

-
-
-

-

-
-
-

-

- $$\vdots$$

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

SYSLOG CLI.

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

•

$$\vdots$$

•

```
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'.**
- **! admin 15 ENABLE-.**

:

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.
- sha2-512 .
- aes256ctr .
- dh-group-exchange-sha256 .
- ip-.
- .

:

telnet. . .

⌵

telnet:

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

:

```

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 authentication algorithm sha2-256 disable
esr(config)# ip ssh encryption algorithm 3des 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 aes256 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

```

:

```

esr# update ssh-host-key dsa
esr# update ssh-host-key ecdsa 256
esr# update ssh-host-key ecdsa 384
esr# update ssh-host-key ecdsa 521
esr# update ssh-host-key ed25519
esr# update ssh-host-key rsa
esr# update ssh-host-key rsa 2048

```

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
```