ClientSPB

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.5.55/28

Шлюз 100.70.5.49

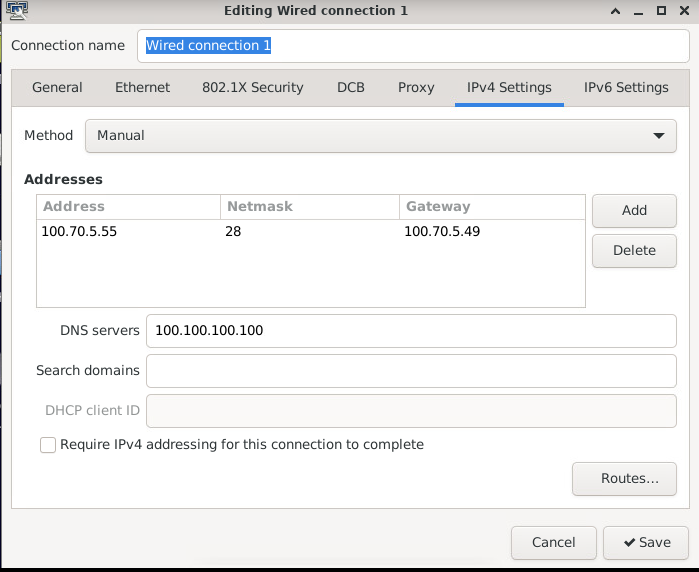
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



VDS

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.6.12/29

Шлюз 100.70.6.9

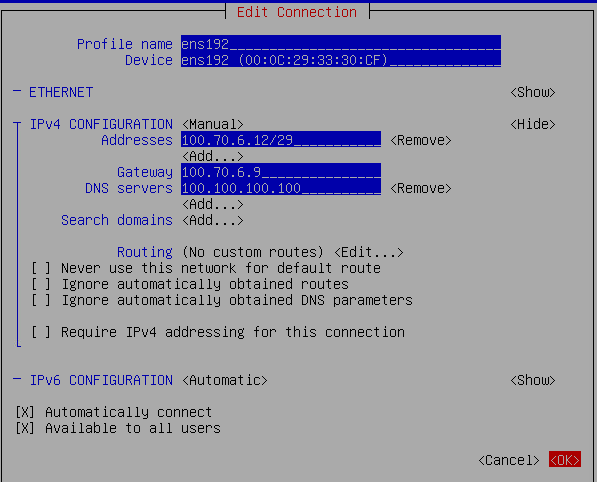
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



ClientEU

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.5.55/28

Шлюз 100.70.5.49

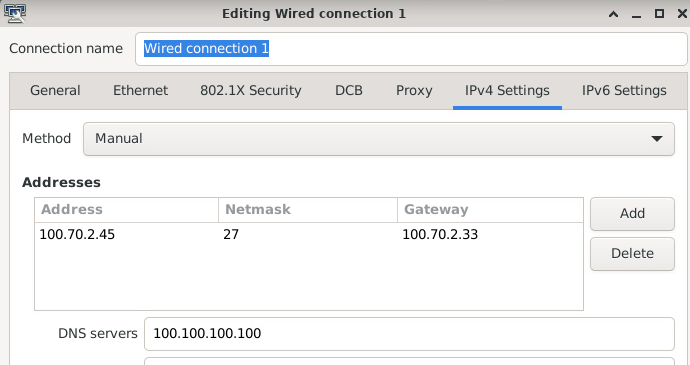
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



VPNClient

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.6.13/29

Шлюз 100.70.6.9

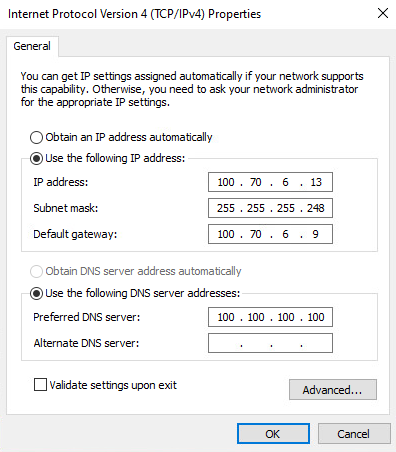
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

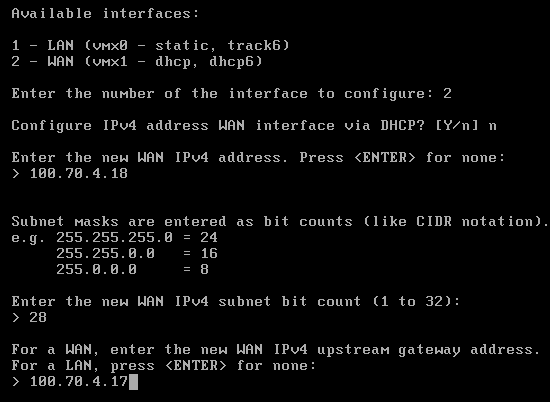
ping ya.ru

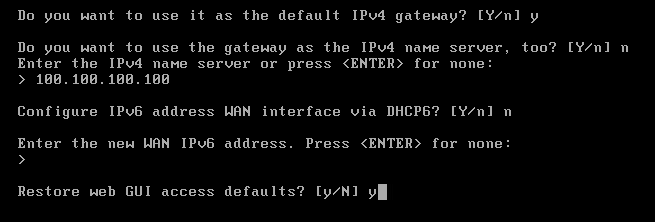


FW-AMS

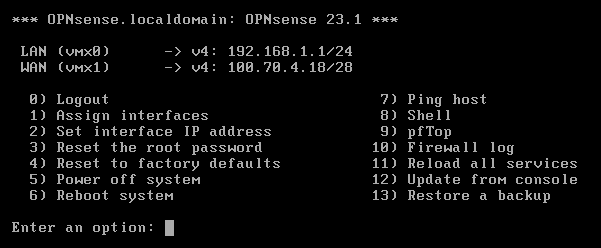
FW-MSK

Выбираем опцию 2 (Set interface IP address)





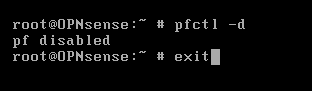
Получаем



Выбираем опцию 8 (Shell)

Вводим команду pfctl -d

Выходим из shell командой exit



Проверка

С ClientSPB

через терминал

ping 100.70.4.18

через браузер

<http://100.70.4.18>

Открываем внешний доступ на FW-MSK

На ClientSPB заходим через браузер 100.70.4.18

Переходим Firewall – Rules – WAN и создаем разрешающее правило

Сохраняем, НО не применяем

Переходим Interfaces – WAN и убираем галочку Block private networks

Сохраняем и применяем настройки

Ждем применения правил. ДОСТУП ПОЛУЧЕН!

Через браузер настраиваем FW-MSK

LAN – 192.168.10.1/24

DMZ – 192.168.20.1/24

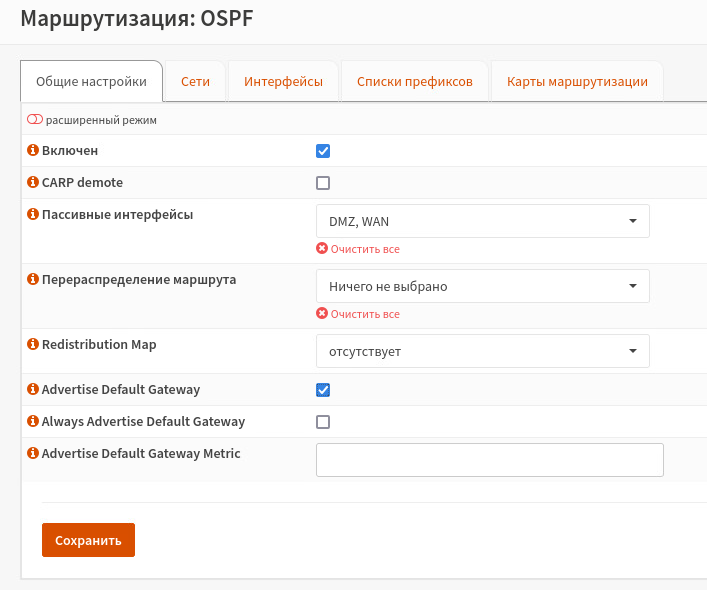
Службы – DHCPv4 – LAN убираем галочку Включен

Обновляем OPNSense (через консоль выбираем опцию 12)

Система – Программное обеспечение – Плагины – os-frr (устанавливаем)

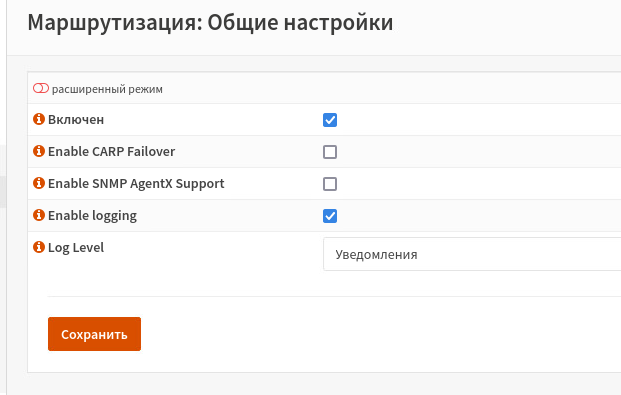
Настраиваем OSPF

Маршрутизация – OSPF





Маршрутизация – Общие настройки



R0

configure

show interfaces

edit interfaces ethernet eth0

set address 192.168.10.2/24

set description FW

exit

edit interfaces ethernet eth1

set address 192.168.11.1/24

set description PC

exit

edit interfaces ethernet eth2

set address 192.168.12.1/24

set description PC

exit

commit

save

show interfaces

set protocols ospf area 0 network 192.168.10.0/24

set protocols ospf area 0 network 192.168.11.0/24

set protocols ospf area 0 network 192.168.12.0/24

set protocols ospf interface eth1 passive

set protocols ospf interface eth2 passive

commit

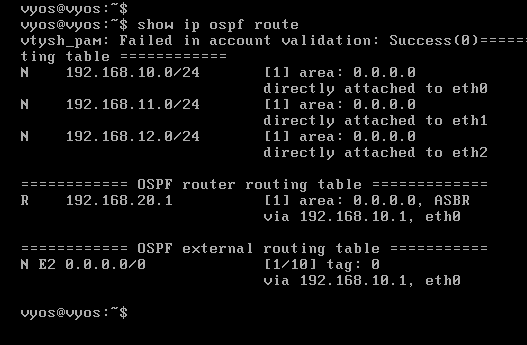
save

show protocols ospf

Проверка

exit

show ip ospf route



SRV1-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

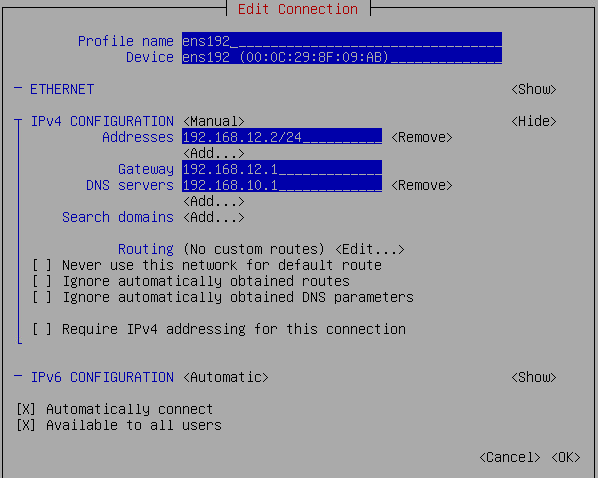
Адрес 192.168.12.2/24

Шлюз 192.168.12.1

DNS 192.168.10.1 (адрес интерфейса LAN на FW-MSK)

Проверка:

ping 192.168.12.1



SRV2-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

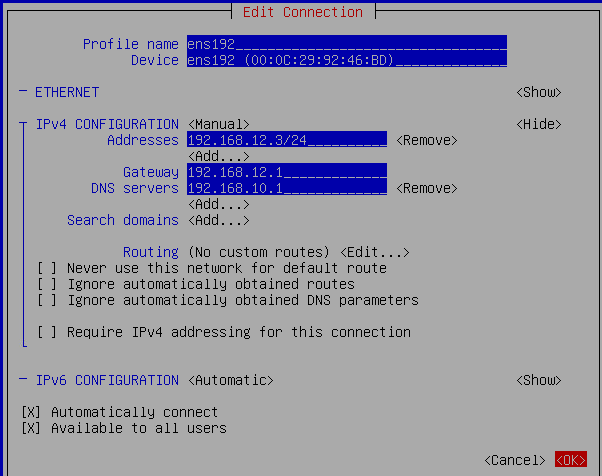
Адрес 192.168.12.3/24

Шлюз 192.168.12.1

DNS 192.168.10.1 (адрес интерфейса LAN на FW-MSK)

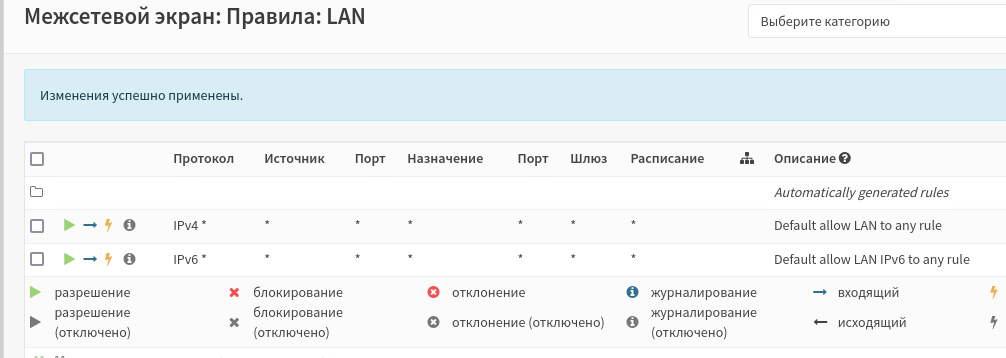
Проверка:

ping 192.168.12.1

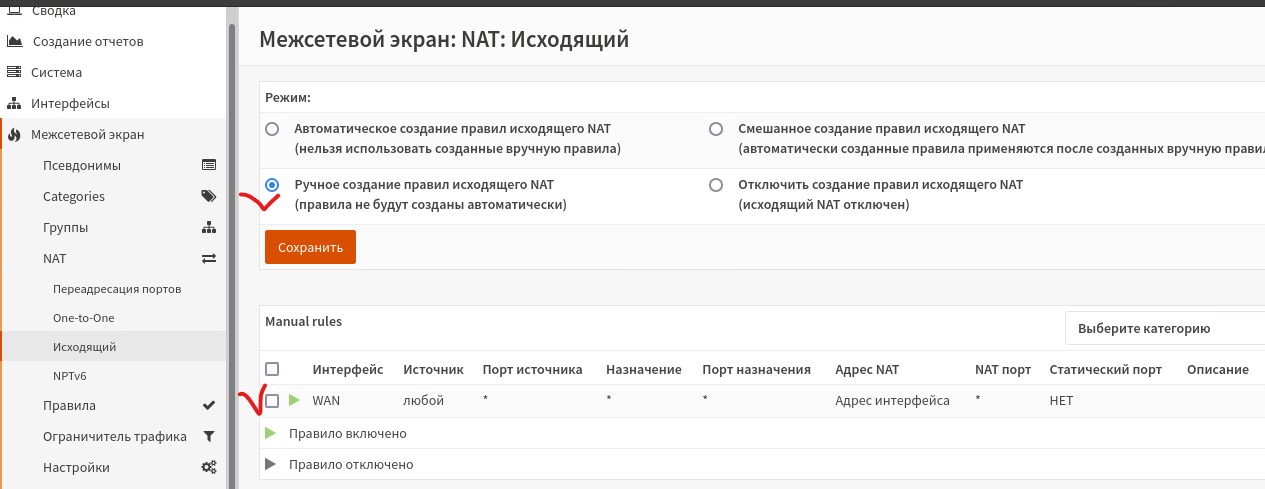


Чтобы клиенты сети LAN-MSK и SRV-MSK имели доступ в интернет, необходимо на FW-MSK подправить правила Межсетевого экрана на интерфейсе LAN, настроить NAT и включить перенаправление DNS запросов

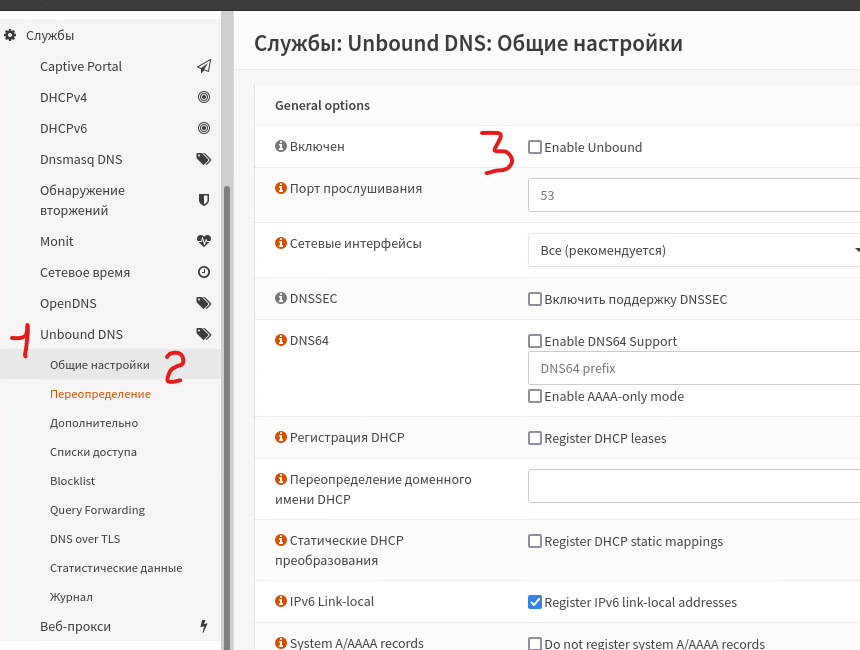
1) Правила Межсетевого экрана на интерфейсе LAN



