apt install chrony bind9 strongswan mdadm samba

1.Смена имени компьютера -

hostnamectl set-hostname “name”; exec bash

В первой части мы меняем имя. Во второй перезапуск оболочки bash

2. Выдача ip адресов

Через редактор текстовых документов (vi, vim, nano)

В /etc/network/interface

auto ens33

iface ens33 inet static

address “ip”

gateway “gate”

3. Включить ip forwarding

Через редактор текстовых документов (vi, vim, nano)

В /etc/sysctl.conf убрать комментарии с net.ipv4.ip_forward=1 на маршрутизаторах и isp

Проверить sysctl -p

4. Настройка NAT на сторонах

На RTR-R и RTR-L в файле /etc/nftables пишем следующие строки

```
  GNU nano 5.4                                /etc/nftables.conf *
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {
                type filter hook input priority 0;
        }
        chain forward {
                type filter hook forward priority 0;
        }
        chain output {
                type filter hook output priority 0;
        }
}
table ip nat {
        chain postrouting {
                type nat hook postrouting priority 0;
                ip saddr 172.16.100.0/24 oifname ens33 counter masquerade;
        }
}
```

Где ip - ip сети текущей, а ens33 порт уходящий в isp

Для проверки используется команда - nft -f /etc/nftables.conf

Для активации NAT надо добавить скрипт в автозапуск - systemctl enable -–now nftables

В конце должен пинговаться параллельный порт ISP

5. GRE тункль U@U.

Пишем BASH скрипт на правом и левом маршрутизаторе.PI

```
  GNU nano 5.4                                          /etc/gre.up
#!/bin/bash
ip tunnel add tun0 mode gre local 4.4.4.100 remote 5.5.5.100
ip addr add 10.5.5.1/30 dev tun0
ip link set up tun0
ip route add 172.16.100.0/24 via 10.5.5.2
```

```
root@RTR-L:~# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             4.4.4.100/24 fe80::20c:29ff:fe27:7dbd/64
ens36            UP             192.168.100.254/24 fe80::20c:29ff:fe27:7dc7/64
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
tun0@NONE        UNKNOWN        10.5.5.1/30 fe80::200:5efe:404:464/64
```

Это всё на одном маршрутизаторе, rtr-l.

На RTR-R прописываем следующее -

```
  GNU nano 5.4                                          /etc/gre.up
#!/bin/bash
ip tunnel add tun0 mode gre local 5.5.5.100 remote 4.4.4.100
ip addr add 10.5.5.2/30 dev tun0
ip link set up tun0
ip route add 192.168.100.0/24 via 10.5.5.1
```

```
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             5.5.5.100/24 fe80::250:56ff:fe2c:f047/64
ens36            UP             172.16.100.254/24 fe80::20c:29ff:fef8:785e/64
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
tun0@NONE        UNKNOWN        10.5.5.2/30 fe80::200:5efe:505:564/64
```

Задаем права доступа при помощи команды chmod +x /etc/gre.up, где x это аргумент, а /etc… путь к файлу.

Далее вписываем путь к файлу, если не выводит ошибок, а в интерфейсах появился туннель, то следует внести в автозапуск в crontab.

Через nano изменяем файл /etc/crontab.

Вписываем туда @reboot root /etc/gre.up в самый низ.

Проверить можно пропинговав параллельный тунель. ISP пинговатся не будет!

6.Настройка IPsec.

Для начало надо установить apt install strongswan, далее на RTR-R, L надо прописать в конфиге /etc/ipsec.conf следующие штуки

```
config setup
        # strictcrlpolicy=yes
        # uniqueids = no

# Add connections here.

# Sample VPN connections

conn vpn
      auto=start
      type=tunnel
      authby=secret
      left=5.5.5.100
      right=4.4.4.100
      leftsubnet=0.0.0.0/0
      rightsubnet=0.0.0.0/0
      leftprotoport=gre
      rightprotoport=gre
      ike=aes128-sha256-modp3072
      esp=aes128-sha256
```

RTR-R

```
config setup
        # strictcrlpolicy=yes
        # uniqueids = no

# Add connections here.

# Sample VPN connections

conn vpn
      auto=start
      type=tunnel
      authby=secret
      left=4.4.4.100
      right=5.5.5.100
      leftsubnet=0.0.0.0/0
      rightsubnet=0.0.0.0/0
      leftprotoport=gre
      rightprotoport=gre
      ike=aes128-sha256-modp3072
      esp=aes128-sha256
```

