1. Имена хостов и адресация:

1.1. Имена хостов

hostnamectl set-hostname … ; exec bash

1.2. Адресация

cp /etc/net/ifaces/ens18/ /etc/net/ifaces/ens19/

редачим конфиги под топологию, default via указывается в сторону ISP, без указания маски.

1.3. Маршрутизация

vim /etc/net/sysctl.conf

net.ipv4_ip.forward = 1

2. Динамическая трансляция на роутерах

2.1. Качаем nftables на ISP

apt-get update

apt-get install nftables

2.2. Редактируем файл /etc/nftables/nftables.nft

```
table inet nat {
        chain my_masquerade {
        type nat hook postrouting priority 0;
        oifname “ens18” masquerade
        }
}
```

2.3. Запускаем nftables

systemctl start nftables

systemclt enable nftables

**Аналогичные шаги проделываем на RTR-L и RTR-R*

3. Установка защищенного туннеля

3.1. Открыть файл /etc/gre.up

vim /etc/gre.up

3.2. Создадим незащищенный туннель RTR-L

Ip tunnel add tun0 mode gre local 100.100.100.10 remote 150.150.150.10

Ip addr add 5.5.5.1/30 dev tun0

Ip link set up tun0

Ip route add 20.20.20.0/24 via 5.5.5.1

3.3. Создадим незащищенный туннель RTR-R

Ip tunnel add tun0 mode gre local 150.150.150.10 remote 100.100.100.10

Ip addr add 5.5.5.2/30 dev tun0

Ip link set up tun0

Ip route add 10.10.10.0/24 via 5.5.5.2

3.4. Выдадим права на исполнение скрипта на обеих RTR и запустим скрипт

chmod +x /etc/gre.up

/etc/gre.up

3.5. Добавить скрипт в автозагрузку

Vim /etc/crontab

@reboot root /etc/gre.up

3.6. Параметры туннеля

vim /etc/strongswan/ipsec.conf

conn vpn

auto=start

type=tunnel

authby=secret

left=100.100.100.10 (Для RTR-R left и right меняются местами)

right=150.150.150.10

leftsubnet=0.0.0.0/0

rightsubnet=0.0.0.0/0

leftprotoport=gre

rightprotoport=gre

ike=aes128-sha256-modp3072

vim /etc/strongswan/ipsec.secrets

100.100.100.10 150.150.150.10 : PSK “P@ssw0rd”

3.7. Добавить в автозагрузку ipsec

Systemctl enable –now ipsec

Ipsec status

4. Настройка удаленного доступа (WEB)

Vim /etc/openssh/sshd_config

Port 2024

AllowUsers sshuser

Banner /etc/bannertext.net

MaxAuthTries 2

Vim /etc/bannertext.net

Authorized access only

Systemctl enable –now sshd

Useradd sshuser

Passwd sshuser

Ssh sshuser@10.10.10.110 -p 2024 Кидать с РТРок

5. Вертела я этот днс

6. Настройка синхронизации времени

6.1. Установка chrony

Apt-get install chrony

6.2. Редачим конфиг /etc/chrony.conf

server 35.35.35.1

allow 100.100.100.0/28

allow 150.150.150.0/28

allow 35.35.35.0/28

(или можно allow all)

local stratum 5

systemctl restart chronyd

chronyc sources

6.3. Настраиваем клиенты (все машины, кроме ISP)

Apt-get install chrony

Vim /etc/chrony.conf

Комментим строку с pool….

server 35.35.35.1 (Это для клиента. Для каждого офиса своя подсеть согласно таблице)

6.4. Проверим на isp

Chronyc clients

7. Файловое хранилище

7.1. Просмотрим текущие диски

Lsblk

7.2. Конфигурируем дисковый массив 5 уровня

mdadm --create /dev/md0 --level=5 --raid-devices=4 /dev/sdb /dev/sdc /dev/sdd /dev/sde

7.3. Размещение в файле

mdadm —detail —scan —verbose | tee -a /etc/mdadm.conf

7.4. Разделы, ext4

mkfs.ext4 /dev/md0 (создание файловой системы)

mkdir /raid5

mount /dev/md0 /raid5

7.5. Автомонтирование

vim /etc/fstab

/dev/md0 /raid5 ext4 defaults 0 0

7.6. Создаем общую директорию

mkdir /raid5/nfs

chmod 777 /raid5/nfs

7.7. Прописываем в Fstab

/dev/md0 /raid/nfs ext4 defaults,nofail 0 0

7.8. Создаем директорию на вебах

mkdir /mnt/nfs

mount //10.10.10.100/raid5/nfs /mnt/nfs/ -o guest

df -h

vim /etc/fstab

//10.10.10.100/raid5/nfs /mnt/nfs/ nfs defaults,nofail 0 0

8. **Пока докер нахер**
    8.1. **Качаем докер и докер компоус**

    Apt-get install docker docker-compose

    8.2. **Vim /home/user/wiki.yml**
    8.3. **Реально нахер**
9. Yandex

su -lc 'apt-get update && apt-get install yandex-browser-stable'