

# Машина ISP

## 1. Настройка доменного имени

### Проверка.

Команда:

```
hostname
```

Вывод:

```
[root@reuug4wfsud lu ~]# hostname  
reuug4wfsud lu  
[root@reuug4wfsud lu ~]#
```

### Настройка.

Команда:

```
hostnamectl set-hostname isp.au-team.irpo
```

Вывод:

```
[root@reuug4wfsud lu ~]# hostnamectl set-hostname isp.au-team.irpo  
[root@reuug4wfsud lu ~]# hostname  
isp.au-team.irpo  
[root@reuug4wfsud lu ~]#
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```

root@isp ~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:cd:3a:00:01:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.0.137.220/24 brd 10.0.137.255 scope global dynamic noprefixroute ens3
        valid_lft 3209sec preferred_lft 2617sec
    inet6 fe80::52cd:3aff:fe00:100/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:cd:3a:00:01:01 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 172.16.1.1/28 brd 172.16.1.15 scope global ens4
        valid_lft forever preferred_lft forever
    inet6 fe80::52cd:3aff:fe00:101/64 scope link
        valid_lft forever preferred_lft forever
4: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:cd:3a:00:01:02 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 172.16.2.1/28 brd 172.16.2.15 scope global ens5
        valid_lft forever preferred_lft forever
    inet6 fe80::52cd:3aff:fe00:102/64 scope link
        valid_lft forever preferred_lft forever
5: ens6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:01:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s6
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens6
        valid_lft 82610sec preferred_lft 71810sec
    inet6 fec0::5200:ff:fe01:fe/64 scope site dynamic mngtmpaddr
        valid_lft 86299sec preferred_lft 14299sec
    inet6 fe80::5200:ff:fe01:fe/64 scope link
        valid_lft forever preferred_lft forever
root@isp ~#

```

Настройка не требуется

### 3. Настройка динамической трансляции адресов

Проверка.

Команда:

```
vim /etc/net/sysctl.conf
```

Вывод:

```

# This file was formerly part of /etc/sysctl.conf
### IPv4 networking options.

# IPv4 packet forwarding.
#
# This variable is special, its change resets all configuration
# parameters to their default state (RFC 1122 for hosts, RFC 1812 for
# routers).
#
net.ipv4.ip_forward = 1

# Source validation by reversed path, as specified in RFC 1812.
#

```

Настройка не требуется

Команда:

```
iptables -t nat -L
```

Вывод:

```

[root@isp ~]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target      prot opt source                destination

Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target      prot opt source                destination
[root@isp ~]#

```

## Настройка.

Команда:

```
iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

```
iptables-save >> /etc/sysconfig/iptables
```

```
systemctl enable --now iptables
```

Вывод:

```

[root@isp ~]# iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
[root@isp ~]# iptables-save >> /etc/sysconfig/iptables
[root@isp ~]# systemctl enable --now iptables
Synchronizing state of iptables.service with SysV service script with /
Executing: /lib/systemd/systemd-sysv-install enable iptables
Created symlink /etc/systemd/system/basic.target.wants/iptables.service
[root@isp ~]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target      prot opt source                destination

Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target      prot opt source                destination
MASQUERADE  all  --  anywhere              anywhere
[root@isp ~]#

```

## 4. Настройка часового пояса

### Проверка.

Команда:

```
timedatectl
```

Вывод:

```
(root@isp ~)# timedatectl
Local time: Sun 2026-04-05 14:18:20 MSK
Universal time: Sun 2026-04-05 11:18:20 UTC
RTC time: Sun 2026-04-05 11:18:20
Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

Настройка не требуется

## ISP НАСТРОЕН

## Машина HQ-RTR

### 1. Настройка доменного имени

Проверка.

Команда:

```
en
sh hostname
```

Вывод:

```
ecorouter>en
ecorouter#sh hostname
ecorouter
ecorouter#
```

Настройка.

Команда:

```
en
conf t
hostname HQ-RTR
ip domain-name au-team.irpo
end
write memory
```

Вывод:

```
ecorouter>en
ecorouter#sh hostname
ecorouter
ecorouter#configure terminal
Enter configuration commands, one per line.
ecorouter(config)#hostname HQ-RTR
HQ-RTR(config)#ip domain-name au-team.irpo
HQ-RTR(config)#end
HQ-RTR#write memory
Building configuration...
```

## 2. Настройка IP-адресов

### Проверка.

Команда:

```
sh ip interface brief
```

Вывод:

```
HQ-RTR#sh ip interface brief
Interface          IP-Address          Status
-----
ssh                169.254.2.101/30    down
isp                172.16.1.2/28       up
vl100              10.10.100.1/27      up
vl200              10.10.200.1/28      up
vl999              10.10.30.1/29       up
HQ-RTR#
```

Настройка не требуется

## 3. Настройка пользователей

### Проверка.

Команда:

```
sh users localdb
```

Вывод:

```
HQ-RTR# show users localdb
Roles:
daemon
User: net_admin
Description:
  Docker socket access: disabled
VR:
```

Настройка не требуется

## 4. Настройка GRE

### Проверка.

Команда:

```
sh interface tunnel.0
```

Вывод:

```
HQ-RTR#sh interface tunnel.0
HQ-RTR#
```

← если пусто, то требуется настройка

### Настройка.

```
en
```

```
conf t
```

```
interface tunnel.0
```

```
ip address 10.10.10.1/30
```

```
ip tunnel 172.16.1.2 172.16.2.2 mode gre
```

```
end
```

```
write memory
```

Вывод:

```
HQ-RTR>en
HQ-RTR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HQ-RTR(config)#interface tunnel.0
HQ-RTR(config-if-tunnel)#ip address 10.10.10.1/30
HQ-RTR(config-if-tunnel)#ip tunnel 172.16.1.2 172.16.2.2 mode gre
2026-04-02 10:24:35      INFO      Interface tunnel.0 changed state to up
HQ-RTR(config-if-tunnel)#end
HQ-RTR#write memory
Building configuration...

HQ-RTR#sh
HQ-RTR#show interface tunnel.0
Interface tunnel.0 is up
  Snmp index: 10
  Ethernet address: (port not configured)
  MTU: 1476
  Tunnel source: 172.16.1.2
  Tunnel destination: 172.16.2.2
  Tunnel mode: GRE
  NAI: no
  ARP Proxy: disable
  ICMP redirects on, unreachable on
  IP URPF is disabled
  Label switching is disabled
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 10.10.10.1/30 broadcast 10.10.10.3/30
  total input packets 0, bytes 0
  total output packets 0, bytes 0
HQ-RTR#
```

## 5. Настройка статической маршрутизации

### Проверка.

Команда:

```
sh ip route
```

Вывод:

```
>en
#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C      10.10.10.0/30 is directly connected, tunnel.0
C      10.10.30.0/29 is directly connected, vl999
C      10.10.100.0/27 is directly connected, vl100
C      10.10.200.0/28 is directly connected, vl200
C      172.16.1.0/28 is directly connected, isp
Gateway of last resort is not set
```

нет значения со \*, значит маршрут по умолчанию не настроен

требуется настройка

### Настройка.

Команда:

```
conf t
```

```
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

```
end
```

```
write memory
```

Вывод:

```
HQ-RTR(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
HQ-RTR(config)#end
HQ-RTR#write
Building configuration...