RTR-L

В файле /etc/ipsec.secrets на обоих маршрутизаторах надо пропиать

```
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

4.4.4.100  5.5.5.100 : PSK "P@ssw0rd"
~
~
```

Далее надо ввести в авто запуск systemctl enable --now ipsec

Чтобы проверить надо написать ipsec status

7. nftables - firewall

Прописываем следующие настройки в правом (RT-R) маршрутизаторе

```
  GNU nano 5.4                                  /etc/nftables.conf *
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {

                type filter hook input priority 0;
                        tcp dport 80 accept;
                        tcp dport 443 accept;
                        ct state {established, related} accept;
                        ip protocol gre accept;
                        ip protocol icmp accept;
                        udp dport 500 accept;
                        ip saddr 192.168.100.0/24 accept;
                        ip saddr 172.16.100.0/24 accept;
                        tcp dport 2244 accept;
                        ip version 4 drop;
        }
        chain forward {
                type filter hook forward priority 0;
        }
        chain output {
                type filter hook output priority 0;
        }
}
table ip nat {
        chain postrouting {
                type nat hook postrouting priority 0;
                ip saddr 172.16.100.0/24 oifname ens33 counter masquerade;
        }
}
```

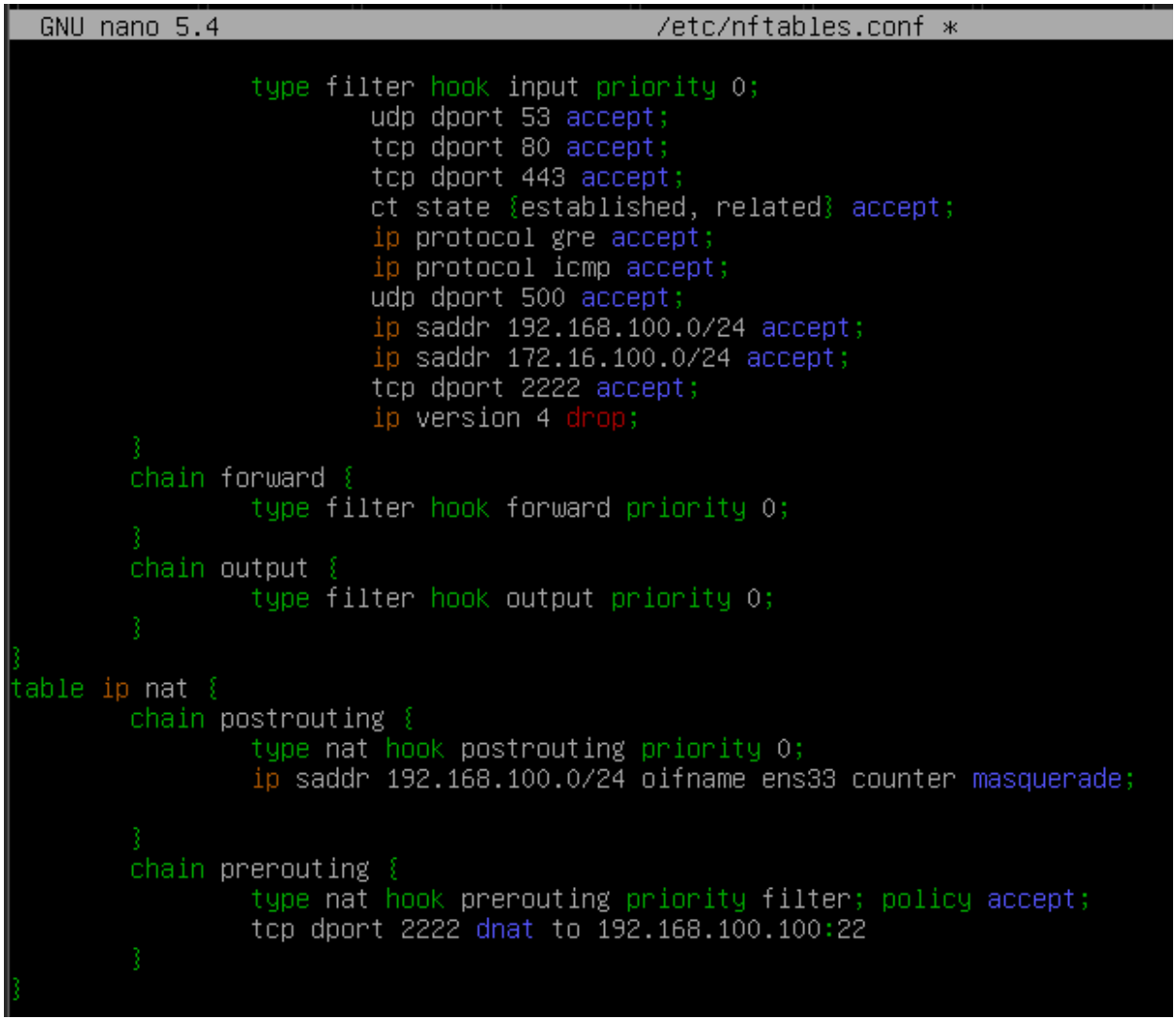
Немного другое но на RTR-L

```
  GNU nano 5.4                                  /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {

                type filter hook input priority 0;
                        udp dport 53 accept;
                        tcp dport 80 accept;
                        tcp dport 443 accept;
                        ct state {established, related} accept;
                        ip protocol gre accept;
                        ip protocol icmp accept;
                        udp dport 500 accept;
                        ip saddr 192.168.100.0/24 accept;
                        ip saddr 172.16.100.0/24 accept;
                        tcp dport 2222 accept;
                        ip version 4 drop;
        }
        chain forward {
                type filter hook forward priority 0;
        }
        chain output {
                type filter hook output priority 0;
        }
}
table ip nat {
        chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 192.168.100.0/24 oifname ens33 counter masquerade;
        }
}
```

