

IPsec VPN

- VPN. IKE
 - access profile
 - address-assignment pool
 - assign-interface
 - authentication algorithm
 - authentication mode
 - authentication method
 - bind-interface vti
 - certificate
 - data-tunnel address
 - dead-peer-detection action
 - dead-peer-detection interval
 - dead-peer-detection timeout
 - description
 - dh-group
 - encryption algorithm
 - ike-policy
 - ip prefix
 - lifetime seconds
 - local address
 - local interface
 - local network
 - management-tunnel address
 - mobike disable
 - mode
 - mode
 - password
 - password local-crt-key
 - pfs dh-group
 - pre-shared-key
 - proposal
 - remote address
 - remote network
 - remote network dynamic client
 - security ike gateway
 - security ike policy
 - security ike proposal
 - security ike session uniqueids
 - show security ike
 - user
 - version
 - xauth access-profile
- VPN. IPsec
 - authentication algorithm
 - description
 - enable
 - encryption algorithm
 - ike dscp
 - ike establish-tunnel
 - ike gateway
 - ike idle-time
 - ike rekey disable
 - ike rekey margin
 - ike rekey randomization
 - ike ipsec-policy
 - lifetime
 - manual authentication algorithm
 - manual authentication key
 - manual bind-interface vti
 - manual encryption algorithm
 - manual encryption key
 - manual mode
 - manual protocol
 - manual spi
 - mode
 - proposal
 - protocol
 - security ipsec policy
 - security ipsec proposal
 - security ipsec vpn
 - show security ipsec
 - show security ipsec vpn authentication
 - show security ipsec vpn status
 - type

VPN. IKE

access profile

IKE-GATEWAY .

(no) IKE-GATEWAY.

[no] access profile <NAME>

<NAME>- IKE-GATEWAY, 31 .

15

CONFIG

```
esr(config)# access profile OFFICE
```

address-assignment pool

IPsec-.

(no) .

[no] address-assignment pool <NAME>

<NAME>- , 31 .

10

CONFIG

```
esr(config)# address-assignment pool CENTER
esr(config-pool)#
```

assign-interface

loopback- IPsec-VPN-.

(no) loopback- IPsec-VPN-.

assign-interface loopback <LOOPBACK>[-<LOOPBACK>

no assign-interface

<LOOPBACK> – loopback-, [1..8].

10

CONFIG-IKE-GW

```
esr(config-ike-gw)# assign-interface loopback 3
```

authentication algorithm

, IKE-. IKE- (authentication, . [password](#)).
(no) .

```
authentication algorithm <ALGORITHM>  
no authentication algorithm
```

<ALGORITHM> – , : md5, sha1, sha2-256, sha2384, sha2-512.

sha1

15

CONFIG-IKE-PROPOSAL

```
esr(config-ike-proposal)# authentication algorithm md5
```

authentication mode

XAUTH , IPsec.
(no) .

```
authentication mode { local | radius | client }  
no authentication mode
```

local – , ;

radius – , RADIUS-;

client – xauth-.

CONFIG-IKE-POLICY

```
esr(config-ike-policy)# authentication mode local
```

authentication method

IKE-. IKE-, IKE- (. [pre-shared-key](#)). IKE- .

(no) .

```
authentication method <METHOD>
```

```
no authentication method
```

<METHOD>- . . :

- pre-shared-key - , ;
- rsa-public-key - , RSA-;
- xauth-psk-key - , .

pre-shared-key

CONFIG-IKE-POLICY

```
esr(config-ike-proposal)# authentication method pre-shared-key
```

bind-interface vti

, «route-based».

(no) .

```
bind-interface vti <VTI>
```

```
no bind-interface vti
```

<VTI>- VTI.

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# bind-interface vti 1
```

certificate

.
(no) .

```
certificate <CERTIFICATE-TYPE> <NAME>  
no certificate <CERTIFICATE-TYPE>
```

<CERTIFICATE-TYPE> - , :

- ca - ;
- crl - ;
- local-crt - ;
- local-crt-key - RSA ;
- local-id - . Subject "any";
- remote-crt - . "any" ;
- remote-id - . Subject "any".

<NAME> - , 31 .

15

CONFIG-IKE-POLICY

```
esr(config-ike-policy)# certificate ca KEY
```

data-tunnel address

IP- GRE data , , IPsec . GRE data . (ELTEX_DATA_IP(28684).
(no) IP- GRE data .