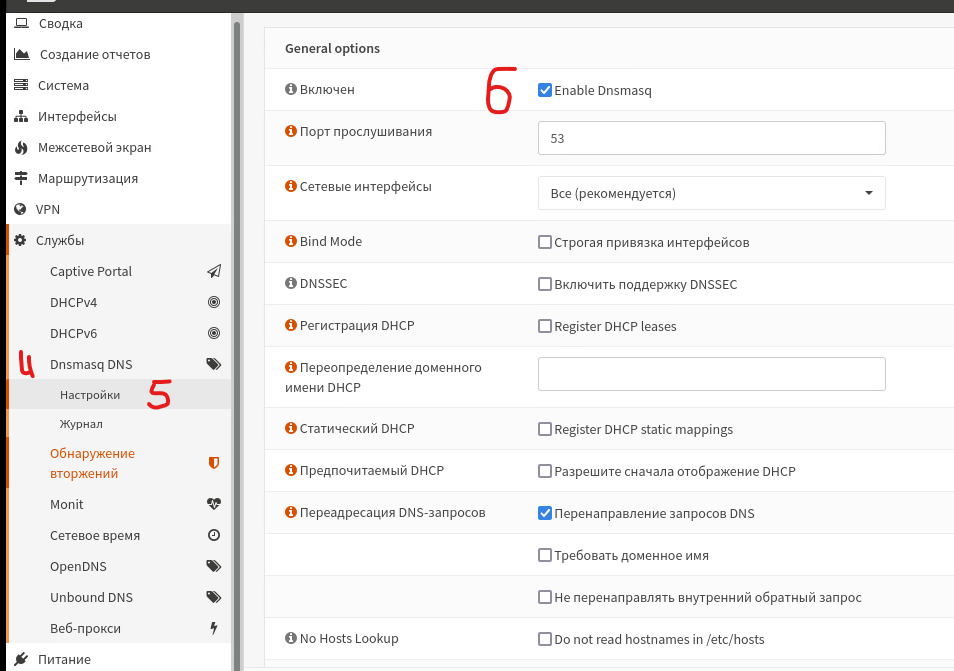
2) Правила NAT



3) Перенаправление DNS запросов



Сохранить настройки



Сохранить настройки

Проверка

На SRV-MSK1 – ping 8.8.8.8 и ping ya.ru

На SRV-MSK2 – ping 8.8.8.8 и ping ya.ru

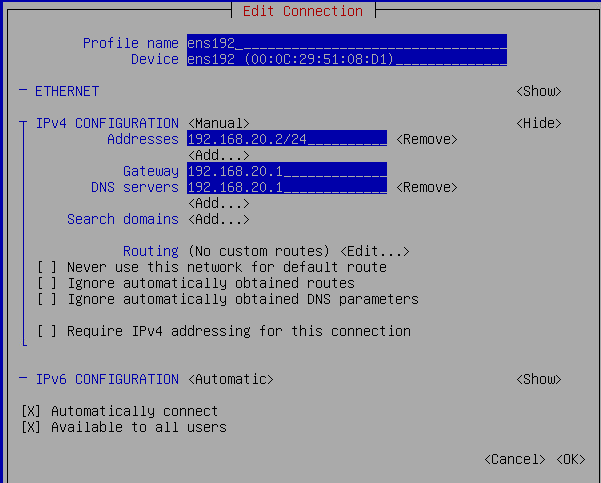
APP-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

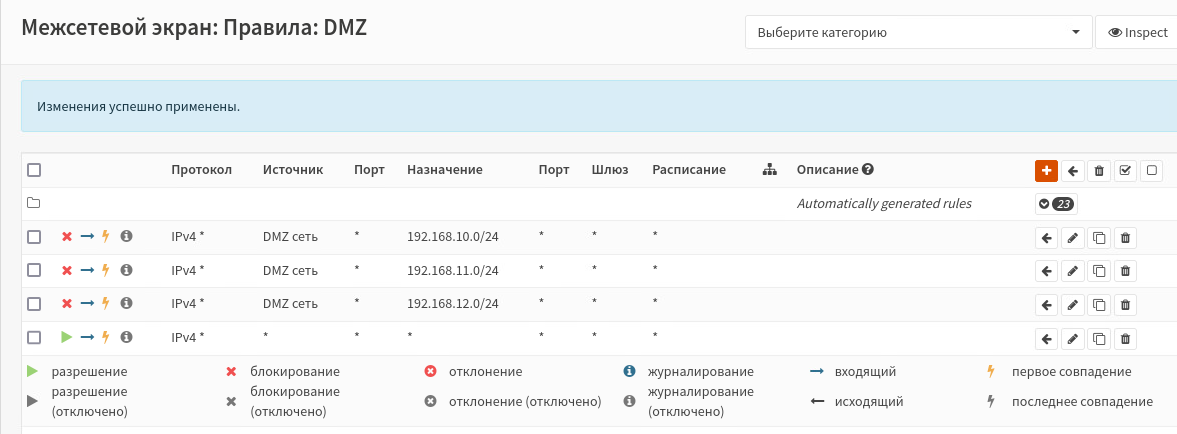
Адрес 192.168.20.2/24

Шлюз 192.168.20.1

DNS 192.168.20.1 (адрес интерфейса DMZ на FW-MSK)



Чтобы клиенты сети DMZ-MSK имели доступ в интернет и не имели доступ к сети LAN-MSK и SRV-MSK, необходимо на FW-MSK создать правило Межсетевого экрана на интерфейсе DMZ



Проверка:

ping 192.168.12.2 – доступа нет

ping 192.168.12.3 – доступа нет

ping 192.168.11.1 – доступа нет

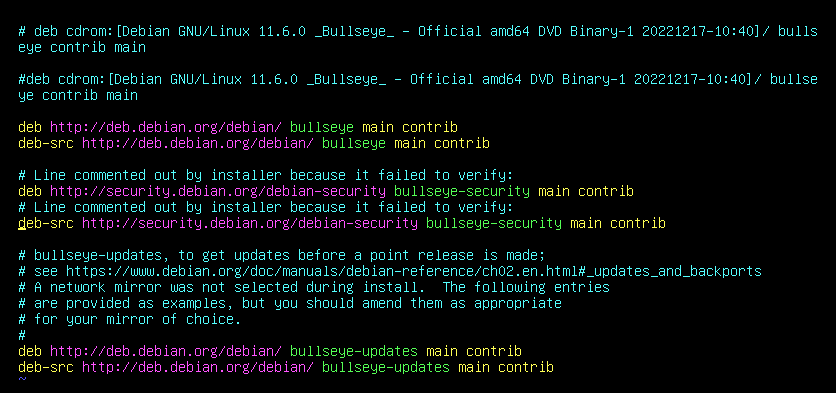
ping 100.100.100.100 – доступ есть

ping ya.ru – доступ есть

Настройка DHCP

SRV1-MSK

nano /etc/apt/sources.list

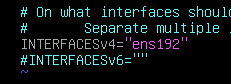


apt update

apt list --upgradable

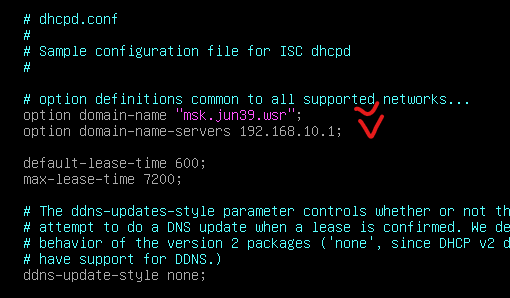
apt install isc-dhcp-server

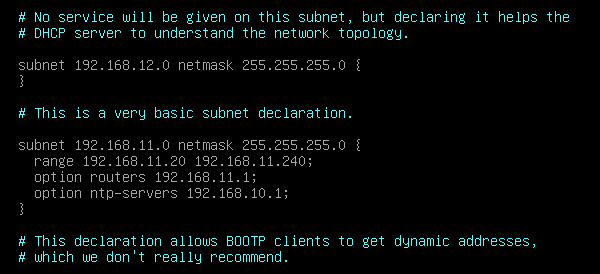
nano /etc/default/isc-dhcp-server



reboot

nano /etc/dhcp/dhcpd.conf





systemctl restart isc-dhcp-server

systemctl status isc-dhcp-server



R0

configure

set service dhcp-relay interface eth1

set service dhcp-relay interface eth2

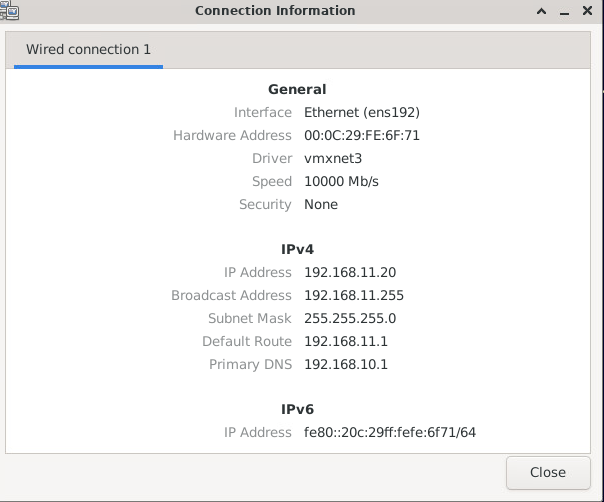
set service dhcp-relay server 192.168.12.2

commit

save

PC-MSK

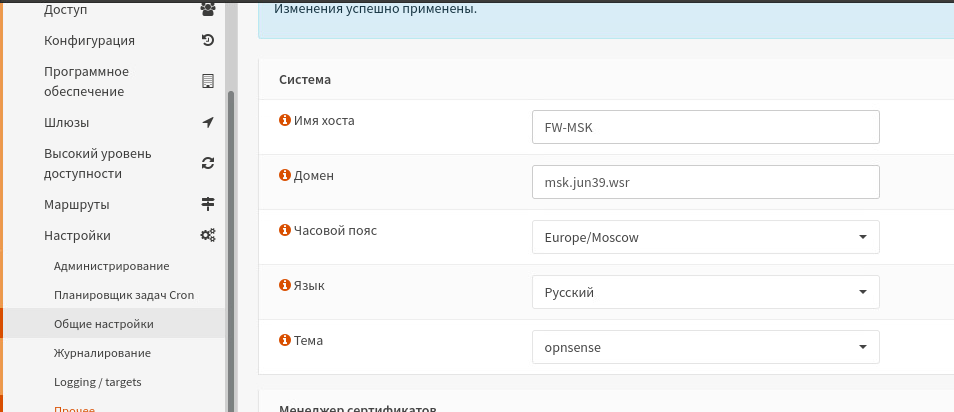
Пробуем получить адрес по DHCP



ping ya.ru

Настройка имени, доменного имени, часового пояса

FW-MSK



SRV1-MSK

hostnamectl set-hostname SRV1-MSK.msk.jun39.wsr

timedatectl set-timezone Europe/Moscow

SRV2-MSK

hostnamectl set-hostname SRV2-MSK.msk.jun39.wsr

timedatectl set-timezone Europe/Moscow

PC-MSK

hostnamectl set-hostname PC-MSK.msk.jun39.wsr

timedatectl set-timezone Europe/Moscow

R0

configure

set system host-name R0-MSK

set system domain-name msk.jun39.wsr

set system time-zone Europe/Moscow

set service ntp server 192.168.10.1

commit

save

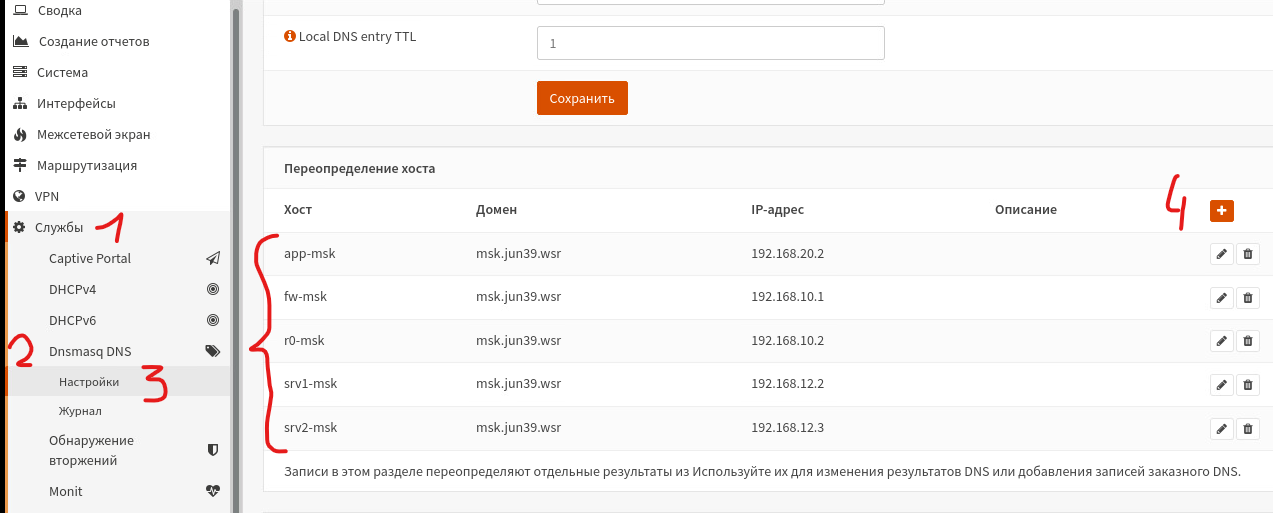
APP-MSK

hostnamectl set-hostname APP-MSK.msk.jun39.wsr

timedatectl set-timezone Europe/Moscow

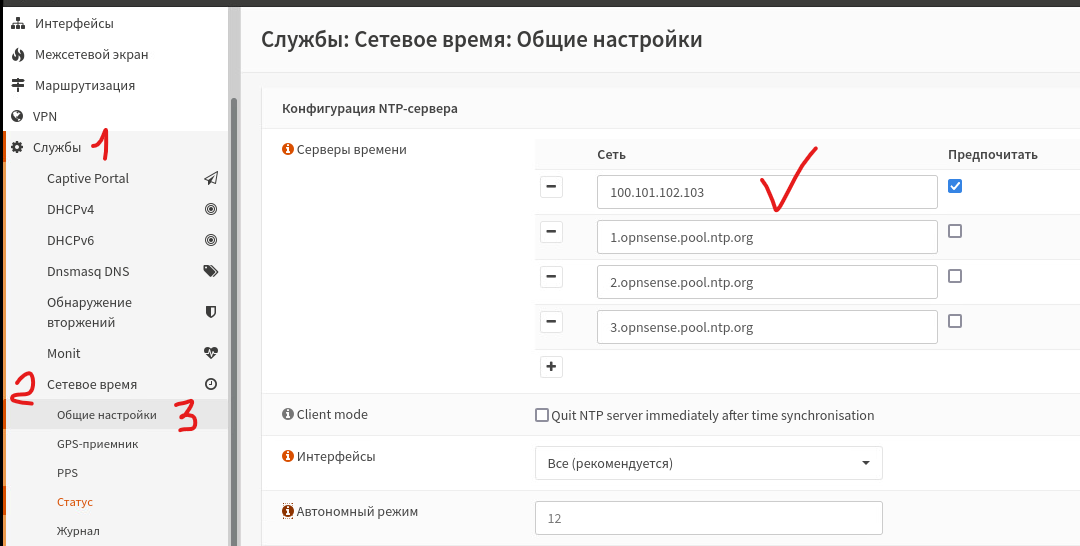
Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией