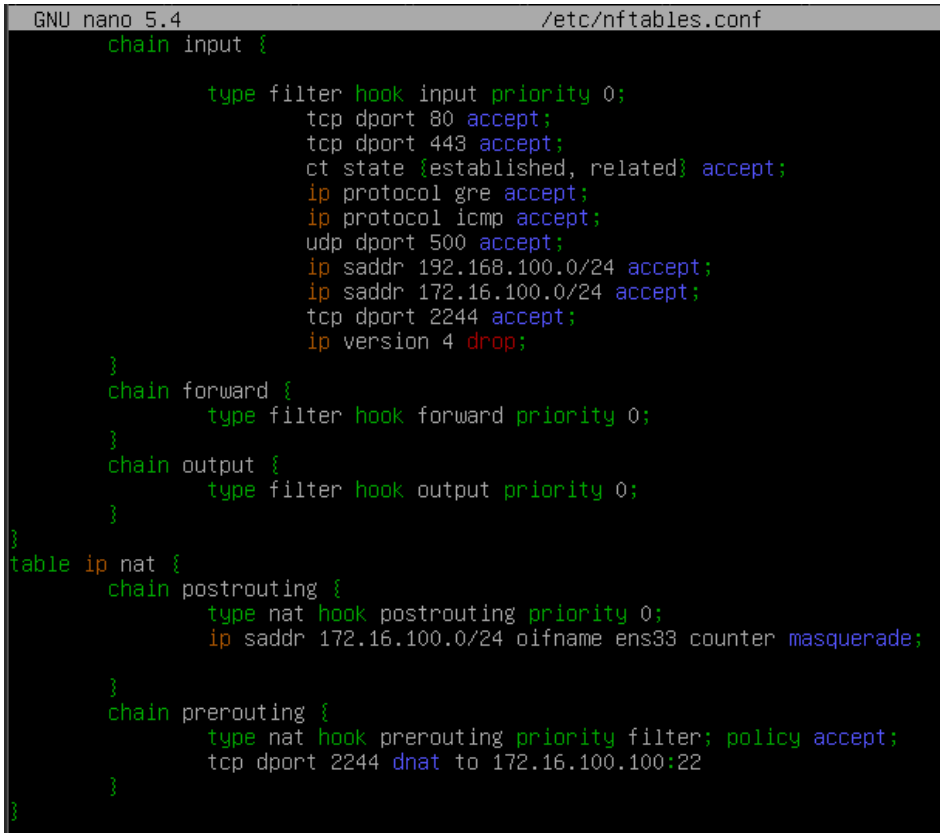
Для проверки nft -f /etc/nftables.conf

8. перенаправление трафика nftables

rtr-l


GNU nano 5.4 /etc/nftables.conf *
type filter hook input priority 0;
udp dport 53 accept;
tcp dport 80 accept;
tcp dport 443 accept;
ct state {established, related} accept;
ip protocol gre accept;
ip protocol icmp accept;
udp dport 500 accept;
ip saddr 192.168.100.0/24 accept;
ip saddr 172.16.100.0/24 accept;
tcp dport 2222 accept;
ip version 4 drop;
}
chain forward {
