

# ESR-Series. Quick guide. 1.14.0

ESR ( ).

, .

, . SNAT , , .

- 2 «Trusted» «Untrusted» . :
1. «Untrusted» (WAN). DHCP- IP- .
- :
- ESR-10/12V: GigabitEthernet 1/0/1;
  - ESR-12VF/ESR-14VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/9;
  - ESR-20: GigabitEthernet 1/0/1;
  - ESR-21: GigabitEthernet 1/0/1;
  - ESR-100/200: GigabitEthernet 1/0/1;
  - ESR-1000/1500/3100: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
  - ESR-1200/1700: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1, TengigabitEthernet 1/0/2;
  - ESR-1511: GigabitEthernet 1/0/1, FortygigabitEthernet 1/0/1-2;
- L2- Bridge 2.
2. «Trusted» (LAN). Telnet SSH , ICMP- , DHCP- IP- . «Untrusted» .
- :
- ESR-10: GigabitEthernet 1/0/2-6;
  - ESR-12V(F)/ESR-14VF: GigabitEthernet 1/0/2-8;
  - ESR-20: GigabitEthernet 1/0/2-4;
  - ESR-21: GigabitEthernet 1/0/2-12;
  - ESR-100: GigabitEthernet 1/0/2-4;
  - ESR-200: GigabitEthernet 1/0/2-8;
  - ESR-1000: GigabitEthernet 1/0/2-24;
  - ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;
  - ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4;
  - ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;
  - ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;
  - ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8.

L2- Bridge 1.

Bridge 2 DHCP- IP- . Bridge 1 IP- 192.168.1.1/24. IP- . DHCP- 192.168.1.2-192.168.1.254 255.255.255.0. Internet Source NAT.

:

1 –

Trusted	Untrusted	TCP, UDP, ICMP	
Trusted	Trusted	TCP, UDP, ICMP	
Trusted	self	TCP/22 (SSH), ICMP, UDP/67 (DHCP Server), UDP/123 (NTP)	
Untrusted	self	UDP/68 (DHCP Client)	

 'admin'. .

 IP- Bridge 1 – 192.168.1.1/24.

# (CLI)

## Ethernet



1. (-) , «*Trusted*», , .

2. DHCP- IP- **192.168.1.0/24**.

IP- -, , , 192.168.1.1, 192.168.1.0/24.

## RS-232

1. RJ-45/DBF9, , «**Console**» RS-232 .

2. (, HyperTerminal Minicom) . VT100.

RS-232:

```
: 115200 /  
: 8  
:  
: 1  
:
```

:

- «admin».
- .
- (Hostname).
- .
- .
- .

## «admin»

«admin».



**techsupport** ;

**remote – RADIUS, TACACS+, LDAP;**

**admin, techsupport, remote .**

«admin» :

```
esr# configure  
esr(config)# username admin  
esr(config-user)# password <new-password>  
esr(config-user)# exit
```

- , , - :

```
esr(config)# username <name>
esr(config-user)# password <password>
esr(config-user)# privilege <privilege>
esr(config-user)# exit
```



1-9 , . 10-14 , . 15 , .

**«fedor» c «12345678» 15 «ivan» «password» 1:**

```
esr# configure
esr(config)# username fedor
esr(config-user)# password 12345678
esr(config-user)# privilege 15
esr(config-user)# exit
esr(config)# username ivan
esr(config-user)# password password
esr(config-user)# privilege 1
esr(config-user)# exit
```



1-9 , . 10-14 , . 15 , .

**«fedor» c «12345678» 15 «ivan» «password» 1:**

```
esr# configure
esr(config)# username fedor
esr(config-user)# password 12345678
esr(config-user)# privilege 15
esr(config-user)# exit
esr(config)# username ivan
esr(config-user)# password password
esr(config-user)# privilege 1
esr(config-user)# exit
```

:

```
esr# configure
esr(config)# hostname <new-name>
```

, <new-name>.

, - IP-, .

**IP- Gigabit Ethernet 1/0/2.150 VLAN 150.**

:

- IP- – 192.168.16.144;
- – 255.255.255.0;
- IP- – 192.168.16.1.

```

esr# configure
esr(config)# interface gigabitethernet 1/0/2.150
esr(config-subif)# ip address 192.168.16.144/24
esr(config-subif)# exit
esr(config)# ip route 0.0.0.0/0 192.168.16.1

```

, , :

```

esr# show ip interfaces

```

IP address	Interface	Type
192.168.16.144/24	gigabitethernet 1/0/2.150	static

. IP- DHCP, DHCP.

