AAA (Authentication, Authorization, Accounting) – .

- Authentication () – () . , .
- Authorization (, ,) – .
- Accounting () – .

1	local .	`esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]`	<NAME> – , 31 . : • local – ; • tacacs – TACACS-; • radius – RADIUS-; • ldap – LDAP-.
2	enable .	`esr(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]`	<NAME> – , 31 . : • local – ; • tacacs – TACACS-; • radius – RADIUS-; • ldap – LDAP-.
3	( ).	`esr(config)# aaa authentication mode <MODE>`	<MODE> – : • chain – FAIL, ; • break – FAIL, . , . : chain.
4	( )	`esr(config)# aaa authentication attempts max-fail <COUNT> <TIME>`	<COUNT> – , , [1..65535]; <TIME> – , , [1..65535]. : <COUNT> – 5; <TIME> – 300

5	admin ( )	esr(config)# security passwords default-expired	
6	( )	esr(config)# security passwords history <COUNT>	<COUNT> – . [1..15]. : 0
7	( )	esr(config)# security passwords lifetime <TIME>	<TIME> – . [1..365]. : .
8	ENABLE- ( )	esr(config)# security passwords min-length <NUM>	<NUM> – . [8..128]. : 0
9	ENABLE- ( )	esr(config)# security passwords max-length <NUM>	<NUM> – . [8..128]. : .
10	, ENABLE- ( )	esr(config)# security passwords symbol-types <COUNT>	<COUNT> – . [1..4]. : 1
11	ENABLE- ( )	esr(config)# security passwords lower-case <COUNT>	<COUNT> – ENABLE-. [0..128]. : 0
12	() ENABLE- ( )	esr(config)# security passwords upper-case <COUNT>	<COUNT> – () . [0..128]. : 0
13	ENABLE- ( )	esr(config)# security passwords numeric-count <COUNT>	<COUNT> – . [0..128]. : 0
14	ENABLE- ( )	esr(config)# security passwords special-case <COUNT>	<COUNT> – . [0..128]. : 0
15		esr(config)# username <NAME>	<NAME> – , 31 .
16		esr(config-user)# password { <CLEAR-TEXT> | encrypted <HASH_SHA512> }	<CLEAR-TEXT> – , [8 .. 32] , [0-9a-fA-F]; <HASH_SHA512> – sha512, 110 .
17		esr(config-user)# privilege <PRIV>	<PRIV> – . [1..15].
18		esr(config)# line console esr(config)# line telnet esr(config)# line ssh	
19		esr(config-line-ssh)# login authentication <NAME>	<NAME> – , 31 .
20		esr(config-line-ssh)# enable authentication <NAME>	<NAME> – , 31 .
21	,	esr(config-line-ssh)# exec-timeout <SEC>	<SEC> – , [1..65535].

AAA RADIUS

1	DSCP IP- RADIUS- ( ).	esr(config)# radius-server dscp <DSCP>	<DSCP> – DSCP, [0..63]. : 63.
2	RADIUS- ( ).	esr(config)# radius-server retransmit <COUNT>	<COUNT> – RADIUS-, [1..10]. : 1.
3	, , RADIUS- ( ).	esr(config)# radius-server timeout <SEC>	<SEC> – , [1..30]. : 3 .

4	RADIUS- .	esr(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>] esr(config-radius-server)#	<IP-ADDR> – IP- RADIUS-, AAA.BBB.CCC.DDD, [0..255]; <IPV6-ADDR> – IPv6- RADIUS-, X:X:X:X::X, [0..FFFF] <VRF> – VRF, 31 .
5	( ).	aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – , , [1..65535]; <TIME> – , , [1..65535]. : <COUNT> – 5; <TIME> – 300
6	RADIUS-.	esr(config-radius-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }	<TEXT> – [8..16] ASCII-; <ENCRYPTED-TEXT> – , [8..16] , [16..32] .
7	RADIUS- ( ).	esr(config-radius-server)# priority <PRIORITY>	<PRIORITY> – , [1..65535]. , . : 1.
8	, , RADIUS- ( ).	esr(config-radius-server)# timeout <SEC>	<SEC> – , [1..30]. : .
9	IPv4/IPv6-, IP/IPv6-RADIUS-.	esr(config-radius-server)# source-address { <ADDR> | <IPV6-ADDR> }	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]; <IPV6-ADDR> – IPv6- , X:X:X:X::X, [0..FFFF].
10	radius .	esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – , 31 . : • local – ; • tacacs – TACACS-; • radius – RADIUS-; • ldap – LDAP-.
11	radius .	esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – 31 ; • default – . <METHOD> – : • enable – enable-; • tacacs – TACACS; • radius – RADIUS; • ldap – LDAP.
12	( ).	esr(config)# aaa authentication mode <MODE>	<MODE> – : • chain – FAIL, ; • break – FAIL, . , . : chain.
13	radius ( ).	esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]	<METHOD> – : • tacacs – TACACS; • radius – RADIUS.
14	.	esr(config)# line <TYPE>	<TYPE> – : • console – ; • ssh – .
15	.	esr(config-line-console)# login authentication <NAME>	<NAME> – , 31 . 8.
16	.	esr(config-line-console)# enable authentication <NAME>	<NAME> – , 31 . 9.