FW-MSK



Настройка синхронизации времени

FW-MSK



SRV1-MSK

apt install chrony

nano /etc/chrony/chrony.conf

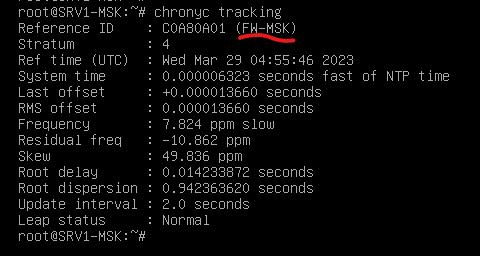


systemctl restart chrony

systemctl status chrony

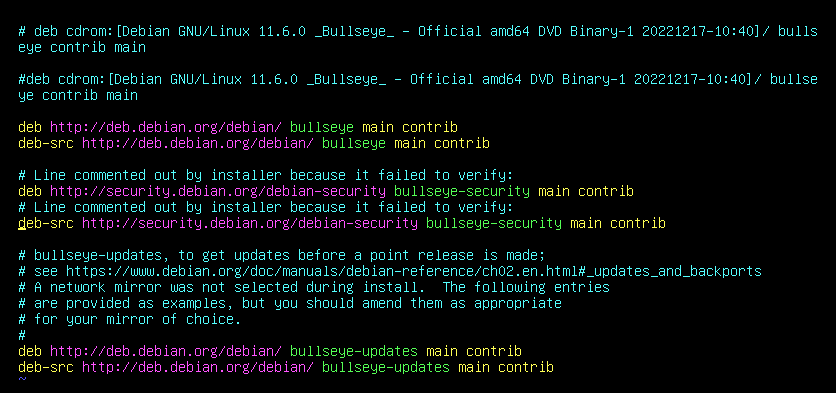
Проверка

chronyc tracking



SRV2-MSK

nano /etc/apt/sources.list



apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf

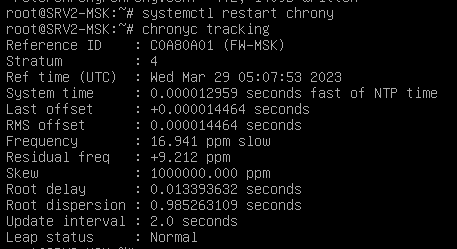


systemctl restart chrony

systemctl status chrony

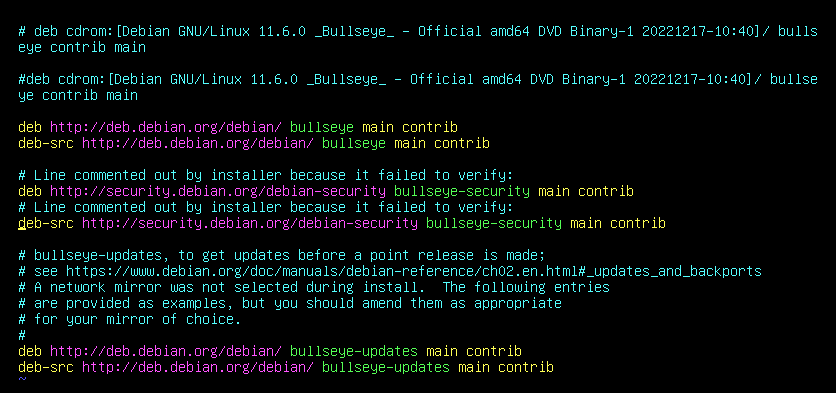
Проверка

chronyc tracking



APP-MSK

nano /etc/apt/sources.list



apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf

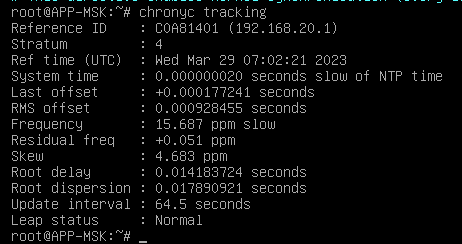


systemctl restart chrony

systemctl status chrony

Проверка

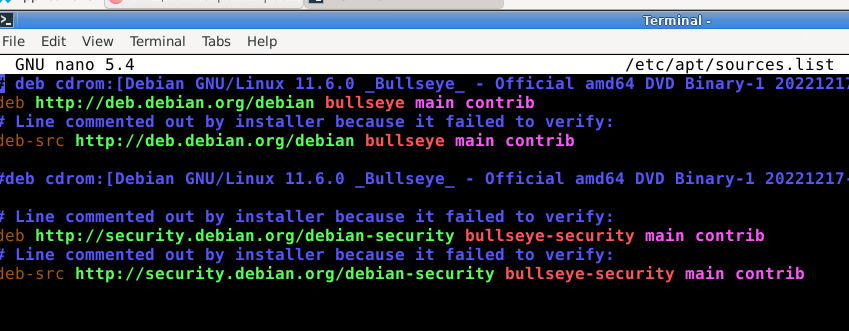
chronyc tracking



ClientSPB

timedatectl set-timezone Europe/Moscow

nano /etc/apt/sources.list

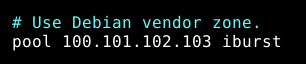


apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf



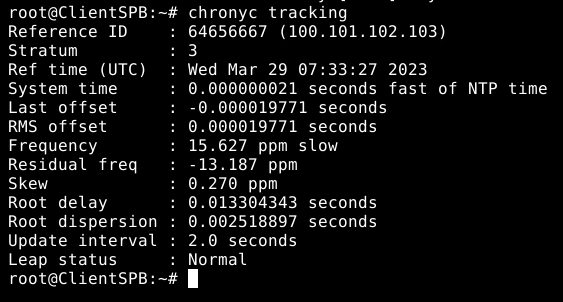
systemctl restart chrony

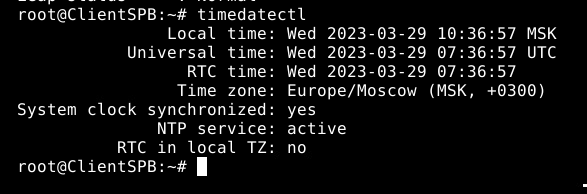
systemctl status chrony

Проверка

chronyc tracking

timedatectl

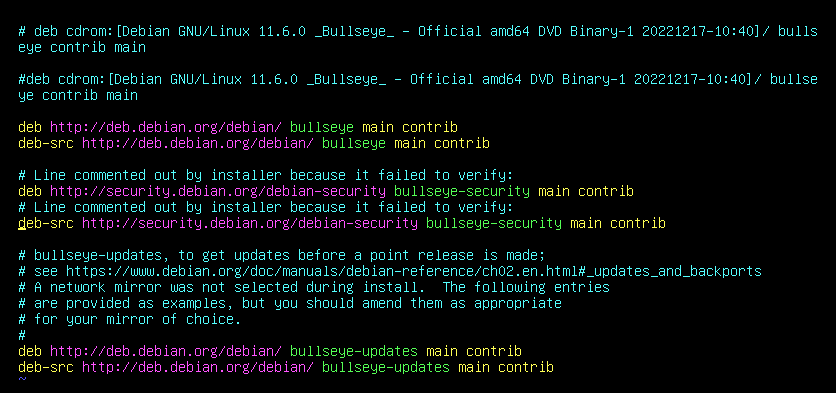




VDS

timedatectl set-timezone Asia/Yekaterinburg

nano /etc/apt/sources.list

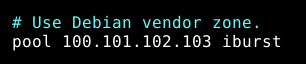


apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf



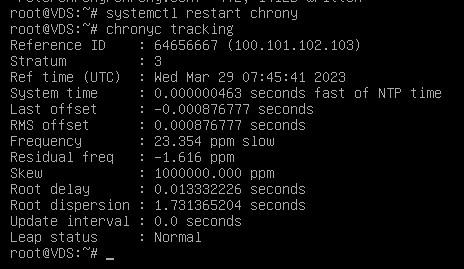
systemctl restart chrony

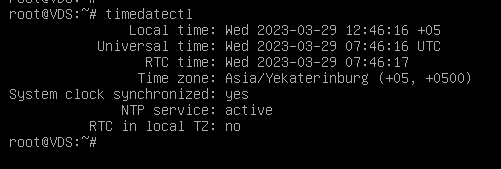
systemctl status chrony

Проверка

chronyc tracking

timedatectl





Сетевое обнаружение по протоколу LLDP

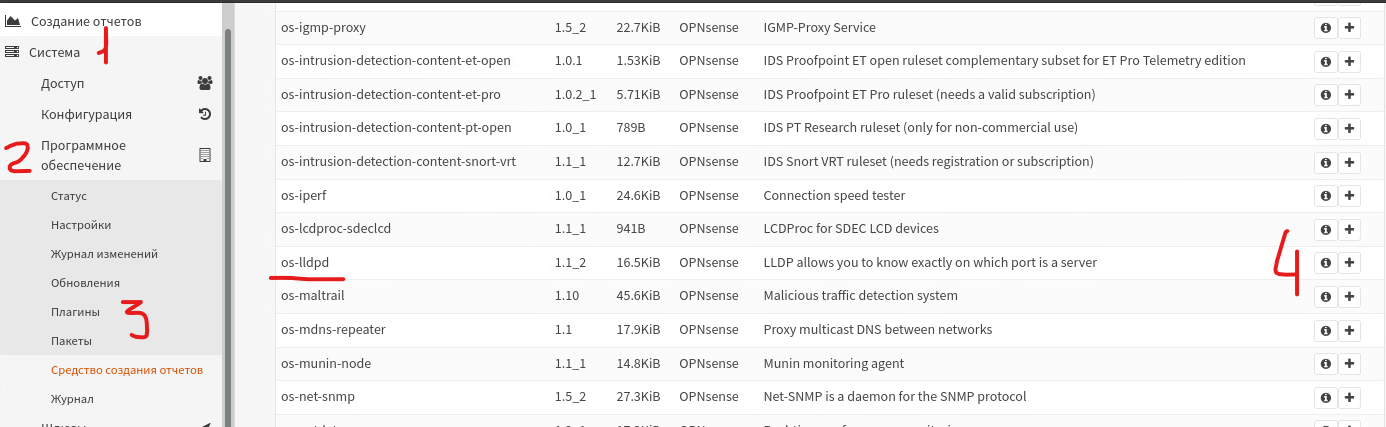
SRV1-MSK, SRV2-MSK, APP-MSK

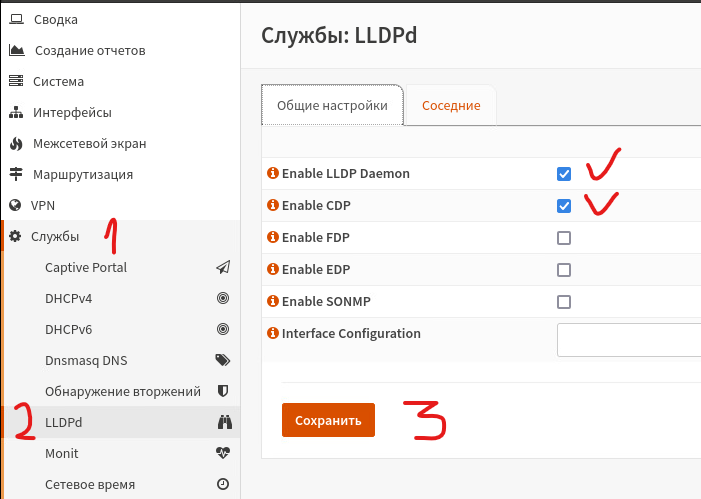
apt install lldpd

Проверка

llpdctl

FW-MSK





R0

configure

set service lldp

commit

save

Проверка

show lldp neighbors

Удаленный доступ по SSH

R0

configure

set service ssh port 22

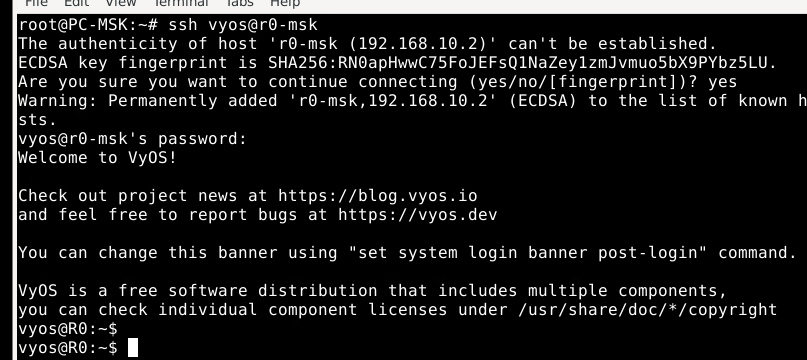
commit

save

Проверка

С PC-MSK подключаемся по SSH

ssh vyos@r0-msk



VDS

apt install ssh

systemctl status sshd

su user

mkdir /home/user/.ssh

На PC-MSK заходим под пользователем user с паролем P@ssw0rd

ssh-keygen

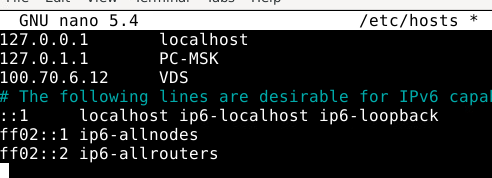
cd /home/user/.ssh/

ls -l

scp id\_rsa.pub user@100.70.6.12:/home/user/.ssh/authorized\_keys

su root

nano /etc/hosts



exit

Проверка

ssh user@VDS



Офис AMS

На FW-AMS

WAN – 100.70.3.45/26, шлюз 100.70.3.1, DNS 100.100.100.100

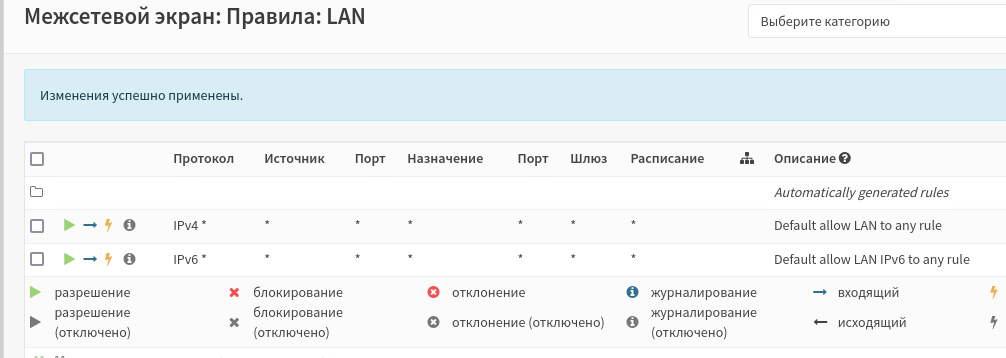
DMZ – 192.168.2.1/24

Обновляем OPNSense (через консоль выбираем опцию 12)

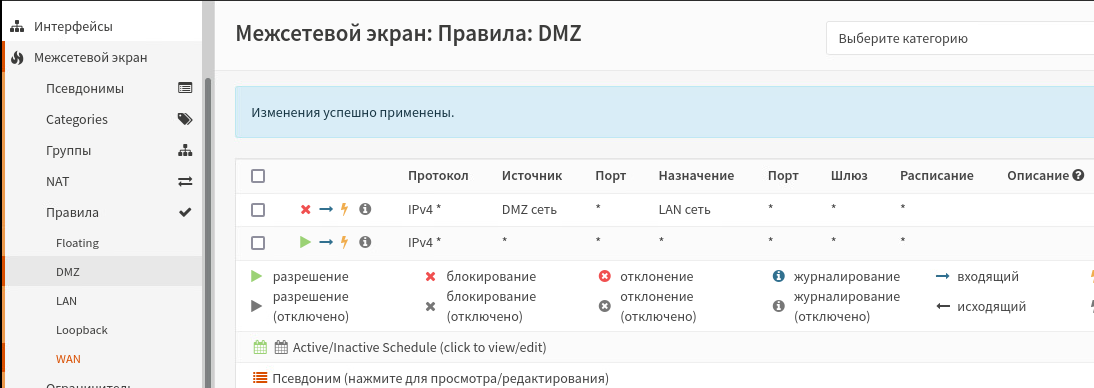
Система – Программное обеспечение – Плагины – os-frr и lldp (устанавливаем)

