

Коротко о том, как выжить Ver. 2.0

1. Настройка виртуальных машин и коммутации

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

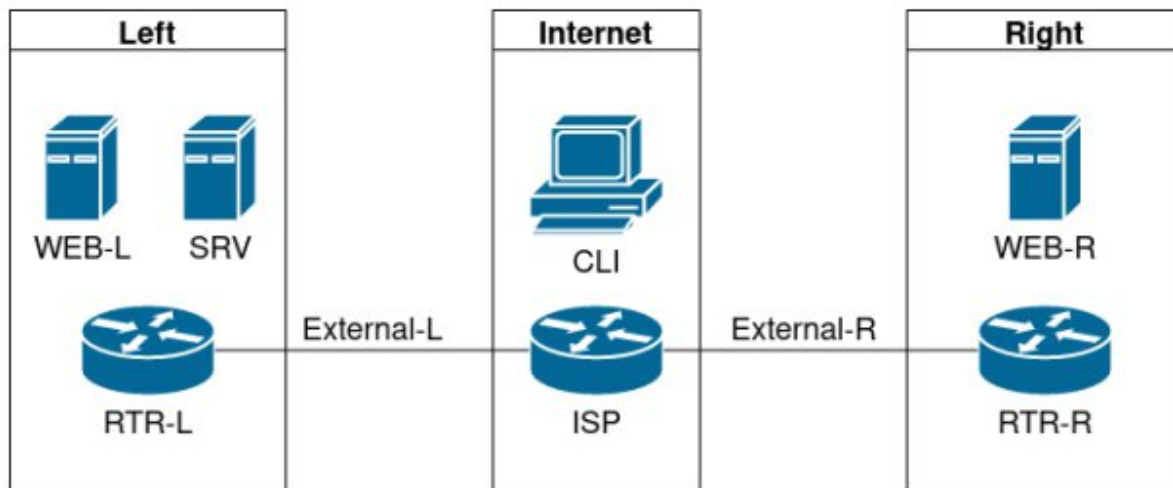


Схема сети

1) Базовая настройка, продельвается на всех VM 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.

```
GNU nano 5.4 /etc/hostname *
RTR-R
```

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33

auto ens33
iface ens33 inet static
    address 5.5.5.100
    netmask 255.255.255.0
    gateway 5.5.5.1
    dns-nameservers 4.4.4.100

auto ens34
iface ens34 inet static
    address 172.16.106.254
    netmask 255.255.255.0
```

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 VM 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;

- раскомментируем строку с параметром и пишем `yes`
`PerminRootLogin yes`
- Перезапуск службы - `systemctl restart sshd`

4. Разрешаем пересылку пакетов - `echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf`, применяем изменения - `sysctl -p`;

5. Настройка **firewalld** (RTR-L, RTR-R):

a. 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);

b. Удаляем интерфейсы из публичных зон - `firewall-cmd --zone=public --remove-interface=[интерфейс]` (Продельываем со всеми интерфейсами)

c. 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];`

d. 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);

e. 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)
```

f. Также добавим порт для vpn - `firewall-cmd --zone=external --add-port=12345/udp`

g. Сохраняем все правила - `firewall-cmd --runtime-to-permanent`, и перезапускаем - `firewall-cmd --reload`.

6. Настройка wireguard (RTR-L, RTR-R):

a. Создаём директорию для ключей - `mkdir /etc/wireguard/keys`, переходим в неё командой `cd - cd /etc/wireguard/keys`;

b. Создаём ключи - `wg genkey | tee srv-sec.key | wg pubkey > srv-pub.key`, `wg genkey | tee cli-sec.key | wg pubkey > cli-pub.key`

c. 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`

d. 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, внутренняя
сеть RTR-R, для RTR-R внутренняя сеть RTR-L]

PersistentKeepalive = 10 (*только для 2
маршрутизатора)

```
GNU nano 5.4 /etc/wireguard/wg0.conf *
[Interface]
Address = 10.20.30.1/30
ListenPort = 12345
PrivateKey = yEk0VaunAL439UNYq11oyPD+jAFjVBPnijsY677MAHY=

[Peer]
PublicKey = e2shigZrRG8CA2tnNc5K0j6diURNep17aQFpTu0KN1s=
AllowedIPs = 10.20.30.0/30, 172.16.106.0/24_
```

Пример для RTR-L

```
GNU nano 5.4 /etc/wireguard/wg0.conf *
[Interface]
Address = 10.20.30.2/30
PrivateKey = kFhVaYu5zHaBWBVT92UtQH4qo+Dju32I73sxqMkvkXk=

[Peer]
PublicKey = WzWX/xeZcWi2qa/yLSN5DH2ryia3Zb+YnFSiXhaCWMY=
Endpoint = 4.4.4.100:12345
AllowedIPs = 10.20.30.0/30, 192.168.106.0/24
PersistentKeepalive = 10
```