AAA TACACS

1	DSCP IP- TACACS- ( ).	esr(config)# tacacs-server dscp <DSCP>	<DSCP> – DSCP, [0..63]. : 63.
2	, , TACACS- ( ).	esr(config)# tacacs-server timeout <SEC>	<SEC> – , [1..30]. : 3 .
3	TACACS- .	esr(config)# tacacs -server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>] esr(config- tacacs -server)#	<IP-ADDR> – IP- TACACS-, AAA.BBB.CCC.DDD, [0..255] <IPV6-ADDR> – IPv6- TACACS -, X:X:X:X::X, [0..FFFF] <VRF> – VRF, 31 .
4	( )	aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – , , [1..65535]; <TIME> – , , [1..65535]. : <COUNT> – 5; <TIME> – 300
5	TACACS-	esr(config-tacacs-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }	<TEXT> – [8..16] ASCII-; <ENCRYPTED-TEXT> – , [8..16] , [16..32] .
6	c TACACS- ( ).	esr(config-tacacs-server)# port <PORT>	<PORT> – TCP- c , [1..65535]. : 49 TACACS-.
7	TACACS ( ).	esr(config-tacacs-server)# priority <PRIORITY>	<PRIORITY> – , [1..65535]. , . : 1.
8	IPv4/IPv6-, IP/IPv6-TACACS-.	esr(config-radius-tacacs)# source-address { <ADDR> | <IPV6-ADDR> }	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255].
9	TACACS .	esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – 31 ; • default – . <METHOD> – : • enable – enable-; • tacacs – TACACS; • radius – RADIUS; • ldap – LDAP.
10	( ).	esr(config)# aaa authentication mode <MODE>	<MODE> – : • chain – FAIL, ; • break – FAIL, . , . : chain.
11	, CLI ( ).	esr(config)# aaa accounting commands stop-only tacacs	
12	tacacs ( ).	esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]	<METHOD> – : • tacacs – TACACS; • radius – RADIUS.
13	.	esr(config)# line <TYPE>	<TYPE> – : • console – ; • ssh – .
14	.	esr(config-line-console)# login authentication <NAME>	<NAME> – , 31 . 7.
15	.	esr(config-line-console)# enable authentication <NAME>	<NAME> – , 31 . 8.

AAA LDAP

1	DN (Distinguished name), .	`esr(config)# ldap-server base-dn <NAME>`	<NAME> – DN, 255 .
2	, , LDAP- ( ).	`esr(config)# ldap-server bind timeout <SEC>`	<SEC> – , [1..30]. : 3 .
3	DN (Distinguished name) , LDAP- .	`esr(config)# ldap-server bind authenticate root-dn <NAME>`	<NAME> – DN , 255 .
4	, LDAP- .	`esr(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }`	<TEXT> – [8..16] ASCII-; <ENCRYPTED-TEXT> – , [8..16] , [16..32] .
5	, LDAP- ( ).	`esr(config)# ldap-server search filter user-object-class <NAME>`	<NAME> – , 127 . : posixAccount.
6	LDAP- ( ).	`esr(config)# ldap-server search scope <SCOPE>`	<SCOPE> – LDAP-, : • onelevel – DN LDAP-; • subtree – DN LDAP . : subtree.
7	, , LDAP- , ( ).	`esr(config)# ldap-server search timeout <SEC>`	<SEC> – , [0..30] : 0 – LDAP-.
8	, LDAP- ( ).	`esr(config)# ldap-server naming-attribute <NAME>`	<NAME> – , 127 . : uid.
9	, ( ).	`esr(config)# ldap-server privilege-level-attribute <NAME>`	<NAME> – , 127 . : priv-lvl
10	DSCP IP- LDAP- ( ).	`esr(config)# ldap-server dscp <DSCP>`	<DSCP> – DSCP, [0..63]. : 63

11	LDAP- .	`esr(config)# ldap -server host { <IP-ADDR> | <IPV6-ADDR> }`
		`[ vrf <VRF> ]`
		`esr(config- ldap -server)#`
			<IP-ADDR> – IP- LDAP-, AAA.BBB.CCC.DDD, [0..255]
			<IPV6-ADDR> – IPv6- LDAP-, X:X:X:X::X, [0..FFFF]
			<VRF> – VRF, 31 .

12	( )	`aaa authentication attempts max-fail <COUNT> <TIME>`	<COUNT> – , , [1..65535]; <TIME> – , , [1..65535]. : <COUNT> – 5; <TIME> – 300
13	c LDAP- ( ).	`esr(config-ldap-server)# port <PORT>`	<PORT> – TCP- c , [1..65535]. : 389 LDAP-.
14	LDAP- ( ).	`esr(config-ldap-server)# priority <PRIORITY>`	<PRIORITY> – , [1..65535]. , . : 1.
15	IPv4/IPv6-, IP/IPv6- LDAP-.	`esr(config-ldap-server)# source-address { <ADDR> | <IPV6-ADDR> }`	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]; <IPV6-ADDR> – IPv6- , X:X:X:X::X, [0..FFFF].
16	LDAP .	`esr(config)# aaa authentication login { default | <NAME> }` `<METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]`	<NAME> – , 31 . : • local – ; • tacacs – TACACS-; • radius – RADIUS-; • ldap – LDAP-.

17	LDAP .	`esr(config)# aaa authentication enable <NAME> <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]`	<NAME> – 31 ; • default – . <METHOD> – : • enable – enable-; • tacacs – TACACS; • radius – RADIUS; • ldap – LDAP.
18 .		`esr(config)# aaa authentication mode <MODE>`	<MODE> – : • chain – FAIL, ; • break – FAIL, . , . : chain.
19 .		`esr(config)# line <TYPE>`	<TYPE> – : • console – ; • ssh – .
20 .		`esr(config-line-console)# login authentication <NAME>`	<NAME> – , 31 . 14.
21 .		`esr(config-line-console)# enable authentication <NAME>`	<NAME> – , 31 . 15.

telnet RADIUS-

:

, Telnet, RADIUS (192.168.16.1/24).

