

- GRE-
  - IP-GRE-
- DMVPN
  - L2TPv3-
- L2TPv3-
  - L2TPv3-
- IPsec VPN
  - Route-based IPsec VPN
  - Route-based IPsec VPN
  - Policy-based IPsec VPN
  - Policy-based IPsec VPN
  - Remote Access IPsec VPN
  - Remote Access IPsec VPN
- LT-
  -

## GRE-

GRE (. Generic Routing Encapsulation — ) — . — OSI IP-. GRE VPN 3- OSI. ESR GRE-, . .

1	L3-, GRE-.		
2	GRE- .	esr(config)# tunnel gre <INDEX>	<INDEX> – : <ul style="list-style-type: none"> <li>• ESR-10/12V(F)/14VF – [1..10];</li> <li>• ESR-20/21/100/200 – [1..250];</li> <li>• ESR-1000/1200/1500/1700 – [1..500].</li> </ul>
3	VRF, GRE- ().	esr(config-gre )# ip vrf forwarding <VRF>	<VRF> – VRF, 31 .
4	( ).	esr(config-gre)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
5	IP- .	esr(config-gre)# local address <ADDR>	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255].
		esr(config-gre)# local interface <IF>	<IF> – , IP- .
6	IP- .	esr(config-gre)# remote address <ADDR>	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255].
7	GRE .	esr(config-gre)# mode <MODE>	<MODE> – GRE : <ul style="list-style-type: none"> <li>• <b>ip</b> – IP- GRE;</li> <li>• <b>ethernet</b> – Ethernet- GRE.</li> </ul> : ip
8	IP- ( ip).	esr(config-gre)# ip address <ADDR/LEN>	<ADDR/LEN> – IP- AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32]. 8 IP- . IPv4- . IP-.
9	GRE- ( ethernet).	esr(config-gre)# bridge-group <BRIDGE-ID>	<BRIDGE-ID> – , : <ul style="list-style-type: none"> <li>• ESR-10/12V(F)/14VF – [1..50];</li> <li>• ESR-20/21/100/200 – [1..250];</li> <li>• ESR-1000/1200/1500/1700 – [1..500]</li> </ul>
10	GRE- firewall (. Firewall).	esr(config-gre)# security-zone<NAME>	<NAME> – , 12 .

		esr(config-gre)# ip firewall disable	
11	MTU (Maximum Transmission Unit) (. MTU 1500 "system jumbo-frames"	esr(config-gre)# mtu <MTU>	<MTU> – MTU, : <ul style="list-style-type: none"> <li>• ESR-10/12V(F)/14VF – [1280..9600];</li> <li>• ESR-20/21 – [1280..9500];</li> <li>• ESR-100/200/1000/1200/1500/1700 [1280..10000].</li> </ul> : 1500.
12	TTL (.)	esr(config-gre)# ttl <TTL>	<TTL> – TTL, [1..255]. : .
13	DSCP IP- (.)	esr(config-gre)# dscp <DSCP>	<DSCP> – DSCP, [0..63]. : .
14	(Key) GRE ( RFC 2890) . . . (.)	esr(config-gre)# key <KEY>	<KEY> – KEY, [1..2000000]. : .
15	GRE- . . ( )	esr(config-gre)# local checksum	
16	GRE-. . ( )	esr(config-gre)# remote checksum	
17	( )	esr(config-gre)# keepalive enable	
18	keepalive ( )	esr(config-gre)# keepalive timeout <TIME>	<TIME> – , [1..32767]. : 10
19	( )	esr(config-gre)# keepalive retries <VALUE>	<VALUE> – , [1..255]. : 5
20	IP- keepalive ( ethernet)	esr(config-gre)# keepalive dst-address <ADDR>	<ADDR> – IP- GRE-.
21	, ( )	esr(config-gre)# load-average <TIME>	<TIME> – , [5..150]. : 5
22	snmp-trap /.	esr(config-gre)# snmp init-trap	
23	IP- DHCP GRE- keepalive ( )	esr(config-gre)# keepalive dhcp dependent-interface <IF>	<IF> – /, IP- DHCP
24	GRE- IP- /, keepalive dhcp dependent-interface ( )	esr(config-gre)# keepalive dhcp link- timeout <SEC>	<SEC> – GRE- IP- DHCP
25	MSS (Maximum segment size) TCP- (.)	esr(config-gre)# ip tcp adjust-mss <MSS>	<MSS> – MSS, [500..1460]. : 1460
26	(.)	esr(config-gre)# history statistics	
27	.	esr(config-gre)# enable	
GRE- : <ul style="list-style-type: none"> <li>• QoS (. QoS);</li> <li>• proxy (. HTTP/HTTPS-);</li> <li>• (. Netflow sFlow);</li> <li>• (. );</li> <li>• BRAS (. BRAS (Broadband Remote Access Server));</li> </ul>			

## IP-GRE-

:

L3-VPN IP-, GRE.

- IP- 115.0.0.1;
- IP- 114.0.0.10;
- IP- 25.0.0.1/24.



:

WAN GRE , , WAN.

GRE 10:

```
esr(config)# tunnel gre 10
```

(IP-, WAN):

```
esr(config-gre)# local address 115.0.0.1
esr(config-gre)# remote address 114.0.0.10
```

IP- 25.0.0.1/24:

```
esr(config-gre)# ip address 25.0.0.1/24
```

, , firewall. :

```
esr(config-gre)# security-zone untrusted
```

:

```
esr(config-gre)# enable
esr(config-gre)# exit
```

. GRE:

```
esr(config)# ip route 172.16.0.0/16 tunnel gre 10
```

, GRE- .