Пример для RTR-R

е. 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

ф. Пишем команду для включения службы - systemctl enable
--now wg-quick@wg0

г. Проверяем настройку командой - wg show all

h. 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 VM ESXi и добавляем репозиторий - apt-cdrom add, apt update;
2. Устанавливаем необходимые пакеты - apt install bind9 bind9utils dnsutils chrony;

3. Настройка bind9 (ISP):

a. Открываем файл конфигурации - nano
/etc/bind/named.conf.options

b. После комментариев прописываем в файле конфигурации следующее:

```
Forwarders { [Внеш. Адрес RTR-L]; };
```

```
Listen-on { any; };
```

```
Recursion no;
```

```
Allow-query { any; };
```

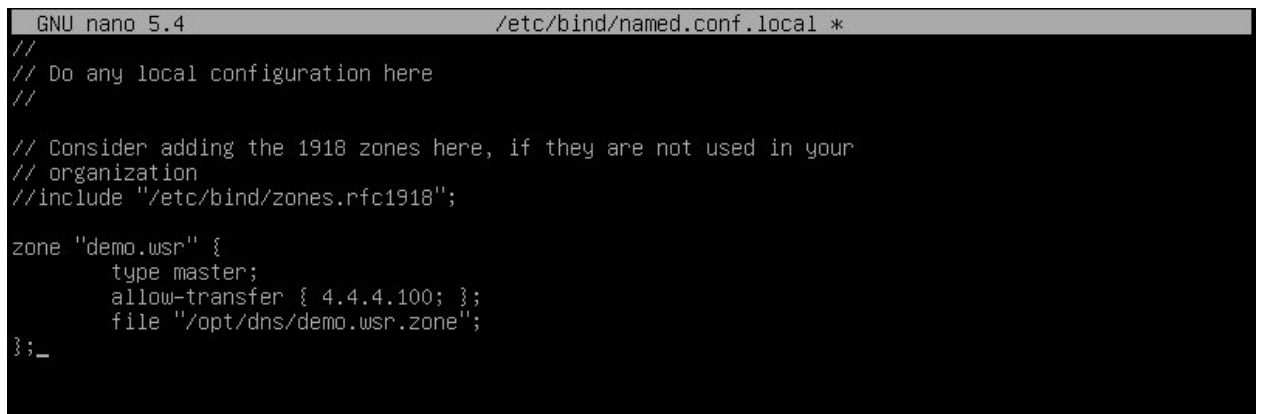
```
Dnssec-validation no;
```

```
Listen-on-v6 { no; };
```

c. Открываем файл конфигурации - nano
/etc/bind/named.conf.local

- d. 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";  
  
};
```



The screenshot shows a terminal window with the GNU nano 5.4 editor open to the file /etc/bind/named.conf.local. The file content is as follows:

```
GNU nano 5.4 /etc/bind/named.conf.local *  
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "demo.wsr" {  
    type master;  
    allow-transfer { 4.4.4.100; };  
    file "/opt/dns/demo.wsr.zone";  
};_
```

Настройка /named.conf.local

- e. Создаём директорию dns командой – `mkdir /opt/dns`
- f. Копируем шаблон настроек в созданную директорию – `cp /etc/bind/db.local /opt/dns/demo.wsr.zone`
- g. Даём право на чтение и исполнение файла, командой `chmod` – `chmod 665 /opt/dns/demo.wsr.zone`
- h. Изменяем параметры безопасности для `apparmor`, открываем файл конфигурации – `nano /etc/apparmor.d/usr.sbin.named`, добавляем строку – `/opt/dns/** rw,`

```

profile named /usr/sbin/named flags=(attach_disconnected) {
    #include <abstractions/base>
    #include <abstractions/nameservice>

    capability net_bind_service,
    capability setgid,
    capability setuid,
    capability sys_chroot,
    capability sys_resource,

    # /etc/bind should be read-only for bind
    # /var/lib/bind is for dynamically updated zone (and journal) files.
    # /var/cache/bind is for slave/stub data, since we're not the origin of it.
    # See /usr/share/doc/bind9/README.Debian.gz
    /etc/bind/** r,
    /var/lib/bind/** rw,
    /var/lib/bind/ rw,
    /var/cache/bind/** lrw,
    /var/cache/bind/ rw,
    /opt/dns/** rw,

```

Настройка /usr/sbin/named

- i. Перезапускаем сервис apparmor командой - `systemctl restart apparmor.service`
- j. Открываем файл и добавляем dns-записи зон, в соответствии с таблицей - `nano /opt/dns/demo.wsr.zone`

```

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      demo.wsr. root.demo.wsr. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       demo.wsr.
@         IN      A        3.3.3.1
isp       IN      A        3.3.3.1
www       IN      A        4.4.4.100
www       IN      A        5.5.5.100
internet  IN      CNAME    isp
~
~

```

Dns-записи в файле dns/demo.wsr.zone

- k. Перезапускаем службу и проверяем загрузку зон - `systemctl restart named, named-checkconf -z`
- l. Проверяем работу dns командой `host` или `nslookup` - `nslookup www.demo.wsr`