(IPS/IDS)

⚠ .

- IPS/IDS
  - description
  - enable
  - show security ips content-provider
  - show security ips content-provider rules-info
  - show security ips counters
  - show security ips status
  - show security ips user-server
  - update security ips content-provider rules
  - update security ips content-provider rules-info
  - update security ips user-server rules
- IPS/IDS
  - category
  - external network-group
  - protect network-group
  - rules action
  - rules count
  - security ips policy
  - vendor
- IPS
  - logging ips severity
  - logging remote-server
  - logging update-interval
  - security ips
  - performance max
  - policy
  - service-ips enable
- IPS/IDS,
  - content-provider
  - host address
  - host port
  - location
  - reboot
  - storage-path
  - system-name
  - upgrade interval
- IPS/IDS
  - auto-upgrade
  - upgrade interval
  - url
  - user-server
- IPS/IDS
  - action
  - destination-address
  - destination-port
  - direction
  - ip dscp
  - ip ftp command
  - ip ftp-data command
  - ip http
  - ip http content-filter
  - ip http method
  - ip icmp code
  - ip icmp code comparison-operator
  - ip icmp id
  - ip icmp sequence-id
  - ip icmp type
  - ip icmp type comparison-operator
  - ip protocol-id
  - ip tcp acknowledgment-number
  - ip tcp sequence-id
  - ip tcp window-size
  - ip ttl
  - ip ttl comparison-operator
  - meta classification-type
  - meta log-message
  - payload content
  - payload data-size
  - payload data-size comparison-operator
  - payload depth
  - payload no-case

- payload offset
- protocol
- rule
- security ips-category user-defined
- source-address
- source-port
- threshold count
- threshold second
- threshold track
- threshold type
-
- rule-advanced
- rule-text

IPS/IDS

description

.

(no) .

```
description <DESCRIPTION>
no description
```

<DESCRIPTION> – , 255 .

10

CONFIG-IPS-CATEGORY

CONFIG-IPS-CATEGORY-RULE

CONFIG-IPS-CATEGORY-RULE-ADVANCED

CONFIG-IPS-POLICY

CONFIG-IPS-UPGRADE-USER-SERVER

CONFIG-CONTENT-PROVIDER

```
esr(config-ips-upgrade-user-server)# description "Etnetera aggressive IP blacklist"
```

enable

IPS/IDS .

(no) IPS/IDS.

```
[no] enable
```

.

IPS/IDS .

15

CONFIG-IPS

CONFIG-IPS-CATEGORY-RULE

CONFIG-IPS-CATEGORY-RULE-ADVANCED

CONFIG-CONTENT-PROVIDER

CONFIG-IPS-UPGRADE-USER-SERVER

```
esr(config-ips)# enable
```

show security ips content-provider

IPS/IDS, .

```
show security ips content-provider
```

10

ROOT

```
esr# show security ips content-provider
 Server: content-provider
                 Last MD5 of received files:        93633ab9a73248ea50d58c25b1ac806c
                 Next update: 06 October 2020 12:27:40
```

show security ips content-provider rules-info

IPS/IDS, . .

```
show security ips content-provider rules-info
```

10

ROOT

```
esr# show security ips content-provider rules-info
Vendor : kaspersky
    Category : IoTURLsDF
        Count of rules : 8000
        Description : Kasperksy Lab IoTURLsDF feed
                      IoTURLsDF URL feed - a set of URLs with context covering malware that infects IoT
(Internet of Things) devices
    Category : MaliciousHashDF
        Count of rules : 1
        Description : Kasperksy Lab MaliciousHashDF feed
                      Malicious Hash feed - a set of hashes of malicious objects
    Category : PhishingURLsDF
        Count of rules : 11167
        Description : Kasperksy Lab PhishingURLsDF feed
                      Phishing URL feed - a set of URLs with context that cover phishing websites and web pages
```

show security ips counters

IPS/IDS.

```
show security ips counters
```

10

ROOT

```
esr# show security ips counters
TCP flows processed : 34687
Alerts generated : 456
Blocked by ips engine : 78
Accepted by ips engine : 1356436
```

show security ips status

, IPS/IDS.

```
show security ips status [detailed]
```

detailed – .

10

ROOT

```
esr# show security ips status

Rule files processed:         3
Rules successfully loaded:    21724
Rules failed:                 0


esr# show security ips status detailed
Rule files processed:         3
Rules successfully loaded:    21724
Rules failed:                 0
Rules processed:              21727
IP-only inspecting:           1
Payload inspecting:           3980
Application layer inspecting: 18951
Decoder event:                0
```

show security ips user-server

IPS/IDS .

show security ips user-server [<WORD>]

<WORD> 1 64 .