```
data-tunnel address <ADDR>  
no data-tunnel address
```

<ADDR> -IP-, GRE data AAA.BBB.CCC.DDD, [0..255].

.

CONFIG-POOL

```
esr(config-pool)# data-tunnel address 192.168.2.66
```

dead-peer-detection action

, , IPsec , Dead Peer Detection.

Dead Peer Detection (DPD) – . R-U-THERE (IKE 1) INFORMATIONAL (IKE 2) IPsec.

(no) .

```
dead-peer-detection action <MODE>
```

```
no dead-peer-detection action
```

<MODE> – DPD:

- restart – ;
- clear – ;
- hold – ;
- none – , .

none

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# dead-peer-detection action clear
```

dead-peer-detection interval

DPD.

DPD [certificate](#).

(no) .

```
dead-peer-detection interval <SEC>
```

```
no dead-peer-detection interval
```

<SEC> – DPD, [1..180].

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# dead-peer-detection interval 15
```

dead-peer-detection timeout

, DPD.

DPD [certificate](#).

(no) .

dead-peer-detection timeout <SEC>

no dead-peer-detection timeout

<SEC> – DPD, [1..180].

30

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# dead-peer-detection timeout 60
```

description

, IKE.

(no) .

description <DESCRIPTION>

no description

<DESCRIPTION> – , 255.

10

CONFIG-IKE-PROPOSAL

CONFIG-IKE-POLICY
CONFIG-IKE-GATEWAY

```
esr(config-ike-proposal)# description "my proposal"
```

dh-group

-. IKE- - , .
(no) .

dh-group <DH-GROUP>
no dh-group

<DH-GROUP> – -, [1, 2, 5, 14, 15, 16, 17, 18].

1

15

CONFIG-IKE-PROPOSAL

```
esr(config-ike-proposal)# dh-group 5
```

encryption algorithm

, IKE-.
(no) .

encryption algorithm <ALGORITHM>
no encryption algorithm

<ALGORITHM> – , : des, 3des, blowfis28, blowfis92, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

3des

15

CONFIG-IKE-PROPOSAL


```
esr(config-ike-proposal)# encryption algorithm aes128
```

ike-policy

IKE .

(no) .

```
[no] ike-policy <NAME>
```

<NAME> – IKE, 31 .

15

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# ike-policy ike_poll
```

ip prefix

, IPsec-.

(no) , IPsec-.

```
ip prefix <ADDR/LEN>
```

```
no ip prefix
```

<ADDR/LEN> – IP-, AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32].

.

10

CONFIG-POOL

```
esr(config-pool)# ip prefix 192.168.0.0/16
```

lifetime seconds

IKE.

(no) .

lifetime seconds <SEC>
no lifetime seconds

<SEC> – , [4..86400] .

10800

10

CONFIG-IKE-POLICY

```
esr(config-ike-proposal)# lifetime 21600
```

local address

IP- IPsec-.

(no) IP- .

local address <ADDR>
no local address

<ADDR> – IP- .

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# local address 192.168.1.1
```

local interface

IP-, IPsec-.

(no) IP-, .

local interface <IF>
no local interface

<IF> – , , .

CONFIG-IKE-GW

```
esr(config-ike-gw)# local interface gigabitethernet 1/0/1
```

local network

IP- , IP- . IPsec-

(no) IP- .

```
[no] local network <ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port <PORT> ] ]
```

<ADDR/LEN> – IP- . AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32];

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

<ID> – IP-, [0x00-0xFF];

<PORT> – TCP/UDP-, [1..65535].

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# local network 192.168.1.0/24 protocol tcp port 22
```

management-tunnel address

IP- GRE management , , IPsec . GRE management . (ELTEX_MANAGEMENT_IP(28683).

(no) IP- GRE management .