GRE- :

- GRE :

```
esr(config-gre)# local checksum
```

- GRE :

```
esr(config-gre)# remote checksum
```

- :

```
esr(config-gre)# key 15808
```

- DSCP, MTU, TTL:

```
esr(config-gre)# dscp 44
esr(config-gre)# mtu 1426
esr(config-gre)# ttl 18
```

- keepalive:

```
esr(config-gre)# keepalive enable
esr(config-gre)# keepalive timeout <TIME>
esr(config-gre)# keepalive retries <VALUE>
```

:

```
esr# show tunnels status gre 10
```

:

```
esr# show tunnels counters gre 10
```

:

```
esr# show tunnels configuration gre 10
```

IPv4-over-IPv4 .



firewall GRE(47).

## DMVPN

DMVPN (*Dynamic Multipoint Virtual Private Network*) – , . DMVPN Hub-and-Spoke, VPN Spoke-to-Spoke Spoke-to-Hub . , , Hub.

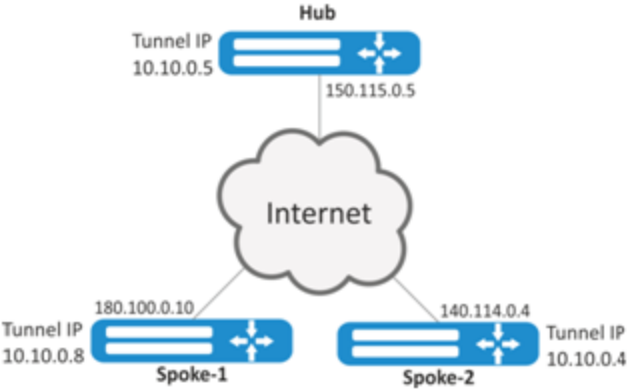
, (NHC) IPsec- () (NBMA) NHRP- (NHS). NHC, , . , c .

1	"" IP-, .		
2	IPsec- GRE-.		. <a href="#">Policy-based IPsec VPN</a> .
2	GRE- .	esr(config)# tunnel gre <INDEX>	<INDEX>- .
3	GRE- multipoint.	esr(config-gre )# multipoint	
4	NHRP ().	esr(config-gre)# ip nhrp authentication <WORD>	<WORD>- , [1..8], [0-9a-fA-F].
5	, NHS ().	esr(config-gre)# ip nhrp holding-time <TIME>	<TIME>- , , [1..65535]. : 7200
6	«()» NHRP.	esr(config-gre)# ip nhrp nhs <ADDR> [ no-registration ]	<ADDR/LEN>- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32]; <ul style="list-style-type: none"><li>• no - registration — NHRP .</li></ul>
7	«» «» NBMA .	esr(config-gre)# ip nhrp map <ADDR> <ADDR>	<ADDR>- IP- AAA.BBB.CCC.DDD, [0..255].

8	.	esr(config-gre)# ip nhrp multicast { dynamic   nhs   <ADDR> }	<ul style="list-style-type: none"><li>• <b>dynamic</b> — , ;</li><li>• <b>nhs</b> — ;</li></ul> <ADDR> — , AAA.BBB.CCC.DDD, [0..255].
9	NHRP Traffic Indication . NHS ( ).	esr(config-gre)# ip nhrp redirect	
10	. NHC( ).	esr(config-gre)# ip nhrp shortcut	
11	IPsec-VPN mGRE ( ).	esr(config-gre)# ip nhrp ipsec <WORD> { static   dynamic }	<WORD> – VPN, 31 ; <ul style="list-style-type: none"><li>• <b>static</b> — , NHS;</li><li>• <b>dynamic</b> — , NHC.</li></ul>
12	NHRP.	esr(config-gre)# ip nhrp enable	
13	IP- .		
- GRE- ( . GRE- )			

:

DMVPN , mGRE-, NHRP (Next Hop Resolution Protocol), (BGP), Ipsec. HUB . HUB – DMVPN c (NHS), – DMPVN (NHC).



Hub IP- — 150.115.0.5;  
Spoke-1 IP- — 180.100.0.10;  
Spoke-2 IP- — 140.114.0.4.

IPsec VPN:

IKE:

- -: 2;
- : AES128;
- : SHA1.

IPsec:

- : AES128;
- : SHA1.

:

1. Hub  
GRE:

```
esr# configure
esr(config)# tunnel gre 5
```

IP-, ISP:

```
esr(config-gre)# local address 150.115.0.5
```

MTU:

```
esr(config-gre)# mtu 1416
```

ttl:

```
esr(config-gre)# ttl 16
```

IP- GRE :

```
esr(config-gre)# ip address 10.10.0.5/24
```

GRE- mutipoint :

```
esr(config-gre)# multipoint
```

NHRP. :

```
esr(config-gre)# ip nhrp multicast dynamic
```

Hub. BGP:

```
esr(config)# router bgp 65005
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.8
esr(config-bgp-neighbor)# remote-as 65008
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 10.10.0.4
esr(config-bgp-neighbor)# remote-as 65004
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

IPsec Hub:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

IPsec GRE , :

```
esr(config-gre)# ip nhrp ipsec IPSECVPN dynamic
```

NHRP :

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

## 2. Spoke

DMVPN :

```
esr# configure
esr(config-gre)# tunnel gre 8
esr(config-gre)# mtu 1416
esr(config-gre)# ttl 16
esr(config-gre)# multipoint
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.8/24
```

:

```
esr(config-gre)# ip nhrp holding-time 300
```

NHS:

```
esr(config-gre)# ip nhrp nhs 10.10.0.5/24
```

-:

```
esr(config-gre)# ip nhrp map 10.10.0.5 150.115.0.5
```

NHRP :

```
esr(config)# ip nhrp multicast nhs
```

BGP spoke:

```
esr(config)# router bgp 65008
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.5
esr(config-bgp-neighbor)# remote-as 65005
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

IPsec. IKE NHS, .A IKE NHC – any:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW_HUB
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ike gateway IKEGW_SPOKE
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```



```

esr(config)# security ipsec vpn IPSECVPN_HUB
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_HUB
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable

```

```

esr(config)# security ipsec vpn IPSECVPN_SPOKE
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_SPOKE
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable

```

IPsec GRE , :

```

esr(config-gre)# ip nhrp ipsec IPSECVPN_HUB static
esr(config-gre)# ip nhrp ipsec IPSECVPN_SPOKE dynamic

```

NHRP :

```

esr(config-gre)# ip nhrp enable
esr(config-gre)# enable

```

NHRP :

```

esr# show ip nhrp

```

NHRP :

```

esr# clear ip nhrp

```

## L2TPv3-

L2TPv3 (Layer 2 Tunneling Protocol Version 3) – 2- OSI IP-. IP UDP. L2TPv3 MPLS P2P L2VPN (VLL) VPN L2. ESR L2TPv3-, .

