# Firewall



## action

  ,  , .

 (no)  .

```
action <ACT> [log]
no action
```

<ACT> –  :

- permit –  ;

- deny – ;
- reject – , ;
- netflow-sample – Netflow;
- sflow-sample – sFlow;
- log – , .

, .

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# action permit
```

## clear ip firewall counters

Firewall.

```
clear ip firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE> [<ORDER>] ] ]
```

<VRF> – VRF, 31 . VRF;

<SOURCE-ZONE> – , ;

<DESTINATION-ZONE> – , ;

<ORDER> – , [1..10000]. .

10

ROOT

```
esr# clear ip firewall counters trusted self
```

## clear ip firewall sessions

IP-.

```
clear ip firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address <ADDR> ] [ outiside-source-address <ADDR> ] [ inside-destination-address <ADDR> ] [ outside-destination-address <ADDR> ] [ inside-source-port <PORT> ] [ outside-source-port <PORT> ] [ inside-destination-port <PORT> ] [ outside-destination-port <PORT> ]
```

<VRF> – VRF, 31 . VRF;

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

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

<PORT> – TCP/UDP , [1..65535];

inside-source-address – IP- , ;

inside-destination-address – IP- , ;

outiside-source-address – IP- , ;

outside-destination-address – IP- ;

inside-source-port – TCP/UDP ;

outside-source-port – TCP/UDP ;

inside-destination-port – TCP/UDP ;

outside-destination-port – TCP/UDP .

10

ROOT

```
esr# clear ip firewall sessions vrf VRF1
```

## clear ipv6 firewall counters

Firewall.

```
clear ipv6 firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE> [<ORDER>] ] ]
```

<VRF> – VRF, 31 . VRF.

<SOURCE-ZONE> – , .

<DESTINATION-ZONE> – , .

<ORDER> – , [1..10000]. .

10

ROOT

```
esr# clear ipv6 firewall counters trusted self
```

## clear ipv6 firewall sessions

IPv6-.

```
clear ipv6 firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address <IPV6-ADDR> ] [ outiside-
source-address <IPV6-ADDR> ] [ inside-destination-address <IPV6-ADDR> ] [ outside-destination-address <IPV6-ADDR>
] [ inside-source-port <PORT> ] [ outside-source-port <PORT> ] [ inside-destination-port <PORT> ] [ outside-
destination-port <PORT> ]
```

<VRF> – VRF, 31 . VRF.

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre.

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

<PORT> – TCP/UDP , [1..65535];

inside-source-address – IPv6- , .

inside-destination-address – IPv6- , .

outiside-source-address – IPv6- , .

outside-destination-address – IPv6- ;

inside-source-port – TCP/UDP ;

outside-source-port – TCP/UDP ;

inside-destination-port – TCP/UDP ;

outside-destination-port – TCP/UDP .

10

ROOT

```
esr# clear ipv6 firewall sessions vrf VRF1
```

## description

. (no) .

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

<DESCRIPTION> – , 255 .

10

CONFIG-ZONE

CONFIG-ZONE-PAIR

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone)# description "Trusted interfaces"
```

## enable

.

(no) .

```
[no] enable
```

.

.

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# enable
```

## ip firewall disable

Firewall .

(no) Firewall .

```
[no] ip firewall disable
```

.

15

CONFIG-GI

CONFIG-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-SERIAL

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-E1

CONFIG-MULTILINK

CONFIG-CELLULAR-MODEM

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-L2TP

CONFIG-LT

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-OPENVPN

```
esr(config-if-gi)# ip firewall disable
```

## ip firewall mode

.

(no) .

```
ip firewall mode <MODE>
no ip firewall mode
```

<MODE> – , :

- stateful – , . , . DPI.
- stateless – , . , . .

stateful

15

CONFIG

```
esr(config-if-gi)# ip firewall mode stateless
```

## ip firewall sessions counters

NAT Firewall. , . . .

show ip firewall counters, show ip firewall sessions, show ipv6 firewall counters show ipv6 firewall sessions .

(no) .

```
[no] ip firewall sessions counters
```

.

.

15

CONFIG

```
esr(config)# ip firewall sessions counters
```

## ip firewall sessions allow-unknown

, - .

(no) .

```
[no] ip firewall sessions allow-unknown
```

.

.

15

CONFIG

```
esr(config)# ip firewall sessions allow-unknown
```

## ip firewall sessions generic-timeout

, .

(no) .