10

ROOT

```
esr# sh security ips user-server
Server name                     Files MD5                       Next update
--------------------------------  --------------------------------  --------------------------------
content-provider                93633ab9a73248ea50d58c25b1ac806c  06 October 2020 12:27:40
TH                              919f51bdf44052bfc0953362aef11c0d  06 October 2020 12:36:40
Traffic-ID                      e5e2f6472a397227c0d96f5df430a207  06 October 2020 12:36:40
Aggressive                      cfc3547b50f3f9fec366ba5a1e51cd1f  06 October 2020 12:36:40
JA3-Fingerprint                 439aa6e57c66826b92337672937d505b  05 October 2020 16:51:40
C2-Botnet                       39e118bd3884b3dc1df4ca3a03c05df1  05 October 2020 16:51:40
SSL-BlackList                   1d9c969f25791b9ee8c8c0ab8449d849  05 October 2020 16:51:40
ET-Open                         d53d92248a1f7cdc040d669a76cf27bc  06 October 2020 12:36:40
```

update security ips content-provider rules

IPS/IDS, .

. 5 .

```
update security ips content-provider rules
```

15

update security ips content-provider rules

ROOT

```
esr# update security ips content-provider rules
```

update security ips content-provider rules-info

IPS/IDS, .

. 5 .

```
update security ips content-provider rules-info
```

15

ROOT

```
esr# update security ips content-provider rules-info
```

update security ips user-server rules

IPS/IDS .

. 5 .

```
update security ips user-server rules <WORD>
```

<WORD> 1 64 .

15

ROOT

```
esr# update security ips user-server rules ET-Open
```

IPS/IDS

category

IPS/IDS , ,

(no) IPS/IDS.

```
category <CATEGORY>
```

```
no category { <CATEGORY> | all }
```

<CATEGORY> – .

:

```
show security ips content-provider rules-info
```

15

CONFIG-IPS-VENDOR

```
esr(config-ips-vendor)# category MobileBotnetCAndCDF
```

external network-group

IP-, IPS/IDS .

IP- .

(no) IPS/IDS.

```
external network-group <OBJ-GROUP-NETWORK-NAME>
no external network-group
```

<OBJ-GROUP-NETWORK-NAME> – IP-, 31 .

15

CONFIG-IPS-POLICY

```
esr(config-ips-policy)# external network-group WAN
```

protect network-group

IP-, IPS/IDS.

IP- .

(no) IPS/IDS.

```
protect network-group <OBJ-GROUP-NETWORK-NAME>
no protect network-group
```

<OBJ-GROUP-NETWORK-NAME> – IP-, 31 .

15

CONFIG-IPS-POLICY

```
esr(config-ips-policy)# protect network-group LAN
```

rules action

, , .

(no) .

, .

```
rules action { alert | reject | pass | drop }
no rules action
```

:

- alert – , IPS/IDS ;
- reject – . TCP TCP-RESET, ICMP-ERROR. C IPS/IDS ;
- pass – ;
- drop – , IPS/IDS .

15

CONFIG-IPS-VENDOR-CATEGORY

```
esr(config-ips-vendor-category)# rules action drop
```

rules count

, IPS/IDS

(no) .

, .

```
rules count <COUNT>
no rules count
```

:

<COUNT> – . 1, .

```
show security ips content-provider rules-info
```

15

CONFIG-IPS-VENDOR-CATEGORY

```
esr(config-ips-vendor-category)# rules count 8000
```

security ips policy

IPS/IDS .

(no) IPS/IDS.

```
[no] security ips policy <POLICY_NAME>
```

<POLICY_NAME> – IPS/IDS, 31 .

15

CONFIG

```
esr(config)# security ips policy OFFICE
```

vendor

IPS/IDS, ,

(no) IPS/IDS.

```
vendor <VENDOR>
no vendor <CATEGORY>
```

<VENDOR> – .

:

```
show security ips content-provider rules-info
```

15

CONFIG-IPS-POLICY

```
esr(config-ips-policy)# vendor kaspersky
```

IPS

logging ips severity

IPS/IDS.
(no) .

```
logging ips severity <SEVERITY>
no logging ips severity
```

<SEVERITY> – , ( ):

- emerg – , ;
- alert – , ;
- crit – , ;
- error – ;
- warning – , ;
- notice – ;
- info – ;
- debug – , ;
- none – syslog-.

info

15

CONFIG

```
esr(config)# logging ips severity error
```

logging remote-server

IPS/IDS EVE (elasticsearch).