```
management-tunnel address <ADDR>
no management-tunnel address
```

<ADDR> –IP- GRE management , AAA.BBB.CCC.DDD, [0..255].

CONFIG-POOL

```
esr(config-pool)# management-tunnel address 192.168.2.87
```

mobike disable

(IP- local address).

(no) local address .

[no] mobike disable

.

.

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gateway)# mobike disable
```

mode

IKE.

(no) .

mode <MODE>

no mode

<MODE> – IKE, :

- main – :
 - , IKE- IKE ;
 - -, . ;
 - . IKE.
- aggressive – , , :
 - () , IKE-: SA, -, ;
 - SA, , IKE-;
 - .

main

15

CONFIG-IKE-POLICY

```
esr(config-ike-policy)# mode aggressive
```

mode

.
(no) .

mode <MODE>
no mode

<MODE> - , :

- policy-based - ;
- route-based - , .

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# mode route-based
```

password

IKE-GETWAY. , sha512.
(no) IKE-GETWAY .

password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }
no password

<CLEAR-TEXT> -, [8..32], [0-9a-fA-F].

<HASH_SHA512> -- sha512, 110 .

15

CONFIG-PROFILE

```
esr(config-profile) password tteesstt
```

password local-crt-key

([certificate](#))

(no) .

```
password local-crt-key ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }  
no password local-crt-key
```

<CLEAR-TEXT> – , [8..32] , [0-9a-fA-F].

<HASH_SHA512> -- sha512, 110 .

15

CONFIG-IKE-POLICY

```
esr(config-ike-policy) password tteesstt
```

pfs dh-group

-. IPsec- – , .

(no) .

```
pfs dh-group <DH-GROUP>  
no pfs dh-group
```

<DH-GROUP> – -, [1, 2, 5, 14, 15, 16, 17, 18].

1

15

CONFIG-IPSEC-PROPOSAL

```
esr(config-isec-proposal)# pfs dh-group 5
```

pre-shared-key

, , .

(no) .

```
pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal { <HEX> | encrypted <ENCRYPTED-HEX> } }
```

```
no pre-shared-key
```

<TEXT> – [1..64] ASCII ;

<HEX> – [1..32] [2..128] (0xYYYY...) (YYYY...).

<ENCRYPTED-TEXT> – [1..32], [2..128];

<ENCRYPTED-HEX> – [2..64], [2..256].

none

15

CONFIG-IKE-POLICY

```
esr(config-ike-policy)# pre-shared-key hexadecimal abc123
```

proposal

IKE .

(no) IKE.

[no] proposal <NAME>

<NAME> – IKE, 31 .

15

CONFIG-IKE-POLICY

```
esr(config-ike-policy)# proposal ike_prop1
```

remote address

IP- IPsec.

(no) IP- .

```
remote address { <ADDR> | any }
```

```
no remote address
```

<ADDR> – IP- .
any – IKE- IP-.

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# remote address 192.168.1.2
```

remote network

IP- , IP- , XAUTH. , , IPsec-
(no) IP- .

```
remote network { dynamic pool <POOL> | <ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port <PORT> ] ] | any }  
no remote network { dynamic pool | <ADDR/LEN> [ protocol { <TYPE> | <ID> } [ port <PORT> ] ] | any }
```

<POOL> – XAUTH;
<ADDR/LEN> – IP- . AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32];
<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;
<ID> – IP-, [0x00-0xFF];
<PORT> – TCP/UDP-, [1..65535];
any – , .

10

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# remote network 192.168.0.0/24 protocol tcp port 22
```

remote network dynamic client

IPsec-VPN-
(no) IPsec-VPN-.

[no] remote network dynamic client

.

10

CONFIG-IKE-GW

```
esr(config-ike-gw)# remote network dynamic client
```

security ike gateway

IKE SECURITY IKE GATEWAY. IKE , . VTI, , IKE, .
(no) IKE.

```
[no] security ike gateway <NAME>
```

<NAME> – IKE, 31 . «all» IKE-.

10

CONFIG

```
esr(config)# security ike gateway ike_gw1  
esr(config-ike-gw)#
```

security ike policy

IKE, IKE, IKE.
(no) . SECURITY IKE POLICY.

