Integrated Networking Solutions

ESR series service routers

ESR-10, ESR-12V, ESR-12VF, ESR-14VF, ESR-15, ESR-20, ESR-21, ESR-30, ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1511, ESR-1700, ESR-3100

Installation and Quick Start Guide

Firmware version 1.18.1

Contents

1 Abstract

This manual presents the factory configuration of the device and recommendations for the initial configuration of ESR series routers (hereinafter referred to as the device).

This manual is intended for technical personnel who perform the installation and configuration of the device.

2 Router factory settings

The device is shipped to the consumer with the factory configuration installed that includes essential basic settings. Factory configuration allows using the router as a gateway with SNAT without applying any additional settings. Also, factory configuration contains settings that allow obtaining network access to the device for advanced configuration.

2.1 Description of factory settings

To establish network connection, the configuration features 2 security zones named 'Trusted' for local area network and 'Untrusted' for public network. All interfaces are divided between two security zones:

1. **'Untrusted' zone** is meant for a public network (WAN) connection. In this zone, DHCP ports are open in order to obtain dynamic IP address from the provider. All incoming connections from this zone to the router are blocked.
   This security zone includes the following interfaces:
   - for ESR-10/12V: GigabitEthernet 1/0/1;
   - for ESR-12VF/ESR-14VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/9;
   - for ESR-15: GigabitEthernet1/0/1; GigabitEthernet1/0/6;
   - for ESR-20: GigabitEthernet 1/0/1;
   - for ESR-21: GigabitEthernet 1/0/1;
   - for ESR-30: GigabitEthernet 1/0/1; TengigabitEthernet 1/0/1-2;
   - for ESR-100/200: GigabitEthernet 1/0/1;
   - for ESR-1000/1500/3100: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - for ESR-1200/1700: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1, TengigabitEthernet 1/0/2;
   - for ESR-1511: GigabitEthernet 1/0/1, FortygigabitEthernet 1/0/1-2;
   - for ESR-3200: Twentyfivegigabitethernet 1/0/1-2.

   Zone interfaces are grouped into a single L2 segment via Bridge 2 network bridge.
2. **'Trusted' zone** is meant for a local area network (LAN) connection. Telnet and SSH ports for remote access, ICMP ports for router availability test, DHCP ports for clients obtaining IP addresses from the router. Outgoing connections from this zone into the Untrusted zone are allowed.
   This security zone includes the following interfaces:
   - for ESR-10: GigabitEthernet 1/0/2-6;
   - for ESR-12V(F)/ESR-14VF: GigabitEthernet 1/0/2-8;
   - for ESR-15: GigabitEthernet 1/0/2-5;
   - for ESR-20: GigabitEthernet 1/0/2-4;
   - for ESR-21: GigabitEthernet 1/0/2-12;
   - for ESR-30: GigabitEthernet 1/0/3-4;
   - for ESR-100: GigabitEthernet 1/0/2-4;
   - for ESR-200: GigabitEthernet 1/0/2-8;
   - for ESR-1000: GigabitEthernet 1/0/2-24;
   - for ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;
   - for ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4;
   - for ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;
   - for ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;
   - for ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8;
   - for ESR-3200: Twentyfivegigabitethernet 1/0/1-2.

   Zone interfaces are grouped into a single L2 segment via *Bridge 1* network bridge.

On the *Bridge 2* interface, DHCP client is enabled to obtain dynamic IP address from the provider. On *Bridge 1* interface, static IP address 192.168.1.1/24 is configured. Created IP address acts as a gateway for LAN

clients. For LAN clients, DHCP address pool 192.168.1.2-192.168.1.254 is configured with the mask 255.255.255.0. For clients in order to access the Internet, the router should have Source NAT service enabled.

Security zone policies have the following configuration:

Table 1 – Security zone policy description

Traffic origin zone	Traffic destination zone	Traffic type	Action
Trusted	Untrusted	TCP, UDP, ICMP	enabled
Trusted	Trusted	TCP, UDP, ICMP	enabled
Trusted	self	TCP/22 (SSH), ICMP, UDP/67 (DHCP Server), UDP/123 (NTP)	enabled
Untrusted	self	UDP/68 (DHCP Client)	enabled

To enable device configuration on the first startup, 'admin' account has been created in the router configuration. The user will be prompted to change administrator password during the initial configuration of the router.

To enable network access to the router on the first startup, static IP address 192.168.1.1/24 has been configured on Bridge 1 interface.