(no) .

```
logging remote-server { <ADDR> | <IPV6-ADDR> } [ <TRANSPORT> ] [ <PORT> ] [ source-address { <SRC-ADDR> | <IPV6-SRC-ADDR> } ]
no logging remote-server
```

<ADDR> – IP-, AAA.BBB.CCC.DDD, [0..255];

<IPV6-ADDR> – IPv6-, X:X:X:X::X, [0..FFFF];

<TRANSPORT> – , - UDP, :

- TCP – TCP;
- UDP – UDP;

<PORT> – TCP/UDP-, , [1..65535], 514;

<SRC-ADDR> – IPv4- , IP- syslog , - ipv4- ;

<IPV6-SRC-ADDR> – IPv6- , IPv6- syslog , - ipv6- ;

15

CONFIG-IPS

```
esr(config-ips)# logging remote-server 192.168.0.101
```

logging update-interval

IPS/IDS EVE (elasticsearch).

(no) .

```
logging update-interval <INTERVAL>
no logging update-interval
```

<INTERVAL> – IPS/IDS, ;

10

15

CONFIG-IPS

```
esr(config-ips)# logging update-interval 10
```

security ips

IPS/IDS .

```
security ips
```

15

CONFIG

```
esr(config)# security ips
```

performance max

IPS/IDS . , IPS/IDS. , IPS/IDS (, BRAS ..).

(no) .

```
[no] performance max
```

15

CONFIG-IPS

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

policy

IPS/IDS.

(no) IPS/IDS.

```
policy <POLICY_NAME>
no policy
```

<POLICY_NAME> – IPS, 32 .

15

CONFIG-IPS

```
esr(config-ips)# policy OFFICE
```

service-ips enable

IPS/IDS .

(no) IPS/IDS .

```
[no] service-ips enable
```

15

CONFIG-GI

CONFIG-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

```
esr(config-if-gi)# service-ips enable
```

IPS/IDS,

content-provider

, .

```
content-provider
```

15

CONFIG

```
esr(config)# content-provider
```

host address

, .

```
host address { <ADDR> | <IPV6-ADDR> | <HOSTNAME> }
```

<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];

<IPV6-ADDR> – IPv6- , X:X:X:X::X, [0..FFFF];

<HOSTNAME> – DNS- , 255 ;

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# host address edm.eltex-co.ru
```

host port

TCP- , .

(no) TCP- , .

```
host port <PORT>
no host port
```

<PORT> – TCP-, [1..65535];

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# host port 8098
```

location

, EDM-Issue.

(no) .

⚠ « » web- EDM-Issue https://docs.eltex-co.ru/x/JQFtCw show EDM-Issue https://docs.eltex-co.ru/x/MAFtCw

```
location <WORD>
no location
```

<WORD> – , 255 .

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# location "Server room in Novokuznetsk office"
```

reboot

. , .

IPS/IDS .

```
reboot { immediately | time <TIME> }
```

immediately – ;

time <TIME> – <TIME>;

<TIME> – HH:MM:SS.

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# reboot time 05:00:00
```

storage-path

, IPS/IDS , .

IPS/IDS exFAT

(no) .

```
storage-path { usb://<USB-NAME>:/<PATH> | mmc://<MMC-NAME>:/<PATH> }
no storage-device
```

<USB-NAME> – USB-. show storage-devices usb;

<MMC-NAME> – MMC-. show storage-devices mmc;

<PATH> – .

config-ips-upgrade-user-server

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# storage-device usb://DATA/IPS
```

system-name

, EDM-Issue

(no) .

⚠ « » web- EDM-Issue https://docs.eltex-co.ru/x/JQFtCw show EDM-Issue https://docs.eltex-co.ru/x/MAFtCw

```
system-name <WORD>
no system-name
```

<WORD> – , 255 .

system-name hostname

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# system-name main-office
```

upgrade interval

, IPS/IDS, .

(no) .

```
upgrade interval <HOURS>
no upgrade interval
```

<HOURS> – , 1 240.

24

15

CONFIG-CONTENT-PROVIDER

```
esr(config-content-provider)# upgrade interval 36
```

IPS/IDS

auto-upgrade

.

```
auto-upgrade
```

15

CONFIG-IPS

```
esr(config-ips)# auto-upgrade
```

upgrade interval

, IPS/IDS / IPD/IDS URL.