Настраиваем Межсетевой экран

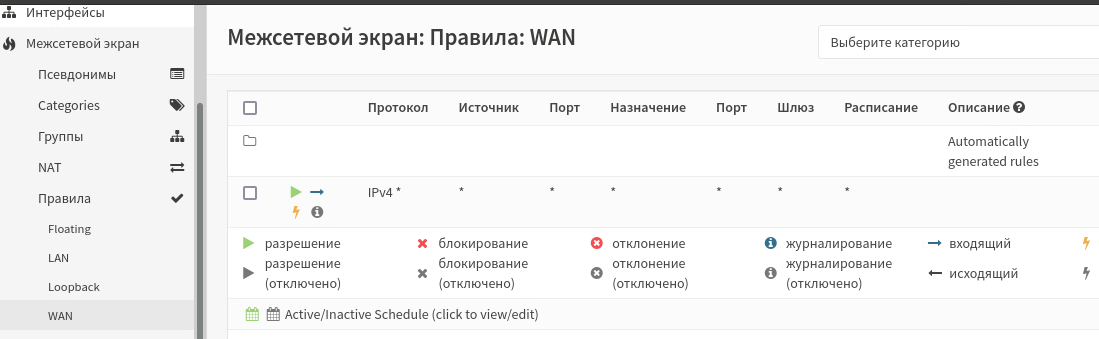
1) на интерфейсе LAN



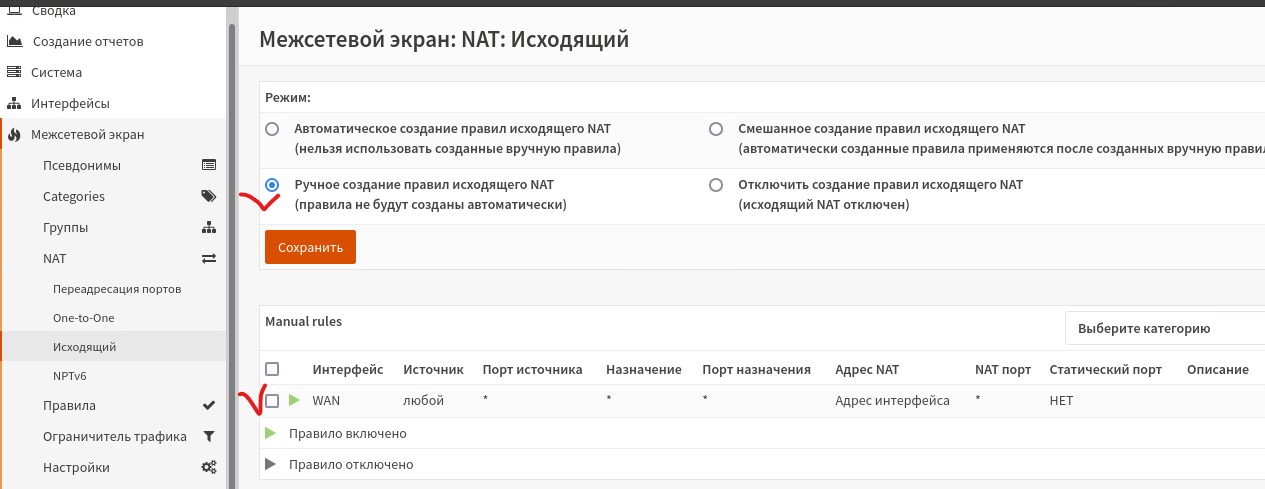
2) на интерфейсе DMZ



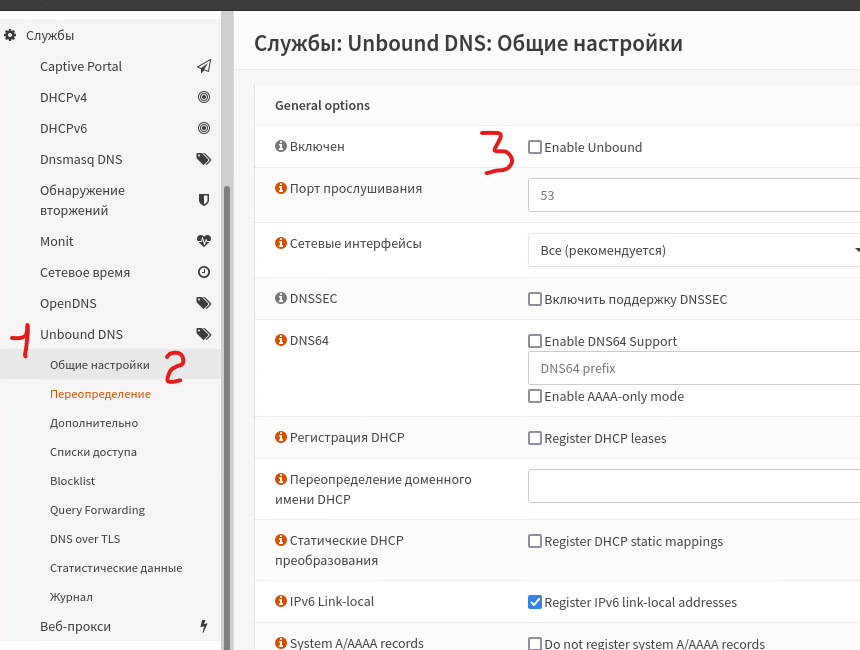
3) на интерфейсе WAN



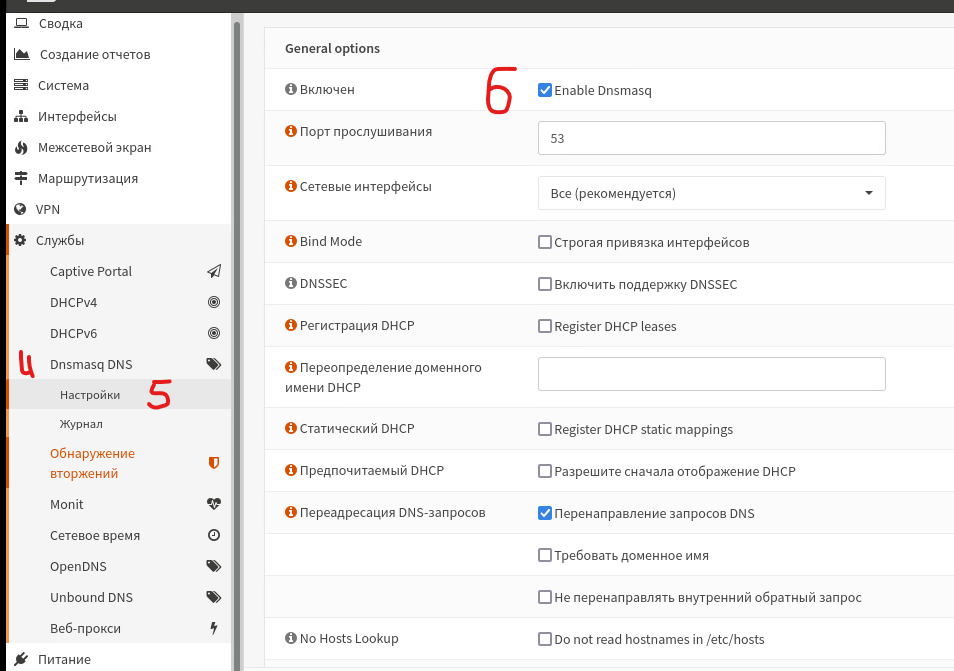
4) Правила NAT



Настраиваем перенаправление DNS запросов



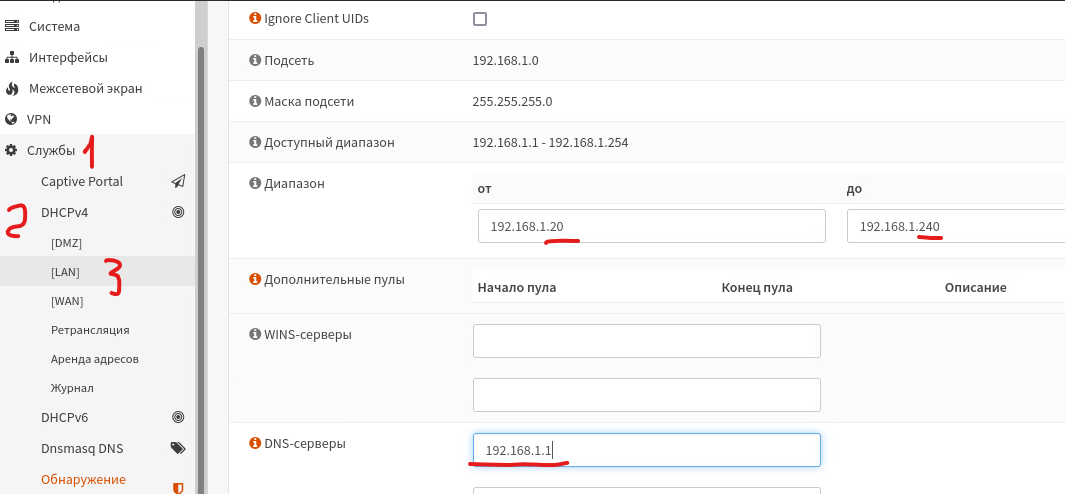
Сохранить настройки

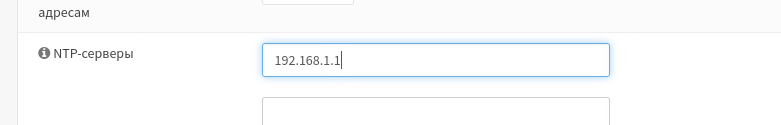


Проверка

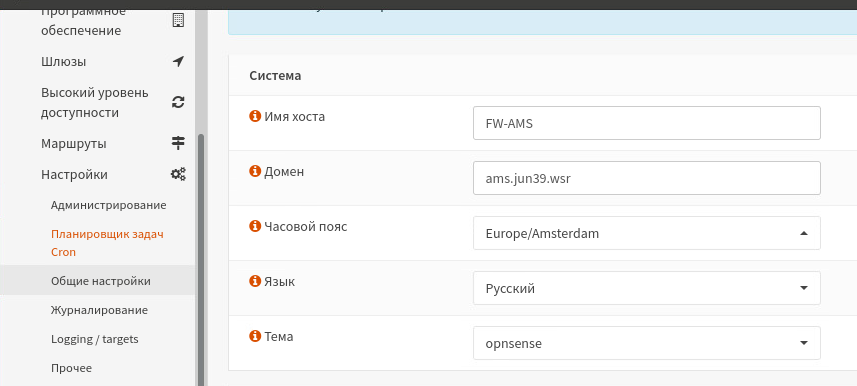
На PC-AMS – ping 8.8.8.8 и ping ya.ru

Настройка DHCP на интерфейсе LAN

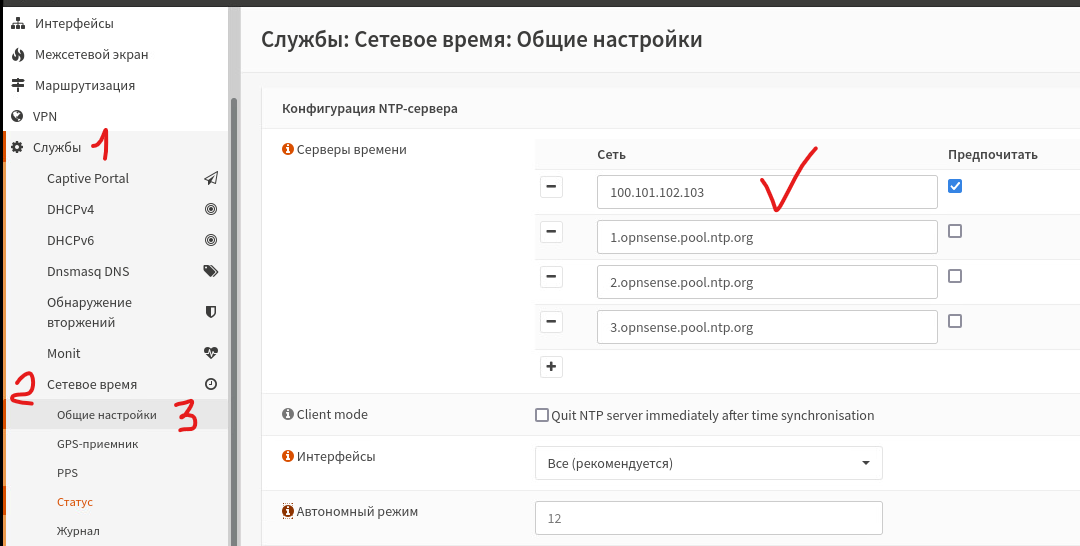




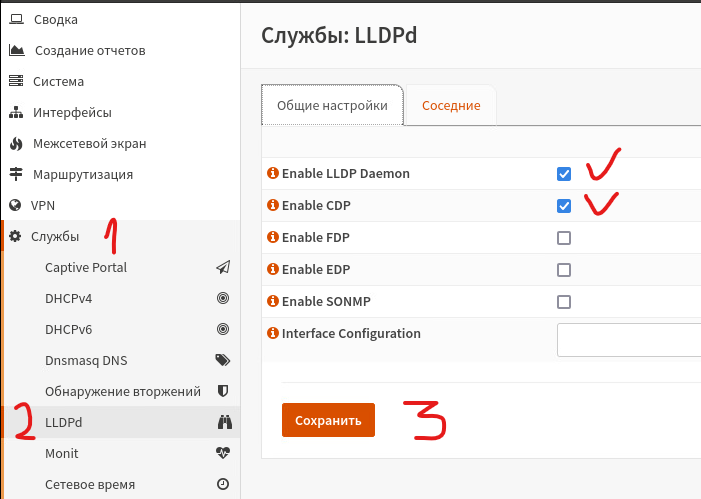
Настройка имени, доменного имени, часового пояса



Настройка синхронизации времени



Настройка LLDP



Настройка доступа по именам



DMZ-AMS

1) Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.2.2/24

Шлюз 192.168.2.1

DNS 192.168.2.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

hostnamectl set-hostname DMZ-AMS.ams.jun39.wsr

timedatectl set-timezone Europe/Amsterdam

apt install chrony

nano /etc/chrony/chrony.conf



systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

3) Устанавливаем LLDP

apt install lldpd

Проверка

llpdctl

APP-AMS

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.2.3/24

Шлюз 192.168.2.1

DNS 192.168.2.1

Проверка:

ping 192.168.2.2 и ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

hostnamectl set-hostname APP-AMS.ams.jun39.wsr

timedatectl set-timezone Europe/Amsterdam

apt install chrony

nano /etc/chrony/chrony.conf



systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

3) Устанавливаем LLDP

apt install lldpd

Проверка

llpdctl

PC-AMS

Устанавливаем имя, время и часовой пояс

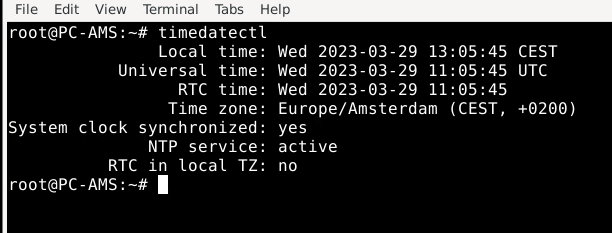
hostnamectl set-hostname PC-AMS.ams.jun39.wsr

timedatectl set-timezone Europe/Amsterdam

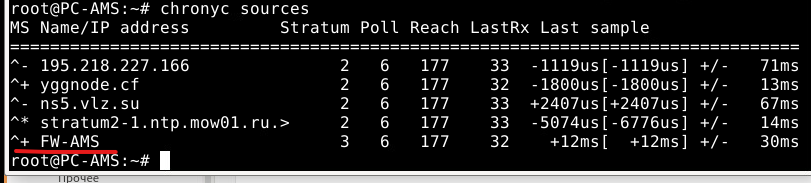
apt install chrony

Проверка

timedatectl



chronyc sources



Офис IKT

На FW-IKT

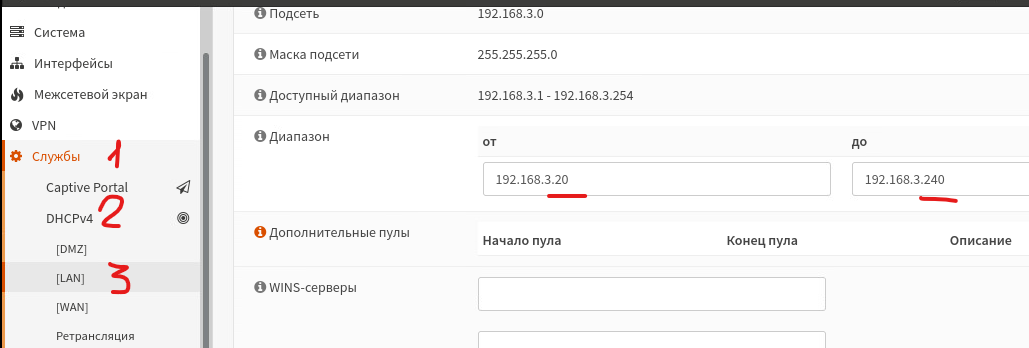
WAN – 100.70.7.99/25, шлюз 100.70.7.1, DNS 100.100.100.100

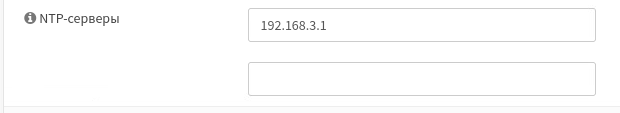
DMZ – 192.168.4.1/24

Обновляем OPNSense (через консоль выбираем опцию 12)

Система – Программное обеспечение – Плагины – os-frr и lldp (устанавливаем)

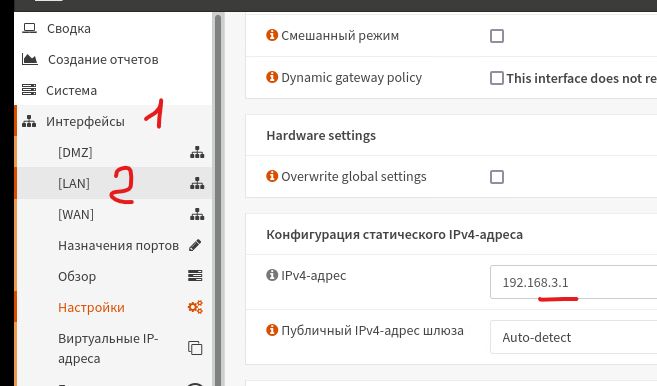
Меняем настройки DHCP сервера





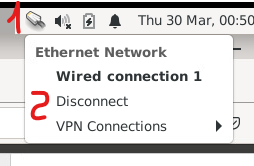
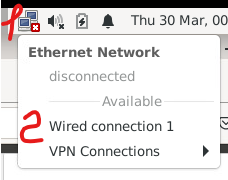
Сохраняем, но настройки НЕ ПРИМЕНЯЕМ

Меняем адрес на LAN

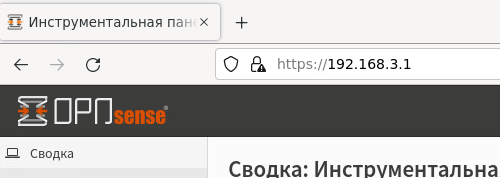


Сохраняем, применяем настройки. ТЕРЯЕТСЯ ДОСТУП!