:

RADIUS- (password):

```
esr# configure
esr(config)# radius-server host 192.168.16.1
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# exit
```

:

```
esr(config)# aaa authentication login log radius
```

, Telnet-:

```
esr(config)# line telnet
esr(config-line-telnet)# login authentication log
esr(config-line-telnet)# exit
esr(config)# exit
```

RADIUS- :

```
esr# show aaa radius-servers
```

:

```
esr# show aaa authentication
```

, (1-15). , .

- *1-9* – (show ...);
- *10-14* – , ;
- *15* – .

CLI :

```
esr(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> – ;

<PRIV> – , [1..15];

<COMMAND> – , 255 .

:

10, «show interfaces bridges». «show interfaces bridges» 3.

:

, 10 3:

```
esr(config)# privilege root level 3 "show interfaces bridge"
esr(config)# privilege root level 10 "show interfaces"
```

1	ICMP flood .	`esr(config)# ip firewall screen dos-defense icmp-threshold { <NUM> }`	<NUM> – ICMP- [1..10000].
2	land .	`esr(config)# firewall screen dos-defense land`	
3	.	`esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }`	<NUM> – IP- [1..10000].
4	, DoS-.	`esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> }`	<NUM> – IP- [1..10000].
5	SYN flood .	`esr(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr]`	<NUM> – TCP SYN [1..10000]. src-dst – TCP SYN .
6	UDP flood .	`esr(config)# ip firewall screen dos-defense udp-threshold { <NUM> }`	<NUM> – UDP [1..10000].
7	winnuke-.	`esr(config)# ip firewall screen dos-defense winnuke`	
8	TCP- FIN ACK.	`esr(config)# ip firewall screen spy-blocking fin-no-ack`	

9	ICMP- .	`esr(config)# ip firewall screen spy-blocking icmp-type`	<TYPE> – ICMP, : • destination-unreachable • echo-request • reserved • source-quench • time-exceeded
10	IP-sweep .	`esr(config)# ip firewall screen spy-blocking ip-sweep { <NUM> }`	<NUM> – ip sweep , [1..1000000].
11	port scan .	`esr(config)# ip firewall screen spy-blocking port-scan { <threshold> } [ <TIME> ]`	<threshold> – , port scan [1..1000000]. <TIME> – [1..1000000].
12	IP spoofing .	`esr(config)# ip firewall screen spy-blocking spoofing`	
13	TCP-, SYN FIN.	`esr(config)# ip firewall screen spy-blocking syn-fin`	
14	TCP-, : FIN, PSH, URG. XMAS.	`esr(config)# ip firewall screen spy-blocking tcp-all-flag`	
15	TCP-, flags.	`esr(config)# ip firewall screen spy-blocking tcp-no-flag`	
16	ICMP-.	`esr(config)# ip firewall screen suspicious-packets icmp-fragment`	
17	IP .	`esr(config)# ip firewall screen suspicious-packets ip-fragment`	
18	ICMP- 1024 .	`esr(config)# ip firewall screen suspicious-packets icmp-fragment`	
19	TCP-, SYN.	`esr(config)# ip firewall screen suspicious-packets syn-fragment`	
20	UDP-.	`esr(config)# ip firewall screen suspicious-packets udp-fragment`	
21	, ID IP 137 .	`esr(config)# ip firewall screen suspicious-packets unknown-protocols`	
22	(SNMP, syslog CLI) .	`esr(config)# ip firewall logging interval <NUM>`	<NUM> – [30 .. 2147483647]
23	CLI.	`esr(config)# logging firewall screen detailed`	
24	DoS CLI, syslog SNMP.	`esr(config)# logging firewall screen dos-defense <ATACK_TYPE>`	<ATACK_TYPE> – DoS , : icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke.
25	CLI, syslog SNMP	`esr(config)# logging firewall screen spy-blocking { <ATACK_TYPE> | icmp-type <ICMP_TYPE> }`	<ATACK_TYPE> – , : fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag. <ICMP_TYPE> – ICMP, : destination-unreachable, echo-request, reserved, source-quench, time-exceeded.
26	CLI, syslog SNMP	`esr(config)# logging firewall screen suspicious-packets <PACKET_TYPE>`	< PACKET_TYPE> – , : icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols.

ip firewall screen dos-defense icmp-threshold	ICMP flood . ICMP- . - .

firewall screen dos-defense land	land . source destination IP-, SYN TCP. - TCP SYN TCP .
ip firewall screen dos-defense limit-session-destination	IP- , (: SYN flood, UDP flood, ICMP flood, ..). , DoS-.
ip firewall screen dos-defense limit-session-source	IP- , (DoS-: SYN flood, UDP flood, ICMP flood, ..). , DoS-.
ip firewall screen dos-defense syn-flood	SYN flood . TCP- SYN . - TCP SYN TCP-.
ip firewall screen dos-defense udp-threshold	UDP flood . UDP . - UDP-.
ip firewall screen dos-defense winnuke	winnuke . TCP- URG 139 . Windows (95).
ip firewall screen spy-blocking fin-no-ack	TCP- FIN ACK. .
ip firewall screen spy-blocking icmp-type destination-unreachable	ICMP- 3 (destination-unreachable), , .
ip firewall screen spy-blocking icmp-type echo-request	ICMP- 8 (echo-request), , .
ip firewall screen spy-blocking icmp-type reserved	ICMP- 2 7 (reserved), , .
ip firewall screen spy-blocking icmp-type source-quench	ICMP- 4 (source quench), , .
ip firewall screen spy-blocking icmp-type time-exceeded	ICMP- 11 (time exceeded), , .
ip firewall screen spy-blocking ip-sweep	IP-sweep . , 10 ICMP- , 10 , 11 . .
ip firewall screen spy-blocking port-scan	port scan . (<threshold>) 10 TCP- SYN TCP-, port scan (<TIME>). .
ip firewall screen spy-blocking spoofing	ip spoofing . . , 10.0.0.1/24 Gi1/0/1, Gi1/0/2, , . source IP-.
ip firewall screen spy-blocking syn-fin	TCP- SYN FIN. .
ip firewall screen spy-blocking tcp-all-flag	TCP- : FIN, PSH, URG. XMAS.
ip firewall screen spy-blocking tcp-no-flag	TCP- flags. .
ip firewall screen suspicious-packets icmp-fragment	ICMP-. ICMP- .
ip firewall screen suspicious-packets ip-fragment	.
ip firewall screen suspicious-packets large-icmp	ICMP- 1024 .
ip firewall screen suspicious-packets syn-fragment	TCP- SYN. TCP SYN . .
ip firewall screen suspicious-packets udp-fragment	UDP-.
ip firewall screen suspicious-packets unknown-protocols	, ID IP 137 .

:

LAN ESR land, syn-flood, ICMP flood SNMP SNMP- 192.168.0.10.

:

firewall (firewall):

