**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.

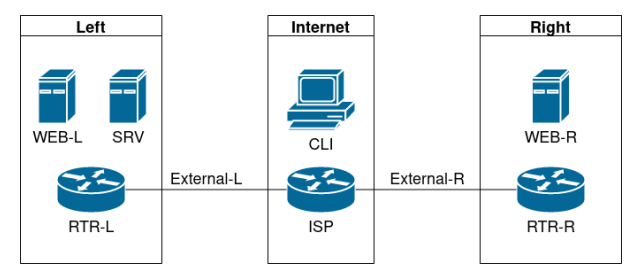


Схема сети

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

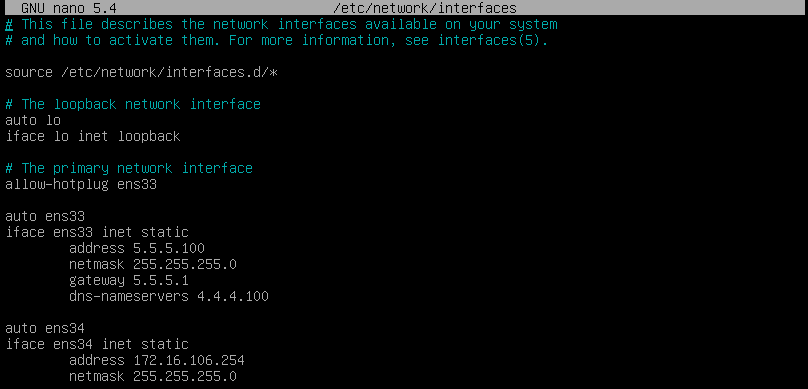
Address [адрес в соответствии с табл.]

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. Подключаем диск в параметрах ВМ ESXi и 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
   3. Создаём файл конфигурации с ключами – cat srv-sec.key cli-pub.key [При настройке 2 маршрутизатора, указываем srv-pub.key и cli-sec.pub] >> /etc/wireguard/wg0.conf
   4. Редактируем файл в текстовом редакторе – nano /etc/wireguard/wg0.conf, сдвигаем ключи вниз и выше прописываем:

[Interface]

Address = 10.20.30.1/30 [для 2 маршрутизатора указываем 10.20.30.2/30]

ListenPort = 12345 [Не указывается для 2 марш-ра]

PrivateKey = [Подставляем первый ключ]

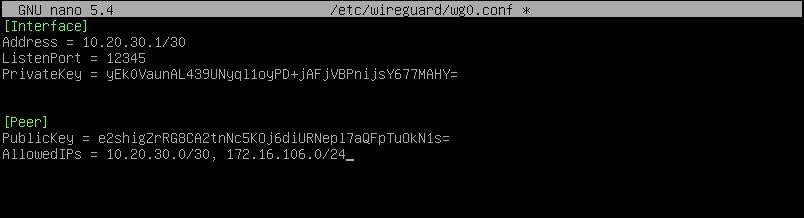
[Peer]

PublicKey = [Подставляем второй ключ]

Endpoint = (\*Указывается только для 2 марш-ра)[Внешний адрес 1 марш-ра с портом:12345]

AllowedIPs = 10.20.30.0/30, [Для RTR-L, внутрення сеть RTR-R, для RTR-R внутрення сеть RTR-L]

PersistentKeepalive = 10 (\*только для 2 маршрутизатора)



Пример для RTR-L



Пример для RTR-R

* 1. Отображаем ключи и файл конфигурации, проверяем на соответствие – cat /etc/wireguard/keys/srv-sec.key, cat /etc/wireguard/keys/cli-pub.key, cat /etc/wireguard/wg0.conf
  2. Пишем команду для включения службы – systemctl enable —-now wg-quick@wg0
  3. Проверяем настройку командой - wg show all
  4. При настройке второго маршрутизатора, создавать ключи НЕ НАДО, нужно передать 2 ключа (srv-pub.key и cli-sec.pub) из первого маршрутизатора, делаем это командой scp (заранее переходим в директорию с ключами на 1 маршрутизаторе, и создаём папку с ключами на 2 маршрутизаторе) – scp cli-sec.key srv-pub.key [внешний адрес RTR-R или RTR-L]:/etc/wireguard/keys

**3. Инфраструктурные службы**

Настройка DNS и NTP - bind9, chrony (ISP, SRV).