1	L3-, L2TPv3-.		
2	L2TPv3- .	esr(config)# tunnel l2tpv3 <INDEX>	<INDEX> – : <ul style="list-style-type: none"> <li>• ESR-10/12V(F)/14VF – [1..10];</li> <li>• ESR-20/21/100/200 – [1..250];</li> <li>• ESR-1000/1200/1500/1700 – [1..500].</li> </ul>
3	( ).	esr(config-l2tpv3)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
4	IP- .	esr(config-l2tpv3)# local address <ADDR>	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255].
5	IP- .	esr(config-l2tpv3)# remote address <ADDR>	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255].
6	L2TPv3.	esr(config-l2tpv3)# protocol <TYPE>	<TYPE> – , : <ul style="list-style-type: none"> <li>• <b>ip</b> - IP-;</li> <li>• <b>udp</b> - UDP-.</li> </ul>

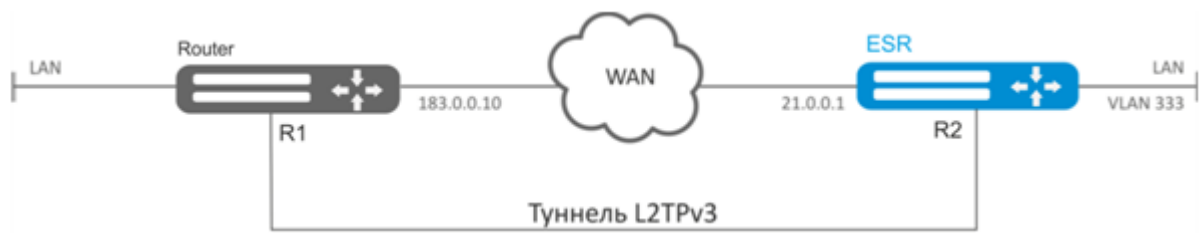
7	.	esr(config-l2tpv3)# local session-id <SESSION-ID>	<SESSION-ID> – , [1..200000].
8	.	esr(config-l2tpv3)# remote session-id <SESSION-ID>	<SESSION-ID> – , [1..200000].
9	UDP- ( UDP ).	esr(config-l2tpv3)# local port <UDP>	<UDP> – UDP- [1..65535].
10	UDP- ( UDP ).	esr(config-l2tpv3)# remote port <UDP>	<UDP> – UDP- [1..65535].
11	L2TPV3- .	esr(config-l2tpv3)# bridge-group <BRIDGE-ID>	<BRIDGE-ID> – , : <ul style="list-style-type: none"><li>• ESR-10/12V(F)/14VF – [1..50];</li><li>• ESR-20/21/100/200 – [1..250];</li><li>• ESR-1000/1200/1500/1700 – [1..500]</li></ul>
12	.	esr(config-l2tpv3)# enable	
13	MTU (MaximumTransmissionUnit) ( ). MTU 1500 "system jumbo-frames"	esr(config-l2tpv3)# mtu <MTU>	<MTU> – MTU, : <ul style="list-style-type: none"><li>• ESR-10/12V(F)/14VF – [1280..9600];</li><li>• ESR-20/21 – [1280..9500];</li><li>• ESR-100/200/1000/1200/1500/1700 [1280..10000].</li></ul> : 1500.
14	cookie ( ).	esr(config-l2tpv3)# local cookie <COOKIE>	<COOKIE> – COOKIE, .
15	cookie ( ).	esr(config-l2tpv3)# remote cookie <COOKIE>	<COOKIE> – COOKIE, .
16	, ( ).	esr(config-l2tpv3)# load-average <TIME>	<TIME> – , [5..150]. : 5.
17	( ).	esr(config-subif)# history statistics	
L2TPV3- : <ul style="list-style-type: none"><li>• QoS (, QoS);</li><li>• BRAS (, BRAS (Broadband Remote Access Server)).</li></ul>			

L2TPv3-

:

L2 VPN IP-, L2TPv3.

- UDP, 519;
- IP- 21.0.0.1;
- IP- 183.0.0.10;
- 2, 3;
- 100, 200;
- bridge 333.



:

L2TPv3 333:

```
esr# configure
esr(config)# tunnel l2tpv3 333
```

(IP- , WAN):

```
esr(config-l2tpv3)# local address 21.0.0.1
esr(config-l2tpv3)# remote address 183.0.0.10
```

UDP-:

```
esr(config-l2tpv3)# protocol udp
esr(config-l2tpv3)# local port 519
esr(config-l2tpv3)# remote port 519
```

:

```
esr(config-l2tpv3)# local session-id 100
esr(config-l2tpv3)# remote session-id 200
```

L2TPv3- , ( [bridge VLAN L2TPv3](#)):

```
esr(config-l2tpv3)# bridge-group 333
```

:

```
esr(config-l2tpv3)# enable
esr(config-l2tpv3)# exit
```

- , , VLAN id 333:

```
esr(config)# interface gi 1/0/2.333
```

- , ( [PPP E1](#)):

```
esr(config-subif)# bridge-group 333
esr(config-subif)# exit
```

, L2TPv3 .