```
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# ex
esr(config-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit
```

land, syn-flood, ICMP flood :

```
esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100
```

:

```
esr(config)# ip firewall logging screen dos-defense land
esr(config)# ip firewall logging screen dos-defense syn-flood
esr(config)# ip firewall logging screen dos-defense icmp-threshold
```

SNMP-, :

```
esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10
```

:

```
esr# show ip firewall screen counters
```

Firewall

Firewall – , .

1	.	esr(config)# security zone <zone-name1> esr(config)# security zone <zone-name2>	<zone-name> – 12 .
2	.	esr(config-zone)# description <description>	<description> – 255 .
3	VRF, ( ).	esr(config- zone)# ip vrf forwarding <VRF>	<VRF> – VRF, 31 .

4	NAT Firewall (,).	esr(config)# ip firewall sessions counters	
5	, - (,).	esr(config)# ip firewall sessions allow-unknown	
6	( )	esr(config)# ip firewall mode <MODE>	<MODE> – , : stateful, stateless. : stateful
7	( ).	esr(config)# ip firewall sessions generic-timeout <TIME>	<TIME> – , [1..8553600]. : 60 .
8	ICMP-, ( ).	esr(config)# ip firewall sessions icmp-timeout <TIME>	<TIME> – ICMP-, [1..8553600]. : 30 .
9	ICMPv6-, ( ).	esr(config)# ip firewall sessions icmpv6-timeout <TIME>	<TIME> – ICMP-, [1..8553600]. : 30 .
10	( ).	esr(config)# ip firewall sessions max-expect <COUNT>	<COUNT> – , [1..8553600]. : 256.
11	( ).	esr(config)# ip firewall sessions max-tracking <COUNT>	<COUNT> – , [1..8553600]. : 512000.
12	TCP- « », ( ).	esr(config)# ip firewall sessions tcp-connect-timeout <TIME>	<TIME> – TCP- " ", [1..8553600]. : 60 .
13	TCP- " ", ( ).	esr(config)# ip firewall sessions tcp-disconnect-timeout <TIME>	<TIME> – TCP- " ", [1..8553600]. : 30 .
14	TCP- " ", ( ).	esr(config)# ip firewall sessions tcp-established-timeout <TIME>	<TIME> – TCP- " ", [1..8553600]. : 120 .
15	, TCP- ( ).	esr(config)# ip firewall sessions tcp-latecome-timeout <TIME>	<TIME> – , [1..8553600]. : 120 .
16	( ).	esr(config)# ip firewall sessions tracking	<PROTOCOL> – [ftp, h323, pptp, netbios-ns, tftp], . <OBJECT-GROUP-SERVICE> – TCP/UDP- sip , 31 . , sip 5060. "all", . – .
17	UDP- " ", ( ).	esr(config)# ip firewall sessions udp-assured-timeout <TIME>	<TIME> – UDP- " ", [1..8553600]. : 180 .
18	UDP- « », .	esr(config)# ip firewall sessions udp-wait-timeout <TIME>	<TIME> – UDP- « », [1..8553600]. : 30 .
19	IP-, .	esr(config)# object-group network <obj-group-name>	<obj-group-name> – 31 .
20	IP- ( ).	esr(config-object-group-network)# description <description>	<description> – , 255 .
21	IPv4/IPv6- .	esr(config-object-group-network)# ip prefix <ADDR/LEN>	<ADDR/LEN> – , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32].
		esr(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – IP- ; <TO-ADDR> – IP- , . , IP-. AAA.BBB.CCC.DDD, [0..255].
		esr(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> – IP- , X:X:X:X::X/EE, X [0..FFFF] EE [1..128].
		esr(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – IPv6- ; <TO-ADDR> – IPv6- , . , IPv6-. X:X:X:X::X, [0..FFFF].

22	, .	esr(config)# object-group service <obj-group-name>	<obj-group-name> – , 31 .
23	( ).	esr(config-object-group-service)# description <description>	<description> – , 255 .
24	(tcp/udp) .	esr(config-object-group-service)# port-range <port>	<port> – [1..65535]. «,» «-».
25	, DPI.	esr(config)# object-group application <NAME>	<NAME> – , 31 .
26	( ).	esr(config-object-group-application)# description <description>	<description> – , 255 .
27	.	esr(config-object-group-application)# application < APPLICATION >	< APPLICATION > –
28	(, , E1/Multilink), (l2tp, openvpn, pptp) (gre, ip4ip4, l2tp, lt, pppoe, pptp) ( ).	esr(config-if-gi)# security-zone <zone-name>	<zone-name> – 12 .
	Firewall (, , E1/Multilink), (l2tp, openvpn, pptp) (gre, ip4ip4, l2tp, lt, pppoe, pptp) ( )	esr(config-if-gi)# ip firewall disable	
29	.	esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2>	<src-zone-name> – 12 . <dst-zone-name> – 12 .
30	.	esr(config-zone-pair)# rule <rule-number>	<rule-number> – 1..10000.
31	( ).	esr(config-zone-rule)# description <description>	<description> – 255 .
32	.	esr(config-zone-rule)# action <action> [log]	<action> – permit/deny/reject/netflow-sample /sflow-sample log – , .
33	IP-, ( ).	esr(config-zone-rule)# match [not] protocol <protocol-type>	<protocol-type> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. «any» .
		esr(config-zone-rule)# match [not] protocol-id <protocol-id>	<protocol-id> – IP-, [0x00-0xFF].
34	IP- , ( ).	esr(config-zone-rule)# match [not] source-address <OBJ-GROUP-NETWORK-NAME>	<OBJ-GROUP-NETWORK-NAME> – IP-, 31 . «any» IP- /.
35	IP- , ( ).	esr(config-zone-rule)# match [not] destination-address <OBJ-GROUP-NETWORK-NAME>	
36	MAC- , ( ).	esr(config-zone-rule)# match [not] source-mac <mac-addr>	<mac-addr> – XX:XX:XX:XX:XX:XX, [00..FF].
37	MAC- , ( ).	esr(config-zone-rule)# match [not] destination-mac <mac-addr>	
38	TCP/UDP- , ( ).	esr(config-zone-rule)# match [not] source-port <PORT-SET-NAME>	<PORT-SET-NAME> – 31 . «any» TCP /UDP- /.
39	TCP/UDP- , ( ).	esr(config-zone-rule)# match [not] destination-port <PORT-SET-NAME>	
40	ICMP, (ICMP) ( ).	esr(config-zone-rule)# match [not] icmp <ICMP_TYPE> <ICMP_CODE>	<ICMP_TYPE> – ICMP, [0..255]; <ICMP_CODE> – ICMP, [0..255]. «any» ICMP.
41	, , IP- .	esr(config-zone-rule)# match [not] destination-nat	
42	(, zone-pair any self zone-pair <zone-name> any).	esr(config-zone-pair-rule)# rate-limit pps <rate-pps>	<rate-pps> – , . [1..10000].

43	IP- (, zone-pair any self zone-pair <zone-name> any).	`esr(config-zone-pair-rule)# match [not] fragment`	
44	IP-, ip-option (, zone-pair any self zone-pair <zone-name> any).	`esr(config-zone-pair-rule)# match [not] ip-option`	
45	.	`esr(config-zone-rule)# enable`	
46	Bridge- (, ESR-1000/1200/1500/1700)	`esr(config-bridge)# ports firewall enable`	

---

[1] not, , .

«match» «not». , .

« CLI».

Firewall

:

ICMP R1, R2 ESR.

:

ESR :

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.12.2/24
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.23.2/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
```