HQ-RTR#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.1.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.1.1, isp
C      10.10.10.0/30 is directly connected, tunnel.0
C      10.10.30.0/29 is directly connected, vl999
C      10.10.100.0/27 is directly connected, vl100
C      10.10.200.0/28 is directly connected, vl200
C      172.16.1.0/28 is directly connected, isp
HQ-RTR#
```

## 6. Настройка динамической маршрутизации (OSPF)

### Проверка.

Команда:

```
sh ip route
```

Вывод:

```
>en
#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C 10.10.10.0/30 is directly connected, tunnel.0
C 10.10.30.0/29 is directly connected, vl999
C 10.10.100.0/27 is directly connected, vl100
C 10.10.200.0/28 is directly connected, vl200
C 172.16.1.0/28 is directly connected, isp
Gateway of last resort is not set
```

если нет буквы O в таблице маршрутизации  
необходима настройка OSPF

### Настройка.

Команда:

```
en
```

```
conf t
```

```
router ospf 0
```

```
network 10.10.100.0/27 area 0
```

```
network 10.10.200.0/28 area 0
```

```
network 10.10.30.0/29 area 0
```

```
network 10.10.10.0/30 area 0
```

```
passive-interface default
```

```
no passive-interface tunnel.0
```

```
area 0 authentication
```

```
exit
```

```
interface tunnel.0
```

```
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 P@ssw0rd
```

```
end
```

```
write memory
```



## Настройка.

Команда:

```
en
conf t
interface isp
ip nat outside
exit
interface vl100
ip nat inside
exit
interface vl200
ip nat inside
exit
interface vl999
ip nat inside
exit
ip nat pool HQ 10.10.0.1-10.10.200.254
ip nat source dynamic inside-to-outside pool HQ overload interface isp
end
write memory
```

Вывод:

```
HQ-RTR#en
HQ-RTR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HQ-RTR(config)#interface isp
HQ-RTR(config-if)#ip nat outside
HQ-RTR(config-if)#exit
HQ-RTR(config)#interface vl
vl100 vl200 vl999
HQ-RTR(config)#interface vl100
HQ-RTR(config-if)#ip nat ind
HQ-RTR(config-if)#ip nat inside
HQ-RTR(config-if)#exit
HQ-RTR(config)#interface vl200
HQ-RTR(config-if)#ip nat inside
HQ-RTR(config-if)#exit
HQ-RTR(config)#interface vl999
HQ-RTR(config-if)#ip nat inside
HQ-RTR(config-if)#exit
HQ-RTR(config)#ip na
name-server nat
HQ-RTR(config)#ip nat pool HQ 10.10.0.1-10.10.200.254
HQ-RTR(config)#ip nat source dynamic inside-to-outside pool HQ overload interface isp
HQ-RTR(config)#
```

## 8. Настройка протокола динамической конфигурации хостов (DHCP)

## Проверка.

Команда:

```
show dhcp-server 1 detailed
```

Вывод:

```
HQ-RTR#show dhcp-server 1 detailed
DHCP-server 1:

* Global options:
  Lease-time: 86400 sec
  Netmask: 255.255.255.0

* Static entries:

* Framed-ip pool entries:

* Pool entries:
** pool VLAN200 1
   Gateway: 10.10.200.1
   DNS-servers: 10.10.100.2
   Domain-name: au-team.irpo
   Netmask: 255.255.255.240
```

Настройка не требуется

## 9. Настройка часового пояса

### Проверка.

Команда:

```
show ntp timezone
```

Вывод:

```
HQ-RTR#show ntp timezone
System Time zone:
HQ-RTR#
```

### Настройка.

Команда:

```
en
```

```
conf t
```

```
ntp timezone utc+3
```

Вывод:

```
HQ-RTR#conf t
Enter configuration commands, one per line. End with CTRL-Z
HQ-RTR(config)#ntp timezone utc+3
HQ-RTR(config)#end
HQ-RTR#show ntp timezone
System Time zone: Europe/Moscow
HQ-RTR#
```

## HQ-RTR НАСТРОЕН

## Машина BR-RTR

### 1. Настройка доменного имени

#### Проверка.

Команда:

```
en
sh hostname
```

Вывод:

```
ecorouter>en
ecorouter#sh hostname
ecorouter
ecorouter#
```

#### Настройка.

Команда:

```
en
conf t
hostname BR-RTR
ip domain-name au-team.irpo
end
write memory
```

Вывод:

```
ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line.
ecorouter(config)#hostname BR-RTR
BR-RTR(config)#ip domain-name au-team.irpo
BR-RTR(config)#end
BR-RTR#write memory
Building configuration...
```

## 2. Настройка IP-адресов

### Проверка.

Команда:

```
sh ip interface brief
```

Вывод:

```
BR-RTR#show ip interface brief
Interface          IP-Address          Status
-----
ssh                169.254.2.101/30    up
isp                172.16.2.2/28       up
fw                 10.20.10.1/30       up
BR-RTR#
```

Настройка не требуется

## 3. Настройка пользователей

### Проверка.

Команда:

```
sh users localdb
```

Вывод:

```
# show users localdb
Roles:
daemon ''
User: net_admin
Description:
  Docker socket access: disabled
VR:
```

Настройка не требуется

## 4. Настройка GRE

### Проверка.

Команда:

```
sh interface tunnel.0
```

Вывод:

```
#sh interface tunnel.0  
#
```

← если пусто, то требуется настройка

## Настройка.

Команда:

```
en
```

```
conf t
```

```
interface tunnel.0
```

```
ip address 10.10.10.2/30
```

```
ip tunnel 172.16.2.2 172.16.1.2 mode gre
```

```
end
```

```
write memory
```

Вывод:

```
BR-RTR>  
BR-RTR>en  
BR-RTR#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
BR-RTR(config)#interface tunnel.0  
BR-RTR(config-if-tunnel)#ip  
ip   ipv6  
BR-RTR(config-if-tunnel)#ip address 10.10.10.2/30  
BR-RTR(config-if-tunnel)#ip tunnel 172.16.2.2 172.16.1.2 mode gre  
  
2026-04-02 11:16:59      INFO      Interface tunnel.0 changed state to up  
BR-RTR(config-if-tunnel)#end  
BR-RTR#write memory  
Building configuration...
```

## 5. Настройка статической маршрутизации

### Проверка.

Команда:

```
sh ip route
```

Вывод:

```

>en
#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C      10.10.10.0/30 is directly connected, tunnel.0
C      10.10.30.0/29 is directly connected, vl999
C      10.10.100.0/27 is directly connected, vl100
C      10.10.200.0/28 is directly connected, vl200
C      172.16.1.0/28 is directly connected, isp
Gateway of last resort is not set

```

нет значения со \*, значит маршрут по умолчанию не настроен  
требуется настройка

## Настройка.

Команда:

```

conf t
ip route 0.0.0.0 0.0.0.0 172.16.2.1
end
write memory

```

Вывод:

```

BR-RTR>en
BR-RTR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BR-RTR(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1
BR-RTR(config)#end
BR-RTR#write memory
Building configuration...