. IP- 183.0.0.10. IP- 21.0.0.1. 519. 200, 100. , .

:

```
esr# show tunnels status l2tpv3 333
```

:

```
esr# show tunnels counters l2tpv3 333
```

:

```
esr# show tunnels configuration l2tpv3 333
```



firewall UDP 519 519.

## IPsec VPN

IPsec – , IP- . (), IP-, .

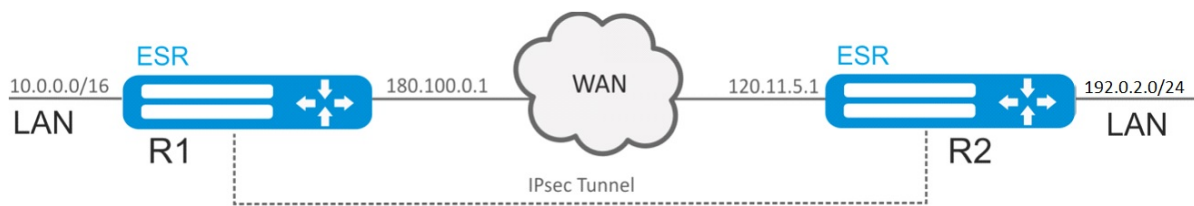
## Route-based IPsec VPN

1	VTI- .	esr(config)# tunnel vti <TUN>	<TUN> – .
2	IP- VTI-.	esr(config-vti)#local address <ADDR>	<ADDR> – IP- .
3	IP- VTI-.	esr(config-vti)#remote address <ADDR>	<ADDR> – IP- .
4	IP- VTI-.	esr(config-vti)# ip address <ADDR/LEN>	<ADDR/LEN> – IP- AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32].
5	VTI- firewall VTI-.	esr(config-vti)# security-zone<NAME>	<NAME> – , 12 .
		esr(config-vti)# ip firewall disable	
6	.	esr(config-vti)#enable	
7	IKE- .	esr(config)# security ike proposal <NAME>	<NAME> – IKE, 31 .
8	IKE- ().	esr(config-ike- proposal)# description<DESCRIPTION>	<DESCRIPTION> – , 255 .
9	IKE. ()	esr(config-ike- proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – , : md5, sha1, sha2-256, sha2384, sha2-512. : sha1
10	IKE. ()	esr(config-ike- proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – , : des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. : 3des
11	-. ()	esr(config-ike- proposal)# dh-group <DH-GROUP>	<DH-GROUP> – -, [1, 2, 5, 14, 15, 16, 17, 18]. : 1
12	IKE. ()	esr(config-ike- proposal)# authentication method <METHOD>	<METHOD> – . : • pre - shared - key – , ; • rsa - public - key – , RSA-. : pre-shared-key
13	ike- .	esr(config)# security ike policy <NAME>	<NAME> – IKE, 31 .
14	IKE ().	esr(config-ike- proposal)# lifetime seconds <SEC>	<SEC> – , [4 ..86400] . : 3600
15	IKE- IKE-.	esr(config-ike-policy)# proposal <NAME>	<NAME> – IKE, 31 .
16	.(, pre-shared-key)	esr(config-ike-policy)# pre-shared-key ascii-text<TEXT>	<TEXT> – [1..64] ASCII .
17	IKE- .	esr(config)# security ike gateway <NAME>	<NAME> – IKE, 31 .
18	IKE- IKE-.	esr(config-ike-gw)# ike-policy <NAME>	<NAME> – IKE, 31 .
19	IKE ().	esr(config-ike-gw)# version <VERSION>	<version> – IKE-: v1-only v2-only. : v1-only

20	- route-based.	esr(config-ike-gw)# mode route-based	
21	DPD ( ).	esr(config-ike-gw)# dead-peer-detection action <MODE>	<MODE> - DPD: <ul style="list-style-type: none"> <li>• restart - ;</li> <li>• clear - ;</li> <li>• hold - ;</li> <li>• none - , .</li> </ul> : none
22	DPD ( ).	esr(config-ike-gw)# dead-peer-detection interval <SEC>	<SEC> - DPD, [1..180]. : 2
23	DPD ( ).	esr(config-ike-gw)# dead-peer-detection timeout <SEC>	<SEC> - DPD, [1..180]. : 30
24	VTI- IKE-.	esr(config-ike-gw)# bind-interface vti <VTI>	<VTI> - VTI.
25	IPsec-.	esr(config)# security ipsec proposal <NAME>	<NAME> - IPsec, 31.
26	IPsec. ( )	esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> - , : md5, sha1, sha2-256, sha2384, sha2-512. : sha1
27	IPsec. ( )	esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> - , : des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. : 3des
28	IPsec ( ).	esr(config-ipsec- proposal)# protocol <PROTOCOL>	<PROTOCOL> - , : esp
29	IPsec- .	esr(config)# security ipsec policy <NAME>	<NAME> - IPsec, 31.
30	IPsec- IPsec-	esr(config-ipsec-policy)# proposal <NAME>	<NAME> - IPsec, 31.
31	IPsec- ( ).	esr(config-ipsec- policy)# lifetime { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC> - IPsec, . [1140..86400]. <PACKETS> - , IPsec-. [4..86400]. <KB> - , IPsec-. [4..86400]. : 28800
32	IPsec VPN .	esr(config)# security ipsec vpn <NAME>	<NAME> - VPN, 31.
33	, VPN.	esr(config-ipsec-vpn)# mode <MODE>	<MODE> - VPN.
34	IPsec- IPsec-VPN.	esr(config-ipsec-vpn)# ike ipsec-policy <NAME>	<NAME> - IPsec, 31.
35	DSCP IP- IKE- ( ).	esr(config-ipsec-vpn)# ike dscp <DSCP>	DSCP> - DSCP, [0..63]. : 63
36	VPN.	esr(config-ipsec-vpn)# ike establish-tunnel <MODE>	<MODE> - VPN: <ul style="list-style-type: none"> <li>• by-request - ;</li> <li>• route - , ;</li> <li>• immediate - .</li> </ul>
37	IKE- IPsec-VPN.	esr(config-ipsec-vpn)# ike gateway <NAME>	<NAME> - IKE-, 31.
38	, , SA ( ).	esr(config-ipsec-vpn)# ike idle-time <TIME>	<TIME> - , [4..86400].