На PC-IKT перезапускаем сетевой интерфейс

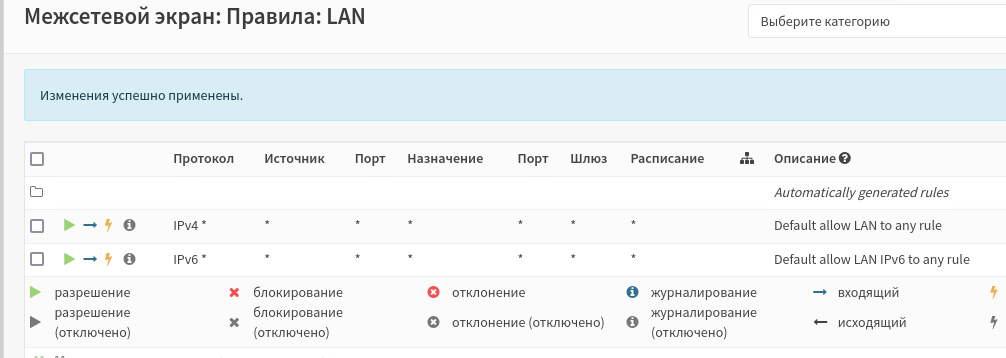
 

ПОЯВЛЯЕТСЯ ДОСТУП по новому адресу

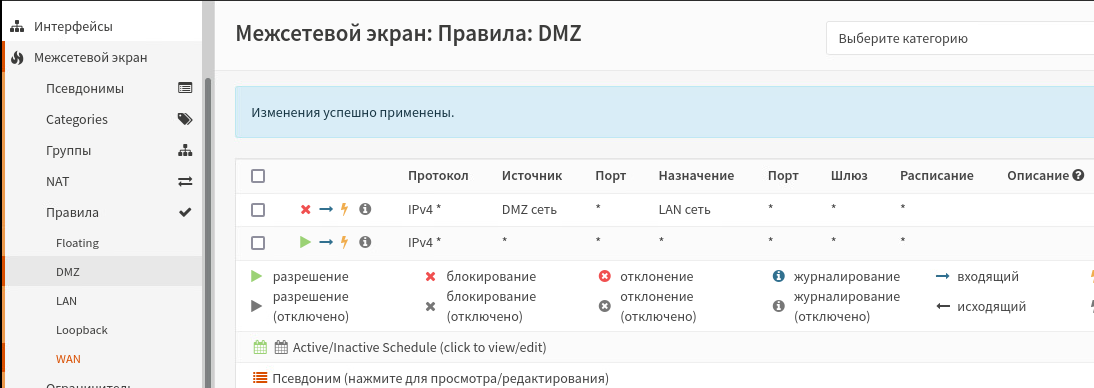


Настраиваем Межсетевой экран

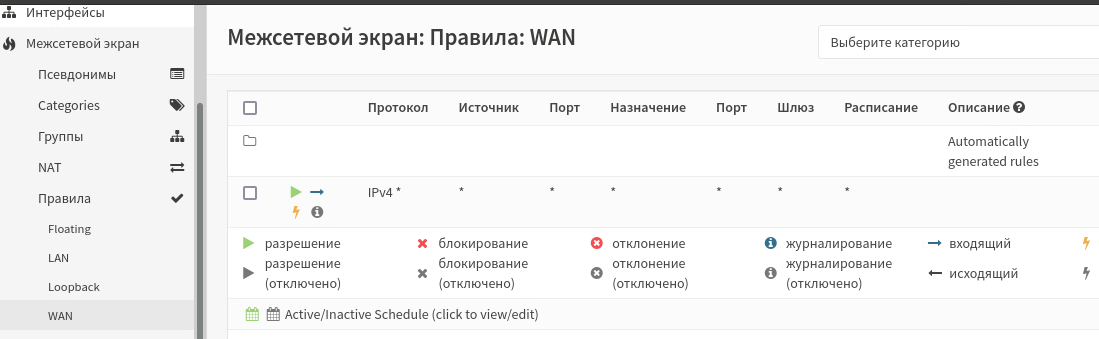
1) на интерфейсе LAN



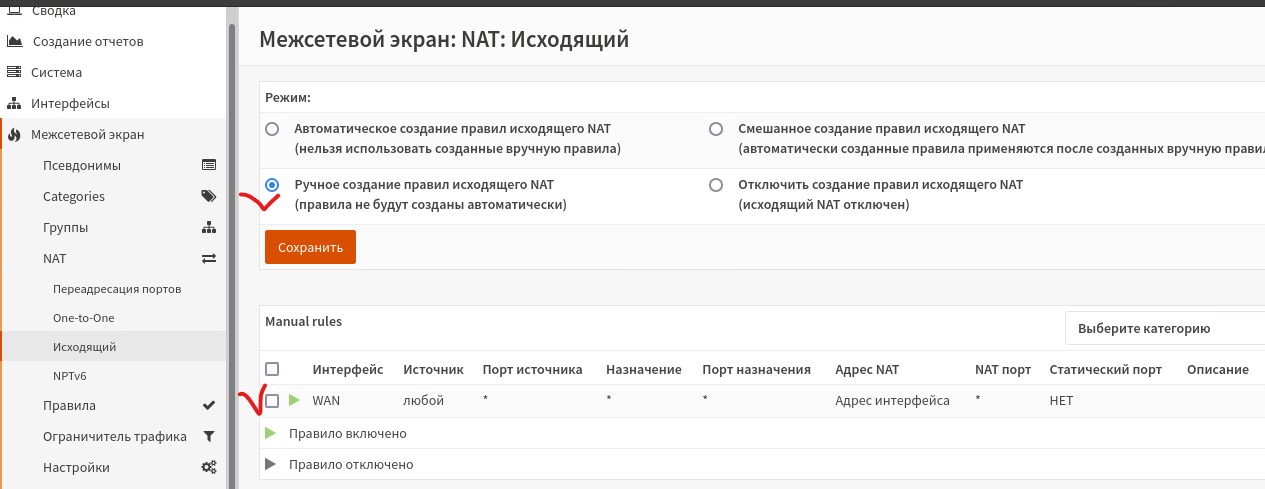
2) на интерфейсе DMZ



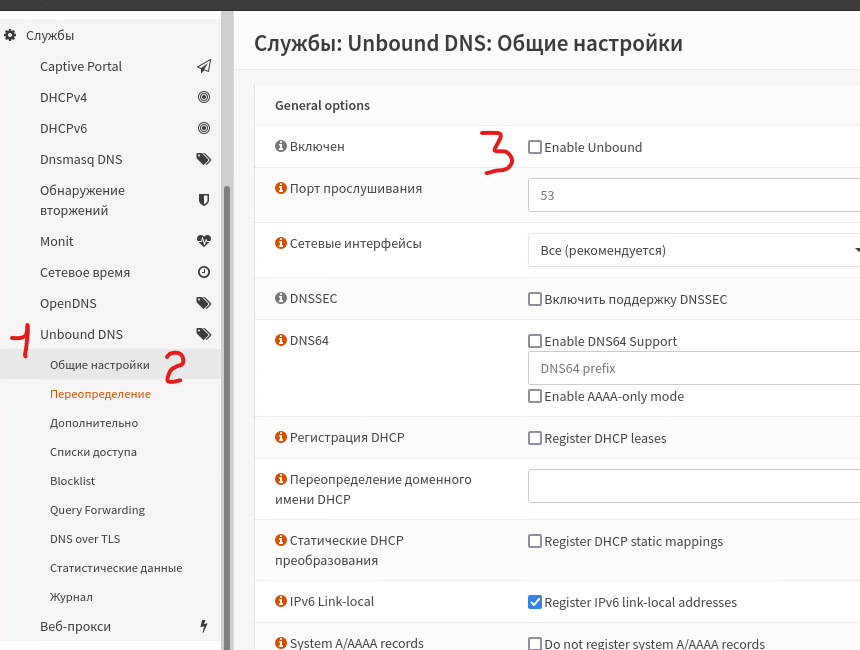
3) на интерфейсе WAN



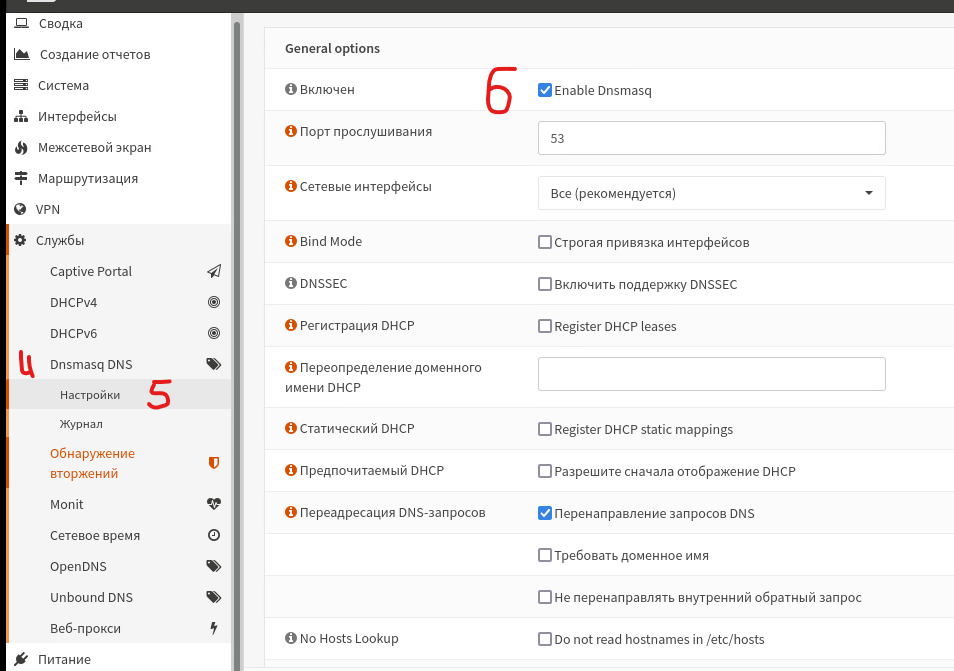
4) Правила NAT



Настраиваем перенаправление DNS запросов



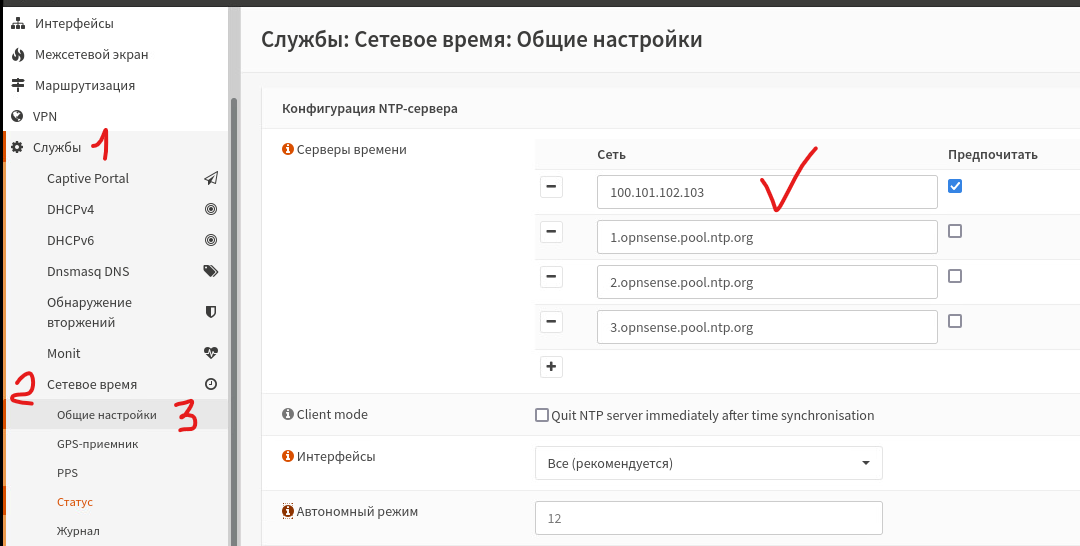
Сохранить настройки



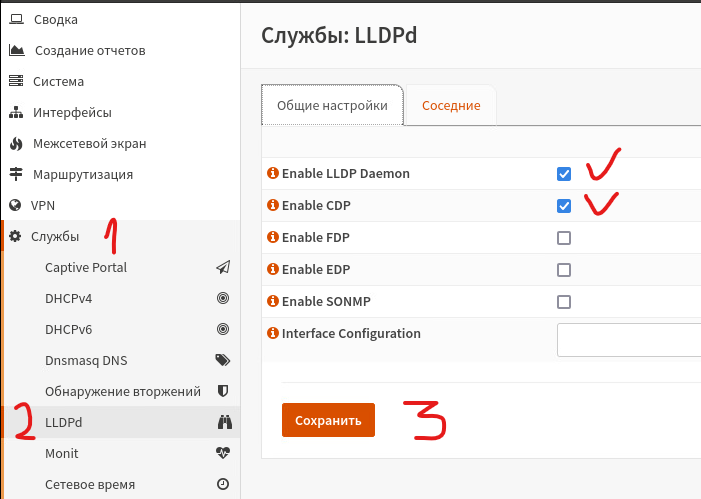
Проверка

На PC-IKT – ping 8.8.8.8 и ping ya.ru

Настройка синхронизации времени



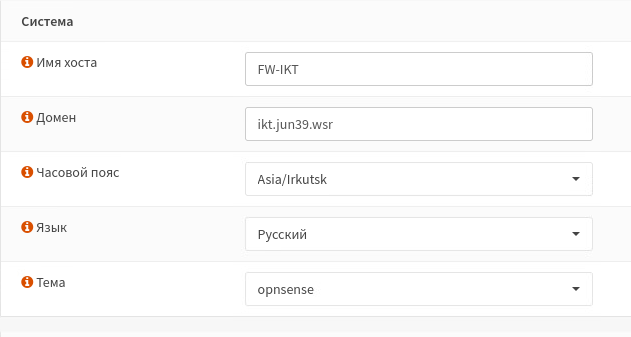
Настройка LLDP



Настройка доступа по именам



Общие настройки



PC-IKT

Устанавливаем имя, время и часовой пояс

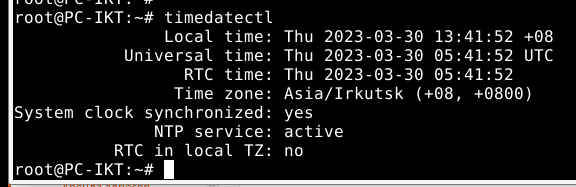
hostnamectl set-hostname PC-IKT.ikt.jun39.wsr

timedatectl set-timezone Asia/Irkutsk

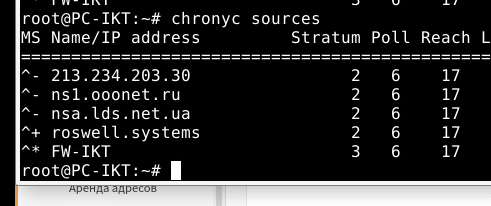
apt install chrony

Проверка

timedatectl



chronyc sources



SRV1-IKT

1) Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.3.2/24

Шлюз 192.168.3.1

DNS 192.168.3.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

hostnamectl set-hostname SRV1-IKT.ikt.jun39.wsr

timedatectl set-timezone Asia/Irkutsk

apt install chrony

nano /etc/chrony/chrony.conf



systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

3) Устанавливаем LLDP

apt install lldpd

Проверка

llpdctl

APP-IKT

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.4.3/24

Шлюз 192.168.4.1

DNS 192.168.4.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

hostnamectl set-hostname APP-IKT.ikt.jun39.wsr

timedatectl set-timezone Asia/Irkutsk

apt install chrony

nano /etc/chrony/chrony.conf



systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

3) Устанавливаем LLDP

apt install lldpd

Проверка

llpdctl

ClientVV

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.8.78/28

Шлюз 100.70.8.65

DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

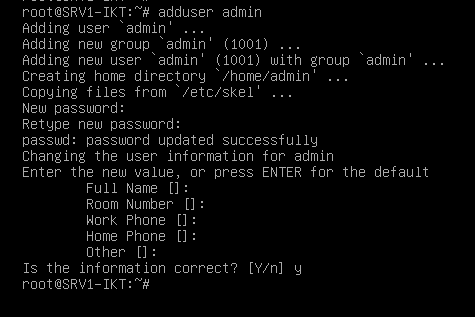
ping ya.ru

Создание пользователя

SRV1-ITK

apt install sudo

adduser admin



usermod -aG sudo admin

Проверка

groups admin



Настройка NFS сервера

SRV1-IKT

apt install nfs-kernel-server

mkdir -p /opt/nfs/rw

mkdir -p /opt/nfs/ro

chmod a+w /opt/nfs/rw

chmod a+w /opt/nfs/ro

touch /opt/nfs/rw/testRW.txt

touch /opt/nfs/ro/testRO.txt

chown -R admin:admin /opt/nfs

nano /etc/exports

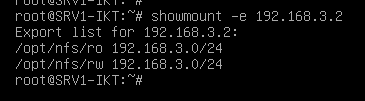
/opt/nfs/rw 192.168.3.0/24(rw,sync)

/opt/nfs/ro 192.168.3.0/24(ro,sync)

systemctl restart nfs-server

Проверка

showmount -e 192.168.3.2



Настройка NFS клиента

PC-IKT

apt install nfs-common

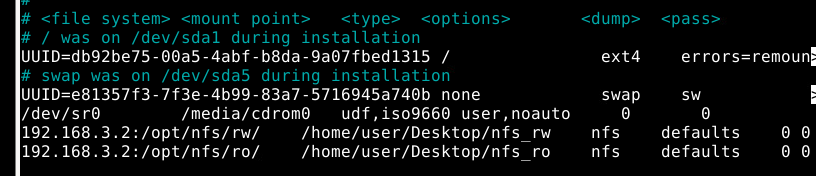
mkdir -p /home/user/Desktop/nfs\_rw

mkdir -p /home/user/Desktop/nfs\_ro

nano /etc/fstab

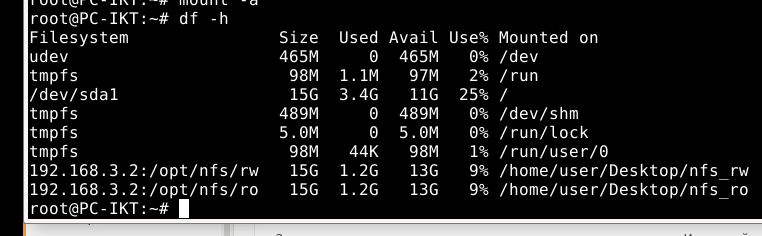
192.168.3.2:/opt/nfs/rw/ /home/user/Desktop/nfs\_rw nfs defaults 0 0