, IP- DHCP- **Gigabit Ethernet 1/0/10**:

```

esr# configure
esr(config)# interface gigabitethernet 1/0/10
esr(config-if)# ip address dhcp
esr(config-if)# exit

```

, , :

```

esr# show ip interfaces

```

IP address	Interface	Type
192.168.11.5/25	gigabitethernet 1/0/10	DHCP

Telnet SSH «trusted». , , firewall.

:

- **source-zone** -, ;
- **self** -, .

:

```

esr# configure
esr(config)# security zone-pair <source-zone> self
esr(config-zone-pair)# rule <number>
esr(config-zone-rule)# action permit
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-address <network object-group>
esr(config-zone-rule)# match destination-address <network object-group>
esr(config-zone-rule)# match destination-port <service object-group>
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit

```

«untrusted» IP- 132.16.0.5-132.16.0.10 IP- 40.13.1.22 SSH:

```

esr# configure
esr(config)# object-group network clients
esr(config-addr-set)# ip address-range 132.16.0.5-132.16.0.10
esr(config-addr-set)# exit
esr(config)# object-group network gateway
esr(config-addr-set)# ip address-range 40.13.1.22
esr(config-addr-set)# exit
esr(config)# object-group service ssh
esr(config-port-set)# port-range 22
esr(config-port-set)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 10
esr(config-zone-rule)# action permit
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-address clients
esr(config-zone-rule)# match destination-address gateway
esr(config-zone-rule)# match destination-port ssh
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit

```

```

esr# commit
esr# confirm

```

, **commit** . , , **confirm**.

**confirm** , , **commit**.

<http://eltex-co.ru> «trusted». — , . , .

. , . . . , .

- **shutdown**. CLI.
- (NTP). NTP [NTP](#) . NTP CLI.
- NTP broadcast client, .
- **ip firewall disable**, . [Firewall](#) . [Firewall](#) CLI.

« Syslog» .

[SYSLOG](#) CLI.

- syslog syslog .
- syslog- .
- syslog- .
- syslog.
- timestamp msec syslog ESR-1500 ESR-1511.

- **tmpsys:syslog** .
- **flash:syslog** , ESR.

:

info syslog syslog. 512. 3-. syslog.

:

syslog- :

```
esr(config)# syslog file tmpsys:syslog/default info
```

:

```
esr(config)# syslog max-files 3
esr(config)# syslog file-size 512
```

:

```
esr(config)# syslog host mylog 192.168.1.2 info udp 514
```

syslog:

```
esr(config)# syslog sequence-numbers
```

AAA CLI.

- admin.
- , , .
- 8.
- , .

:

- , 1 12 .
- 16, —64.
- 3 , 5 , 4 2. 4 .

:

admin:

```
esr(config)# security passwords default-expired
```

30 12:

```
esr(config)# security passwords lifetime 30
esr(config)# security passwords history 12
```

:

```
esr(config)# security passwords min-length 16
esr(config)# security passwords max-length 64
```

:

```
esr(config)# security passwords upper-case 3
esr(config)# security passwords lower-case 5
esr(config)# security passwords special-case 2
esr(config)# security passwords numeric-count 4
esr(config)# security passwords symbol-types 4
```

## AAA

.

AAA CLI.

- .
- .
- .
- ., . RADIUS/TACACS/LDAP .
- **admin 1.**
- .
- AAA.

- admin .
- **no username admin admin,** . , **admin** .
- **no password admin admin,** . **admin** 'password'.
- **!**

:

AAA:

- SSH RADIUS.
- RADIUS, RADIUS- .
- **ENABLE- RADIUS, RADIUS- ENABLE-**
- admin .
- .
- .
- .