39	IKE- , ( ).	esr(config-ipsec-vpn)# ike rekey disable	
40	IKE- ( ).	esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC>- , ( lifetimeseconds, . 22.2.13). [4..86400]. <PACKETS>- , ( lifetimepackets). [4..86400] <KB>- , ( lifetimekilobytes). [4..86400] : • - 540 . • - .
41	margin seconds, margin packets, margin kilobytes ( ).	esr(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE>- , [1..100]. : 100%
42	IPsec-VPN ( ).	esr(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION>- , 255 .
43	IPsec VPN.	esr(config-ipsec-vpn)# enable	

## Route-based IPsec VPN



:

IPsec- R1 R2.

- R1 IP- – 120.11.5.1;
- R2 IP- – 180.100.0.1;

IKE:

- -: 2;
- : AES 128 bit;
- : MD5.

IP sec:

- : AES 128 bit;
- : MD5.

:

1. R1

:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

VTI. VTI IPsec-. IP-, WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# local address 180.100.0.1
esr(config-vti)# remote address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

LAN-, IPsec-, VTI-:

```
esr(config)# ip route 192.0.2.0/24 tunnel vti 1
```

IKE. -2, AES 128 bit, MD5. IKE-:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

IKE. IKE, :

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

IKE. VTI-, :

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

IPsec-. AES 128 bit, MD5. IPsec-:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

IPsec-. IPsec-, .

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

IPsec VPN. VPN IKE-, IP sec-, . *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

VTI. VTI IPsec-. IP-, WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# remote address 180.100.0.1
esr(config-vti)# local address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

LAN-. , IPsec-, VTI-:

```
esr(config)# ip route 10.0.0.0/16 tunnel vti 1
```

IKE. -2, AES 128 bit, MD5. IKE-:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

IKE. IKE, :

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

IKE. VTI-, , :

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

IPsec-. AES 128 bit, MD5. IPsec-:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

IPsec-. IPsec-, .



```

esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit

```

IPsec VPN. VPN IKE-, IP sec-, . *enable*.

```

esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit

```

:

```

esr# show security ipsec vpn status ipsec1

```

:

```

esr# show security ipsec vpn configuration ipsec1

```



firewall ESP ISAKMP (UDP- 500).

## Policy-based IPsec VPN

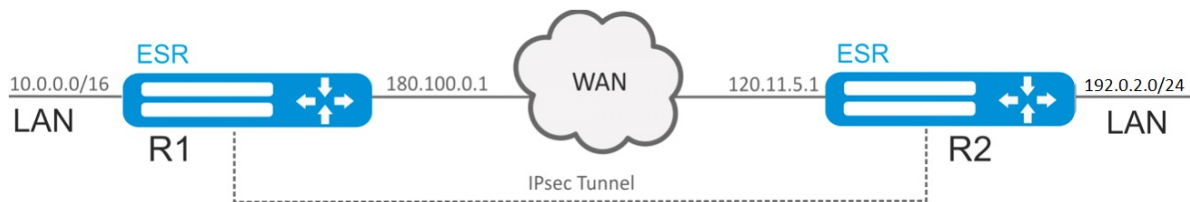
1	IKE- .	esr(config)# security ike proposal <NAME>	<NAME>- IKE, 31.
2	( ).	esr(config-ike- proposal)# description<DESCRIPTION>	<DESCRIPTION>- , 255 .
3	IKE.	esr(config-ike- proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM>- , : md5, sha1, sha2-256, sha2384, sha2-512.
4	IKE.	esr(config-ike- proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM>- , : des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.
5	-. .	esr(config-ike- proposal)# dh-group <DH-GROUP>	<DH-GROUP>- -, [1, 2, 5, 14, 15, 16, 17, 18].
6	. .	esr(config-ike- proposal)# authentication method <METHOD>	<METHOD>- . : <ul style="list-style-type: none"> <li>• pre - shared - key - , ;</li> <li>• rsa - public - key - , RSA-.</li> </ul>
7	IKE .	esr(config)# security ike policy <NAME>	<NAME>- IKE, 31 .
8	IKE ( ).	esr(config-ike- proposal)# lifetime seconds <SEC>	<SEC>- , [4 ..86400] .
9	. .	esr(config-ike-policy)# proposal <NAME>	<NAME>- IKE, 31 .