```
ip firewall sessions generic-timeout <TIME>
no ip firewall sessions generic-timeout
```

<TIME> – , [1..8553600].

60

15

CONFIG

```
esr(config)# ip firewall sessions generic-timeout 60
```

## ip firewall sessions icmp-timeout

ICMP-, .

(no) .

```
ip firewall sessions icmp-timeout <TIME>
no ip firewall sessions icmp-timeout
```

<TIME> – ICMP-, [1..8553600].

30

15

CONFIG

```
esr(config)# ip firewall sessions icmp-timeout 60
```

## ip firewall sessions icmpv6-timeout

ICMPv6-, .

(no) .

```
ip firewall sessions icmpv6-timeout <TIME>
no ip firewall sessions icmpv6-timeout
```

<TIME> – ICMPv6-, [1..8553600].

30

15

CONFIG

```
esr(config)# ip firewall sessions icmpv6-timeout 60
```

## ip firewall sessions max-expect

.

(no) .

```
ip firewall sessions max-expect <COUNT>
no ip firewall sessions max-expect
```

<COUNT> – , [1..8553600].

256

15

CONFIG

```
esr(config)# ip firewall sessions max-expect 512
```

## ip firewall sessions max-tracking

.

(no) .

```
ip firewall sessions max-tracking <COUNT>
no ip firewall sessions max- tracking
```

<COUNT> – , [1..8553600].

512000

15

CONFIG

```
esr(config)# ip firewall sessions max-tracking 256000
```

## ip firewall sessions tcp-connect-timeout

TCP- « », .

(no) .

```
ip firewall sessions tcp-connect-timeout <TIME>
no ip firewall sessions tcp-connect-timeout
```

<TIME> – TCP- "", [1..8553600].

60

15

CONFIG

```
esr(config)# ip firewall sessions tcp-connect-timeout 120
```

## ip firewall sessions tcp-disconnect-timeout

TCP- "", .

(no) .

```
ip firewall sessions tcp-disconnect-timeout <TIME>
no ip firewall sessions tcp-disconnect-timeout
```

<TIME> – TCP- "", [1..8553600].

30

15

CONFIG

```
esr(config)# ip firewall sessions tcp-disconnect-timeout 10
```

## ip firewall sessions tcp-estabilished-timeout

TCP- "", .

(no) .

```
ip firewall sessions tcp-estabilished-timeout <TIME>
no ip firewall sessions tcp-estabilished-timeout
```

<TIME> – TCP- " ", [1..8553600].

120

15

CONFIG

```
esr(config)# ip firewall sessions tcp-estabilished-timeout 3600
```

## ip firewall sessions tcp-latecome-timeout

, TCP- .

(no) .

```
ip firewall sessions tcp-latecome-timeout <TIME>
no ip firewall sessions tcp-latecome-timeout
```

<TIME> – , [1..8553600].

120

15

CONFIG

```
esr(config)# ip firewall sessions tcp-latecome-timeout 10
```

## ip firewall sessions tracking

.

(no) .

```
ip firewall sessions tracking { <PROTOCOL> | sip [ port <OBJECT-GROUP-SERVICE> ] }
no ip firewall sessions tracking { <PROTOCOL> | sip [ port <OBJECT-GROUP-SERVICE> ] | all }
```

<PROTOCOL> – , , [ftp, h323, pptp, netbios-ns].

<OBJECT-GROUP-SERVICE> – TCP/UDP- sip , 31 . , sip 5060.

"all", .

.

15

CONFIG

```
esr(config)# ip firewall sessions tracking ftp
```

## ip firewall sessions udp-assured-timeout

UDP- " ", .

(no) .

```
ip firewall sessions udp-assured-timeout <TIME>
no ip firewall sessions udp-assured-timeout
```

<TIME> – UDP- " ", [1..8553600].

180

15

CONFIG

```
esr(config)# ip firewall sessions udp-assured-timeout 3600
```

## ip firewall sessions udp-wait-timeout

UDP- « », .

(no) .

```
ip firewall sessions udp-wait-timeout <TIME>
no ip firewall sessions udp-wait-timeout
```

<TIME> – UDP- « », [1..8553600].

30

10

CONFIG

```
esr(config)# ip firewall sessions udp-wait-timeout 60
```

## match application

, . ( DPI)

«not» , .

(no) .