BR-RTR#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter a
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.2.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.2.1, isp
C     10.10.10.0/30 is directly connected, tunnel.0
C     10.20.10.0/30 is directly connected, fw
C     169.254.2.100/30 is directly connected, ssh
C     172.16.2.0/28 is directly connected, isp
BR-RTR#

```

## 6. Настройка динамической маршрутизации (OSPF)

### Проверка.

Команда:

```
sh ip route
```

Вывод:

```
>en
#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C 10.10.10.0/30 is directly connected, tunnel.0
C 10.10.30.0/29 is directly connected, vl999
C 10.10.100.0/27 is directly connected, vl100
C 10.10.200.0/28 is directly connected, vl200
C 172.16.1.0/28 is directly connected, isp
Gateway of last resort is not set
```

если нет буквы O в таблице маршрутизации  
необходима настройка OSPF

## Настройка.

Команда:

```
en
```

```
conf t
```

```
router ospf 0
```

```
network 10.20.10.0/30 area 0
```

```
network 10.10.10.0/30 area 0
```

```
passive-interface default
```

```
no passive-interface tunnel.0
```

```
no passive-interface fw
```

```
area 0 authentication
```

```
exit
```

```
interface tunnel.0
```

```
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 P@sswOrd
```

```
exit
```

```
interface fw
```

```
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 P@sswOrd
```

```
end
```

```
write memory
```

Вывод:

```
BR-RTR#conf t
Enter configuration commands, one per line. End with CNTL/Z
BR-RTR(config)#router ospf 0
BR-RTR(config-router)#network 10.20.10.0/30 area 0
BR-RTR(config-router)#network 10.10.10.0/30 area 0
BR-RTR(config-router)#passive-interface default
BR-RTR(config-router)#no passive-interface tunnel.0
BR-RTR(config-router)#no passive-interface fw
BR-RTR(config-router)#area 0 authentication
BR-RTR(config-router)#exit
BR-RTR(config)#interface fw
BR-RTR(config-if)#ip ospf authentication-key P@ssw0rd
BR-RTR(config-router)#exit
BR-RTR(config)#interface tunnel.0
BR-RTR(config-if-tunnel)#ip ospf authentication-key P@ssw
BR-RTR(config-if-tunnel)#
```

```
BR-RTR#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 0 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address        Interface
172.16.1.2     1    Full/Backup     00:00:32   10.10.10.1    tunnel.0
BR-RTR#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.2.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.1, isp
C     10.10.10.0/30 is directly connected, tunnel.0
O     10.10.30.0/29 [110/11] via 10.10.10.1, tunnel.0, 00:02:34
O     10.10.100.0/27 [110/11] via 10.10.10.1, tunnel.0, 00:02:34
O     10.10.200.0/28 [110/11] via 10.10.10.1, tunnel.0, 00:02:34
C     10.20.10.0/30 is directly connected, fw
C     169.254.2.100/30 is directly connected, ssh
C     172.16.2.0/28 is directly connected, isp
BR-RTR#
```

## 7. Настройка динамической трансляции адресов (NAT)

Проверка.

Команда:

С BR-RTR выполнить: `show ip nat translations`

Вывод:

```

#sh ip nat translations
Static translations:

Source                               Translated                               VRF
                                     Если пусто, необходимо настроить

Destination                           Translated                               VRF

Empty list.
Total: 0

PAT translations:

Source                               Translated                               Destination

Empty list.
Total: 0

```

## Настройка.

Команда:

```

en
conf t
interface isp
ip nat outside
exit
interface fw
ip nat inside
exit
ip nat pool BR 10.0.0.1-10.254.254.254
ip nat source dynamic inside-to-outside pool BR overload interface isp
end
write memory

```

Вывод:

```

BR-RTR#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
BR-RTR(config)#interface isp
BR-RTR(config-if)#ip nat outside
BR-RTR(config-if)#exit
BR-RTR(config)#interface fw
BR-RTR(config-if)#ip nat inside
BR-RTR(config-if)#exit
BR-RTR(config)#ip nat pool BR 10.0.0.1-10.254.254.254
BR-RTR(config)#ip na
name-server nat
BR-RTR(config)#ip nat source dynamic inside-to-outside pool BR overload interface isp
BR-RTR(config)#end
BR-RTR#write memory
Building configuration...

```

## 8. Настройка часового пояса

### Проверка.

Команда:

```
show ntp timezone
```

Вывод:

```
HQ-RTR#show ntp timezone
System Time zone:
HQ-RTR#
```

### Настройка.

Команда:

```
en
```

```
conf t
```

```
ntp timezone utc+3
```

Вывод:

```
HQ-RTR#conf t
Enter configuration commands, one per line.
HQ-RTR(config)#ntp timezone utc+3
HQ-RTR(config)#end
HQ-RTR#show ntp timezone
System Time zone: Europe/Moscow
HQ-RTR#
```

## BR-SRV НАСТРОЕН

## Машина HQ-SW

### 1. Настройка доменного имени

#### Проверка.

Команда:

```
hostname
```

Вывод:

```
[root@reuug4wfsud lu ~]# hostname
reuug4wfsud lu
```

## Настройка.

Команда:

```
hostnamectl set-hostname hq-sw.au-team.irpo
```

Вывод:

```
[root@reuug4wfsudlu ~]# hostnamectl set-hostname hq-sw.au-team.irpo
[root@reuug4wfsudlu ~]# hostname
hq-sw.au-team.irpo
[root@reuug4wfsudlu ~]# _
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```
[root@reuug4wfsudlu ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 50:62:e4:00:1e:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 fe80::5262:e4ff:fe00:1e00/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 50:62:e4:00:1e:01 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet6 fe80::5262:e4ff:fe00:1e01/64 scope link
        valid_lft forever preferred_lft forever
4: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 50:62:e4:00:1e:02 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet6 fe80::5262:e4ff:fe00:1e02/64 scope link
        valid_lft forever preferred_lft forever
5: ens6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:03:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s6
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens6
        valid_lft 77534sec preferred_lft 66734sec
    inet6 fec0::5200:ff:fe03:fe/64 scope site dynamic mngtmpaddr
        valid_lft 86117sec preferred_lft 14117sec
    inet6 fe80::5200:ff:fe03:fe/64 scope link
        valid_lft forever preferred_lft forever
6: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether ce:fb:0f:34:fb:14 brd ff:ff:ff:ff:ff:ff
7: hq-sw: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 50:62:e4:00:1e:00 brd ff:ff:ff:ff:ff:ff
8: MGMT: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 1e:84:d8:d4:84:5c brd ff:ff:ff:ff:ff:ff
    inet 10.10.30.2/29 scope global MGMT
        valid_lft forever preferred_lft forever
    inet6 fe80::1c84:d8ff:fed4:845c/64 scope link
        valid_lft forever preferred_lft forever
```

Настройка не требуется

## 3. Настройка коммутации в сегменте HQ (VLAN)

### Проверка.

Команда:

```
ovs-vsctl show
```

Вывод:

```

[root@hq-sw ~]# ovs-vsctl show
a4a93a7a-e450-4ce7-ad85-67474373690c
  Bridge hq-sw
    Port hq-sw
      Interface hq-sw
        type: internal
    Port ens5
      tag: 200
      Interface ens5
    Port ens3
      trunks: [100, 200, 999]
      Interface ens3
    Port MGMT
      tag: 999
      Interface MGMT
        type: internal
    Port ens4
      tag: 100
      Interface ens4
  ovs_version: "2.17.11"
[root@hq-sw ~]#

```

Настройка не требуется

HQ-SW НАСТРОЕН

## Машина HQ-SRV

### 1. Настройка доменного имени

Проверка.

Команда:

```
hostname
```

Вывод:

```

[root@reug4wfsud lu ~]# hostname
reug4wfsud lu

```

Настройка.

Команда:

```
hostnamectl set-hostname hq-srv.au-team.irpo
```

Вывод:

```

[root@reug4wfsud lu ~]# hostnamectl set-hostname hq-srv.au-team.irpo
[root@reug4wfsud lu ~]# hostname
hq-srv.au-team.irpo

```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```
root@reug41:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:90:76:00:00:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 fe80::5290:76ff:fe00:d00/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:04:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens4
        valid_lft 65932sec preferred_lft 55132sec
    inet6 fec8::5200:ff:fe04:fe/64 scope site dynamic mngtmpaddr
        valid_lft 86392sec preferred_lft 14392sec
    inet6 fe80::5200:ff:fe04:fe/64 scope link
        valid_lft forever preferred_lft forever
```

на интерфейсе ens3 нет ip-адреса, необходимо настроить

### Настройка.

Команда:

Зайти в файл: `vim /etc/net/ifaces/ens3/options`

Проверить содержимое файла

```
TYPE=eth
CONFIG_WIRELESS=no
BOOTPROTO=static
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
```

Зайти в файл: `vim /etc/net/ifaces/ens3/ipv4address`

Внести в файл информацию

```
10.10.100.2/27
```

Зайти в файл: `vim /etc/net/ifaces/ens3/ipv4route`

Внести в файл информацию

```
default via 10.10.100.1
```

Зайти в файл: `vim /etc/net/ifaces/ens3/resolv.conf`

Внести в файл информацию

```
search au-team.irpo
nameserver 77.88.8.8
nameserver 127.0.0.1
```

```
systemctl restart network
```

Вывод:

```
[root@hq-srv ~]# systemctl restart network
[root@hq-srv ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:90:76:00:0d:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.10.100.2/27 brd 10.10.100.31 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::5290:76ff:fe00:d00/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:04:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens4
        valid_lft 86397sec preferred_lft 75597sec
    inet6 fec0::5200:ff:fe04:fe/64 scope site dynamic mngtmpaddr
        valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::5200:ff:fe04:fe/64 scope link
        valid_lft forever preferred_lft forever
```

### 3. Настройка локальной учетной записи

Проверка.

Команда:

```
vim /etc/passwd
```

Вывод:

```
_nslcd:x:490:475:NSS-LDAP Daemon:/:/sbin/nologin
_chrony:x:489:474:Chrony User:/var/lib/chrony:/dev/null
ntpd:x:488:472:/:/dev/null:/dev/null
tcpdump:x:487:471:/:/dev/null:/dev/null
_dhcpd:x:486:468:dhcpd user:/var/lib/dhcpd:/dev/null
user:x:500:500:/:/home/user:/bin/bash
sshuser:x:2026:501:/:/home/sshuser:/bin/bash
sshadmin:x:1025:1025:/:/home/sshadmin:/bin/bash
```

Команда:

```
vim /etc/group
```

Вывод:

```
root:x:0:
bin:x:1:root
daemon:x:2:root
sys:x:3:root,bin,adm
adm:x:4:root
tty:x:5:
disk:x:6:root
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:root,zabbix,user,sshuser
firewall:x:11:
```

Команда:

```
visudo
```

Вывод:

```
## Uncomment to allow members of group wheel to execute any command
# WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
# WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# SUDO_USERS ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw # Ask for the password of the target user
# ALL ALL=(ALL:ALL) ALL # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
```

## Настройка.

Команда:

```
vim +123 /etc/sudoers
```

```
## Same thing without a password
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL ← раскомментировать строку

## Uncomment to allow members of group sudo to execute any co
# SUDO_USERS ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the p
## of the user they are running the command as (root by defau
# Defaults targetpw # Ask for the password of the target use
# ALL ALL=(ALL:ALL) ALL # WARNING: only use this together wi

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
-- INSERT --
```

#### 4. Настройка безопасного удаленного доступа (SSH)

##### Проверка.

Команда:

```
vim /etc/openssh/sshd_config
```

Вывод:

```
#PermitRootLogin without-password
#StrictModes yes
MaxAuthTries 2      Попытки ввода пароля есть
#MaxSessions 10
```

```
#Banner none      баннера нет
```

##### Настройка.

Команда:

```
vim /etc/openssh/sshd_config
```

Внести в файл информацию

```
# no default banner path
Banner /etc/openssh/banner_
```

```
vim /etc/openssh/banner
```

Внести в файл информацию

```
Authorized access only_
```

```
systemctl restart sshd
```

#### 5. Настройте инфраструктуру разрешения доменных имён (DNS)

##### Проверка.

Команда:

```
vim /etc/bind/options.conf
```

Вывод:

```
options {
  version "unknown";
  directory "/etc/bind/zone";
  dump-file "/var/run/named/named_dump.db";
  statistics-file "/var/run/named/named.stats";
  recursing-file "/var/run/named/named.recursing";
  secroots-file "/var/run/named/named.secroots";

  // disables the use of a PID file
  pid-file none;

  /*
   * Oftenly used directives are listed below.
   */

  listen-on { 127.0.0.1; };
  listen-on-v6 { ::1; };

  /*
   * If the forward directive is set to "only", the server will only
   * query the forwarders.
   */
  //forward only;
  //forwarders { };

  /*
   * Specifies which hosts are allowed to ask ordinary questions.
   */
  //allow-query { localnets; };

  /*
   * This lets "allow-query" be used to specify the default zone access
   * level rather than having to have every zone override the global
   * value. "allow-query-cache" can be set at both the options and view
   * levels. If "allow-query-cache" is not set then "allow-recursion" is
   * used if set, otherwise "allow-query" is used if set unless
   * "recursion no;" is set in which case "none;" is used, otherwise the
   * default (localhost; localnets;) is used.
   */
  //allow-query-cache { localnets; };
}
```

