

Zone-Based StateFull Firewall

ESR Zone-Based-Firewall StateFull-

Zone-Based?

1. :

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)#
```

2. , ip-, / :

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# mode routerport
esr(config-if-gi)# ip address 192.0.2.1/30
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

```
esr(config)# bridge 1
esr(config-bridge)# vlan 1
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.1.1/24
esr(config-bridge)# enable
esr(config-bridge)# exit
```

```
esr(config)# bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.10.1/24
esr(config-bridge)# enable
esr(config-bridge)# exit
```

3. , ip- , , , . , trusted untrusted:

```
esr(config)# security zone-pair trusted untrusted
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)# exit
```

4. , ip-, ip- . ip- "self". "self" .
, "self".
, trusted ip- 192.168.1.15, 192.168.1.37 192.168.1.142 ssh:

```

esr(config)# object-group service SSH
esr(config-object-group-service)# port-range 22
esr(config-object-group-service)# exit

esr(config)# object-group network SSH_TRUSTED_PERMIT
esr(config-object-group-network)# ip address-range 192.168.1.15
esr(config-object-group-network)# ip address-range 192.168.1.37
esr(config-object-group-network)# ip address-range 192.168.1.142
esr(config-object-group-network)# exit

esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match destination-port SSH
esr(config-zone-pair-rule)# match source-address SSH_TRUSTED_PERMIT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

, ip- 192.51.100.6esr-10(config)# object-group network GRE_UNTRUSTED_PERMIT untrusted gre- :

```

esr(config-object-group-network)# ip address-range 192.51.100.6
esr(config-object-group-network)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol gre
esr(config-zone-pair-rule)# match source-address GRE_UNTRUSTED_PERMIT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule
esr(config-zone-pair-rule)# action deny
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

firewall StateFull?

1. , .
 , :

```

esrvf# show ip firewall sessions
Codes: E - expected, U - unreplied,
       A - assured, C - confirmed

```

Prot	Inside source	Inside destination	Outside source	Outside
destination	Pkts	Bytes	Status	
tcp	192.168.1.15:54366	192.168.1.1:22	192.168.1.15:54366	192.168.1.1:
22	--	AC		

```

2.      ,      .
2.1.    ,      .
2.2.    source-zone ,
2.3.    destination-zone , .2.1
2.4.    "security zone-pair <source-zone> <destination-zone>"
      ( "enable") .
      ("match") ("action")
2.5.    .2.4. "action permit" , .

      . ( source-zone destination-zone) ( destination-zone source-zone).
, StateFull firewall "" . ().

ip-, , Firewall'.
-      trusted:

```

```

esr(config)# security zone-pair trusted trusted
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)# exit

```

```

Zone-Based-Firewall , "log" "action"
, :

```

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 10000
esr(config-zone-pair-rule)# action deny log
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

```

syslog ( ) .

```

```

2022-11-21T12:27:31+00:00 %FIREWALL-I-LOG: zone-pair 'untrusted self' rule 10000 denied tcp 192.168.1.15:40900
(gi1/0/1 60:e3:27:00:ee:e9) -> 192.168.1.1:23 dscp 4, 1 packets

```

```

"log" , :

```

```

esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit log
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match destination-port SSH
esr(config-zone-pair-rule)# match source-address SSH_TRUSTED_PERMIT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

```

syslog ..:

```

```

2022-11-21T12:28:25+00:00 %FIREWALL-I-LOG: zone-pair 'untrusted self' rule 100 permitted tcp 192.168.1.15:43596
(gi1/0/1 60:e3:27:00:ee:e9) -> 192.168.1.1:22 dscp 0, 1 packets

```

```

/      :

```

```

esr(config)# ip firewall sessions counters

```

```

,      :

```

```
esrf# show ip firewall sessions
Codes: E - expected, U - unreplied,
       A - assured, C - confirmed
```

Prot	Inside source	Inside destination	Outside source	Outside
destination	Pkts	Bytes	Status	
-----	-----	-----	-----	-----
--	-----	-----		
tcp	192.168.1.15:43552	192.168.1.1:22	192.168.1.15:43552	192.168.1.1:
22	28	4081	AC	

```
esr# show ip firewall sessions
Codes: E - expected, U - unreplied,
       A - assured, C - confirmed
```

Prot	Inside source	Inside destination	Outside source	Outside
destination	Pkts	Bytes	Status	
-----	-----	-----	-----	-----
--	-----	-----		
tcp	192.168.1.15:43552	192.168.1.1:22	192.168.1.15:43552	192.168.1.1:
22	52	6049	AC	



firewall- CPU .

firewall?

/ :

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

```
, firewall . .
      "ip firewall disable" .
      "ip firewall disable" , .
```

security-zone Firewall?

, .

security-zone, security-zone firewall?

```
, , security-zone, .. ("security zone-pair <source-zone> <destination-zone>"),
security-zone . , security-zone (security zone-pair).
, security-zone firewall, security-zone security zone-pair.
```