

- - ip firewall screen dos-defense icmp-threshold
 - ip firewall screen dos-defense land
 - ip firewall screen dos-defense limit-session-destination
 - ip firewall screen dos-defense limit-session-source
 - ip firewall screen dos-defense syn-flood
 - ip firewall screen dos-defense udp-threshold
 - ip firewall screen dos-defense winnuke
 - ip firewall screen spy-blocking fin-no-ack
 - ip firewall screen spy-blocking icmp-type destination-unreachable
 - ip firewall screen spy-blocking icmp-type echo-request
 - ip firewall screen spy-blocking icmp-type reserved
 - ip firewall screen spy-blocking icmp-type source-quench
 - ip firewall screen spy-blocking icmp-type time-exceeded
 - ip firewall screen spy-blocking ip-sweep
 - ip firewall screen spy-blocking port-scan
 - ip firewall screen spy-blocking spoofing
 - ip firewall screen spy-blocking syn-fin
 - ip firewall screen spy-blocking tcp-all-flags
 - ip firewall screen spy-blocking tcp-no-flag
 - ip firewall screen suspicious-packets icmp-fragment
 - ip firewall screen suspicious-packets ip-fragment
 - ip firewall screen suspicious-packets large-icmp
 - ip firewall screen suspicious-packets syn-fragment
 - ip firewall screen suspicious-packets udp-fragment
 - ip firewall screen suspicious-packets unknown-protocols
- - ip firewall logging interval
 - logging firewall screen detailed
 - logging firewall screen dos-defense
 - logging firewall screen spy-blocking
 - logging firewall screen suspicious-packets
 - show ip firewall screens counters

ip firewall screen dos-defense icmp-threshold

ICMP flood . icmp- .

(no) ICMP flood .

```
ip firewall screen dos-defense icmp-threshold { <NUM> }
no ip firewall screen dos-defense icmp-threshold
```

<NUM> – icmp- [1..10000]

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense icmp-threshold 2000
```

ip firewall screen dos-defense land

land- source destination ip, SYN TCP.

(no) land-.

```
[no] ip firewall screen dos-defense land
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense land
```

ip firewall screen dos-defense limit-session-destination

IP- , (DoS-: SYN flood, UDP flood, ICMP flood, ..). , , DoS-.

(no) .

```
ip firewall screen dos-defense limit-session-destination { <NUM> }
```

```
no ip firewall screen dos-defense limit-session-destination
```

<NUM> – ip- [1..10000].

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense limit-session-destination 1000
```

ip firewall screen dos-defense limit-session-source

IP- , (DoS-: SYN flood, UDP flood, ICMP flood, ..). , , DoS-.

(no) .

```
ip firewall screen dos-defense limit-session-source { <NUM> }
no ip firewall screen dos-defense limit-session-source
```

<NUM> – ip- [1..10000].

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense limit-session-source 1000
```

ip firewall screen dos-defense syn-flood

SYN flood. TCP SYN .

(no) SYN flood .

```
ip firewall screen dos-defense syn-flood { <NUM> } [src-dst]
no ip firewall screen dos-defense syn-flood
```

<NUM> – TCP- SYN [1..10000].

src-dst – TCP- SYN .

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dsr
```

ip firewall screen dos-defense udp-threshold

UDP flood. UDP .

(no) UDP flood.

```
ip firewall screen dos-defense udp-threshold { <NUM> }
no ip firewall screen dos-defense udp-threshold
```

<NUM> - UDP- [1..10000].

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense udp-threshold
```

ip firewall screen dos-defense winnuke

winnuke- TCP- URG 139 .

(no) winnuke-.

```
[no] ip firewall screen dos-defense winnuke
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen dos-defense winnuke
```

ip firewall screen spy-blocking fin-no-ack

TCP- FIN ACK.

(no) TCP- FIN ACK.

```
[no] ip firewall screen spy-blocking fin-no-ack
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking fin-no-ack
```

ip firewall screen spy-blocking icmp-type destination-unreachable

ICMP- 3 (destination-unreachable), , .

(no) ICMP- 3 .

```
[no] ip firewall screen spy-blocking icmp-type destination-unreachable
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking icmp-type destination-unreachable
```

ip firewall screen spy-blocking icmp-type echo-request

ICMP 8 (echo-request), , .

(no) ICMP- 8 .

```
[no] ip firewall screen spy-blocking icmp-type echo-request
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking icmp-type echo-request
```

ip firewall screen spy-blocking icmp-type reserved

ICMP- 2 7 (reserved), , .

(no) ICMP- 2 7 .

```
[no] ip firewall screen spy-blocking icmp-type reserved
```

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking icmp-type reserved
```

ip firewall screen spy-blocking icmp-type source-quench

ICMP- 4 (source quench), , .

(no) ICMP- 4 .

```
[no] ip firewall screen spy-blocking icmp-type source-quench
```

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking icmp-type source-quench
```

ip firewall screen spy-blocking icmp-type time-exceeded

ICMP- 11 (time exceeded), , .

(no) ICMP- 11 .

```
[no] ip firewall screen spy-blocking icmp-type time-exceeded
```

.

.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking icmp-type time-exceeded
```

ip firewall screen spy-blocking ip-sweep

IP-sweep . , 10 ICMP- , 10 , 11 .

(no) ip-sweep .

```
ip firewall screen spy-blocking ip-sweep <THRESHOLD> [ <TIME> ]
```

```
no ip firewall screen spy-blocking ip-sweep
```

<THRESHOLD> – ip sweep , [1..10000].

<TIME> – [1..1000000].

.