```
[no] security ike policy <NAME>
```

<NAME> – IKE, 31 . «all» IKE .

10

CONFIG

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)#
```

security ike proposal

IKE (Internet Key Exchange), , -, IKE VPN Security Association (SA). , SA. (no) .

```
[no] security ike proposal <NAME>
```

<NAME> - IKE, 31 . «all» IKE-.

10

CONFIG

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)#
```

security ike session uniqueids

- XAUTH /.

(no) .

```
security ike session uniqueids <MODE>
no security ike session uniqueids
```

<MODE> - -, :

- no - XAUTH , XAUTH "INITIAL_CONTACT", IP-. , XAUTH . XAUTH IP-.
- never - XAUTH . XAUTH IP-. "INITIAL_CONTACT" .
- replace - XAUTH . XAUTH IP-.
- keep - XAUTH . XAUTH .

never

10

CONFIG

```
esr(config)# security ike session uniqueids replace
```

show security ike

, .

```
show security ike { gateway | policy | proposal } [<NAME>]
```

```
gateway - «gateway» ;
policy - «policy» ;
proposal - «proposal» ;
<NAME> - . , , .
```

ROOT

esr# show security ike proposal

Proposal

~~~~~

| Name | Auth    | Encryption | DH | Hash | Lifetime |
|------|---------|------------|----|------|----------|
| aaa  | pre-sha | 3des       | 1  | sha1 | 3600     |
|      | red-key |            |    |      |          |

esr# show security ike policy

Policy

~~~~~

Name	Mode	Proposal
ike_poll	main	ike_prop1

esr# show security ike gateway ik_gw

Description: --

IKE Policy: ike_poll

IKE Version: v1-only

Mode: route-based

Binding interface: vti1

IKE Dead Peer Detection:

Action: none

Interval: 2

Timeout: 30

user

```
IKE-GETWAY.
(no) .
(config-profile).
```

```
[no] user <NAME>
```

```
<NAME> - , 31 .
```

CONFIG-ACCESS-PROFILE

```
esr(config-access-profile)# user connector963
```

version

IKE.

(no) .

version <VERSION>

no version

<version> – IKE-: v1-only v2-only.

v1-only

15

CONFIG-IKE-GATEWAY

```
esr(config-ike-gw)# version v2-only
```

xauth access-profile

XAUTH.

(no) .

[no] xauth access-profile <NAME> [client <USER-NAME>

<NAME> – XAUTH, 31;

<USER-NAME> – xauth-, 31.

15

CONFIG-IKE-GATEWAY

```
esr(config-ike-gateway)# xauth access-profile OFFICE
```

VPN. IPsec

authentication algorithm

. (no) .

authentication algorithm <ALGORITHM>

no authentication algorithm

<ALGORITHM> – , : md5, sha1, sha2-256, sha2384, sha2-512.

sha1

15

CONFIG-IPSEC-PROPOSAL

```
esr(config-ipsec-proposal)# authentication algorithm md5
```

description

.
(no) .

description <DESCRIPTION>

no description

<DESCRIPTION> – , 255 .

10

CONFIG-IPSEC-VPN

CONFIG-IPSEC-PROPOSAL

CONFIG-IPSEC-POLICY

```
esr(config-ipsec-vpn)# description "VPN to Moscow Office"
```

enable

IPsec VPN.

(no) IPsec VPN.

[no] enable

.

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# enable
```

encryption algorithm

. (no) .

encryption algorithm <ALGORITHM>

no encryption algorithm

<ALGORITHM> – , : null, des, 3des, blowfis28, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

3des

15

CONFIG-IPSEC-PROPOSAL

```
esr(config-ipsec-proposal)# encryption algorithm blowfish128
```

ike dscp

DSCP IP- IKE-.

(no) DSCP .

ike dscp <DSCP>

no ike dscp

<DSCP> – DSCP, [0..63].

63

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike dscp 40
```

ike establish-tunnel

VPN. , VPN «ike». [mode](#).

(no) .

ike establish-tunnel <MODE>

no ike establish-tunnel

<MODE> – VPN:

- by-request – ;
- route – , ;
- immediate – . VPN immediate, VPN CLI .

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike establish-tunnel route
```

ike gateway

IKE- VPN. , VPN «ike». [mode](#).

ike gateway <NAME>

no ike gateway

<NAME> – IKE-, 31 .