← требуется настройка

Команда:

```
vim /etc/bind/rfc1912.conf
```

Вывод:

```
zone "10.10.in-addr.arpa" {
  type master;
  file "10.10.in-addr.arpa";
  allow-update { none; };
};

zone "au-team.irpo" {
  type master;
  file "au-team.irpo.zone";
  allow-update { none; };
};
```

Команда:

```
vim /etc/bind/zone/au-team.irpo.zone
```

Вывод:

```

$TTL 86400
@ IN SOA hq-srv.au-team.irpo. admin.au-team.irpo. (
    2024010101 : Serial
    3600      : Refresh
    1800     : Retry
    604800   : Expire
    86400    : Minimum TTL

@ IN NS      hq-srv.au-team.irpo.
@ IN A      10.10.100.2
hq-rtr     IN A      172.16.1.2
br-rtr     IN A      172.16.2.2
hq-srv     IN A      10.10.100.2
hq-cli     IN A      10.10.200.2
br-srv     IN A      10.20.20.2
br-cli     IN A      10.20.30.2
br-fw      IN A      10.20.10.2

; Записи для ISP
web        IN A      172.16.1.1
docker     IN A      172.16.2.1

```

исправить на root.au-team.irpo.

Команда:

```
vim /etc/bind/zone/10.10.in-addr.arpa
```

Вывод:

```

$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025110600      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
1.100    IN      NS       au-team.irpo.
2.100    IN      PTR      hq-rtr.au-team.irpo.
2.200    IN      PTR      hq-srv.au-team.irpo.

```

исправить на au-team.irpo. root.au-team.irpo.

**Настройка.**

Команда:

```
Зайти в файл: vim /etc/bind/options.conf
```

Внести в файл информацию

```
*/
listen-on { 10.10.100.2; };
listen-on-uv { none; };

/*
 * If the forward directive is set to "only", the server will
 * query the forwarders.
 */
//forward only;
forwarders { 77.88.8.8; };

/*
 * Specifies which hosts are allowed to ask ordinary questions.
 */
allow-query { any; };
```

Команда:

Зайти в файл: `vim /etc/bind/zone/au-team.irpo.zone`

Внести в файл информацию

```
$TTL 86400
@ IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (
    2024010101 ; Serial
    3600      ; Refresh
    1800      ; Retry
    604800    ; Expire
    86400     ; Minimum TTL

@ IN NS      hq-srv.au-team.irpo.
@ IN A      10.10.100.2
hq-rtr     IN A      172.16.1.2
br-rtr     IN A      172.16.2.2
hq-srv     IN A      10.10.100.2
hq-cli     IN A      10.10.200.2
br-srv     IN A      10.20.20.2
br-cli     IN A      10.20.30.2
br-fw     IN A      10.20.10.2

; Записи для ISP
web        IN A      172.16.1.1
docker     IN A      172.16.2.1
```

Команда:

Зайти в файл: `vim /etc/bind/zone/10.10.in-addr.arpa`

Внести в файл информацию

```

$TTL      1D
e         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025110600 ; serial
                                12H       ; refresh
                                1H        ; retry
                                1W        ; expire
                                1H        ; ncache
)

         IN      NS      au-team.irpo.
1.100    IN      PTR     hq-rtr.au-team.irpo.
2.100    IN      PTR     hq-srv.au-team.irpo.
2.200    IN      PTR     hq-cli.au-team.irpo.

```

Команда:

```
systemctl enable --now bind.service
```

## 6. Настройка часового пояса

### Проверка.

Команда:

```
timedatectl
```

Вывод:

```

[root@isp ~]# timedatectl
          Local time: Sun 2026-04-05 14:18:20 MSK
          Universal time: Sun 2026-04-05 11:18:20 UTC
             RTC time: Sun 2026-04-05 11:18:20
          Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no

```

Настройка не требуется

## HQ-SRV НАСТРОЕН

## Машина HQ-CLI

### 1. Настройка доменного имени

#### Проверка.

Команда:

```
hostname
```

Вывод:

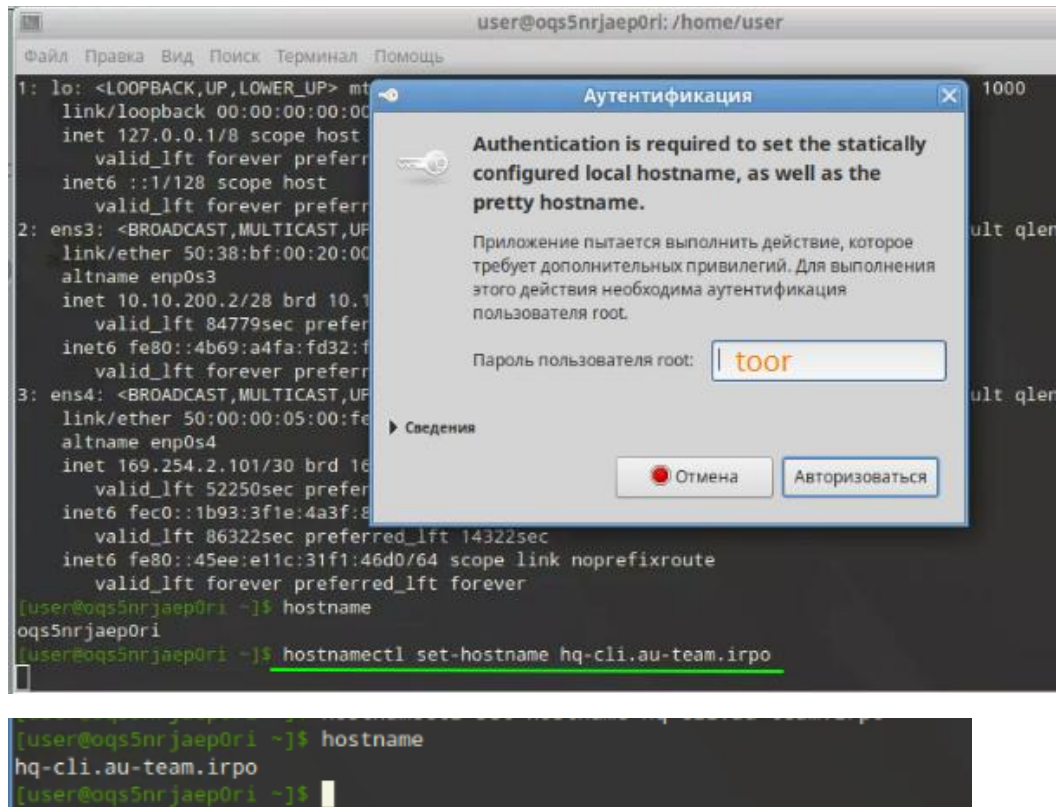
```
valid_lft forever preferred_lft
[user@oqs5nrjaep0r1 ~]$ hostname
oqs5nrjaep0r1
[user@oqs5nrjaep0r1 ~]$
```