```
match [not] application <OBJ-GROUP-APPLICATION>
no match application
```

<OBJ-GROUP-APPLICATION> – , 31 .

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match application APP_DENY
```

## match destination-address

IP- , .

«not» IP- , .

(no) .

```
match [not] destination-address <OBJ-GROUP-NETWORK-NAME>
no match destination-address
```

<OBJ-GROUP-NETWORK-NAME> – IP-, 31 . «any» IP- .

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match destination-address local
```

## match destination-address-port

IP- TCP/UDP- , .

«not» IP- TCP/UDP- , .

(no) .

```
match [not] destination-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
no match destination-address
```

<OBJ-GROUP-ADDRESS-PORT-NAME> – IP- TCP/UDP-, 31 . «any» .

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match destination-address local
```

## match destination-mac

MAC- , .

«not» (match not) MAC- , .

(no) .

```
match [not] destination-mac <ADDR>
no match destination-mac <ADDR>
```

<ADDR> – - , XX:XX:XX:XX:XX:XX, [00..FF].

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match destination-mac A8:F9:4B:AA:00:40
```

## match destination-nat

, , IP- .

«not» , IP- . (no) .

```
match [not] destination-nat
no match destination-nat
```

.

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match destination-nat
```

## match destination-port

TCP/UDP- , .

«not» TCP/UDP- , .

(no) .

```
match [not] destination-port <PORT-SET-NAME>
no match destination-port
```

<PORT-SET-NAME> – TCP/UDP-, 31 . «any» TCP/UDP- .

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match destination-port ssh
```

## match fragment

, . any self. . DNAT.

«not» .

(no) .

```
match [not] fragment
no match fragmen
```

.

.

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-pair-rule)# match fragment
```

## match icmp

ICMP, «match protocol». ICMP, .

«not» ICMP, .

(no) .

```
match [not] icmp { <ICMP_TYPE> <ICMP_CODE> | <OPTION> }
no match icmp
```

<ICMP_TYPE> – ICMP, [0..255];

<ICMP_CODE> – ICMP, [0..255]. «any» ICMP

<OPTION> – ICMP-, :

- administratively-prohibited;
- alternate-address;
- conversion-error;
- dod-host-prohibited;
- dod-network-prohibited;
- echo;
- echo-reply;
- host-isolated;
- host-precedence;
- host-redirect;
- host-tos-redirect;
- host-tos-unreachable;
- host-unknown;
- host-unreachable;
- information-reply;
- information-request;
- mask-reply;
- mask-request;
- network-redirect;
- network-tos-redirect;
- network-tos-unreachable;
- network-unknown;
- network-unreachable;
- option-missing;
- packet-too-big;
- parameter-problem;
- port-unreachable;
- precedence;
- protocol-unreachable;

- reassembly-timeout;
- router-advertisement;
- router-solicitation;
- source-quench;
- source-route-failed;
- time-exceeded;
- timestamp-reply;
- timestamp-request;
- traceroute.

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match icmp 2 any
```

## match ip-option

, IP-. any self.

«not» , IP-.

(no) .

```
match [not] ip-option
no match ip-option
```

.

.

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-pair-rule)# match ip-options
```

## match protocol

IP-, .

«not» , .

(no) .

```
match [not] protocol <TYPE>
no match protocol
match [not] protocol-id <ID>
```

```
no match protocol-id
```

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre.

«any» ;

<ID> – IP-, [0x00-0xFF].

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match protocol udp
```

## match source-address

IP- , .

«not» (match not) IP- , .

(no) .

```
match [not] source-address <OBJ-GROUP-NETWORK-NAME>
no match source-address <OBJ-GROUP-NETWORK-NAME>
```

<OBJ-GROUP-NETWORK-NAME> – IP-, 31 . «any» IP- .

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match source-address remote
```

## match source-address-port

IP- TCP/UDP- , .

«not» (match not) IP- TCP/UDP- , .

(no) .

```
match [not] source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
no match source-address-port <OBJ-GROUP-ADDRESS-PORT-NAME>
```

<OBJ-GROUP-ADDRESS-PORT-NAME> – IP- TCP/UDP-, 31 . «any» .

any

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match source-address-port admin
```

## match source-mac

MAC- , .

«not» (match not) MAC- , .

(no) .