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike gateway ike_gw1
```

ike idle-time

SA.

(no) .

```
ike idle-time <TIME>
```

```
no ike idle-time
```

<TIME> - , [4..86400]

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike idle-time 3600
```

ike rekey disable

IKE- , .

(no) .

```
[no] ike rekey disable
```

.

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike rekey disable
```

ike rekey margin

IKE- .

(no) .

```
Ike rekey margin { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }  
no ike rekey margin { seconds | packets | kilobytes }
```

<SEC> – , (lifetime seconds, . [lifetime](#)). [4..86400].

<PACKETS> – , (lifetime packets, . [lifetime](#)). [4..86400].

<KB> – , (lifetime kilobytes, . [lifetime](#)). [4..86400].

– 540 .

– .

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike rekey margin seconds 1800
```

ike rekey randomization

margin seconds, margin packets, margin kilobytes.

(no) .

```
ike rekey randomization <VALUE>
```

```
no ike rekey randomization
```

<VALUE> – , [1..100]

100%

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike rekey randomization 10
```

ike ipsec-policy

IPsec- VPN. , VPN «ike». [mode](#).

```
ike ipsec-policy <NAME>
no ike ipsec-policy
```

<NAME> – IPsec-, 31 .

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
```

lifetime

IPsec-.

(no) .

```
lifetime { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }
no lifetime { seconds | packets | kilobytes }
```

<SEC> – IPsec-, . [1140..86400].

<PACKETS> – , IPsec-. [4..86400].

<KB> – , IPsec-. [4..86400].

3600

10

CONFIG-IPSEC-POLICY

```
esr(config-ipsec-proposal)# lifetime seconds 3600
```

manual authentication algorithm

. , VPN «manual». [mode](#).

(no) .

manual authentication algorithm <ALGORITHM>

no manual authentication algorithm

<ALGORITHM> – , [md5, md5-128, sha1, sha1-160, aesxcbc, sha2-256, sha2-384, sha2-512].

none

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual authentication algorithm sha1
```

manual authentication key

. , VPN «manual». [mode](#).

manual authentication key { ascii-text {<TEXT> | encrypted <ENCRYPTED-TEXT>} | hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }

no manual authentication key

<TEXT> – [1..64] ASCII ;

<HEX> – [1..32] [2..128] (0xYYYYY...) (YYYYY...);

<ENCRYPTED_TEXT> – [1..32], [2..128];

<ENCRYPTED_HEX> – [2..64], [2..256] .

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual authentication key hexadecimal abcdef
```

manual bind-interface vti

, route-based. , VPN «manual». [mode](#).

(no) .

manual bind-interface vti <VTI>

no manual bind-interface vti

<VTI> – VTI, :

ESR-10/12V/12VF/14VF – [1..10];

ESR-20/21/100/200 – [1..250];

ESR-1000/1200/1500/1511/1700/3100 – [1..500].

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual bind-interface vti 0
```

manual encryption algorithm

. , VPN «manual». [mode](#).

(no) .

manual encryption algorithm <ALGORITHM>

no manual encryption algorithm

<ALGORITHM> – , : des, 3des, blowfis28, blowfis92, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

3des

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual encryption algorithm blowfis28
```

manual encryption key

. , VPN «manual». [mode](#).

(no) .

manual encryption key { ascii-text { < TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal { <HEX> | encrypted <ENCRYPTED-HEX> } }

no manual encryption key

<TEXT> – [1..36] ASCII ;

<HEX> – [1..24] [2..72] (0xYYYY...) (YYYY...);

<ENCRYPTED-TEXT> – [1..24], [2..72];

<ENCRYPTED-HEX> – [2..36], [2..144].

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual encryption key hexadecimal 0x123456
```

manual mode

. , VPN «manual». [mode](#).

(no) .

manual mode <MODE>

no manual mode

<MODE> – :

- policy-based – ;
- route-based – , .

10

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual mode route-based
```

manual protocol

. , VPN «manual». [mode](#).