(no) .

```
upgrade interval <HOURS>
no upgrade interval
```

<HOURS> – , 1 240.

24

15

CONFIG-IPS-UPGRADE-USER-SERVER

```
esr(config-ips-upgrade-user-server)# upgrade interval 36
```

url

URL-.

(no) IPS/IDS.

```
url <URL>
no url
```

<URL> – , URL- 8 255 .

URL- :

- .rule,
- classification.config
- / .

15

CONFIG-IPS-UPGRADE-USER-SERVER

```
esr(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/rules/
```

user-server

IPS/IDS .

(no) IPS/IDS .

```
user-server <WORD>
```

```
no user-server { <WORD> | all }
```

<WORD> 1 64 .

15

CONFIG-IPS-AUTO-UPGRADE

```
esr(config-ips-auto-upgrade)# user-server ET-Open
```

IPS/IDS

action

 , , .

 (no) .

```
action { alert | reject | pass | drop }
```

```
no action
```

:

- alert – , IPS/IDS ;
- reject – . TCP-, TCP-RESET, ICMP-ERROR. C IPS/IDS ;
- pass – ;
- drop – , IPS/IDS .

15

CONFIG-IPS-CATEGORY-RULE

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

destination-address

IP- , .

 (no) .

```
destination-address { ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group {
protect | external } | any }
```

```
no destination-address
```

<ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];

<ADDR/LEN> – IP-, AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32];

<OBJ_GR_NAME> – IP-, IP- , 31 ;

destination-address policy-object-group protect protect-, IPS/IDS;

destination-address policy-object-group external external-, IPS/IDS;

«any» IP- .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# destination-address ip 10.10.10.1
```

destination-port

TCP/UDP- , .

(no) .

```
destination-port { any | <PORT> | object-group <OBJ-GR-NAME> }
no destination-port
```

<PORT> – TCP/UDP- , [1..65535;

<OBJ_GR_NAME> – TCP/UDP- , 31 .

«any» TCP/UDP- .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# destination-port 22
```

direction

, .

(no) .

```
direction { one-way | round-trip }
no direction
```

- one-way – ;
- round-trip – .

15

CONFIG-IPS-CATEGORY-RULE

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

ip dscp

DSCP, .

(no) .

```
ip dscp <DSCP>
[no] ip dscp
```

<DSCP> – DSCP, [0..63].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip dscp 8
```

ip ftp command

FTP, .

protocol ftp.

(no) .

```
ip ftp command <COMMAND>
[no] ip ftp command
```

<COMMAND> – :

- <retr> – ;
- <stor> – ;
- <mkd> – ;
- <rmd> – ;
- <appe> – ( );
- <dele> – .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# protocol ftp
esr(config-ips-category-rule)# ip ftp command allo
```

ip ftp-data command

FTP-DATA, .

protocol ftp-data.

(no) .

```
ip ftp-data command <COMMAND>
```

```
[no] ip ftp-data command
```

<COMMAND> – :

- <retr> – ;
- <stor> – ;
- <appe> – ( ).

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# protocol ftp-data
esr(config-ips-category-rule)# ip ftp-data command stor
```

ip http

HTTP, .

protocol http.

(no) .

```
ip http <COMMAND>
```

```
[no] ip http
```

<COMMAND> – :

- accept;
- accept-enc;
- accept-lang;
- client-body;
- connection;
- content-len;
- content-type;
- cookie;

- file-data;
- header;
- header-names;
- host;
- protocol;
- referer;
- request-line;
- response-line;
- server-body;
- start;
- stat-code;
- stat-msg;
- uri;
- urilen <VALUE>;
- urilen comparison-operator { greater-than | less-than};
- user-agent.

HTTP SNORT 2.X / Suricata 4.X.

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload content "HTTP/1.0"
esr(config-ips-category-rule)# ip http protocol
```

ip http content-filter

. http-, .

.

protocol http.

(no) .

```
ip http content-filter <NAME>
[no] ip http content-filter
```

<NAME> – 31 .

any – http- .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip http content-filter Black-List
```

ip http method

http, .

protocol http.

(no) .

```
ip http method <COMMAND>
[no] ip http method
```

<COMMAND> – :

- <GET> – . ;
- <HEAD> – , GET, ;
- <POST> – ;
- <PUT> – ;
- <DELETE> – ;
- <CONNECT> – «» , ;
- <OPTIONS> – ;
- <TRACE> – ;
- <PATCH> – .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip http method get
```

ip icmp code

ICMP CODE, .

protocol icmp.