## Настройка.

Команда:

```
hostnamectl set-hostname hq-cli.au-team.irpo
```

Вывод:



The screenshot shows a terminal window with the following content:

```
user@oqs5nrjaep0r1: /home/user
Файл Правка Вид Поиск Терминал Помощь
1: lo: <LOOPBACK,UP,LOWER_UP> mt
  link/loopback 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host
    valid_lft forever preferred_lft
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft
2: ens3: <BROADCAST,MULTICAST,UP
  link/ether 50:38:bf:00:20:00
  altname enp0s3
  inet 10.10.200.2/28 brd 10.10.200.3
    valid_lft 84779sec preferred_lft
  inet6 fe80::4b69:a4fa:fd32:f...
    valid_lft forever preferred_lft
3: ens4: <BROADCAST,MULTICAST,UP
  link/ether 50:00:00:05:00:fe
  altname enp0s4
  inet 169.254.2.101/30 brd 169.254.2.102
    valid_lft 52250sec preferred_lft
  inet6 fec0::1b93:3fte:4a3f:8...
    valid_lft 86322sec preferred_lft 14322sec
  inet6 fe80::45ee:e11c:31f1:46d0/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
[user@oqs5nrjaep0r1 ~]$ hostname
oqs5nrjaep0r1
[user@oqs5nrjaep0r1 ~]$ hostnamectl set-hostname hq-cli.au-team.irpo
```

An authentication dialog box titled "Аутентификация" (Authentication) is overlaid on the terminal. It contains the following text:

Authentication is required to set the statically configured local hostname, as well as the pretty hostname.

Приложение пытается выполнить действие, которое требует дополнительных привилегий. Для выполнения этого действия необходима аутентификация пользователя root.

Пароль пользователя root:

Buttons: Отмена (Cancel), Авторизоваться (Authorize).

Below the dialog, the terminal shows the result of the command:

```
[user@oqs5nrjaep0r1 ~]$ hostname
hq-cli.au-team.irpo
[user@oqs5nrjaep0r1 ~]$
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```
[user@oqs5nrjaep0r1 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:38:bf:00:20:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.10.200.2/28 brd 10.10.200.15 scope global dynamic noprefixroute ens3
        valid_lft 84779sec preferred_lft 84779sec
    inet6 fe80::4b69:a4fa:fd32:fcd8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:05:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope link dynamic noprefixroute ens4
        valid_lft 52250sec preferred_lft 52250sec
    inet6 fec0::1b93:3f1e:4a3f:855a/64 scope site dynamic noprefixroute
        valid_lft 86322sec preferred_lft 14322sec
    inet6 fe80::45ee:e11c:31f1:46d0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Настройка не требуется

### 3. Настройка часового пояса

Проверка.

Команда:

```
timedatectl
```

Вывод:

```
[root@isp ~]# timedatectl
    Local time: Sun 2026-04-05 14:18:20 MSK
    Universal time: Sun 2026-04-05 11:18:20 UTC
    RTC time: Sun 2026-04-05 11:18:20
    Time zone: Europe/Moscow (MSK, +0300)
    System clock synchronized: yes
    NTP service: active
    RTC in local TZ: no
```

Настройка не требуется

HQ-CLI НАСТРОЕН

## Машина BR-CLI

### 1. Настройка доменного имени

Проверка.

Команда:

```
hostname
```

Вывод:

```
valid_etc_forever_preferred_etc
[user@oqs5nrjaep0ri ~]$ hostname
oqs5nrjaep0ri
[user@oqs5nrjaep0ri ~]$
```

## Настройка.

Команда:

```
hostnamectl set-hostname br-cli.au-team.irpo
```

Вывод:

```
[user@oqs5nrjaep0ri ~]$ hostnamectl set-hostname br-cli.au-team.irpo
```

```
[user@oqs5nrjaep0ri ~]$ hostname
br-cli.au-team.irpo
[user@oqs5nrjaep0ri ~]$
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```
[user@oqs5nrjaep0r1 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:a5:0a:00:24:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 fe80::7e71:3456:ee6f:c023/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:09:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope link dynamic noprefixroute ens4
        valid_lft 51038sec preferred_lft 51038sec
    inet6 fec0::c97d:73d9:f89d:d85/64 scope site dynamic noprefixroute
        valid_lft 86378sec preferred_lft 14378sec
    inet6 fe80::ca1c:78dc:8d9:3ec5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

требуется настройка

## Настройка.

Команда:

su -

```
[user@br-cl1 ~]$ su -
Password: toor
```

mv /etc/net/ifaces/ens18 /etc/net/ifaces/ens3

Зайти в файл: vim /etc/net/ifaces/ens3/options

Проверить содержимое файла

```
TYPE=eth
CONFIG_WIRELESS=no
BOOTPROTO=static
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
```

Зайти в файл: vim /etc/net/ifaces/ens3/ipv4address

Внести в файл информацию

```
10.20.30.2/29
```

Зайти в файл: vim /etc/net/ifaces/ens3/ipv4route

Внести в файл информацию

```
default via 10.20.30.1
```

Зайти в файл: vim /etc/net/ifaces/ens3/resolv.conf

Внести в файл информацию

```
search au-team.irpo
nameserver 10.10.100.2
```

`systemctl restart network`

`reboot`

Вывод:

```
[user@br-cli ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:a5:0a:00:24:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.20.30.2/29 brd 10.20.30.7 scope global noprefixroute ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::52a5:aff:fe00:2400/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:09:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope link dynamic noprefixroute ens4
        valid_lft 86328sec preferred_lft 86328sec
```

### 3. Настройка часового пояса

#### Проверка.

Команда:

`timedatectl`

Вывод:

```
[root@isp ~]# timedatectl
Local time: Sun 2026-04-05 14:18:20 MSK
Universal time: Sun 2026-04-05 11:18:20 UTC
RTC time: Sun 2026-04-05 11:18:20
Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

Настройка не требуется

**BR-CLI НАСТРОЕН**

**Машина BR-SRV**

## 1. Настройка доменного имени

### Проверка.

Команда:

```
hostname
```

Вывод:

```
[root@reuug4wfsud lu ~]# hostname
reuug4wfsud lu
```

### Настройка.

Команда:

```
hostnamectl set-hostname br-srv.au-team.irpo
```

Вывод:

```
[root@reuug4wfsud lu ~]# hostnamectl set-hostname br-srv.au-team.irpo
[root@reuug4wfsud lu ~]# hostname
br-srv.au-team.irpo
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

Вывод:

```
[root@reuug4wfsud lu ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:90:76:00:00:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 fe80::5290:76ff:fe00:d00/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:04:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens4
        valid_lft 65932sec preferred_lft 55132sec
    inet6 fec0::5200:ff:fe04:fe/64 scope site dynamic mngtppaddr
        valid_lft 86392sec preferred_lft 14392sec
    inet6 fe80::5200:ff:fe04:fe/64 scope link
        valid_lft forever preferred_lft forever
```

