit ip 10.3.3.0 0.0.0.255 host 10.1.1.1
```

- Туннель создается только после того как через маршрутизатор пройдет соответствующий трафик (указанный в ACL)
- Выключить туннель можно командой:

```
clear crypto ipsec client ezvpn
```

Traffic-Triggered activation

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Connect : ACL based with access-list CONNECT_EASY
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 192.168.1.6 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Allowed
Split Tunnel List: 1
       Address    : 10.1.1.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 16.0.0.1
```

Backup Peer
DPD

Backup Peer

Backup Peers на EasyVPN Server

```
crypto isakmp client configuration group LVV_GROUP
 dns 10.1.1.100
 domain xguru.ru
 pool POOL_LVV
 acl EASY_VPN_ACL
 save-password
 backup-gateway 27.0.0.2
 backup-gateway 35.0.0.3
```

Backup Peers на EasyVPN Remote

```
crypto ipsec client ezvpn TEST_EASY
 connect manual
 mode network-extension
 peer 16.0.0.1
 peer 22.2.2.2
 peer 33.3.3.3
 virtual-interface 3
 username cisco password cisco
 xauth userid mode local
```

Список Backup Peer на EasyVPN Remote

Список Backup Peers, который отправляет EasyVPN Server приоритетнее того, который задан локально на клиенте (Cisco VPN Client или EasyVPN Remote), и переписывает значения списком сервера.

```
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
DNS Primary: 10.1.1.100
Default Domain: xguru.ru
Save Password: Allowed
Split Tunnel List: 1
       Address    : 10.1.1.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 16.0.0.1
Backup Gateways
 (0): 27.0.0.2
 (1): 35.0.0.3
```

DPD

crypto isakmp keepalive 10 2

```
lvv3#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.

1001 38.0.0.3  16.0.0.1 ACTIVE des  sha  rsig 2  23:56:41 CDX
       Engine-id:Conn-id =  SW:1
```

Переключение на Backup Peer на EasyVPN Remote

```
lvv3#sh run | i keep
crypto isakmp keepalive 10

lvv3#sh clock
*08:51:56.021 UTC Sat Aug 1 2015
lvv3#
EZVPN: Failing over to BACKUP SERVER list
%CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=cisco  Group=
Server_public_addr=16.0.0.1
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
lvv3#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to down

lvv3#sh clock
*08:52:25.505 UTC Sat Aug 1 2015
lvv3#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : TEST_EASY
Inside interface list: Ethernet0/1
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: READY
Last Event: CONN_DOWN
Save Password: Allowed
Current EzVPN Peer: 27.0.0.2
Backup Gateways
 (0): 27.0.0.2
 (1): 35.0.0.3
```

Настройка EasyVPN на маршрутизаторах Cisco

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

Сетевые Дни