```
match [not] source-mac <ADDR>
no match source-mac <ADDR>
```

<ADDR> – - , XX:XX:XX:XX:XX:XX, [00..FF].

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match source-mac A8:F9:4B:AA:00:40
```

## match source-port

TCP/UDP- , .

«not» TCP/UDP- , .

(no) .

```
match [not] source-port <PORT-SET-NAME>
no match source-port
```

<PORT-SET-NAME> – TCP/UDP-, 31 . «any» TCP/UDP- .

10

CONFIG-ZONE-PAIR-RULE

```
esr(config-zone-rule)# match source-port telnet
```

## ports firewall enable

Bridge-.

(no) .

```
[no] ports firewall enable
```

.

.

15

CONFIG-BRIDGE

```
esr(config-bridge)# ports firewall enable
```

## rate-limit pps

. any self action permit .

(no) .

```
rate-limit pps <RATE>
no rate-limit
```

<PPS> – , [1..10000].

.

15

CONFIG-ZONE-PAIR-RULE

```
esr(config-if-gi)# rate-limit pps 200
```

## rearrange

.

```
rearrange <VALUE>
```

<VALUE> – , [1..50].

10

CONFIG-ZONE-PAIR

```
esr(config-zone-pair)# rearrange 10
```

## renumber rule

.

```
renumber rule <CUR_ORDER> <NEW_ORDER>
```

<CUR_ORDER> – , [1..10000];

<NEW_ORDER> – , [1..10000].

10

CONFIG-ZONE-PAIR

```
esr(config-zone-pair)# renumber rule 13 100
```

## rule

SECURITY ZONE PAIR RULE. .

(no) .

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

<ORDER> – , [1..10000]. "all", .

10

CONFIG-ZONE-PAIR

```
esr(config-zone-pair)# rule 10
esr(config-zone-rule)#
```

## security zone

.

(no) .

```
[no] security zone [ <NAME> | all ]
```

<NAME> – , 12 . «all» .

10

CONFIG

```
esr(config)# security zone trusted
esr(config-zone)#
```

## security-zone

. (no) .

```
security-zone <NAME>
no security-zone
```

<NAME> – , 12 .

15

CONFIG-GI

CONFIG-TE

CONFIG-SUBIF

CONFIG-QINQ-IF

CONFIG-SERIAL

CONFIG-PORT-CHANNEL

CONFIG-BRIDGE

CONFIG-CELLULAR-MODEM

CONFIG-E1

CONFIG-MULTILINK

CONFIG-VTI

CONFIG-GRE

CONFIG-IP4IP4

CONFIG-LT

CONFIG-PPPOE

CONFIG-PPTP

CONFIG-L2TP

CONFIG-OPENVPN

CONFIG-L2TP-SERVER

CONFIG-OPENVPN-SERVER

CONFIG-PPTP-SERVER

```
esr(config-if-gi)# security-zone trusted
```

## security zone-pair

.

(no) .

```
[no] security zone-pair <SOURCE-ZONE> <DESTINATION-ZONE>
```

<SOURCE-ZONE> – , ;

<DESTINATION-ZONE> – , . «self». , , «self». «all», .

10

CONFIG

```
esr(config)# security zone-pair trusted self
```

## show ip firewall counters

, , .

```
show ip firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE> [ <ORDER> ] ] ]
```

<VRF> – VRF, 31 . VRF;

<DESTINATION-ZONE> – , ;

<SOURCE-ZONE> – , ;

<ORDER> – , [1..10000]. .

1

ROOT

```
esr# show ip firewall counters trusted self
Zone-pair                       Rule         Action            Pkts         Bytes
------------------------------  ----------   ---------------   ----------   ----------
any/any                         default      deny              0            0
trusted/self                    1            permit            0            0
trusted/trusted                 1            permit            0            0
```

## show ip firewall sessions

IP-.

```
show ip firewall sessions [ vrf <VRF> ] [ protocol <TYPE> ] [ inside-source-address <ADDR>] [ outside-source-address <ADDR> ] [ inside-destination-address <ADDR> ] [ outside-destination-address <ADDR> ] [ inside-source-port <PORT> ] [ outside-source-port <PORT> ] [ inside-destination-port <PORT> ] [ outside-destination-port <PORT> ] [ summary ] [ configuration ] [ expected ]
```

<VRF> – VRF, 31 . VRF;

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

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

<PORT> – TCP/UDP , [1..65535];

inside-source-address – IP- , ;

inside-destination-address – IP- , ;

outiside-source-address – IP- , ;

outside-destination-address – IP- ;

inside-source-port – TCP/UDP ;

outside-source-port – TCP/UDP ;

inside-destination-port – TCP/UDP ;

outside-destination-port – TCP/UDP ;

summary – IP-;

configuration – IP-;

expected – , .

