**Коротко о том, как выжить Ver. 2.0**

1. **Настройка виртуальных машин и коммутации**

Создаём виртуальные машины в соответствии со схемой, настраиваем характеристики ВМ в соответствии с таблицей, настраиваем имена хостов и адресацию.

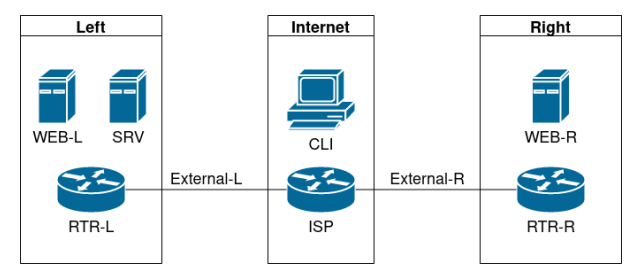


Схема сети

1. Базовая настройка, проделывается на всех ВМ с debian (ISP, RTR-L, RTR-R, WEB-L, WEB-R, SRV)

* Изменение имени хоста – nano /etc/hostname;
* Настройка адресации: nano /etc/network/interfaces, прописываем: auto [интерфейс] (смотрим командой ip a);

Iface [интерфейс] inet static

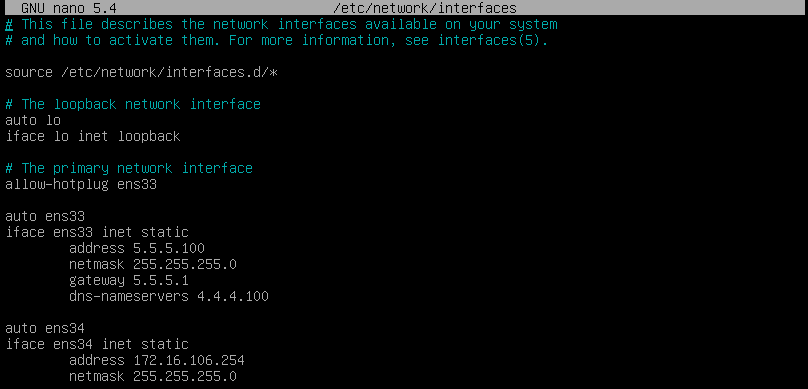
Address [адрес в соответствии с табл.]

Netmask 255.255.255.0

Gateway [если требуется]

Dns-nameservers [для RTR-R, WEB-R будет адрес RTR-L из внешней сети, для RTR-L, WEB-L - адрес SRV, для ISP указываем адрес самого ISP для сети с CLI]

* Reboot;
* Пингуемся, проверяем на возможные ошибки.



Пример для RTR-R

**2. Сетевая связность**

Настройка правил контроля трафика, туннеля, ssh (firewalld, wireguard) (ISP, RTR-R, RTR-L)

1. Добавляем репозиторий – apt-cdrom add, apt update;
2. Устанавливаем необходимые пакеты – apt install ssh firewalld wireguard (за исключением ISP);
3. Разрешаем доступ по ssh для рута - nano /etc/ssh/sshd\_config;

* раскомменти́руем строку с параметром и пишем *yes* PerminRootLogin yes
* Перезапуск службы - systemctl restart ssh sshd

1. Разрешаем пересылку пакетов – echo net.ipv4.ip\_forward=1 >> /etc/sysctl.conf, применяем изменения – sysctl –p;
2. Настройка firewalld (RTR-L, RTR-R):
   1. Просмотр активных зон – firewall-cmd —-get-active-zones, просмотр всех зон – firewall-cmd —-list-all-zones | less, просмотр правил - firewall-cmd —-zone=external --list-all(Эти команды нужны для проверки настроек);
   2. Удаляем интерфейсы из публичных зон – firewall-cmd —-zone=public —-remove-interface=[интерфейс] (Проделываем со всеми интерфейсами)
   3. Добавляем интерфейсы в зоны *external* и *trusted:* firewall-cmd —-zone=external —-add-interface=[интерфейс направленный во ВНЕШНЮЮ СЕТЬ]

firewall-cmd —-zone=trusted —-add-interface=[интерфейс направленный во ВНУТРЕННЮЮ СЕТЬ];

* 1. Разрешаем подключения к портам DNS, HTTP, HTTPS, из внешней сети:

firewall-cmd —-zone=external —-add-service=[dns, http, https] (\*три одинаковые команды, различия только в сервисах)(\*\*по заданию, для RTR-R, dns – не разрешается);

* 1. Проброс портов ssh, http, dns:

firewall-cmd —-zone=external —-add-forward-port=port=[2222 или 2244]:proto=tcp:toport=22:toaddr=[адрес WEB-L или WEB-R]

firewall-cmd —-zone=external —-add-forward- port=port=80:proto=tcp:toport=80:toaddr=[адрес WEB-L или WEB-R]

firewall-cmd —-zone=external —-add-forward- port=port=53:proto=udp:toport=53:toaddr=[адрес SRV] (\*только для RTR-L)

* 1. Также добавим порт для vpn – firewall-cmd —-zone=external —-add-port=12345/udp
  2. Сохраняем все правила – firewall-cmd —-runtime-to-permanent, и перезапускаем – firewall-cmd —-reload.

1. Настройка wireguard (RTR-L, RTR-R):
   1. Создаём директорию для ключей – mkdir /etc/wireguard/keys, переходим в неё командой cd – cd /etc/wireguard/keys;
   2. Создаём ключи – wg genkey | tee srv-sec.key | wg pubkey > srv-pub.key, wg genkey | tee cli-sec.key | wg pubkey > cli-pub.key