:

**local-operator 8:**

```
esr(config)# username local-operator
esr(config-user)# password Pa$$w0rd1
esr(config-user)# privilege 8
esr(config-user)# exit
```

ENABLE-:

```
esr(config)# enable password $6e5c4r3e2t!
```

admin:

```
esr(config)# username admin
esr(config-user)# privilege 1
esr(config-user)# exit
```

RADIUS-, 192.168.1.11 192.168.2.12:

```
esr(config)# radius-server host 192.168.1.11
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# priority 100 esr(config-radius-server)# exit
esr(config)# radius-server host 192.168.2.12
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# priority 150
esr(config-radius-server)# exit
```

:

```
esr(config)# aaa authentication login CONSOLE radius local
esr(config)# aaa authentication login SSH radius
esr(config)# aaa authentication enable default radius enable
esr(config)# aaa authentication mode break
esr(config)# line console
esr(config-line-console)# login authentication CONSOLE
esr(config-line-console)# exit esr(config)# line ssh
esr(config-line-ssh)# login authentication SSH
esr(config-line-ssh)# exit
```

:

```
esr(config)# logging userinfo
esr(config)# logging aaa
esr(config)# syslog cli-commands
```

SSH, Telnet CLI.

- telnet.
- .
- sha2-256, sha2-512 .
- aes256, aes256ctr .
- dh-group-exchange-sha256 .
- ip-.

:

telnet. . .

:

telnet:

```
esr(config)# no ip telnet server
```

:



```

esr-20(config)# crypto key generate dsa
esr-20(config)# crypto key generate ecdsa
esr-20(config)# crypto key generate ed25519
esr-20(config)# crypto key generate rsa
esr-20(config)# crypto key generate rsa1

```

:

```

esr(config)# ip ssh server
esr(config)# ip ssh authentication algorithm md5 disable
esr(config)# ip ssh authentication algorithm md5-96 disable
esr(config)# ip ssh authentication algorithm ripemd160 disable
esr(config)# ip ssh authentication algorithm sha1 disable
esr(config)# ip ssh authentication algorithm sha1-96 disable
esr(config)# ip ssh encryption algorithm aes128 disable
esr(config)# ip ssh encryption algorithm aes128ctr disable
esr(config)# ip ssh encryption algorithm aes192 disable
esr(config)# ip ssh encryption algorithm aes192ctr disable
esr(config)# ip ssh encryption algorithm arcfour disable
esr(config)# ip ssh encryption algorithm arcfour128 disable
esr(config)# ip ssh encryption algorithm arcfour256 disable
esr(config)# ip ssh encryption algorithm blowfish disable
esr(config)# ip ssh encryption algorithm cast128 disable
esr(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
esr(config)# ip ssh key-exchange algorithm dh-group1-sha1 disable
esr(config)# ip ssh key-exchange algorithm dh-group14-sha1 disable
esr(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp256 disable
esr(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp384 disable
esr(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp521 disable

```

CLI.

- ip spoofing.
- TCP- .
- TCP- SYN
- ICMP- .
- ICMP- .
- ip- .
- .

:

:

ip spoofing :

```

esr(config)# ip firewall screen spy-blocking spoofing
esr(config)# logging firewall screen spy-blocking spoofing

```

TCP- :

```
esr(config)# ip firewall screen spy-blocking syn-fin
esr(config)# logging firewall screen spy-blocking syn-fin
esr(config)# ip firewall screen spy-blocking fin-no-ack
esr(config)# logging firewall screen spy-blocking fin-no-ack
esr(config)# ip firewall screen spy-blocking tcp-no-flag
esr(config)# logging firewall screen spy-blocking tcp-no-flag
esr(config)# ip firewall screen spy-blocking tcp-all-flags
esr(config)# logging firewall screen spy-blocking tcp-all-flags
```

ICMP- :

```
esr(config)# ip firewall screen suspicious-packets icmp-fragment
esr(config)# logging firewall screen suspicious-packets icmp-fragment
```

ICMP- :

```
esr(config)# ip firewall screen suspicious-packets large-icmp
esr(config)# logging firewall screen suspicious-packets large-icmp
```

ip- :

```
esr(config)# ip firewall screen suspicious-packets unknown-protocols
esr(config)# logging firewall screen suspicious-packets unknown-protocols
```

« » .

: <http://eltex-co.ru/support/>

Sevicedesk: <https://servicedesk.eltex-co.ru/>

« », , :

: <http://eltex-co.ru/>

: <http://eltex-co.ru/forum>

: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

: <http://eltex-co.ru/support/downloads>