«LAN», , «WAN», «WAN».

```
esr(config)# object-group network WAN
esr(config-object-group-network)# ip address-range 192.168.23.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN
esr(config-object-group-network)# ip address-range 192.168.12.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.12.1
esr(config-object-group-network)# exit
esr(config)# object-group network WAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.23.3
esr(config-object-group-network)# exit
```

«LAN» «WAN» , ICMP- R1 R2. *enable:*

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN_GATEWAY
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

«WAN» «LAN» , ICMP- R2 R1. *enable:*

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN_GATEWAY
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

«self». , , «self». , «WAN» «self». , ICMP- R2 ESR, ICMP- «WAN»:

```
esr(config)# security zone-pair WAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

, «LAN» «self». , ICMP- R1 ESR, ICMP- «LAN»:

```
esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

:

```
esr# show security zone
```

:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

:

```
esr# show ip firewall sessions
```

(DPI)

- . .

:

youtube, bittorrent facebook.

:

ESR :

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-te)# ip address 192.168.0.1/24
esr(config-if-te)# security-zone LAN
esr(config-if-te)# exit
```

, .

```
esr(config)# object-group application APP
esr(config-object-group-application)# application youtube
esr(config-object-group-application)# application bittorrent
esr(config-object-group-application)# application facebook
esr(config-object-group-application)# exit
```

«WAN» «LAN» , , , . *enable:*

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action deny
esr(config-zone-pair-rule)# match application APP
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)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

«LAN» «WAN» , . *enable:*

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

:

```
esr# show security zone
```

:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

:

```
esr# show ip firewall sessions
```

(ACL)

Access Control List ACL — , , .

1	.	esr(config)# ip access-list extended <NAME>	<NAME> – , 31 .
2	( ).	esr(config-acl)# description <DESCRIPTION>	<DESCRIPTION> – , 255 .
3	. .	esr(config-acl)# rule <ORDER>	<ORDER> – , [1..4094].
4	, , .	esr(config-acl-rule)# action <ACT>	<ACT> – : • permit – ; • deny – .
5	/ , ( ).	esr(config-acl-rule)# match protocol <TYPE>	<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. «any» ;
		esr(config-acl-rule)# match protocol-id <ID>	<ID> – IP-, [0x00-0xFF].
6	IP- , ( ).	esr(config-acl-rule)# match source-address { <ADDR> <MASK> | any }	<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]; <MASK> – IP-, AAA.BBB.CCC.DDD, [0..255]. , 0, IP-, .

7	IP- , ( ).	esr(config-acl-rule)# match destination-address { <ADDR> <MASK> | any }	«any» IP- /.
8	MAC- , ( ).	esr(config-acl-rule)# match source-mac <ADDR><WILDCARD>	<ADDR> – - , XX:XX:XX:XX:XX:XX, [00..FF]; <WILDCARD> – -, XX:XX:XX:XX:XX:XX, [00..FF]. , 0, MAC-, .
9	MAC- , ( ).	esr(config-acl-rule)# match destination-mac <ADDR><WILDCARD>	
10	TCP/UDP- , ( ).	esr(config-acl-rule)# match source-port { <PORT> | any }	<PORT> – TCP/UDP- , [1..65535]. «any» TCP/UDP- .
11	TCP/UDP- , ( ).	esr(config-acl-rule)# match destination-port { <PORT> | any }	
12	802.1p , ( ).	esr(config-acl-rule)# match os <COS>	<COS> – 802.1p , [0..7].
13	DSCP, ( ). IP Precedence.	esr(config-acl-rule)# match dscp <DSCP>	<DSCP> – DSCP, [0..63].
14	IP Precedence, ( ). DSCP.	esr(config-acl-rule)# match ip-precedence <IPP>	<IPP> – IP Precedence, [0..7].
15	VLAN, ( ).	esr(config-acl-rule)# match vlan <VID>	<VID> – VLAN, [1..4094].
16	.	esr(config-acl-rule)# enable	
17	.	esr(config-if-gi)# service-acl input <NAME>	<NAME> – , 31 .

QoS.

:

192.168.20.0/24.

:

:

```
esr# configure
esr(config)# ip access-list extended white
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Gi1/0/19 :

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# service-acl input white
```

:

```
esr# show ip access-list white
```

IPS/IDS

IPS/IDS (*Intrusion Prevention System / Intrusion Detection System*) – – , .

. IPS/IDS . ESR . - CLI , .

ESR EmergingThreats .

1	IPS/IDS.	`esr(config)# security ips policy <NAME>`	<NAME> – , 32
2	( ).	`esr(config-ips-policy)# description <DESCRIPTION>`	<DESCRIPTION> – 255 .
3	IP-, IPS/IDS.	`esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>`	<OBJ-GROUP-NETWORK-NAME> – IP-, 32 .
4	IP- , IPS/IDS ( ).	`esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>`	<OBJ-GROUP-NETWORK-NAME> – IP-, 32 .
5	IPS/IDS.	`esr(config)# security ips`	
6	IPS/IDS.	`esr(config-ips)# policy <NAME>`	<NAME> – , 32
7	ESR IPS /IDS. ( ).	`esr(config-ips)# perfomance max`	IPS/IDS .
8	USB , EVE. ( ).	`esr(config-ips)# logging storage-device <DEVICE_NAME>`	<DEVICE_NAME> usb .
9	IPS/IDS.	`esr(config- ips )# enable`	
10	IPS/IDS .	`esr(config-if-gi)# service-ips enable`	

IPS/IDS

1	.	`esr(config-ips)# auto-upgrade`	
2	.	`esr(config-ips-auto-upgrade)# user-server <WORD>`	<WORD> – , 32 .
3	. ( ).	`esr(config-ips-upgrade-user-server)# description <DESCRIPTION>`	<DESCRIPTION> – 255 .
4	URL.	`esr(config-ips-upgrade-user-server)# url <URL>`	<URL> – , URL- 8 255 . URL- : • .rule; • classification.config; • / .
5	. ( ).	`esr(config-ips-upgrade-user-server)# upgrade interval <HOURS>`	<HOURS> – , 1 240. : 24

https://sslbl.abuse.ch/	SSL Blacklist «» SSL , .. , . SHA1 SSL .
https://feodotracker.abuse.ch/	Feodo Tracker – Feodo. Feodo (Cridex Bugat) (, /) . (A, B, C D), .
https://rules.emergingthreats.net/open/suricata/rules/botcc.rules	. : Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker.
https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules	www.cinsarmy.com.
https://rules.emergingthreats.net/open/suricata/rules/compromised.rules	. : Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects.
https://rules.emergingthreats.net/open/suricata/rules/drop.rules	/ www.spamhaus.org.

https://rules.emergingthreats.net/open/suricata/rules/dshield.rules	www.dshield.org.
https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules	ActiveX-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules	, .
https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules	, .
https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules	DNS, DNS , DNS.
https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules	DOS-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules	FTP, FTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules	: World of Warcraft, Starcraft ..
https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules	ICMP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules	ICMP-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules	IMAP, IMAP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules	, HTTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules	NetBIOS, NetBIOS.
https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules	P2P- (Bittorrent, Gnutella, Limewire).
https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules	(MySpace, Ebay).
https://rules.emergingthreats.net/open/suricata/rules/emerging-poprules	POP3, POP3.
https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules	RPC, RPC.
https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules	SCADA-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules	, (Nessus, Nikto, portscanning).
https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules	, - .
https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules	SMTP, SMTP.

https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules	SQL.
https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules	telnet, telnet.
https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules	TFTP, TFTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules	.
https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules	HTTP- (HTTP- User-Agent).
https://rules.emergingthreats.net/open/suricata/rules/emerging-l.rules	VOIP-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules	-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules	-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules	-.
https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules	.

IPS/IDS

:

.

192.168.1.0/24 –

:

, :

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

ESR DNS- IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain name-server 8.8.8.8
```

IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

IPS/IDS bridge 1:

```
esr(config)# bridge 1
esr(config-bridge)# service-ips enable
```

IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# logging storage-device usb://DATA
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