(no) .

```
ip icmp code <CODE>
[no] ip icmp code
```

<CODE> – CODE ICMP, [0..255].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp code 5
```

ip icmp code comparison-operator

ip icmp code. .

(no) .

```
ip icmp code comparison-operator { greater-than | less-than }
```

```
[no] ip icmp code comparison-operator
```

- greater-than – ;
- less-than – .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp code 5
esr(config-ips-category-rule)# ip icmp code comparison-operator less-than
```

ip icmp id

ICMP ID, .

protocol icmp.

(no) .

```
ip icmp id <ID>
```

```
[no] ip icmp id
```

<ID> – ID ICMP, [0..65535].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp id 65000
```

ip icmp sequence-id

ICMP sequence-ID, .

protocol icmp.

(no) .

```
ip icmp sequence-id <SEQ-ID>
```

```
[no] ip icmp sequence-id
```

<SEQ-ID> – Sequence-ID ICMP, [0..4294967295].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp sequence-id 8388608
```

ip icmp type

ICMP TYPE, .

protocol icmp.

(no) .

```
ip icmp type <TYPE>
[no] ip icmp type
```

<TYPE> – TYPE ICMP, [0..255].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp type 12
```

ip icmp type comparison-operator

ip icmp type. .

(no) .

```
ip icmp type comparison-operator { greater-than | less-than }
[no] ip icmp type comparison-operator
```

- greater-than – ;
- less-than – .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip icmp type 14
esr(config-ips-category-rule)# ip icmp code comparison-operator greater-than
```

ip protocol-id

IP-, .

protocol any.

(no) .

```
ip protocol-id <ID>
[no] ip protocol-id
```

<ID> – IP- [1..255].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip protocol-id 250
```

ip tcp acknowledgment-number

TCP Acknowledgment-Number, .

protocol tcp.

(no) .

```
ip tcp acknowledgment-number <ACK-NUM>
[no] ip tcp acknowledgment-number
```

<ACK-NUM> – Acknowledgment-Number TCP, [0..4294967295].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip tcp acknowledgment-number 32
```

ip tcp sequence-id

TCP Sequence-ID, .

protocol tcp.

(no) .

```
ip tcp sequence-id <SEQ-ID>
[no] ip tcp sequence-id
```

<SEQ-ID> – Sequence-ID TCP, [0..4294967295].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip tcp sequence-id 2542
```

ip tcp window-size

TCP Window Size, .

protocol tcp.

(no) .

```
ip tcp window-size <SIZE>
[no] ip tcp window-size
```

<SIZE> – Window-Size TCP, [1..65535]

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip tcp window-size 50
```

ip ttl

IP-, .

(no) .

```
ip ttl <TTL>
[no] ip ttl
```

<TTL> – IP-, [1..255].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip ttl 8
```

ip ttl comparison-operator

ip ttl. .

(no) .

```
ip ttl comparison-operator { greater-than | less-than }
[no] ip ttl comparison-operator
```

- greater-than – ;
- less-than – .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# ip ttl 5
esr(config-ips-category-rule)# ip ttl comparison-operator less-than
```

meta classification-type

, IPS/IDS, .

(no) .

```
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 }
[no] 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 – 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 – /.

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# meta classification-type misc-attack
```

meta log-message

, IPS/IDS, .

(no) .

```
meta log-message <MESSAGE>
[no] mera log-message
```

<MESSAGE> – , 128 .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# meta log-message "Possible SlowLorys attack"
```

payload content

IP-, .

(no) .

```
payload content <CONTENT>
[no] payload content <CONTENT>
```

<CONTENT> – , 1024 .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload content "virus"
```

payload data-size

, .

(no) .

```
payload data-size <SIZE>
[no] payload data-size
```

<SIZE> – , [1..65535]

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload data-size 1024
```

payload data-size comparison-operator

ip icmp type. .

(no) .

```
payload data-size comparison-operator { greater-than | less-than }
[no] payload data-size comparison-operator
```

- greater-than – ;

- less-than – .

15

CONFIG-IPS-CATEGORY-RULE

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

payload depth

. payload content. payload offset.

(no) .

```
payload depth <DEPTH>
[no] payload content depth
```

<DEPTH> – , [1..65535].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload content "abc"
esr(config-ips-category-rule)# payload depth 3
```

«abcdef», «abc123», «abcabcabc» ..

payload no-case

. payload content.