на интерфейсе ens3 нет ip-адреса,  
необходимо настроить

### Настройка.

Команда:

Зайти в файл: `vim /etc/net/ifaces/ens3/options`

Проверить содержимое файла

```
TYPE=eth
CONFIG_WIRELESS=no
BOOTPROTO=static
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
```

Зайти в файл: `vim /etc/net/ifaces/ens3/ipv4address`

Внести в файл информацию

```
10.20.20.2/28
```

Зайти в файл: `vim /etc/net/ifaces/ens3/ipv4route`

Внести в файл информацию

```
default via 10.20.20.1_
```

Зайти в файл: `vim /etc/net/ifaces/ens3/resolv.conf`

Внести в файл информацию

```
search au-team.irpo
nameserver 10.10.100.2_
```

`systemctl restart network`

Вывод:

```
root@hq-srv ~# systemctl restart network
root@hq-srv ~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:90:76:00:0d:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.10.100.2/27 brd 10.10.100.31 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::5290:76ff:fe00:d00/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:00:00:04:00:fe brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 169.254.2.101/30 brd 169.254.2.103 scope global dynamic noprefixroute ens4
        valid_lft 86397sec preferred_lft 75597sec
    inet6 fec0::5200:ff:fe04:fe/64 scope site dynamic mngtmpaddr
        valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::5200:ff:fe04:fe/64 scope link
        valid_lft forever preferred_lft forever
```

### 3. Настройка локальной учетной записи

## Проверка.

Команда:

```
vim /etc/passwd
```

Вывод:

```
_nslcd:x:490:475:NSS-LDAP Daemon:/:/sbin/nologin
_chrony:x:489:474:Chrony User:/var/lib/chrony:/dev/null
ntpd:x:488:472:/:/dev/null:/dev/null
tcpdump:x:487:471:/:/dev/null:/dev/null
_dhcpd:x:486:468:dhcpd user:/var/lib/dhcpd:/dev/null
user:x:500:500:/:/home/user:/bin/bash
sshuser:x:2026:501:/:/home/sshuser:/bin/bash
sshadmin:x:1025:1025:/:/home/sshadmin:/bin/bash
```

Команда:

```
vim /etc/group
```

Вывод:

```
root:x:0:
bin:x:1:root
daemon:x:2:root
sys:x:3:root,bin,adm
adm:x:4:root
tty:x:5:
disk:x:6:root
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:root,zabbix,user,sshuser
firewall:x:11:
```

Команда:

```
visudo
```

Вывод:

```
## Uncomment to allow members of group wheel to execute any command
# WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
# WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# SUDO_USERS ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw # Ask for the password of the target user
# ALL ALL=(ALL:ALL) ALL # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
```

## Настройка.

Команда:

```
vim +123 /etc/sudoers
```

```
## Same thing without a password
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL ← раскомментировать строку
## Uncomment to allow members of group sudo to execute any co
# SUDO_USERS ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the p
## of the user they are running the command as (root by defau
# Defaults targetpw # Ask for the password of the target use
# ALL ALL=(ALL:ALL) ALL # WARNING: only use this together wi

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
-- INSERT --
```

## 4. Настройка безопасного удаленного доступа (SSH)

### Проверка.

Команда:

```
vim /etc/openssh/sshd_config
```

Вывод:

```
#PermitRootLogin without-password
#StrictModes yes
MaxAuthTries 2 Попытки ввода пароля есть
#MaxSessions 10

#Banner none баннера нет
```

## Настройка.

Команда:

```
vim /etc/openssh/sshd_config
```

Внести в файл информацию

```
# no default banner path
Banner /etc/openssh/banner_
```

```
vim /etc/openssh/banner
```

Внести в файл информацию

```
Authorized access only_
```

```
systemctl restart sshd
```

## 5. Настройка часового пояса

### Проверка.

Команда:

```
timedatectl
```

Вывод:

```
[root@isp ~]# timedatectl
Local time: Sun 2026-04-05 14:18:20 MSK
Universal time: Sun 2026-04-05 11:18:20 UTC
RTC time: Sun 2026-04-05 11:18:20
Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

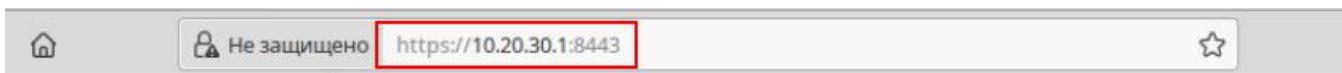
Настройка не требуется

## BR-SRV НАСТРОЕН

## Машина BR-FW (Настраивается через браузер на BR-CLI)

### 0. Подключение к BR-FW

В **BR-CLI** открыть браузер и ввести адрес и порт BR-FW – **10.20.30.1:8443**, далее принять все риски



Скорее всего, эта проблема связана с самим веб-сайтом, и вы ничего не сможете с этим сделать.

Если вы находитесь в корпоративной сети или используете антивирусную программу, вы можете связаться со службой поддержки для получения помощи. Вы также можете сообщить администратору веб-сайта об этой проблеме.

[Подробнее...](#)

Вернуться назад (рекомендуется)

Дополнительно **1**

Кто-то может пытаться подменить настоящий сайт и вам лучше не продолжать.

Веб-сайты подтверждают свою подлинность с помощью сертификатов. Firefox не доверяет 10.20.30.1:8443, потому что издатель его сертификата неизвестен, сертификат является самоподписанным, или сервер не отправляет корректные промежуточные сертификаты.

Код ошибки: [SEC\\_ERROR\\_UNKNOWN\\_ISSUER](#)

[Просмотреть сертификат](#)

Вернуться назад (рекомендуется)      Принять риск и продолжить **2**

Залогиниться (Логин: **Admin** Пароль: **IdecoP@ssw0rd**)

**IDECO NGFW NOVUM**

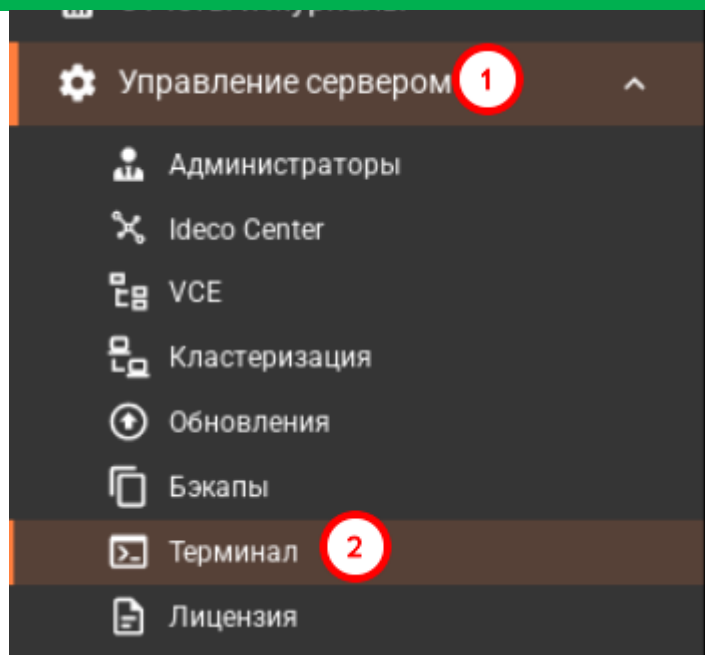
Логин **Admin**

Пароль **IdecoP@ssw0rd**

**Войти**

1. Настройка доменного имени

## Проверка.



Команда:

```
hostname
```

Вывод:

```
[admin@bez-nazvaniya-58d7182b-a2bb-4114-aefc-7ad496032041 ~]# hostname  
bez-nazvaniya-58d7182b-a2bb-4114-aefc-7ad496032041
```

## Настройка.

Команда:

```
hostnamectl set-hostname br-fw.au-team.irpo
```

Вывод:

```
[admin@bez-nazvaniya-58d7182b-a2bb-4114-aefc-7ad496032041 ~]# hostnamectl set-hostname br-fw.au-team.irpo  
[admin@bez-nazvaniya-58d7182b-a2bb-4114-aefc-7ad496032041 ~]# hostname  
br-fw.au-team.irpo
```

## 2. Настройка интерфейсов

### Проверка.

Команда:

```
ip a
```

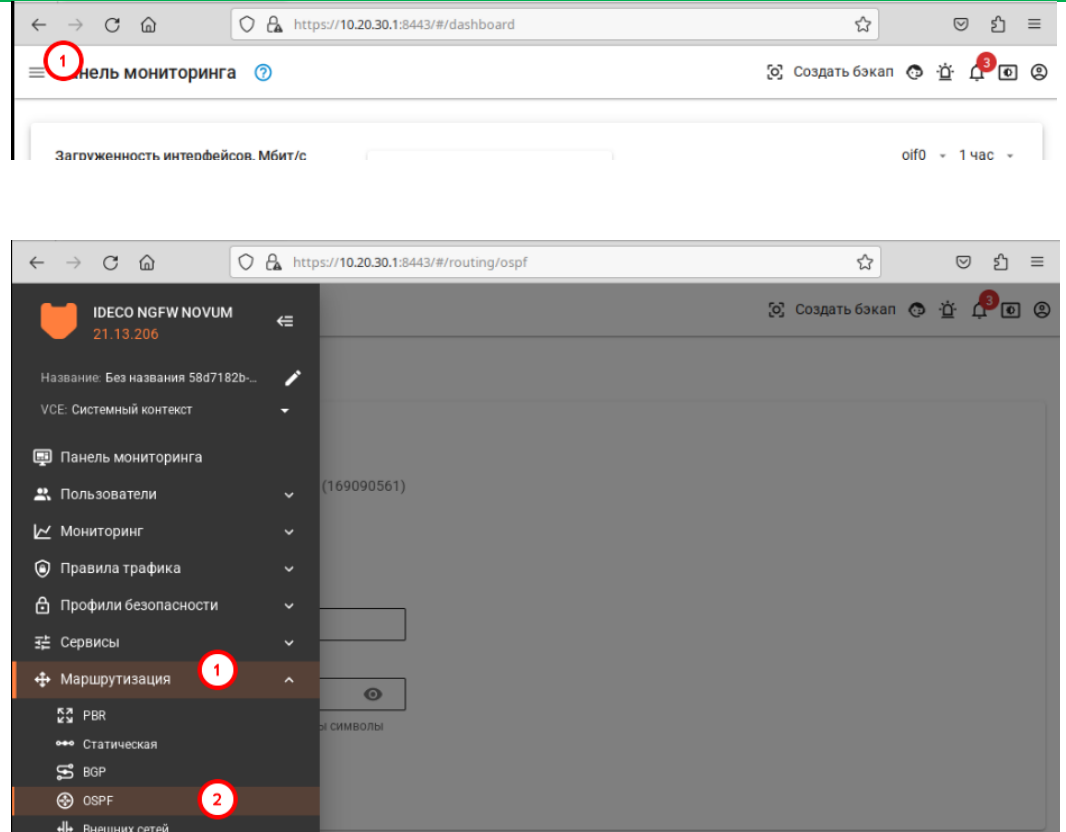
Вывод:

```
[admin@br-fw ~]# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet 169.254.254.254/32 scope global lo
    valid_lft forever preferred_lft forever
2: Leth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
  altnam enp0s3
  altnam ens3
  altnam phyport.id.eth0_00
  altnam interface.id.01KG87FX44MEJFRGDG1V33W7W4
  inet 10.20.10.2/30 scope global Leth2
    valid_lft forever preferred_lft forever
3: Leth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
  altnam enp0s4
  altnam ens4
  altnam phyport.id.eth1_01
  altnam interface.id.01KG87HCHSNM9G8MGZV4DFKNVV
  inet 10.20.20.1/28 scope global Leth3
    valid_lft forever preferred_lft forever
4: Leth4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
  altnam enp0s5
  altnam ens5
  altnam phyport.id.eth2_02
  altnam interface.id.01KG87JQVM82G1SN4JXT809V3W
  inet 10.20.30.1/29 scope global Leth4
    valid_lft forever preferred_lft forever
7: sw_dhcp1@sw_dhcp0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
```

Настройка не требуется

### 3. Настройка динамической маршрутизации (OSPF)

#### Настройка.



^ **Настройки**

Router ID ..... 10.20.30.1 (169090561)

**Аутентификация соседей**

Без пароля

**MD5**

Key ID

1

Целое число от 1 до 255

Пароль

..... P@sswOrd



Максимум 16 символов. Разрешены символы ASCII, кроме пробела.

**Сохранить**

**Локальные интерфейсы**

+ **Добавить**

☰ Фильтры

☰ Отображение

🔍 Поиск

☰ **OSPF** 6 ?  
Работает

**ОСНОВНЫЕ** ДОПОЛНИТЕЛЬНЫЕ

### Настройка OSPF на локальном интерфейсе

Интерфейс  1

Область (Area)  2 В  
Целое число от 0 до 4 294 967 295

Тип области  3  
Для области с номером «0» доступен только тип «Normal»

Стоимость  4  
Целое число от 1 до 65 535

#### Дополнительно

Целое число от 1 до 65 535

Целое число от 1 до 65 535

5

#### 4. Настройка часового пояса

Проверка.

Команда:

```
timedatectl
```

Вывод:

```
(root@isp ~)# timedatectl
    Local time: Sun 2026-04-05 14:18:20 MSK
    Universal time: Sun 2026-04-05 11:18:20 UTC
    RTC time: Sun 2026-04-05 11:18:20
    Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
    NTP service: active
    RTC in local TZ: no
```

Настройка не требуется

**BR-FW НАСТРОЕН**