192.168.3.2:/opt/nfs/ro/ /home/user/Desktop/nfs\_ro nfs defaults 0 0

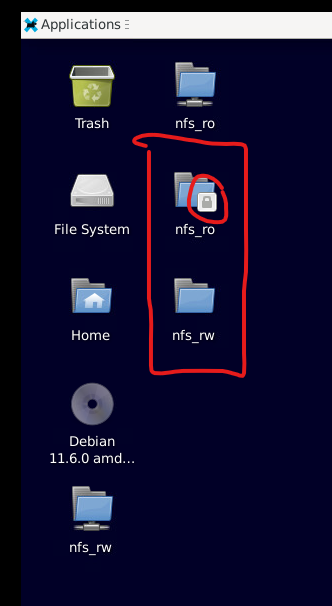


mount -a

df -h



Заходим на PC-IKT под пользователем user с паролем P@ssw0rd



WEB сервер на APP-\*

APP-AMS

apt install nginx

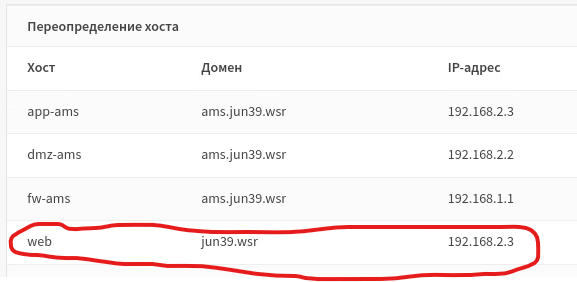
touch /var/www/html/index.html

nano /var/www/html/index.html

Welcome to Minecraft server mc.jun39.wsr site in European region

systemctl restart nginx

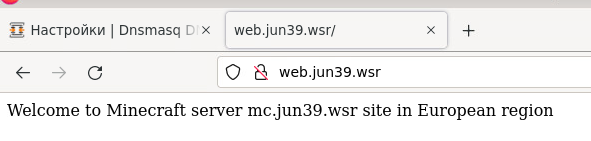
На FW-AMS



На PC-AMS

Проверка

В браузере вводим http://web.jun39.wsr



APP-MSK

apt install nginx

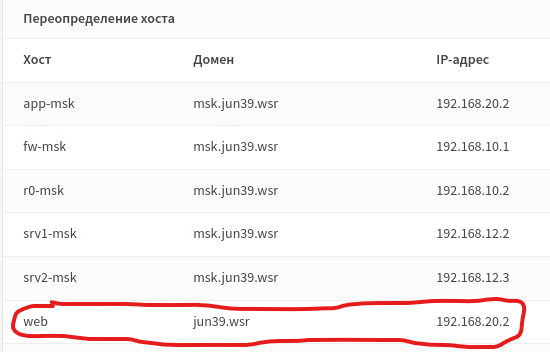
touch /var/www/html/index.html

nano /var/www/html/index.html

Welcome to Minecraft server mc.jun39.wsr site in Central region

systemctl restart nginx

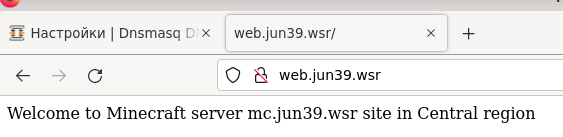
На FW-MSK



На PC-MSK

Проверка

В браузере вводим http://web.jun39.wsr



APP-IKT

apt install nginx

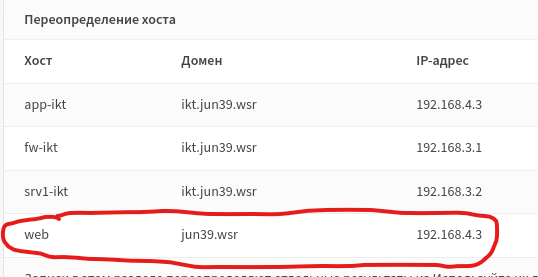
touch /var/www/html/index.html

nano /var/www/html/index.html

Welcome to Minecraft server mc.jun39.wsr site in Siberian region

systemctl restart nginx

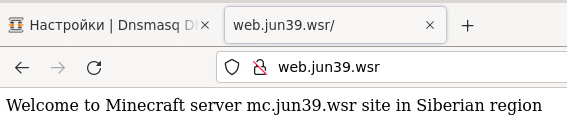
На FW-IKT



На PC-IKT

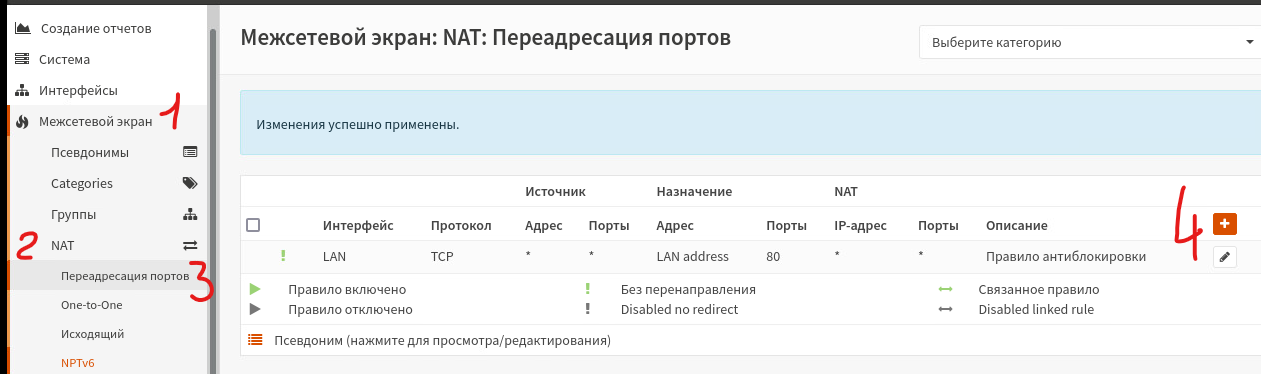
Проверка

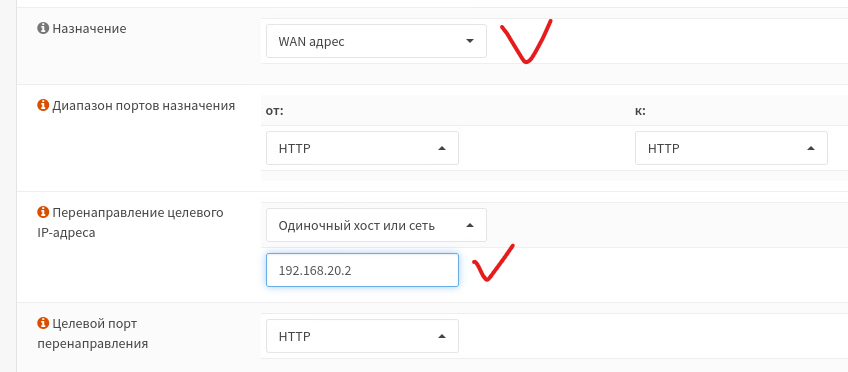
В браузере вводим http://web.jun39.wsr

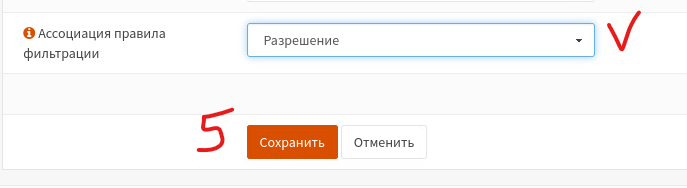


Проброс порта для сайта на APP-\*

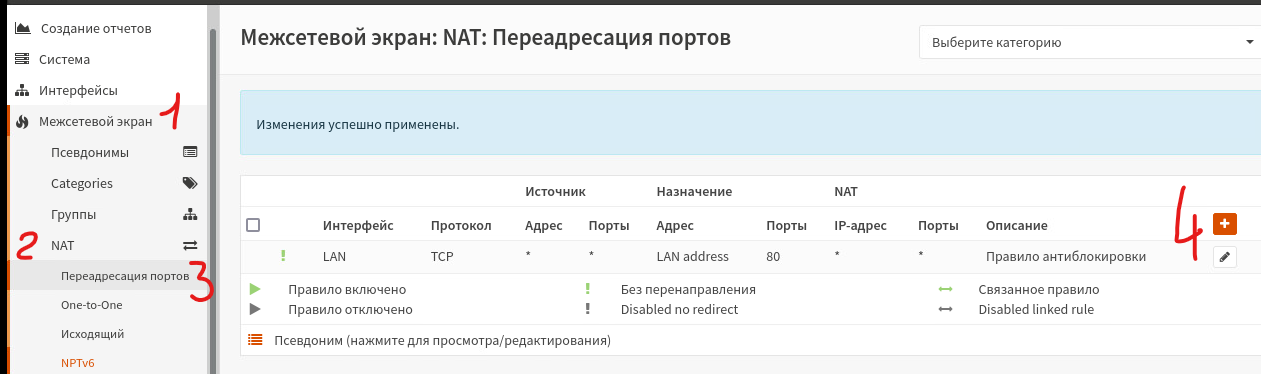
FW-MSK (подключаемся через PC-MSK)

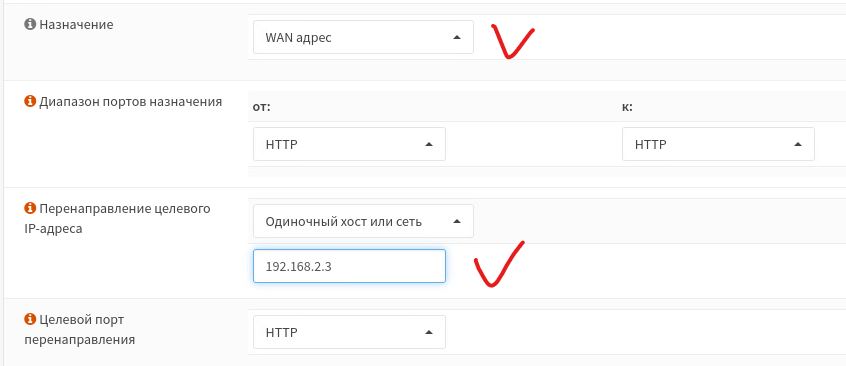


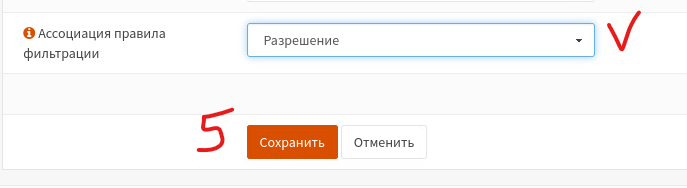




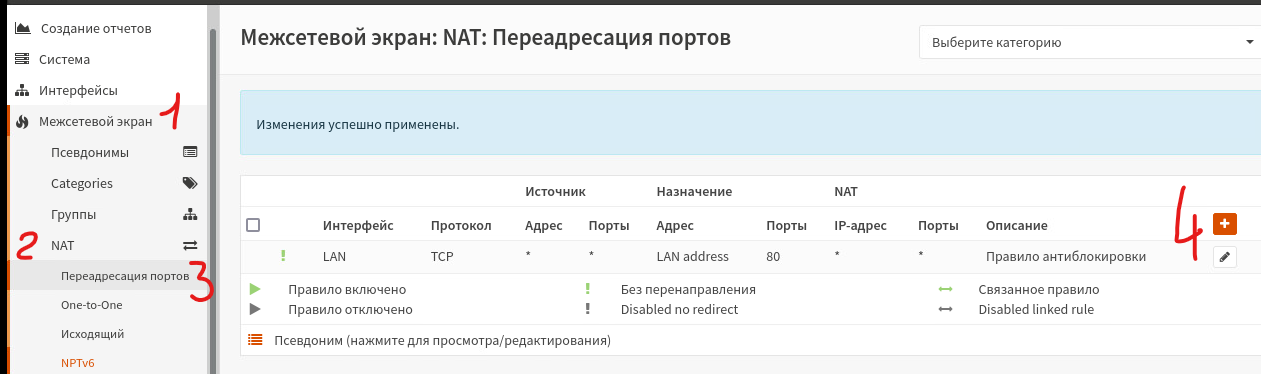
FW-AMS (подключаемся через PC-AMS)

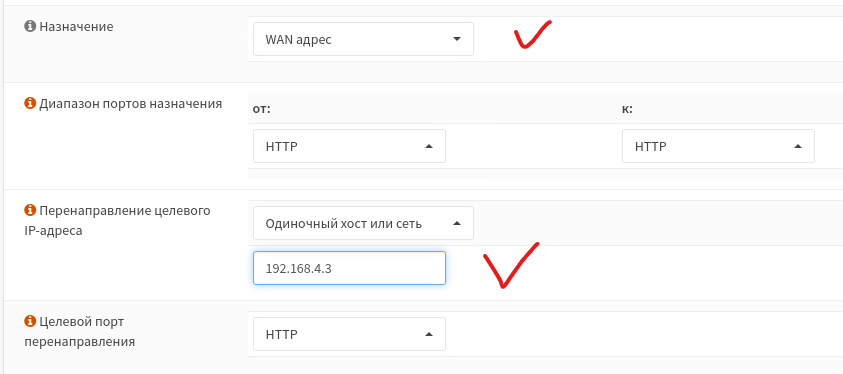


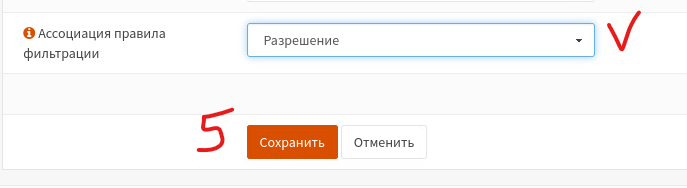




FW-IKT (подключаемся через PC-IKT)







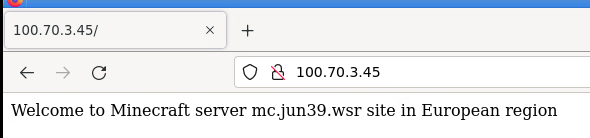
Проверка

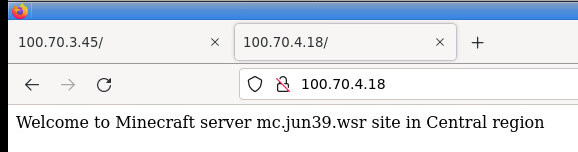
На ClientSPB в браузере вводим

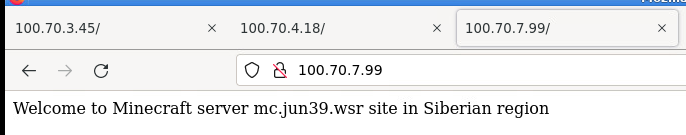
<http://100.70.3.45>

<http://100.70.4.18>

<http://100.70.7.99>







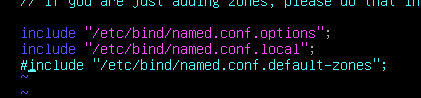
Настройка DNS сервера

VDS

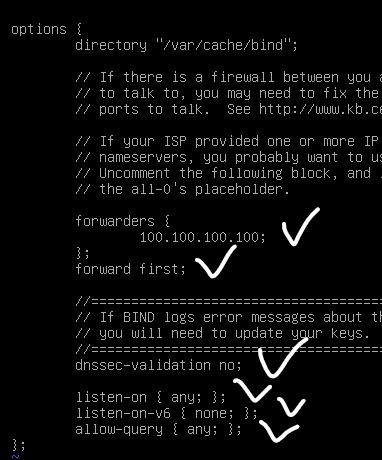
apt install bind9

nano /etc/bind/named.conf

Закомментируем последнюю строку



nano /etc/bind/named.conf.options

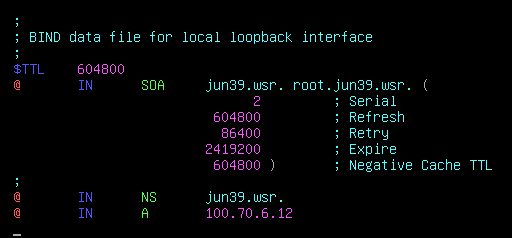


systemctl restart bind9

systemctl status bind9

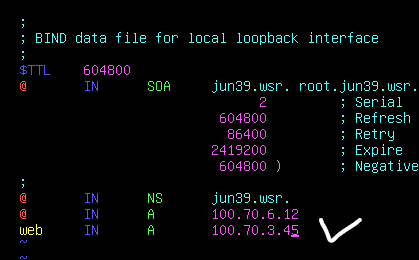
cp /etc/bind/db.local /var/cache/bind/jun39.wsr

nano /var/cache/bind/jun39.wsr



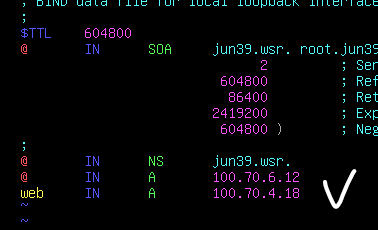
cp /var/cache/bind/jun39.wsr /var/cache/bind/ams.jun39.wsr

nano /var/cache/bind/ams.jun39.wsr



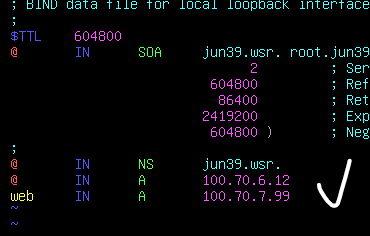
cp /var/cache/bind/jun39.wsr /var/cache/bind/msk.jun39.wsr

nano /var/cache/bind/msk.jun39.wsr



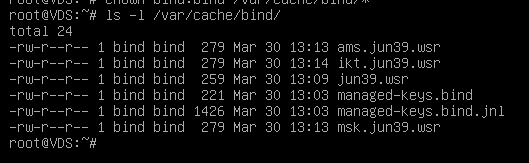
cp /var/cache/bind/jun39.wsr /var/cache/bind/ikt.jun39.wsr

nano /var/cache/bind/ikt.jun39.wsr



chown bind:bind /var/cache/bind/\*

ls -l /var/cache/bind/



nano /etc/bind/named.conf.local

view "ams" {

match-clients { 100.70.2.45; };

zone "jun39.wsr" {

type master;

file "/var/cache/bind/ams.jun39.wsr";