1

ROOT

```
esr# show ip firewall sessions
Prot Inside source  Inside destination  Outside source Outside destination Pkts Bytes
---  ------------  -----------------     -------------   ----------------  -----  ----
vrrp   4.4.4.4      224.0.0.18              4.4.4.4       224.0.0.18       --     --
```

## show ip firewall sessions tracking

.

```
show ip firewall sessions tracking
```

.

1

ROOT

```
esr# show ip firewall sessions tracking
Tracking Status:
    FTP:        Enabled
    H.323:      Enabled
    GRE:        Enabled
    PPTP:       Enabled
    NETBIOS-NS: Enabled
    SIP:        Enabled
```

## show ipv6 firewall counters

, , .

```
show ipv6 firewall counters [ vrf <VRF> ] [ <SOURCE-ZONE> [ <DESTINATION-ZONE> [ <ORDER> ] ] ]
```

<VRF> – VRF, 31 . VRF;

<DESTINATION-ZONE> – , ;

<SOURCE-ZONE> – , ;

<ORDER> – , [1..10000]. .

1

ROOT

```
esr# show ipv6 firewall counters trusted self
Zone-pair                       Rule         Action            Pkts         Bytes
------------------------------  ----------   ---------------   ----------   ----------
any/any                         default      deny              0            0
trusted/self                    1            permit            0            0
trusted/trusted                 1            permit            0            0
```

## show ipv6 firewall sessions

IPv6-.

```
show ipv6 firewall sessions [ vrf <VRF> ] [summary] [ protocol <TYPE> ] [ inside-source-address <IPV6-ADDR>] [
outiside-source-address <IPV6-ADDR> ] [ inside-destination-address <IPV6-ADDR> ] [ outside-destination-address
<IPV6-ADDR> ] [ inside-source-port <PORT> ] [ outside-source-port <PORT> ] [ inside-destination-port <PORT> ] [
outside-destination-port <PORT> ] [ expected ] [ summary ]
```

<VRF> – VRF, 31 . VRF;

<TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;

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

<PORT> – TCP/UDP , [1..65535];

inside-source-address – IPv6- , ;

inside-destination-address – IPv6- , ;

outiside-source-address – IPv6- , ;

outside-destination-address – IPv6- ;

inside-source-port – TCP/UDP ;

outside-source-port – TCP/UDP ;

inside-destination-port – TCP/UDP ;

outside-destination-port – TCP/UDP ;

expected – , ;

summary – IPv6-.

1

ROOT

```
esr# show ipv6 firewall sessions
Prot  Inside source  Inside destination  Outside source Outside destination  Pkts  Bytes       -----
-------------- ------------------ -------------- -------------------- ----- -----
icmp6 fc00::2         fc00::2            fc00::2        fc00::2               --     --
icmp6 fc00::2         fc00::1            fc00::2        fc00::1               --     --
```

## show security zone

, .

```
show security zone [<NAME>]
```

<NAME> – , 31 .

1

ROOT

```
esr# show security zone
Zone name       Interfaces
-------------   ----------------------------------------
trusted         gi1/0/2-6, gi1/0/8-24, bridge 1
untrusted       gi1/0/1, te1/0/1-2, bridge 2
```

## show security zone-pair

.

```
show security zone-pair
```

.

1

ROOT

```
esr# show security zone-pair
From zone       To zone
-------------   -------------
trusted         untrusted
trusted         trusted
trusted         self
untrusted       self
```

## show security zone-pair configuration

.

```
show security zone-pair configuration <SOURCE-ZONE> <DESTINATION-ZONE> [<ORDER>]
```

<SOURCE-ZONE> – , ;

<DESTINATION-ZONE> – ,  ;

<ORDER> – ,  [1..10000].  .

1

ROOT

```
esr# show security zone-pair configuration trusted self
Order:              1
Description:        --
Matching pattern:
    Protocol:       tcp(6)
    Src-addr:       any
    src-port:       any
    Dest-addr:      any
    dest-port:      23
0            0
```