(no) .

manual protocol <TYPE>

no manual protocol

<TYPE> – , :

- ah – , ;
- esp – .

esp

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual protocol ah
```

manual spi

, VPN «manual». [mode](#).
(no) .

manual spi <HEX>
no manual spi

<HEX> – , 32 (8) (0xYYYY...) (YYYY...).

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# manual spi FF
```

mode

, VPN.

mode <MODE>
no mode

- <MODE> – VPN:
- ike – , , IKE;
 - manual – VPN. IKE- . , .

15

CONFIG-IPSEC-VPN

```
esr(config-ipsec-vpn)# mode ike
```

proposal

IPsec.

(no) .

[no] proposal <NAME>

<NAME> - IPsec, 31 .

15

CONFIG-IPSEC-POLICY

```
esr(config-ipsec-policy)# proposal ipsec_prop1
```

protocol

.

(no) .

protocol <PROTOCOL>

no protocol

<PROTOCOL> - , :

- ah - , ;
- esp - .

esp

15

CONFIG-IPSEC-PROPOSAL

```
esr(config-ipsec-proposal)# protocol ah
```

security ipsec policy

IPsec, IPsec IKE.

(no) .

SECURITY IPSEC POLICY.

[no] security ipsec policy <NAME>

<NAME> – IPsec, 31. «all» IPsec-.

10

CONFIG

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)#
```

security ipsec proposal

IPsec. IPsec , IPsec, .

(no) .

SECURITY IPSEC PROPOSAL.

[no] security ipsec proposal <NAME>

<NAME> – IPsec, 31. «all» IPsec-.

10

CONFIG

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)#
```

security ipsec vpn

VPN IPsec SECURITY IPSEC VPN.

(no) VPN.

[no] security ipsec vpn <NAME>

<NAME> – VPN, 31. «all» VPN.

CONFIG

```
esr(config)# security ipsec vpn ipsec_vpnl
esr(config-ipsec-vpn)#
```

show security ipsec

VPN, IPsec.

show security ipsec { vpn configuration | policy | proposal } [<NAME>]

vpn configuration – VPN;

policy – IPsec;

proposal – IPsec;

<NAME> – . VPN, .

ROOT

```
esr# show security ipsec proposal
Proposal
~~~~~
Name          Prot  Enc. alg.      Auth. alg.      Lifetime
-----
ipsec_prop1   esp  aes128         sha1             28800 sec
esr# show secu      rity ipsec policy
Name          Description      Proposal
-----
ipsec_poll1               ipsec_prop1
Master# show security ipsec vpn configuration IPSECVPN
Description:      --
State:            Enabled
IKE:
  Establish tunnel:      immediate
  IPsec policy:          IPSECPOLICY
  IKE gateway:           IKEGW
  IKE DSCP:              63
  IKE idle-time:         0s
  IKE rekeying:          Enabled
    Margin time:         540s
    Margin kilobytes:    0
    Margin packets:      0
    Randomization:       100%
```

show security ipsec vpn authentication

IPsec-VPN-.

```
show security ipsec vpn authentication <NAME> [ vrf <VRF> ]
```

<NAME>- IPsec VPN, 31 .

<VRF>- VRF, 31 , DNS-.

10

ROOT

```
esr# show security ipsec vpn authentication
Local host      Remote host      Local subnet      Remote subnet
Authentication                                     State
-----
2.2.2.1         2.2.2.2         192.168.2.0/24    192.168.1.1/32    Xauth PSK, login:
ipsec                               Established
```

show security ipsec vpn status

VPN, IKE- VPN .

```
show security ipsec vpn status [ vrf <VRF> ] [ <NAME> ]
```

<NAME>- VPN, 31 ;

<VRF>- VRF, 31 .

10

ROOT

```
esr# show security ipsec vpn status
Name      Local host  Remote host  Initiator spi  Responder spi  State
-----
ipsec_vpn1 10.100.14.1 10.100.14.2 0x05d8e0ac3543f0cb 0xcfa1c4179d001154 Established
```

type

IPsec.

(no) .

```
type <TYPE>  
no type
```

<TYPE> – IPsec, :

- tunnel;
- transport.

tunnel

15

CONFIG-IPSEC-VPN

```
esr(config-access-vpn)# type transport
```