};

};

view "msk" {

match-clients { 100.70.5.55; };

zone "jun39.wsr" {

type master;

file "/var/cache/bind/msk.jun39.wsr";

};

};

view "ikt" {

match-clients { 100.70.8.78; };

zone "jun39.wsr" {

type master;

file "/var/cache/bind/ikt.jun39.wsr";

};

};

view "Default" {

match-clients { any; };

zone "jun39.wsr" {

type master;

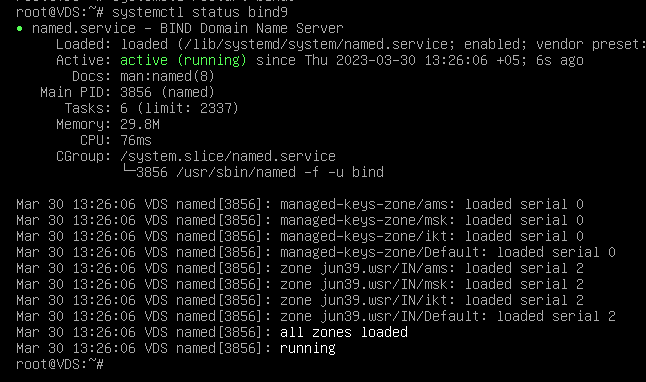
file "/var/cache/bind/jun39.wsr";

};

};

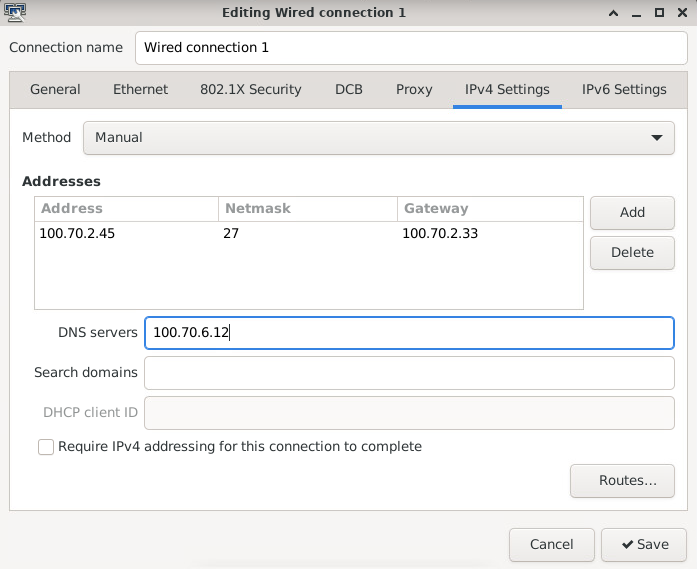
systemctl restart bind9

systemctl status bind9

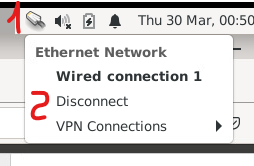
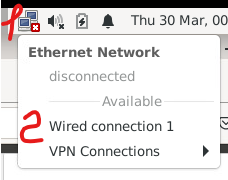


ClientEU

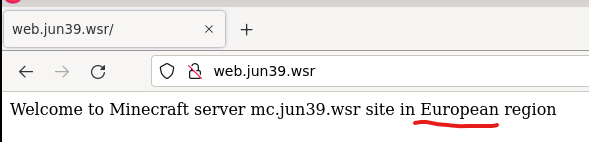
Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12



Перезапускаем сетевое подключение

В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-AMS

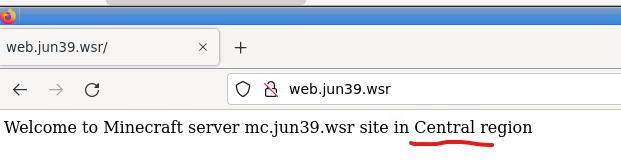


ClientSPB

Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12

Перезапускаем сетевое подключение

В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-MSK



ClientVV

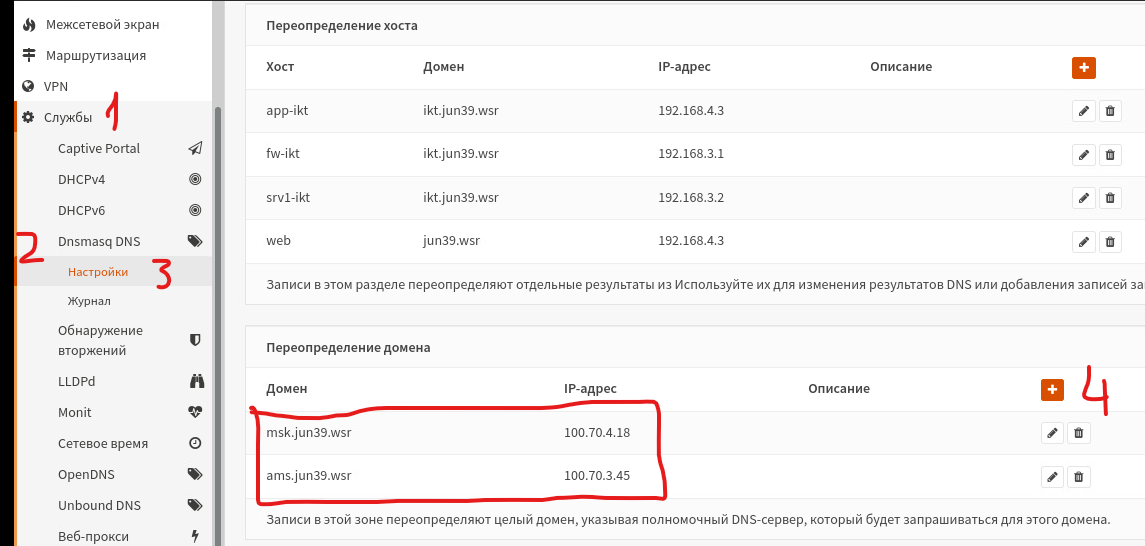
Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12

Перезапускаем сетевое подключение

В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-IKT



Настройка инфраструктуры DNS для доступа к другим филиалам по доменным именам

FW-IKT

Настройка IPSEC

<https://docs.opnsense.org/manual/how-tos/ipsec-s2s-route.html>

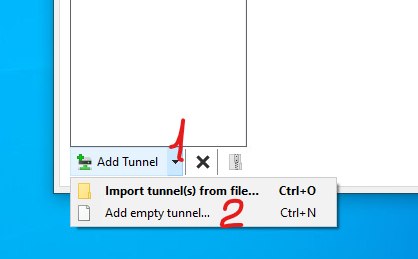
VPN

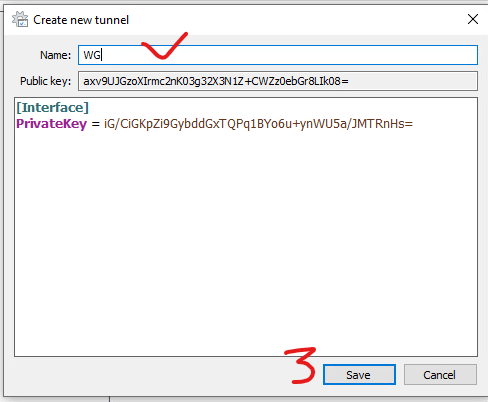
VPNClient

На VPNClient скачиваем и устанавливаем wireguard клиент

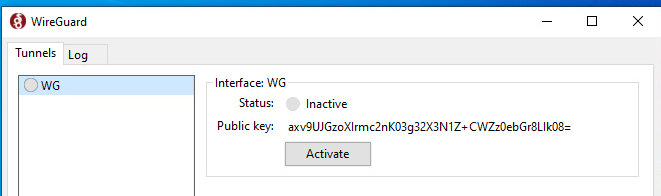
<https://www.wireguard.com/install/>

Запускаем Wireguard и создаем новый туннель





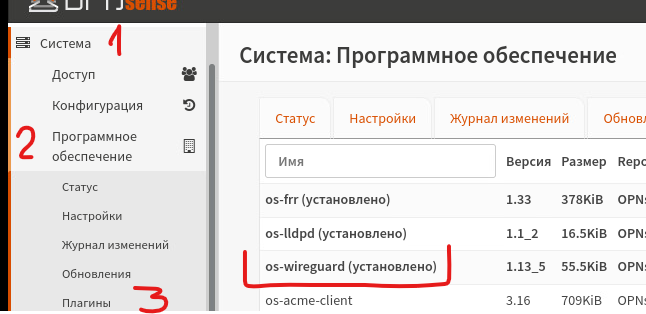
Получаем

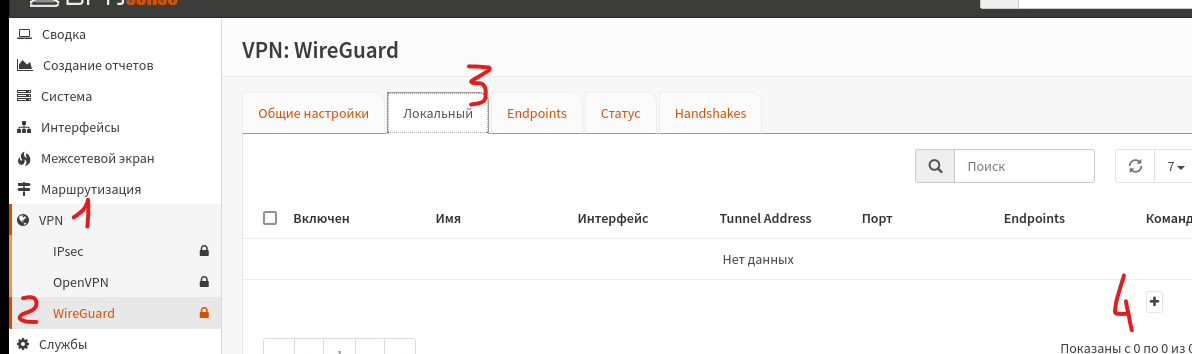


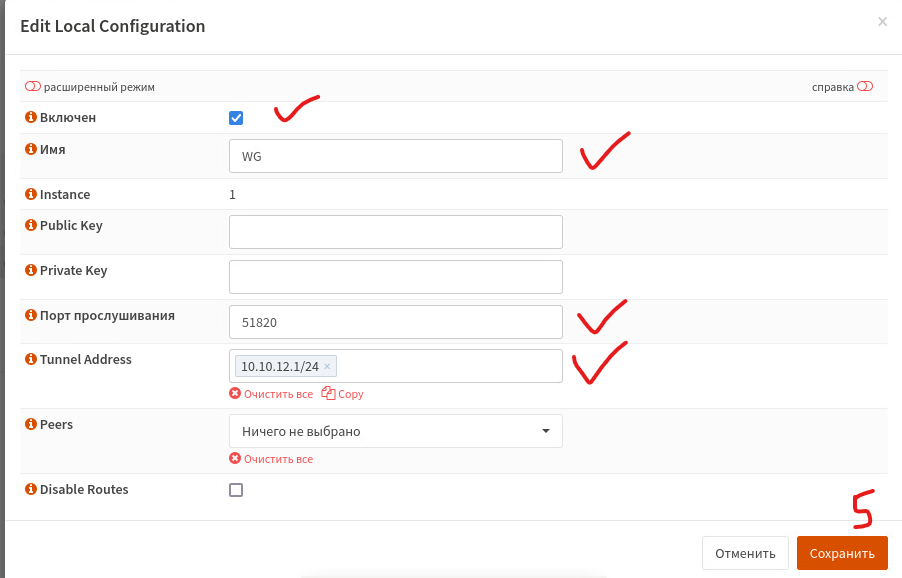
FW-MSK

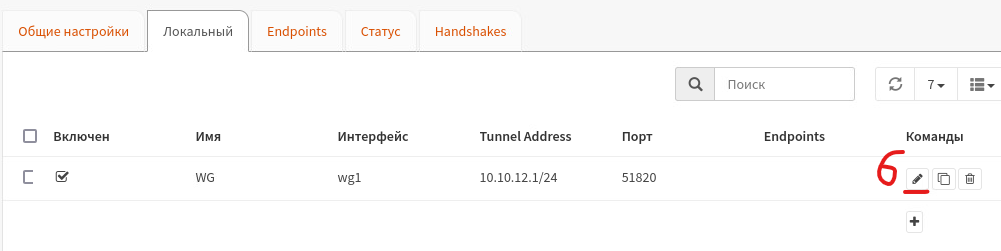
<https://docs.opnsense.org/manual/how-tos/wireguard-client.html>