1. Подключаем диск в параметрах ВМ ESXi и добавляем репозиторий – apt-cdrom add, apt update;
2. Устанавливаем необходимые пакеты – apt install bind9 bind9utils dnsutils chrony;
3. **Настройка bind9 (ISP):**
   1. Открываем файл конфигурации – nano /etc/bind/named.conf.options
   2. После комментариев прописываем в файле конфигурации следующее:

Forwarders { [Внеш. Адрес RTR-L]; };

Listen-on { any; };

Recursion no;

Allow-query { any; };

Dnssec-validation no;

Listen-on-v6 { no; };

* 1. Открываем файл конфигурации – nano /etc/bind/named.conf.local
  2. После комментариев прописываем в файле конфигурации следующее:

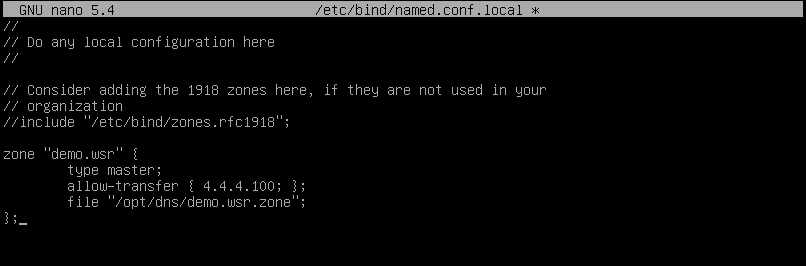
zone "demo.wsr" {

type master;

allow-transfer { 4.4.4.100 [внеш. Адрес RTR-L]};

file "/opt/dns/demo.wsr.zone";

};



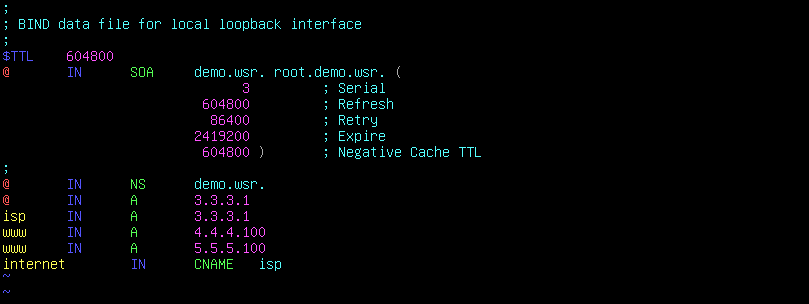
Настройка /named.conf.local

* 1. Создаём директорию dns командой – mkdir /opt/dns
  2. Копируем шаблон настроек в созданную директорию – cp /etc/bind/db.local /opt/dns/demo.wsr.zone
  3. Даем право на чтение и исполнение файла, командой chmod – chmod 665 /opt/dns/demo.wsr.zone
  4. Изменяем параметры безопасности для apparmor, открываем файл конфигурации – nano /etc/apparmor.d/usr.sbin.named, добавляем строчку - /opt/dns/\*\* rw,



Настройка /usr.sbin.named

* 1. Перезапускаем сервис apparmor командой – systemctl restart apparmor.service
  2. Открываем файл и добавляем dns-записи зон, в соответствии с таблицей – nano /opt/dns/demo.wsr.zone



Dns-записи в файле dns/demo.wsr.zone

* 1. Перезапускаем службу и проверяем загрузку зон – systemctl restart named, named-checkconf –z
  2. Проверяем работу dns командой host или nslookup – nslookup [www.demo.wsr](http://www.demo.wsr)