, IPS/IDS :

```
esr(config-ips)# perfomance max
```

EmergingThreats.net, etnetera.cz Abuse.ch:

```
esr(config-ips)# auto-upgrade
esr(config-auto-upgrade)# user-server ET-Open
esr(config-ips-upgrade-user-server)# description «emerging threats open rules»
esr(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/rules/
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server Aggressive
esr(config-ips-upgrade-user-server)# description «Etnetera aggressive IP blacklist»
esr(config-ips-upgrade-user-server)# url https://security.etnetera.cz/feeds/etn_aggressive.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server SSL-BlackList
esr(config-ips-upgrade-user-server)# description «Abuse.ch SSL Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server C2-Botnet
esr(config-ips-upgrade-user-server)# description «Abuse.ch Botnet C2 IP Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslipblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
```

1		esr(config)# security ips-category user-defined <WORD>	<WORD> – , 32 .
2	( ).	esr(config-ips-category)# description <DESCRIPTION>	<DESCRIPTION> – 255 .
3	.	esr(config-ips-category)# rule <ORDER>	<ORDER> – , [1..512].
4	( )	esr(config-ips-category-rule)# description <DESCRIPTION>	<DESCRIPTION> – 255 .
5		esr(config-ips-category-rule)# action { alert | reject | pass | drop }	• alert – , IPS/IDS ; • reject – . TCP TCP-RESET, ICMP-ERROR. IPS/IDS ; • pass – ; • drop – , IPS/IDS .
6	IP-,	esr(config-ips-category-rule)# protocol <PROTOCOL>	<PROTOCOL> – any/ip/icmp/http/tcp/udp «any»

7	IP-	`esr(config-ips-category-rule)# source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }`	<<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]; <ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32]. < OBJ_GR_NAME> – IP-, ip , 31 . • protect – , protect IPS/IDS; • external – , external IPS/IDS. «any» IP- .
8	TCP/UDP- , . protocol icmp, source-port any	esr(config-ips-category-rule)# source-port {any | <PORT> | object-group <OBJ-GR-NAME> }	<PORT> – TCP/UDP- , [1..65535]. <OBJ_GR_NAME> – TCP/UDP , 31 . «any» TCP/UDP- .
9	IP-	`esr(config-ips-category-rule)# destination-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }`	<<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]; <ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32]. < OBJ_GR_NAME> – IP-, ip , 31 . • protect – , protect IPS/IDS; • external - , external IPS/IDS. «any» IP- .
10	TCP/UDP- , . protocol icmp, destination-port any	`esr(config-ips-category-rule)# destination-port {any | <PORT> | object-group <OBJ-GR-NAME> }`	<PORT> – TCP/UDP- , [1..65535]. <OBJ_GR_NAME> – TCP/UDP , 31 . «any» TCP/UDP- .
11	,	`esr(config-ips-category-rule)# direction { one-way | round-trip }`	• one-way – . • round-trip – .
12	IPS/IDS ,	`esr(config-ips-category-rule)# meta log-message <MESSAGE>`	<MESSAGE> – , 129 .
13	, , ( )	`esr(config-ips-category-rule)# meta classification-type { not-suspicious | unknown | bad-unknown | attempted-recon | successful-recon-limited | successful-recon-largescale | attempted-dos | successful-dos | attempted-user | unsuccessful-user | successful-user | attempted-admin | successful-admin | rpc-portmap-decode | shellcode-detect | string-detect | suspicious-filename-detect | suspicious-login | system-call-detect | tcp-connection | trojan-activity | unusual-client-port-connection | network-scan | denial-of-service | non-standard-protocol | protocol-command-decode | web-application-activity | web-application-attack | misc-activity | misc-attack | icmp-event | inappropriate-content | policy-violation | default-login-attempt }`	• not-suspicious – . • unknown – . • bad-unknown – . • attempted-recon – . • successful-recon-limited – . • successful-recon-largescale – . • attempted-dos – . • successful-dos – . • attempted-user – . • unsuccessful-user – . • successful-user – . • attempted-admin – . • successful-admin – . • rpc-portmap-decode – RPC. • shellcode-detect – . • string-detect – . • suspicious-filename-detect – -. • suspicious-login – . • system-call-detect – . • tcp-connection – TCP-. • trojan-activity – . • unusual-client-port-connection – . • network-scan – . • denial-of-service – . • non-standard-protocol – . • protocol-command-decode – . • web-application-activity – -. • web-application-attack – -. • misc-activity – . • misc-attack – . • icmp-event – ICMP. • inappropriate-content – . • policy-violation – . • default-login-attempt – /.
14	DSCP, ( ).	`esr(config-ips-category-rule)# ip dscp <DSCP>`	<DSCP> – DSCP, [0..63].
15	(TTL), ( ).	`esr(config-ips-category-rule)# ip ttl <TTL>`	<TTL> – TTL, [1..255].