3 Connecting to the Command Line Interface (CLI) of the router

3.1 Ethernet LAN connection

> ⚠ **Upon the initial startup, the router starts with the factory configuration. The factory configuration is described in the** Router factory settings **section of this manual.**

Step 1. Connect the network data cable (patch cord) to any port within the ***'Trusted'*** zone and to the PC intended for management tasks.

Step 2. In the router factory configuration, DHCP server is enabled with IP address pool in **192.168.1.0/24** subnet.

When network interface is connected to the management computer, the latter should obtain the network address from the server.

If IP address is not obtained for some reason, assign the interface address manually using any address except for 192.168.1.1 in 192.168.1.0/24 subnet.

3.2 RS-232 console port connection

Step 1. Using RJ-45/DBF9 cable included into device delivery package, connect the router **Console** port to the computer RS-232 port.

Step 2. Launch terminal application (e.g. HyperTerminal or Minicom) and create a new connection. VT100 terminal emulation mode should be used.

Specify the following settings for RS-232 interface:

```
Data rate: 115200 bps
Data bits: 8 bits
Parity: none
Stop bits: 1
Flow control: none
```

4 Basic router configuration

Upon the first startup, the router configuration procedure includes the following steps:

- Changing password for "admin" user.
- Creation of new users.
- Assigning device name (Hostname).
- Setting parameters for public network connection in accordance with the provider requirements.
- Configuring remote connection to router.
- Applying basic settings.

4.1 Changing password for 'admin' user

To ensure the secure system access, you should change the password for the privileged 'admin' user.

> ⚠ **'techsupport' account ('eltex' up to version 1.0.7) is required for service centre specialist remote access.**
> **'remote' account – RADIUS, TACACS+, LDAP authentication.**
> **'admin', 'techsupport', 'remote' users cannot be deleted. Only passwords and a privilege level can be changed.**
> **By default, the 'admin' user with the 'password' password is defined in factory settings.**

Username and password are required for login during the device administration sessions.

To change 'admin' password, use the following commands:

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

4.2 Creating new users

To create a new system user or configure any of the parameters: username, password, privilege level, the following commands are used:

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

> ⚠ **Privilege levels 1–9 allow access to the device and viewing its operation status, but the device configuration is disabled. Privilege levels 10-14 allow both the access to the device and configuration of majority of its functions. Privilege level 15 allows both the access to the device and configuration of all its functions.**

Example of commands, that allow you to create user **'fedor'** with password **'12345678'** and privilege level **15** and create user **'ivan'** with password **'password'** and privilege level **'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
```

Privilege levels 1–9 allow accessing the device and viewing its operation status, but the device configuration is disabled. Privilege levels 10-14 allow both the access to the device and configuration of majority of its functions. Privilege level 15 allows both the access to the device and configuration of all its functions.

Example of commands, that allow you to create user **'fedor'** with password **'12345678'** and privilege level **15** and create user **'ivan'** with password **'password'** and privilege level **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
```

4.3 Assigning device name

To assign the device name, use the following commands:

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

When a new configuration is applied, command prompt will change to the value specified by **<new-name>** parameter.

4.4 Configuring public network parameters

To configure router network interface in the public network, you should assign parameters defined by the network provider – default IP address, subnet mask and gateway address – to the device.

Example of static IP address configuration commands for **Gigabit Ethernet 1/0/2.150** sub-interface used for obtaining access to the router via **VLAN 150**.

Interface parameters:

- IP address: 192.168.16.144;
- Subnet mask: 255.255.255.0;
- Default gateway IP address: 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
```

To ensure the correct IP address assigning for the interface, enter the following command when the configuration is applied:

```
esr# show ip interfaces
IP address            Interface                          Type
-------------------   --------------------------------   -------
192.168.16.144/24     gigabitethernet 1/0/2.150          static
```

Provider may use dynamically assigned addresses in their network. To get IP address, the DHCP protocol can be used if there is a DHCP server on the network

Configuration example for obtaining dynamic IP address from DHCP server on **Gigabit Ethernet 1/0/10** interface:

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

To ensure the correct IP address assigning for the interface, enter the following command when the configuration is applied:

```
esr# show ip interfaces
IP address            Interface                          Type
-------------------   --------------------------------   -------
192.168.11.5/25       gigabitethernet 1/0/10             DHCP
```

4.5 Configuring remote connection to router

In the factory configuration, remote access to the router may be established via Telnet or SSH from the '**trusted**' zone. To enable remote access to the router from other zones, e.g. from the public network, you should create the respective rules in the firewall.

When configuring access to the router, rules should be created for the following pair of zones:

- **source-zone** – zone that the remote access will originate from;
- **self** – zone which includes router management interface.

Use the following commands to create the allowing rule:

```
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
```

Example of commands that allow users from '**untrusted**' zone with IP addresses in range **132.16.0.5-132.16.0.10** to connect to the router with IP address **40.13.1.22** via 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
```

4.6 Applying basic settings

To apply the changes made to the router configuration, you must enter the following commands from the root section of the command interface.

```
esr# commit
esr# confirm
```

If remote access to the device was used during configuration and the network parameters of the control interface have changed, the connection to the device may be lost after entering the **commit** command. Use the new network parameters set in the configuration to connect to the device and enter the **confirm** command.

If the **confirm** command fails, when the confirm timer expires, the device configuration will revert to the previous state that existed before the **commit** command was entered.

4.7 Checking the settings made

To check if the settings are correct, try accessing *http://eltex-co.com* from the '**trusted**' zone. If access is granted, it means that the traffic goes through the service router. If access is not granted, make sure that the settings are correct.

5 Safe configuration recommendations

The safe configuration recommendations are general and suitable for most installations. These recommendations greatly improve the safe operation of the unit, but are not exhaustive. Depending on the application of the device, other safety parameters must also be configured. In some specific cases, the implementation of these recommendations may result in a non-functional network. When configuring the device, firstly it is necessary to follow the technical requirements and regulations of the networks in which the device will be used.

5.1 General recommendations

- It is recommended to always disable unused physical interfaces with the **shutdown** The command is described in detail in the *Interface monitoring and configuration* section of the CLI Command Reference.
- It is recommended to always set the system clock to synchronize with trusted network time sources (NTP). The NTP setup algorithm is described in the *NTP configuration section* of the user manual. For detailed information on the NTP configuration commands, see *System timer management* in the CLI Command Reference.
- It is recommended to disable the NTP broadcast client, which is enabled by default in the factory configuration.
- It is not recommended to use the **ip firewall disable** command that disables firewalling. Always assign appropriate security zones to interfaces and configure the correct firewall rules. The firewall configuration algorithm is described in the *Firewall configuration* section of the User manual. For detailed information on the Firewall configuration commands, see *Firewall management* in the CLI Command Reference.

5.2 Event logging system configuration

Event logging system configuration algorithms are described in the **Syslog configuration** subsection of the *Monitoring section* of the User manual.

For detailed information on the Event logging system configuration commands, see *SYSLOG management* section in the CLI Command Reference.

5.2.1 Recommendations

- It is recommended to configure the event message storage in a syslog file on the device and transfer these events to an external syslog server.
- It is recommended to limit the size of the syslog file on the device.
- It is recommended to configure syslog file rotation on the device.
- It is recommended to enable syslog message enumeration.
- It is recommended that timestamp msec tags be added to syslog messages on ESR-1500 and ESR-1511.

5.2.2 Warnings

- The data stored in the **tmpsys:syslog** file system is not saved when the device is rebooted. This type of file system is recommended for storing operational logs.
- It is not recommended to use the **flash:syslog** file system to store logs, as it may cause premature ESR device failure.

5.2.3 Configuration example

Objective:

Configure the storage of event messages of info level and higher in a syslog file on the device and configure transmission of these events to an external syslog server. Limit the file size to 512kb. Enable rotation of 3 files. Enable syslog message enumeration.

Solution:

Configure the storage of syslog messages in the file:

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

Configure size limitation and file rotation:

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

Configure the transmission of messages to an external server:

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

Enable syslog message enumeration:

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

5.3 Password usage policy configuration

The configuration algorithms for the password usage policy are described in the *AAA configuration* section of the User manual.

For detailed information on the configuration commands for the password usage policy, see *AAA configuration* in the CLI Commands Reference.

5.3.1 Recommendations

- It is recommended to always enable the default password change request for the admin user.
- It is recommended to limit the lifetime of passwords and prohibit reusing at least the previous password.
- It is recommended to set the minimum password length requirement greater than 8 characters.
- It is recommended to set requirements for the use of lowercase and uppercase letters, numbers and special characters.

5.3.2 Configuration example

Objective:

- Configure a password policy with a requirement to change the default password, a password validity period of 1 month, and a ban on using the last 12 passwords.
- Set the minimum password length to 16 characters, the maximum to 64 characters.
- The password must contain at least 3 uppercase letters, at least 5 lowercase letters, at least 4 digits and at least 2 special characters. The password must contain all 4 types of characters.