10	.	esr(config-ike-policy)#pre-shared-key ascii-text<TEXT>	<TEXT> – [1..64] ASCII .
11	IKE .	esr(config)# security ike gateway <NAME>	<NAME> – IKE, 31 .
12	IKE.	esr(config-ike-gw)# ike-policy <NAME>	<NAME> – IKE, 31 .
13	IKE ().	esr(config-ike-gw)# version <VERSION>	<version> – IKE-: <b>v1-only v2-only</b> .
14	.	esr(config-ike-gw)#mode<MODE>	<MODE> – , :  <ul style="list-style-type: none"> <li>• <b>policy - based</b> – ;</li> <li>• <b>route - based</b> – , .</li> </ul>
15	DPD ().	esr(config-ike-gw)# dead-peer-detection action <MODE>	<MODE> – DPD:  <ul style="list-style-type: none"> <li>• <b>restart</b> – ;</li> <li>• <b>clear</b> – ;</li> <li>• <b>hold</b> – ;</li> <li>• <b>none</b> – , .</li> </ul>
16	DPD ().	esr(config-ike-gw)#dead-peer-detection interval <SEC>	<SEC> – DPD, [1..180] .
17	DPD ().	esr(config-ike-gw)# dead-peer-detection timeout <SEC>	<SEC> – DPD, [1..180] .
18	IKE ().	esr(config-ike-gw)# version <VERSION>	<version> – IKE-: <b>v1-only v2-only</b> .
19	IP .	esr(config-ike-gw)# 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].
20	IP- IPsec-.	esr(config-ike-gw)#local address <ADDR>	<ADDR> – IP- .
21	IP- IPsec-.	esr(config-ike-gw)#remote address <ADDR>	<ADDR> – IP- .
22	IP- , IP- .	esr(config-ike-gw)# remote 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].
23	IPsec.	esr(config)# security ipsec proposal <NAME>	<NAME> – IPsec, 31 .
24	IPsec.	esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – , : md5, sha1, sha2-256, sha2384, sha2-512.
26	IPsec.	esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – , : des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.
26	().	esr(config-ipsec- proposal) #protocol <PROTOCOL>	<PROTOCOL> – ,
27	IPsec	esr(config)# security ipsec policy <NAME>	<NAME> – IPsec, 31 .
28		esr(config-ipsec-policy)# proposal <NAME>	<NAME> – IPsec, 31 .

29	IPsec ( ).	esr(config-ipsec- policy)# lifetime { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC> – IPsec-, . [1140..86400]. <PACKETS> – , IPsec-. [4..86400]. <KB> – , IPsec-. [4..86400].
30	IPsec VPN .	esr(config)# security ipsecvpn <NAME>	<NAME> – VPN, 31 .
31	, VPN.	esr(config-ipsec-vpn)# mode <MODE>	<MODE> – VPN.
32	IPsec VPN.	esr(config-ipsec-vpn)#ike ipsec- policy <NAME>	<NAME> – IPsec-, 31 .
33	DSCP IP- IKE- ( ).	esr(config-ipsec-vpn)#ike dscp <DSCP>	DSCP> – DSCP, [0..63].
34	VPN.	esr(config-ipsec-vpn)#ike establish-tunnel <MODE>	<MODE> – VPN: <ul style="list-style-type: none"> <li>• by - request – ;</li> <li>• route – , ;</li> <li>• immediate – .</li> </ul>
35	IKE- VPN.	esr(config-ipsec-vpn)# ike gateway <NAME>	<NAME> – IKE-, 31 .
36	, , SA ( ).	esr(config-ipsec-vpn)# ike idle- time <TIME>	<TIME> – , [4..86400].
37	IKE , ( ).	esr(config-ipsec-vpn)#ike rekey disable	
38	IKE ( ).	esr(config-ipsec-vpn)# Ike rekey margin { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC> – , ( lifetimeseconds). [4..86400]. <PACKETS> – , ( lifetimepackets). [4..86400]. <KB> – , ( lifetimakilobytes). [4..86400]
39	marginseconds, marginpackets, marginkilobytes ( ).	esr(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE> – , [1..100].
40	VPN ( ).	esr(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
41	IPsec VPN.	esr(config-ipsec-vpn)# enable	

## Policy-based IPsec VPN

:



IPsec- R1 R2.

R1 IP- – 120.11.5.1;

R2 IP- – 180.100.0.1;

IKE:

- -: 2;
- : AES 128 bit;
- : MD5.

IPsec:

- : AES 128 bit;
- : MD5.

:

## 1. R1

:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 120.11.5.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

### ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

IKE. -2, AES 128 bit, MD5. IKE-:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

IKE. IKE, :

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

IKE. VTI-, :

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 120.11.5.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

IPsec-. AES 128 bit, MD5. IPsec-:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

IPsec-. IPsec-, .

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

IPsec VPN. VPN IKE-, IP sec-, . *enable*.

```

esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit

```

## 2. R2 :

```

esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit

```

### ISAKMP:

```

esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500
esr(config-addr-set)# exit

```

### IKE. -2, AES 128 bit, MD5. IKE-:

```

esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#

```

### IKE. IKE, :

```

esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit

```

### IKE. VTI-,, :

```

esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit

```

### IPsec-. AES 128 bit, MD5. IPsec-:

```

esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

### IPsec-. IPsec-, .

```

esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit

```

IPsec VPN. VPN IKE-, IP sec-, . *enable*.

```

esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit

```

:

```

esr# show security ipsec vpn status ipsec1

```

:

```

esr# show security ipsec vpn configuration ipsec1

```



firewall ESP ISAKMP (UDP- 500).

## Remote Access IPsec VPN

Remote Access IPsec VPN – VPN-, IPsec VPN , .

RA IPsec VPN IPsec – Extended Authentication (XAUTH), - IPsec VPN.

1	IKE- .	esr(config)# security ike proposal <NAME>	<NAME> – IKE, 31.
2	( ).	esr(config-ike- proposal)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
3	IKE ( ).	esr(config-ike- proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – , : md5, sha1, sha2-256, sha2384, sha2-512. : sha1
4	IP- VTI- ( ).	esr(config-vti)# ip address <ADDR/LEN>	<ADDR/LEN> – IP- AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..31].
5	- ( ).	esr(config-ike- proposal)# dh- group <DH-GROUP>	<DH-GROUP> – -, [1, 2, 5, 14, 15, 16, 17, 18]. : 1
6	IKE .	esr(config)# security ike policy <NAME>	<NAME> – IKE, 31.
7	.	esr(config-ike- policy)# authentication method <METHOD>	<METHOD> – . : • xauth - psk - key – , - .
8	( ).	esr(config-ike- policy)# authentication mode client	
9	IKE ( ).	esr(config-ike- policy)# lifetime seconds <SEC>	<SEC> – , [4 ..86400] . : 3600

10	.	esr(config-ike-policy)# proposal <NAME>	<NAME> – IKE, 31.
11	.	esr(config-ike-policy)#pre- shared-key ascii-text <TEXT>	<TEXT> – [1..64] ASCII.
12	.	esr(config)# access profile <NAME>	<NAME> – , 31.
13	.	esr(config-access-profile)# user <LOGIN>	<LOGIN> – , 31.
14	.	esr(config-profile)# password ascii-text <TEXT>	<TEXT> – [8..32] ASCII.
15	( ).	esr(config)# address-assignment pool <NAME>	<NAME> – , 31.
16	, IP ( ).	esr(config-pool)# ip prefix <ADDR/LEN>	<ADDR/LEN> – .
17	IKE .	esr(config)# security ike gateway <NAME>	<NAME> – IKE, 31.
18	IKE.	esr(config-ike-gw)# ike-policy <NAME>	<NAME> – IKE, 31.
19	.	esr(config-ike-gw)# mode <MODE>	<MODE> – , :  • <b>policy - based</b> – .
20	DPD ( ).	esr(config-ike-gw)# dead-peer- detection action <MODE>	<MODE> – DPD:  • <b>restart</b> – ; • <b>clear</b> – ; • <b>hold</b> – ; • <b>none</b> – , .  : none
21	DPD ( ).	esr(config-ike-gw)#dead-peer- detection interval <SEC>	<SEC> – DPD, [1..180]. : 2
22	DPD ( ).	esr(config-ike-gw)# dead-peer- detection timeout <SEC>	<SEC> – DPD, [1..180]. : 30
23	IKE ( ).	esr(config-ike-gw)# version <VERSION>	<VERSION> – IKE:: <b>v1-only v2-only</b> .  : v1-only
24	IP ( ).	esr(config-ike-gw)# 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].
25	IP- IPsec.	esr(config-ike-gw)#local address <ADDR>	<ADDR> – IP- .
26	IP- IPsec.	esr(config-ike-gw)#remote address [any   <ADDR/LEN> [ protocol { <TYPE>   <ID> } [ port <PORT> ] ]	Any – - , ;  <ADDR/LEN> – IP- , .
27	IP- ( ).	esr(config-ike-gw)# remote network dynamic pool <NAME>	<NAME> – , 31.
28	( ).	esr(config-ike-gw)# remote network dynamic client	
29	XAUTH ( ).	esr(config-ike-gw)# xauth access-profile <NAME>	<NAME> – , 31.

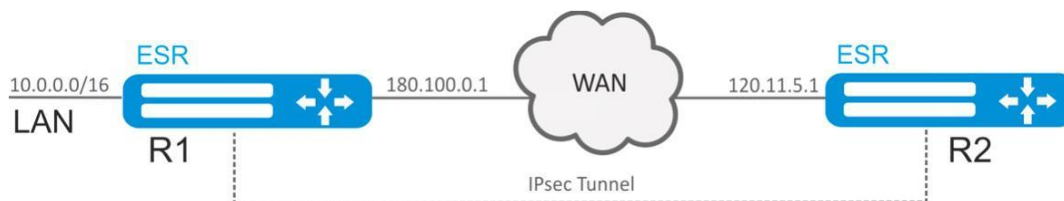
30	XAUTH ( ).	esr(config-ike-gw)# xauth access-profile <NAME> client <LOGIN>	<NAME> - , 31; <LOGIN> - , 31.
31	IP IPsec VPN ( ).	esr(config-ike-gw)# assign- interface loopback <INDEX>	<INDEX> - , [1..65535].
32	IPsec.	esr(config)# security ipsec proposal <NAME>	<NAME> - IPsec, 31.
33	IPsec ( ).	esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> - , : md5, sha1, sha2-256, sha2384, sha2-512. : sha1
34	IPsec ( ).	esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> - , : des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. : 3des
35	( ).	esr(config-ipsec- proposal) #protocol <PROTOCOL>	<PROTOCOL> - , .
36	IPsec	esr(config)# security ipsec policy <NAME>	<NAME> - IPsec, 31.
37		esr(config-ipsec-policy)# proposal <NAME>	<NAME> - IPsec, 31.
38	IPsec ( ).	esr(config-ipsec-policy)# lifetime { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC> - IPsec-, . [1140..86400]. : 540 <PACKETS> - , IPsec-. [4..86400]. :.. <KB> - , IPsec-. [4..86400]. :..
39	IPsec VPN .	esr(config)# security ipsec vpn <NAME>	<NAME> - VPN, 31.
40	, VPN.	esr(config-ipsec-vpn)# mode <MODE>	<MODE> - VPN, : ike, manual.
41	IPsec VPN.	esr(config-ipsec-vpn)#ike ipsec- policy <NAME>	<NAME> - IPsec-, 31.
42	DSCP IP- IKE- ( ).	esr(config-ipsec-vpn)#ike dscp <DSCP>	DSCP> - DSCP, [0..63]. : 63
43	VPN.	esr(config-ipsec-vpn)#ike establish-tunnel <MODE>	<MODE> - VPN: • by - request - , ; • route - , , ; • immediate - , .
44	IKE- VPN.	esr(config-ipsec-vpn)# ike gateway <NAME>	<NAME> - IKE-, 31.
45	, , SA ( ).	esr(config-ipsec-vpn)# ike idle- time <TIME>	<TIME> - , [4..86400]. : 0
46	IKE , ( ).	esr(config-ipsec-vpn)#ike rekey disable	:..



47	IKE ().	esr(config-ipsec-vpn)# Ike rekey margin { seconds <SEC>   packets <PACKETS>   kilobytes <KB> }	<SEC> – , ( lifetimeseconds). [4..86400]. :540  <PACKETS> – , ( lifetimepackets). [4..86400]. :..  <KB> – , ( lifetimekilobytes). [4..86400] :..
48	marginseconds, marginpackets, marginkilobytes ().	esr(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE> – , [1..100]. :100
49	VPN ().	esr(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
50	IPsec VPN.	esr(config-ipsec-vpn)# enable	
51	- XAUTH /( )().	esr(config-ipsec-vpn)# security ike session uniqueids <MODE>	<MODE> – -, :  <ul style="list-style-type: none"> <li>• no - XAUTH , XAUTH "INITIAL_CONTACT", IP-. , XAUTH . XAUTH IP-.</li> <li>• never - XAUTH . XAUTH IP-. "INITIAL_CONTACT" .</li> <li>• replace - XAUTH . XAUTH IP-.</li> <li>• keep - XAUTH . XAUTH .</li> </ul>

## Remote Access IPsec VPN

:



Remote Access IPsec VPN R1 R2 IPsec - XAUTH. IPsec VPN R1, R2 IPsec VPN.

R2 IP- – 120.11.5.1;

R1 IP- – 180.100.0.1;

IPsec VPN:

- 192.0.2.0/24
- LAN 10.0.0.0/16

IKE:

- -: 2;
- : 3DES;
- : SHA1.

IPsec:

- : 3DES;
- : SHA1.

XAUTH:

- : client1;
- : password123.

:

1. R1

:

```
esr# configure
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# exit
```

ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500,4500
esr(config-object-group-service)# exit
```

IKE. -2, 3DES, SHA1. IKE-:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit
```

IKE. IKE, , XAUTH :

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

IPsec VPN:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

, IP IPsec VPN:

```
esr-1000(config)# address-assignment pool CLIENT_POOL
esr-1000(config-pool)# ip prefix 192.0.2.0/24
esr-1000(config-pool)# exit
```

IKE. IKE, , , XAUTH:

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network dynamic pool CLIENT_POOL
esr(config-ike-gw)# dead-peer-detection action clear
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile XAUTH
esr(config-ike-gw)# exit
```

IPsec-. 3DES, SHA1. IPsec-:

```

esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm sha1
esr(config-ipsec-proposal)# encryption algorithm 3des
esr(config-ipsec-proposal)# exit

```

IPsec-. IPsec-, .

```

esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit

```

IPsec VPN. VPN IKE-, IP sec-, IPsec – *by-request*. *enable*.

```

esr(config)# security ipsec IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel by-request
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit

```

esp udp 500,4500 firewall IPsec VPN:

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end

```

## 2. R2

:

```

esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit

```

ISAKMP:

```

esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500,4500
esr(config-addr-set)# exit

```

IKE. -2, 3 DES, SHA1. IKE-:

```

esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit

```

IKE. IKE, , , XAUTH -:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# authentication mode client
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

loopback IP, IPsec VPN:

```
esr(config)# interface loopback 8
esr(config-loopback)# exit
```

IKE. , , , XAUTH :

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# assign-interface loopback 8
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network dynamic client
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile xauth client client1
esr(config-ike-gw)# exit
```

IPsec-. 3DES, SHA1. IPsec-:

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

IPsec-. IPsec-, .

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

IPsec VPN. VPN IKE-, IP sec-, . enable.

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

esp udp 500,4500 firewall IPsec VPN:

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end

```

:

```
esr# show security ipsec vpn status IPSECVPN
```

:

```
esr# show security ipsec vpn configuration IPSECVPN
```



firewall ESP ISAKMP (UDP- 500,4500).

## LT-

LT (. Logical Tunnel – ) – , (VRF Lite), . LT- VRF firewall.

1	LT- VRF.	esr(config)# tunnel lt <ID>	<ID> – [1..128].
2	(.).	esr(config-lt)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
3	LT- VFR.	esr(config-lt)# ip vrf forwarding <VRF>	<VRF> – VRF, 31 .
4	LT- firewall LT-.	esr(config-lt)# security- zone<NAME>	<NAME> – , 12 .
		esr(config-lt)# ip firewall disable	
5	LT- LT ( VRF).	esr(config-lt)# peer lt <ID>	<ID> – [1..128].
6	LT- IP- . LT-, IP- IP-.	esr(config-lt)# ip address <ADDR/LEN>	<ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32].
7	.	esr(config-lt)# enable	
8	VRF LT-.		

9	, ()	esr(config-lt)# load-average <TIME>	<TIME> – , [5..150]. : 5
10	MTU (Maximum Transmission Unit), bridge (;, bridge VLAN). MTU 1500 "system jumbo-frames"	esr(config-lt)# mtu <MTU>	<MTU> – MTU, : <ul style="list-style-type: none"><li>• ESR-10/12V(F)/14VF – [1280..9600];</li><li>• ESR-20/21 – [1280..9500];</li><li>• ESR-100/200/1000/1200/1500/1700 [1280..10000].</li></ul> : 1500.

:

, VRF vrf\_1 vrf\_2.

:

```
hostname esr
ip vrf vrf_1
exit
ip vrf vrf_2
exit
interface gigabitethernet 1/0/1
    ip vrf forwarding vrf_1
    ip firewall disable
    ip address 10.0.0.1/24
exit
interface gigabitethernet 1/0/2
    ip vrf forwarding vrf_2
    ip firewall disable
    ip address 10.0.1.1/24
exit
```

:

LT- VRF IP- :

```
esr(config)# tunnel lt 1
esr(config-lt)# ip vrf forwarding vrf_1
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.1/30
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# ip vrf forwarding vrf_2
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.2/30
esr(config-lt)# exit
```

LT-LT- VRF, , :

```
esr(config)# tunnel lt 1
esr(config-lt)# peer lt 2
esr(config-lt)# enable
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# peer lt 1
esr(config-lt)# enable
esr(config-lt)# exit
```



VRF , VRF:

```
esr(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2  
esr(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1
```