(no) .

```
payload no-case
[no] payload content no-case
```

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload content "virus"
esr(config-ips-category-rule)# payload no-case
```

«virus», «VIRUS», «ViRuS» ..

payload offset

, . payload content. payload depth.

(no) .

```
payload offset <OFFSET>
```

```
[no] payload content offset
```

<OFFSET> – , [1..65535].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# payload content "abc"
esr(config-ips-category-rule)# payload depth 6
esr(config-ips-category-rule)# payload offset 3
```

«123abcdef», «defabc», «abcabcabc» ..

protocol

IP-, . (no) .

```
protocol { any | ip | icmp | http | tcp | udp }
```

```
[no] protocol
```

- any – ;
- ip – ip. ip protocol-id;
- icmp – icmp. source-port destination-port any. ip icmp;
- http – http. ip http;
- tp – tp. ip tp;
- udp – tp. ip udp;
- ftp – ftp. ip ftp;
- ftp-data – data ftp. ip ftp-data;.

15

CONFIG-IPS-CATEGORY-RULE

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

rule

CONFIG-IPS-CATEGORY-RULE. .

(no) .

```
[no] rule <ORDER>
```

<ORDER> – , [1..512].

15

CONFIG-IPS-CATEGORY

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)#
```

security ips-category user-defined

IPS/IDS .

(no) IPS.

```
[no] security ips-category user-defined <CATEGORY_NAME>
```

<CATEGORY_NAME> – IPS/IDS, 31 .

⚠ «_» () <CATEGORY_NAME>

15

CONFIG

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

source-address

IP- , .

(no) .

```
source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }
no source-address
```

<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 .

destination-address policy-object-group protect , protect IPS/IDS

destination-address policy-object-group external , external IPS/IDS

«any» IP- .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# source-address ip-prefix 192.168.0.0/16
```

source-port

TCP/UDP- , .

(no) .

```
source-port { any | <PORT> | object-group <OBJ-GR-NAME> }
no source-port
```

<PORT> – TCP/UDP- , [1..65535].

<OBJ_GR_NAME> – TCP/UDP , 31 .

«any» TCP/UDP- .

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# source-port 22
```

threshold count

, .

(no) .

```
threshold count <COUNT>
[no] threshold count
```

<COUNT> – , [1..65535]

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# threshold count 1024
```

threshold second

, . , . threshold count.

(no) .

```
threshold second <SECOND>
[no] threshold second
```

<SECOND> – , [1..65535].

15

CONFIG-IPS-CATEGORY-RULE

```
esr(config-ips-category-rule)# threshold second 1
```

threshold track

, . threshold count.

(no) .

```
threshold track { by-src | by-dst }
[no] threshold track
```

- by-src – IP-;
- by-dst – IP-.

```
esr(config-ips-category-rule)# threshold track by-src
```

threshold type

. threshold count.

(no) .

```
threshold type { treshhold | limit | both }
[no] threshold type
```

- threshold – ;
- limit – <COUNT> <SECOND>;
- both – threshold limit. , <SECOND> <COUNT> , , ;


```
esr(config-ips-category-rule)# threshold count 1024
esr(config-ips-category-rule)# threshold second 1
esr(config-ips-category-rule)# threshold track by-src
esr(config-ips-category-rule)# threshold type treshold
```

*1025 , 1 IP-.

rule-advanced

CONFIG-IPS-CATEGORY-RULE-ADVANCED. .

(no) .

```
[no] rule-advanced <ORDER>
```

<ORDER> – , [1..4294967295].

```
esr(config-ips-category)# rule-advanced 10
esr(config-ips-category-rule-advanced)#
```

rule-text

SNORT 2.X / Suricata 4.X

(no) .

`rule-text <LINE>`

`[no] rule-text`

<LINE> – SNORT 2.X / Suricata 4.X, 1024 .

" '.

15

CONFIG-IPS-CATEGORY-RULE-ADVANCED

```
esr(config-ips-category-rule-advanced)# rule-text "alert tcp any any -> $HOME_NET any (msg: 'ATTACK
[PTsecurity] Attempt to crash named using malformed RNDC packet'; flow: established, to_server;
content:'_auth'; depth: 20; fast_pattern; content: !'|02 00 00 00|'; within: 4; content: '_ctrl'; content:
'_ser'; content: '_tim'; content: '_exp'; reference: cve, 2016-1285; classtype: attempted-dos; reference: url,
github.com/ptresearch/AttackDetection; metadata: Open Ptsecurity.com ruleset; sid: 10000005; rev: 3; )"
```