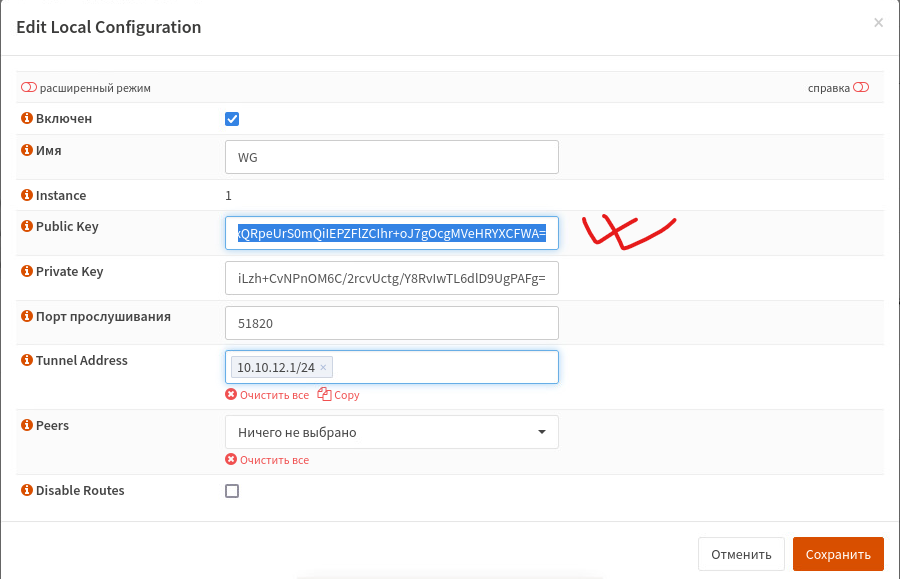
Устанавливаем плагин os-wireguard



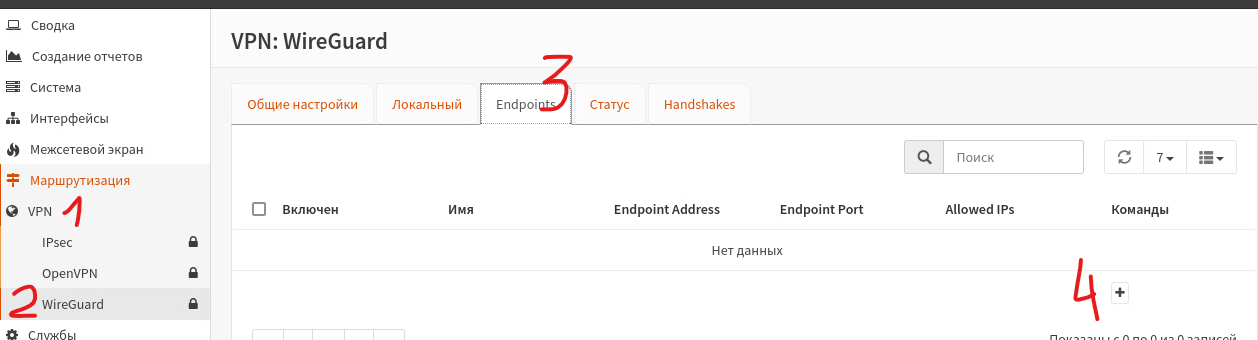


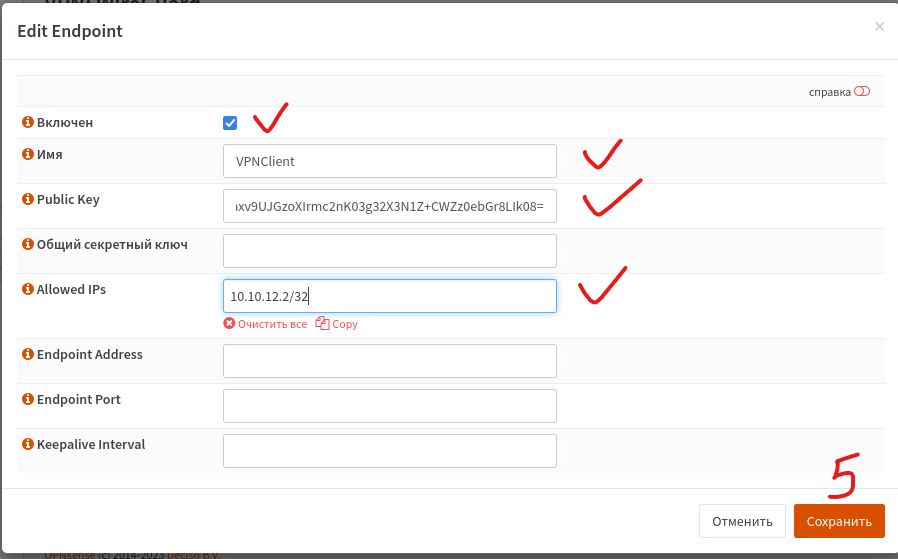




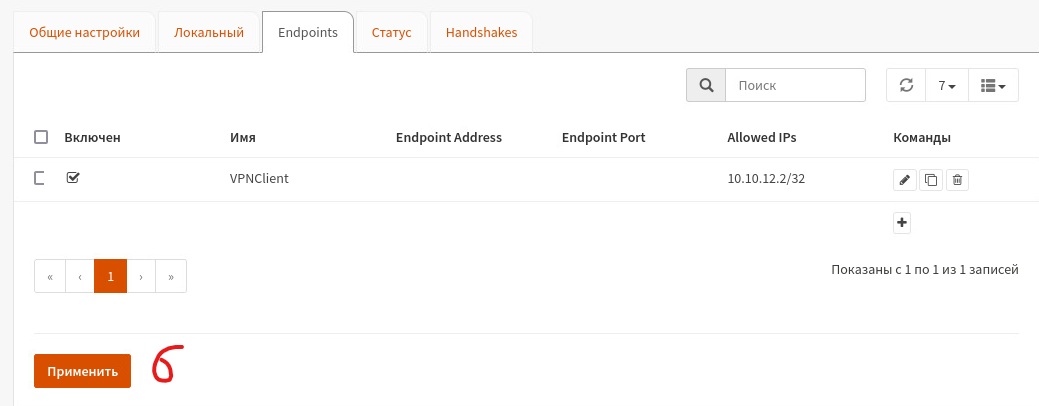


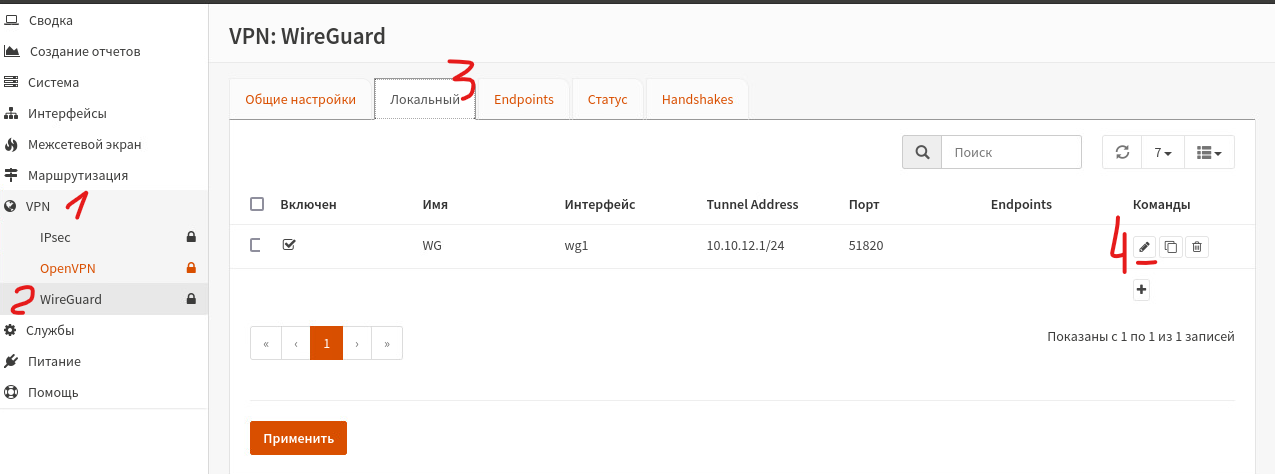
Нужно сохранить Peblic Key

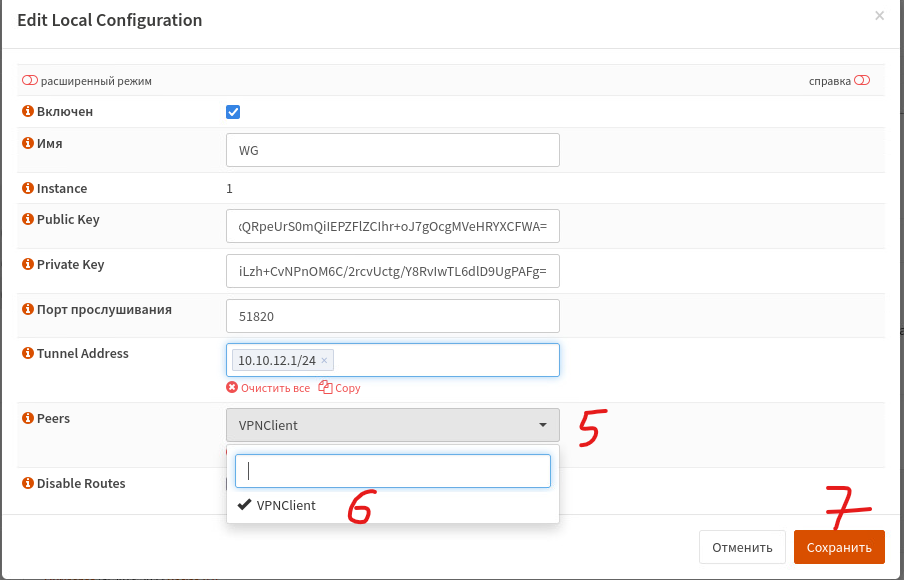


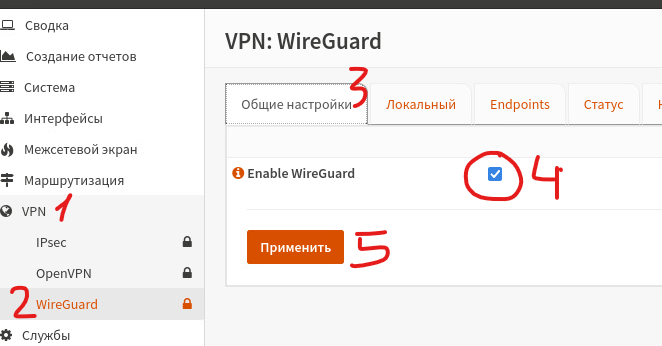


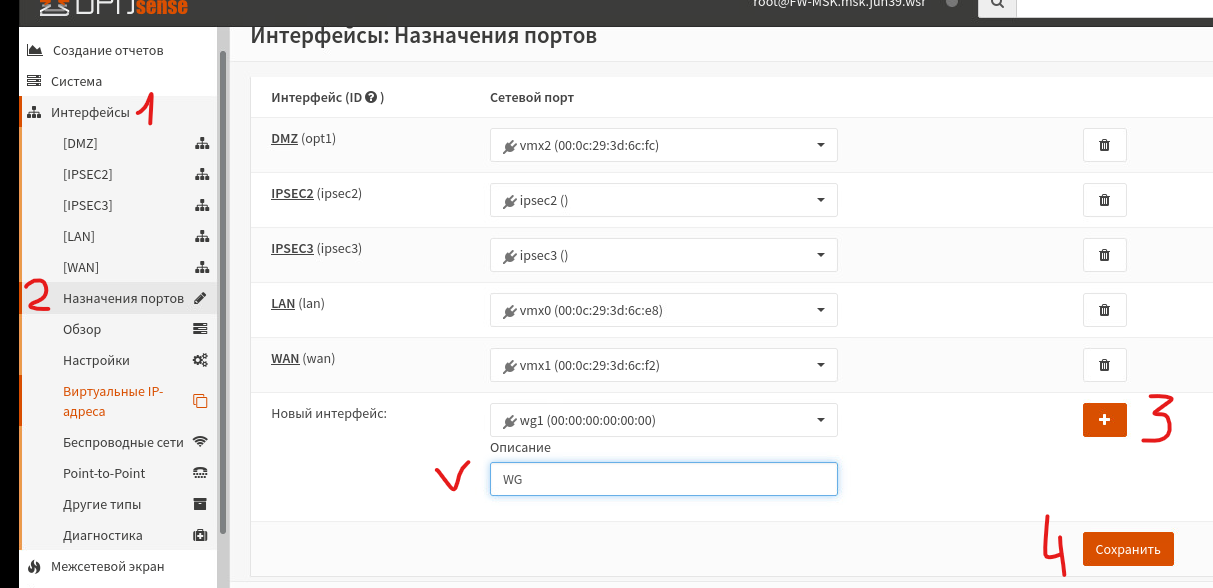
ВНИМАНИЕ Public Key берется от VPNClient

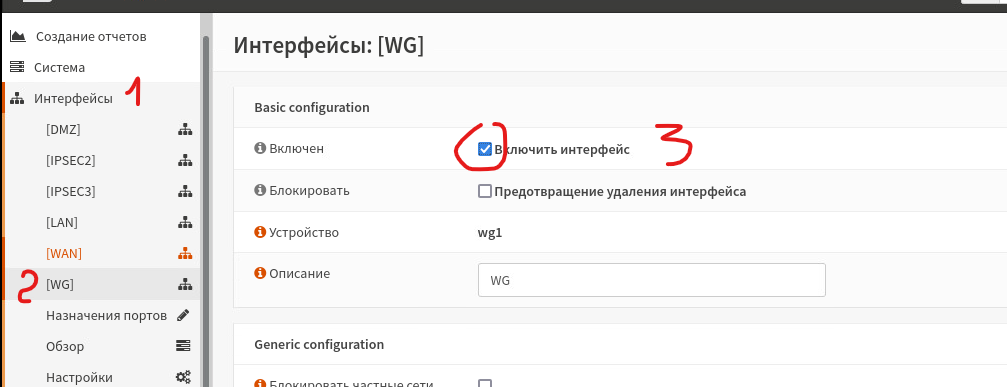


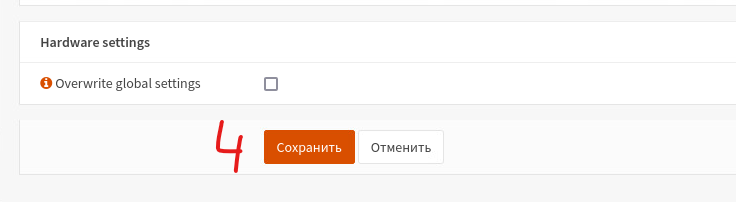


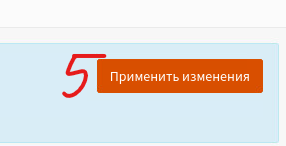


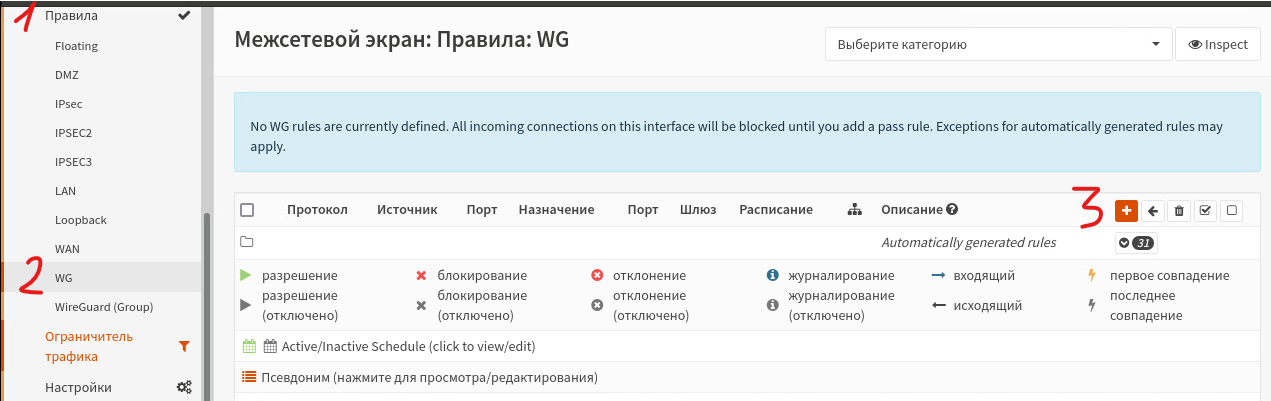


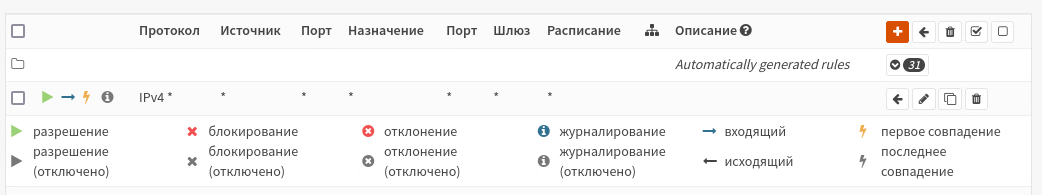




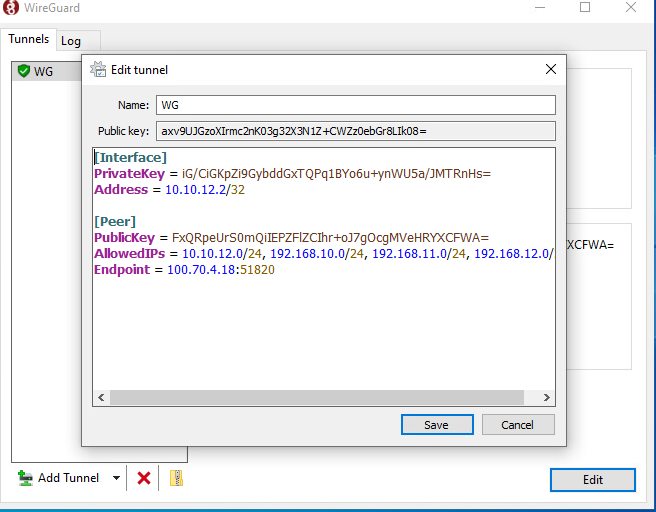




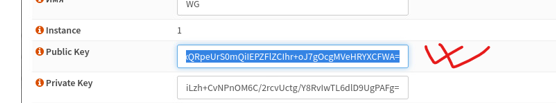


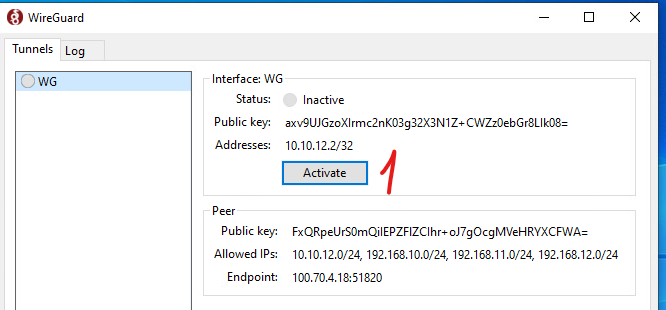


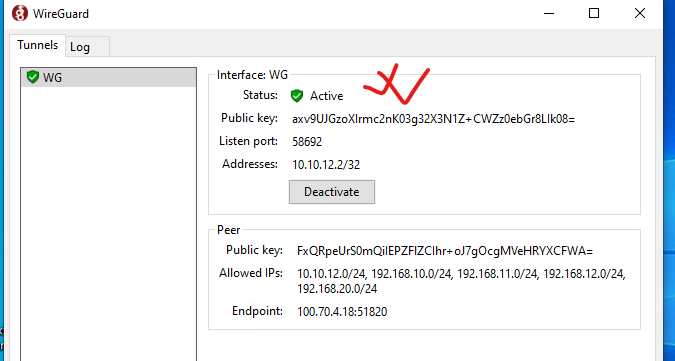
На VPNClient



Где [Peer] PublicKey = Публичный ключ FW







Проверка

ping 192.168.12.2

ping 192.168.12.3

ping 192.168.20.2

Настройка журналирования

SRV1-MSK

mkdir /opt/logs

chmod 777 /opt/logs/

nano /etc/rsyslog.conf

**#Раскомментируем 2 строчки (убирает #)**

module(load=”imudp”)

input(type=”imudp port=”514”)

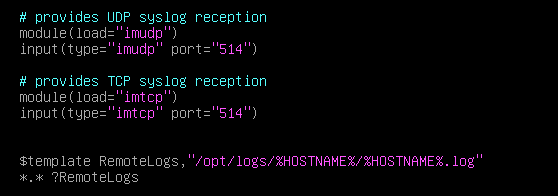
module(load=”imtcp”)

input(type=”imtcp port=”514”)

**В добавляем**

$template RemoteLogs,"/opt/log/%HOSTNAME%/%HOSTNAME%.log"

\*.\* ?RemoteLogs



systemctl restart rsyslog

systemctl status rsyslog

SRV2-MSK

nano /etc/rsyslog.conf

**В конце файла добавляем**

\*.warn @192.168.12.2

systemctl restart rsyslog

systemctl status rsyslog

Проверка

logger -p local4.warn "Warning SRV2-MSK"

PC-MSK

nano /etc/rsyslog.conf

**В конце файла добавляем**

\*.err @192.168.12.2

systemctl restart rsyslog

systemctl status rsyslog

Проверка

logger -p local4.err "Error PC-MSK"

FW-MSK

