

# (ACL)

- [action](#)
- [description](#)
- [enable](#)
- [ip access-list extended](#)
- [match cos](#)
- [match destination-address](#)
- [match destination-mac](#)
- [match destination-port](#)
- [match dscp](#)
- [match ip-precedence](#)
- [match protocol](#)
- [match source-address](#)
- [match source-mac](#)
- [match source-port](#)
- [match vlan](#)
- [rule](#)
- [service-acl input](#)
- [show ip access-list](#)

## action

`action {deny|permit} {protocol} {source-address} {source-port} {destination-address} {destination-port} {dscp} {precedence} {cos} {vlan} {rule} {service-acl input} {show ip access-list}`

`action <ACT>`  
`no action`

`<ACT> - :`

- `permit - ;`
- `deny - .`

10

CONFIG-ACL-RULE

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

## description

`description {description}`  
`(no) description`

`description <DESCRIPTION>`  
`no description`

`<DESCRIPTION> - , 255.`

10

## CONFIG-ACL

```
esr(config-acl)# description "Drop SSH traffic"
```

## enable

.

(no) .

[no] enable

.

.

10

## CONFIG-ACL-RULE

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

## ip access-list extended

.

(no) .

[no] ip access-list extended <NAME>

<NAME> - , 31.

10

## CONFIG

```
esr(config)# ip access-list extended acl-ssh-drop
esr(config-acl)#
```

## match cos

802.1p, .

(no) .

```
match cos <COS>
```

```
no match cos
```

<COS> – 802.1p, [0..7]

10

CONFIG-ACL-RULE

```
esr(config-acl-rule)# match cos 2
```

## match destination-address

IP-, .

(no) .

```
match destination-address { <ADDR> <MASK> | any }
```

```
no match destination-address
```

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

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

«any» IP-.

any

10

CONFIG-ACL-RULE

```
esr(config-acl-rule)# match destination-address 10.10.10.0 255.255.255.0
```

## match destination-mac

MAC-, .

(no) .

```
match destination-mac <ADDR> <WILDCARD>
no match destination-mac
```

<ADDR> --, XX:XX:XX:XX:XX:XX, [00..FF];  
<WILDCARD> --, XX:XX:XX:XX:XX:XX, [00..FF]., 0, MAC-, .

10

CONFIG-ACL-RULE

```
esr(config-acl-rule)# match destination-mac A8:F9:4B:AA:00:41 00:00:00:00:00:FF
```

## match destination-port

TCP/UDP-, .  
(no) .

```
match destination-port {<PORT> | any}
no match destination-port
```

<PORT> – TCP/UDP-, [1..65535]. «any» TCP/UDP-.

any

10

CONFIG-ACL-RULE

```
esr(config-acl-rule)# match destination-port 22
```

## match dscp

DSCP, .  
(no) .

```
match dscp <DSCP>
no match dscp
```

<DSCP> – DSCP, [0..63].

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match dscp 55
```

**match ip-precedence**

IP Precedence, .

(no) .

```
match ip-precedence <IPP>
```

```
no match ip-precedence
```

<IPP> – IP Precedence, [0..7].

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match ip-precedence 5
```

**match protocol**

IP-, .

(no) .

```
match protocol <TYPE>
```

```
no match protocol
```

```
match 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» .

any

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match protocol tcp
```

**match source-address**

IP-, .

(no) .

```
match source-address { <ADDR> <MASK> | any }
no match source-address
```

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

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

«any» IP- .

any

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match source-address 10.100.100.0 255.255.255.0
```

**match source-mac**

MAC-, .

(no) .

```
match source-mac <ADDR> <WILDCARD>
no match source-mac
```

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

<WILDCARD> – -, XX:XX:XX:XX:XX:XX, [00..FF]. , 0, MAC-, .

## CONFIG-ACL-RULE

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

### match source-port

TCP/UDP-, .

(no) .

```
match source-port { <PORT> | any }
```

```
no match source-port
```

<PORT> – TCP/UDP-, [1..65535]. «any» TCP/UDP-.

any

10

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match source-port any
```

### match vlan

VLAN, .

(no) .

```
match vlan <VID>
```

```
no match vlan
```

<VID> – VLAN, [1...4094].

10

## CONFIG-ACL-RULE

```
esr(config-acl-rule)# match vlan 100
```

## rule

CONFIG-ACL-RULE. .

(no) .

[no] rule <ORDER>

<ORDER> – , [1..4094].

10

CONFIG-ACL

```
esr(config-acl)# rule 10
esr(config-acl-rule)#
```

## service-acl input

.

(no) .

service-acl input <NAME>

no service-acl input

<NAME> – , 31 .

15

CONFIG-GI

CONFIG-TE

CONFIG-PORT-CHANNEL

```
esr(config-if-gi)# service-acl input acl-ssh-drop
```

## show ip access-list

.

show ip access-list [ <NAME> [ <ORDER> ] ]

<NAME> – , 31 ;



<ORDER>- , [1..4096]. .

1

ROOT

```
esr# show ip access-list
Name                               Description
-----
acl-telnet-drop                    --
acl-ssh-drop                       Drop SSH traffic
esr# show ip access-list acl-ssh-drop
Index:                             1
Matching pattern:
  Protocol:                         TCP(6)
  Source MAC address:               any
  Source IP address:                any
  Source port:                      any
  Destination MAC address:          any
  Destination IP address:           any
  Destination port:                 22
Action:                             Deny
Status:                             Enabled
-----
Index:                             2
Matching pattern:
  Protocol:                         any
  Source MAC address:               any
  Source IP address:                any
  Destination MAC address:          any
  Destination IP address:           any
Action:                             Permit
Status:                             Enabled
-----
```