Solution:

Enables the default password reset request for admin user:

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

Set the password lifetime to 30 days and prohibit the use of the previous 12 passwords:

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

Set a limit to the password length:

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

Set a limit on the minimum number of characters of the respective types:

```
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
```

5.4 AAA policy configuration

The configuration algorithms for the AAA policy are described in the *AAA configuration* section of the User manual.

For detailed information on the commands for AAA policy, see *AAA configuration* in the CLI Commands Reference.

5.4.1 Recommendations

- It is recommended to use a role-based access model on the device.
- It is recommended to use personal accounts to authenticate on the device.
- It is recommended to enable logging of commands entered by the user.
- It is recommended to use several authentication methods for logging in to devices via console, remote login to devices and privilege escalation. A combination of RADIUS/TACACS/LDAP authentication and local authentication is considered optimal.
- It is recommended to lower the built-in **admin** account privileges to 1.
- It is recommended to configure logging of changes of local accounts.
- It is recommended to configure AAA policy change logging.

5.4.2 Warnings

- The built-in admin account cannot be deleted.
- The **no username admin** command does not remove the **admin** user, it resets his configuration to defaults. After applying this command, the **admin** user will not appear in the configuration.
- The **no password** command for the **admin** user also does not remove the **admin** user's password, but resets it to its default value. After applying this command, the **admin** user password is no longer displayed in the configuration and becomes 'password'.
- Attention! You must have a user with privilege level 15 or an ENABLE password configured before you can set the admin user to downgrade privileges.

5.4.3 Configuration example

Objective:

Configure AAA policy:

- Use RADIUS authentication for remote login via SSH.
- Use RADIUS authentication for local console login, use local authentication if there is no connection to RADIUS servers.
- Use ENABLE password set via RADIUS, if there is no connection to RADIUS servers, use local ENABLE password.
- Set the admin user to a reduced privilege level.
- Configure logging of changes of local accounts.
- Configure AAA policy changes logging.
- Configure the logging of entered commands.

Solution:

Create a **local-operator** user with privilege level 8:

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

Set local ENABLE password:

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

Lower the privileges of the admin user:

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

Configure the connection to the two RADIUS servers, the primary 192.168.1.11 and the backup 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
```

Configure AAA policy:

```
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
```

Configure logging:

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

5.5 Remote management configuration

For more information on remote access configuration commands, see *SSH, Telnet access configuration* in the CLI command reference.

5.5.1 Recommendations

- It is recommended to disable remote control via telnet.
- It is recommended to generate new cryptographic keys.
- It is recommended to use crypto-resistant sha2-256, sha2-512 authentication algorithms and disable all others.
- It is recommended to use crypto-resistant aes256, aes256ctr encryption algorithms and disable all others.
- It is recommended to use dh-group-exchange-sha256 crypto-proof encryption key exchange algorithm and disable all others.
- It is recommended to allow access to remote control of the device only from certain IP addresses.

5.5.2 Configuration example

Objective:

Disable Telnet. Generate new encryption keys. Use crypto-resistant algorithms.

Solution:

Disable remote telnet control:

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

Disable outdated and not crypto-resistant algorithms:

```
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
```

5.6 Configuration of protection against network attacks mechanisms

The algorithms for configuring the network attack protection mechanisms are described in the Logging and network protection configuration section of the user manual.

For detailed information about the commands to configure the password policy, see Management of logging and protection against network attacks in the CLI Command Reference.

5.6.1 Recommendations

- It is recommended to always enable protection against IP spoofing.
- It is recommended to always enable protection against TCP packets with incorrectly set flags.
- It is recommended to always enable protection against fragmented TCP packets with the SYN flag set.
- It is recommended to always enable protection against fragmented ICMP packets.
- It is recommended to always enable protection against large ICMP packets.
- It is recommended to always enable protection against unregistered IP protocols.
- It is recommended to enable logging of the protection mechanism against network attacks.

5.6.2 Configuration example

Objective:

Configure the protection mechanism against network attacks in accordance with the recommendations.

Solution:

Enable protection against ip spoofing and logging of the protection mechanism:

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

Enable protection against TCP packets with incorrectly set flags and logging of the protection mechanism:

```
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
```

Enable protection against fragmented ICMP packets and protection mechanism logging:

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

Enable protection against large ICMP packets and logging of the protection mechanism:

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

Enable protection against unregistered IP protocols and logging protection mechanism:

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

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

http://www.eltex-co.com/support

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist in our technical forum.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/