, 10000.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking ip-sweep 1000
```

ip firewall screen spy-blocking port-scan

port scan . (<threshold>) 10 TCP- SYN TCP- 10 UDP- UDP-, port scan (<TIME>).

(no) port scan .

```
ip firewall screen spy-blocking port-scan <THRESHOLD> [ <TIME> ]
no ip firewall screen spy-blocking port-scan
```

<THRESHOLD> – port scan , [1..10000].

<TIME> – [1..1000000].

.

, 10000.

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking port-scan 100 1000
```

ip firewall screen spy-blocking spoofing

IP spoofing . , 10.0.0.1/24 Gi1/0/1, Gi1/0/2, .

(no) ip spoofing .

```
[no] ip firewall screen spy-blocking spoofing
```

.

.

15

CONFIG

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

ip firewall screen spy-blocking syn-fin

TCP-, SYN FIN.

(no) TCP-, SYN FIN.

```
[no] ip firewall screen spy-blocking syn-fin
```


15

CONFIG

```
esr(config)# ip firewall screen spy-blocking syn-fin
```

ip firewall screen spy-blocking tcp-all-flags

TCP-, : FIN, PSH, URG. XMAS.

(no) TCP-, : FIN, PSH, URG.

```
[no] ip firewall screen spy-blocking tcp-all-flag
```

10

CONFIG

```
esr(config)# ip firewall screen spy-blocking tcp-all-flag
```

ip firewall screen spy-blocking tcp-no-flag

TCP-, flags.

(no) TCP-, flags.

```
[no] ip firewall screen spy-blocking tcp-no-flag
```

15

CONFIG

```
esr(config)# ip firewall screen spy-blocking tcp-no-flag
```

ip firewall screen suspicious-packets icmp-fragment

ICMP-.

(no) ICMP-.

```
[no] ip firewall screen suspicious-packets icmp-fragment
```

.

10

CONFIG

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

ip firewall screen suspicious-packets ip-fragment

IP-.

(no) .

```
[no] ip firewall screen suspicious-packets ip-fragment
```

.

15

CONFIG

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

ip firewall screen suspicious-packets large-icmp

ICMP- 1024 .

(no) ICMP- 1024 .

```
[no] ip firewall screen suspicious-packets large-icmp
```

.

15

CONFIG

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

ip firewall screen suspicious-packets syn-fragment

TCP-, SYN.

(no) TCP-, SYN.

```
[no] ip firewall screen suspicious-packets syn-fragment
```

.

15

CONFIG

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

ip firewall screen suspicious-packets udp-fragment

UDP-.

(no) UDP-.

```
[no] ip firewall screen suspicious-packets udp-fragment
```

.

.

15

CONFIG

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

ip firewall screen suspicious-packets unknown-protocols

, ID IP 137 .

(no) , ID IP 137 .

```
[no] ip firewall screen suspicious-packets unknown-protocols
```

.

.

15

CONFIG

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

ip firewall logging interval

(SNMP, syslog CLI) . , , .

(no) .

```
ip firewall logging interval <NUM>
```

no ip firewall logging interval

<NUM> – [30 .. 2147483647]

30

15

CONFIG

```
esr(config)# ip firewall logging interval 60
```

logging firewall screen detailed

CLI.

, , , IP- IP- , MAC- , .

(no) .

[no] logging firewall screen detailed

.

.

15

CONFIG

```
esr(config)# logging firewall screen detailed
```

logging firewall screen dos-defense

DoS- CLI, syslog SNMP. DoS .

(no) DoS-.

[no] logging firewall screen dos-defense <ATTACK_TYPE>

<ATTACK_TYPE> – DoS-, :

- icmp-threshold;

- land;
- limit-session-destination;
- limit-session-source;
- syn-flood;
- udp-threshold;
- winnuke.

DoS- .

.

15

CONFIG

```
esr(config)# logging firewall screen dos-defense land
```

logging firewall screen spy-blocking

CLI, syslog SNMP. .

(no) .

```
[no] logging firewall screen spy-blocking { <ATAACK_TYPE> | icmp-type <ICMP_TYPE> }
```

<ATAACK_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.

.

.

15

CONFIG

```
esr(config)# logging firewall screen spy-blocking icmp-type echo-request
```

logging firewall screen suspicious-packets

CLI, syslog SNMP.

(no)

```
[no] logging firewall screen suspicious-packets <PACKET_TYPE>
```

< PACKET_TYPE> – , :

- icmp-fragment;
- ip-fragment;
- large-icmp;
- syn-fragment;
- udp-fragment;
- unknown-protocols.

15

CONFIG

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

show ip firewall screens counters

```
show ip firewall screens counters
```

10

ROOT

```
esr# show ip firewall screens counters
```

```
DDoS:
```

```
  Destination limit screen:  --
  Source limit screen:      --
  ICMP threshold screen:    1
  UDP threshold screen:     --
  SYN flood screen:         0
  Land attack screen:       1
  Winnuke attack screen:    --
```

```
Suspicious packets:
```

```
  ICMP fragmented screen:  --
  UDP fragmented screen:   --
  Large ICMP screen:       4
  Fragmented SYN screen:   --
  Unknown protocol screen: --
  Fragmented IP screen:    --
```

```
Spying:
```

```
  Port scanning screen:    --
  IP sweep screen:         --
  SYN-FIN screen:          --
  TCP all flags screen:    --
  FIN no ACK screen:       --
  TCP no flags screen:     --
  Spoofing screen:        --
```

```
ICMP types:
```

```
  ICMP reserved screen:    --
  ICMP quench screen:      --
  ICMP echo request screen: --
  ICMP time exceeded screen: --
  ICMP unreachable screen: --
```