16	IP-, protocol any ( ).	`esr(config-ips-category-rule)# ip protocol-id <ID>`	<ID> – IP-, [1..255].
17	ICMP CODE, protocol icmp ( ).	`esr(config-ips-category-rule)# ip icmp code <CODE>`	<CODE> – CODE ICMP, [0..255].
		`esr(config-ips-category-rule)# ip icmp code comparison-operator { greater-than | less-than }`	ip icmp code: • greater-than – .. • less-than – ..
18	ICMP ID, protocol icmp ( ).	`esr(config-ips-category-rule)# ip icmp id <ID>`	<ID> – ID ICMP, [0.. 65535].
19	ICMP Sequence-ID, protocol icmp ( ).	`esr(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID>`	<SEQ-ID> – Sequence-ID ICMP, [0.. 4294967295].
20	ICMP TYPE, protocol icmp ( ).	`esr(config-ips-category-rule)# ip icmp type <TYPE>`	<TYPE> – TYPE ICMP, [0..255].
		`esr(config-ips-category-rule)# ip icmp type comparison-operator { greater-than | less-than }`	ip icmp type: • greater-than – .. • less-than – ..
21	TCP Acknowledgment-Number, protocol tcp ( ).	`esr(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM>`	<ACK-NUM> – Acknowledgment-Number TCP, [0.. 4294967295].
22	TCP Sequence-ID, protocol tcp ( ).	`esr(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID>`	<SEQ-ID> – Sequence-ID TCP, [0.. 4294967295].
23	TCP Window-Size, protocol tcp ( ).	`esr(config-ips-category-rule)# ip tcp window-size <SIZE>`	<SIZE> – Window-Size TCP, [0.. 65535].
24	HTTP, protocol http ( ).	`esr(config-ips-category-rule)# ip http { accept | accept-enc | accept-lang | client-body | connection | content-type | cookie | file-data | header | header-names | host | method | protocol | referer | request-line | response-line | server-body | start | start-code | start-msg | uri | user-agent }`	Suricata 4.X. https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html
25	URI LEN HTTP, protocol http ( ).	`esr(config-ips-category-rule)# ip http urilen <LEN>`	<LEN> – [0.. 65535].
		`esr(config-ips-category-rule)# ip http urilen comparison-operator { greater-than | less-than }`	ip http urilen: • greater-than – .. • less-than – ..
26	(Payload content), ( ).	`esr(config-ips-category-rule)# payload content <CONTENT>`	<CONTENT> – , 1024 .
27	. payload content ( ).	`esr(config-ips-category-rule)# payload no-case`	
28	. payload content ( ).	`esr(config-ips-category-rule)# payload depth <DEPTH>`	<DEPTH> – , [1.. 65535]. .

29	. payload content ( ).	`esr(config-ips-category-rule)# payload offset <OFFSET>`	<OFFSET> – , [1.. 65535]. .
30	, . ( )	`esr(config-ips-category-rule)# payload data-size <SIZE>`	<SIZE> – , [0.. 65535].
		`esr(config-ips-category-rule)# payload data-size comparison-operator { greater-than | less-than }`	payload data-size: • greater-than – .. • less-than – .
31	, ( )	`esr(config-ips-category-rule)# threshold count <COUNT>`	<COUNT> – , [1.. 65535].
32	, . (threshold count)	`esr(config-ips-category-rule)# threshold second <SECOND>`	<SECOND> – , [1.. 65535].
33	. (threshold count)	`esr(config-ips-category-rule)# threshold track { by-src | by-dst }`	• by-src – IP-. • by-dst – IP-.
34		`esr(config-ips-category-rule)# threshold type {threshold | limit | both }`	• threshold – . • limit – <COUNT> <SECOND>. • both – threshold limit. , <SECOND> <COUNT> , <SECOND>

:

IP 192.168.1.10 DOS- ICMP- .

:

:

```
esr(config)# security ips-category user-defined USER
```

:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description «Big ICMP DoS»
```

:

```
esr(config-ips-category-rule)# action drop
```

:

```
esr(config-ips-category-rule)# meta log-message «Big ICMP DoS»
esr(config-ips-category-rule)# meta classification-type successful-dos
```

:

```
esr(config-ips-category-rule)# protocol icmp
```

icmp, any:

```
esr(config-ips-category-rule)# source-port any
esr(config-ips-category-rule)# destination-port any
```

:

```
esr(config-ips-category-rule)# destination-address ip 192.168.1.10
```

:

```
esr(config-ips-category-rule)# source-address any
```

:

```
esr(config-ips-category-rule)# direction one-way
```

1024:

```
esr(config-ips-category-rule)# payload data-size 1024
esr(config-ips-category-rule)# payload data-size comparison-operator greate
r-than
```

3/, :

```
3 / = 3145728
  1 = 8192
3145728 / 8192 = 384
384 * 60 = 23040
```

```
esr(config-ips-category-rule)# threshold count 2340
esr(config-ips-category-rule)# threshold second 60
esr(config-ips-category-rule)# threshold track by-dst
esr(config-ips-category-rule)# threshold type both
```

1	.	esr(config)# security ips-category user-defined <WORD>	<WORD> – , 32 .
2	().	esr(config-ips-category)# description <DESCRIPTION>	<DESCRIPTION> – 255 .
3	.	esr(config-ips-category)# rule-advanced <SID>	<SID> – , [1.. 4294967295]
4	()	esr(config-ips-category-rule-advanced)# description <DESCRIPTION>	<DESCRIPTION> – 255 .
5		esr(config-ips-category-rule-advanced)# rule-text <LINE>	<CONTENT> - SNORT 2.X / Suricata 4.X, 1024 . „ ‘

:

Slowloris.

:

:

```
esr(config)# security ips-category user-defined ADV
```

:

```
esr(config-ips-category)# rule-advanced 1
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 1»
esr(config-ips-category-rule-advanced)# rule-text "alert tcp any any -> any 80 (msg:'Possible Slowloris Attack
Detected';
flow:to_server,established; content:'X-a|3a|'; distance:0; pcre:'/\d\d\d\d/'; distance:0; content:'|0d 0a|';
sid:10000001;)"
```

, , :

```
esr(config-ips-category)# rule-advanced 2
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 2»
esr(config-ips-category-rule-advanced)# rule-text «alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:'SlowLoris.py DoS attempt'; flow:established,to_server,no_stream; content:'X-a:'; dsize:<15;
detection_filter:track by_dst, count 3, seconds 30; classtype:denial-of-service; sid: 10000002; rev:1; )
```