type filter hook forward priority 0;
}
chain output {
type filter hook output priority 0;
}
}
table ip nat {
chain postrouting {
type nat hook postrouting priority 0;
ip saddr 192.168.100.0/24 oifname ens33 counter masquerade;
}
chain prerouting {
type nat hook prerouting priority filter; policy accept;
tcp dport 2222 dnat to 192.168.100.100:22
}
}

rtr-r

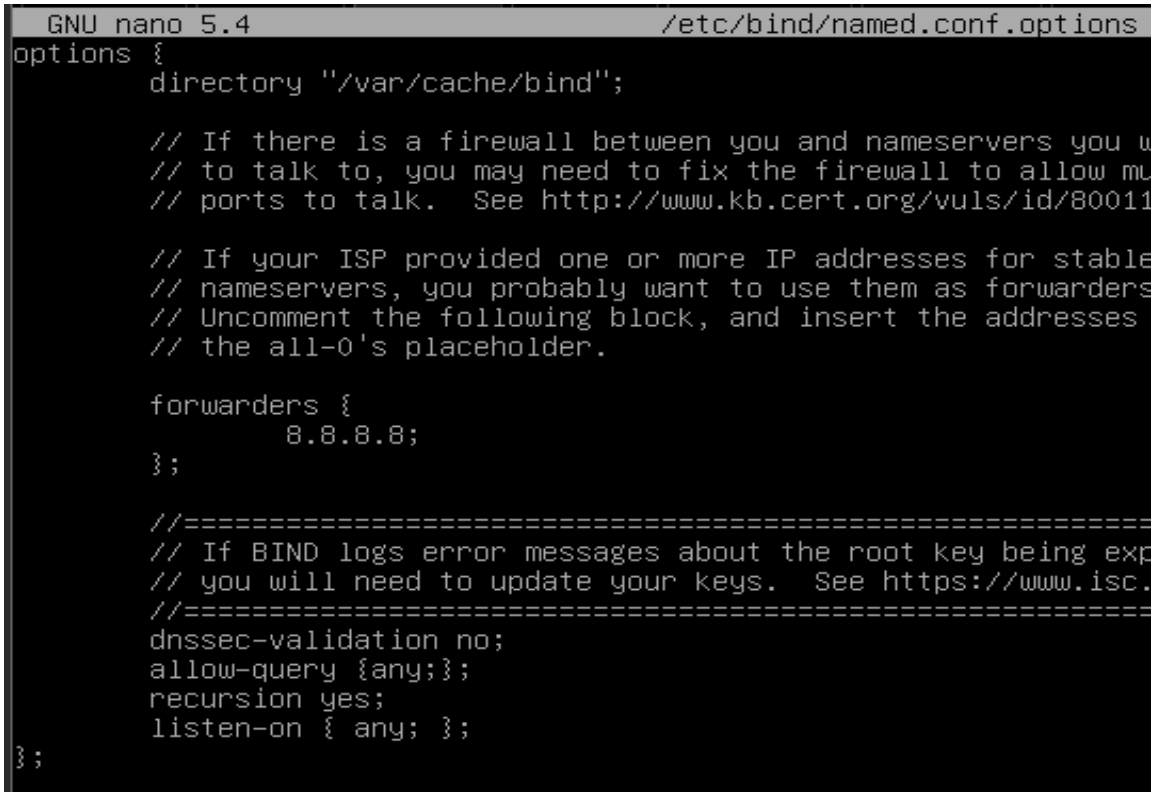


Проверить nft -f /etc/nftables.conf

ssh user@5.5.5.100 -p 2244

DNS - First AND Second

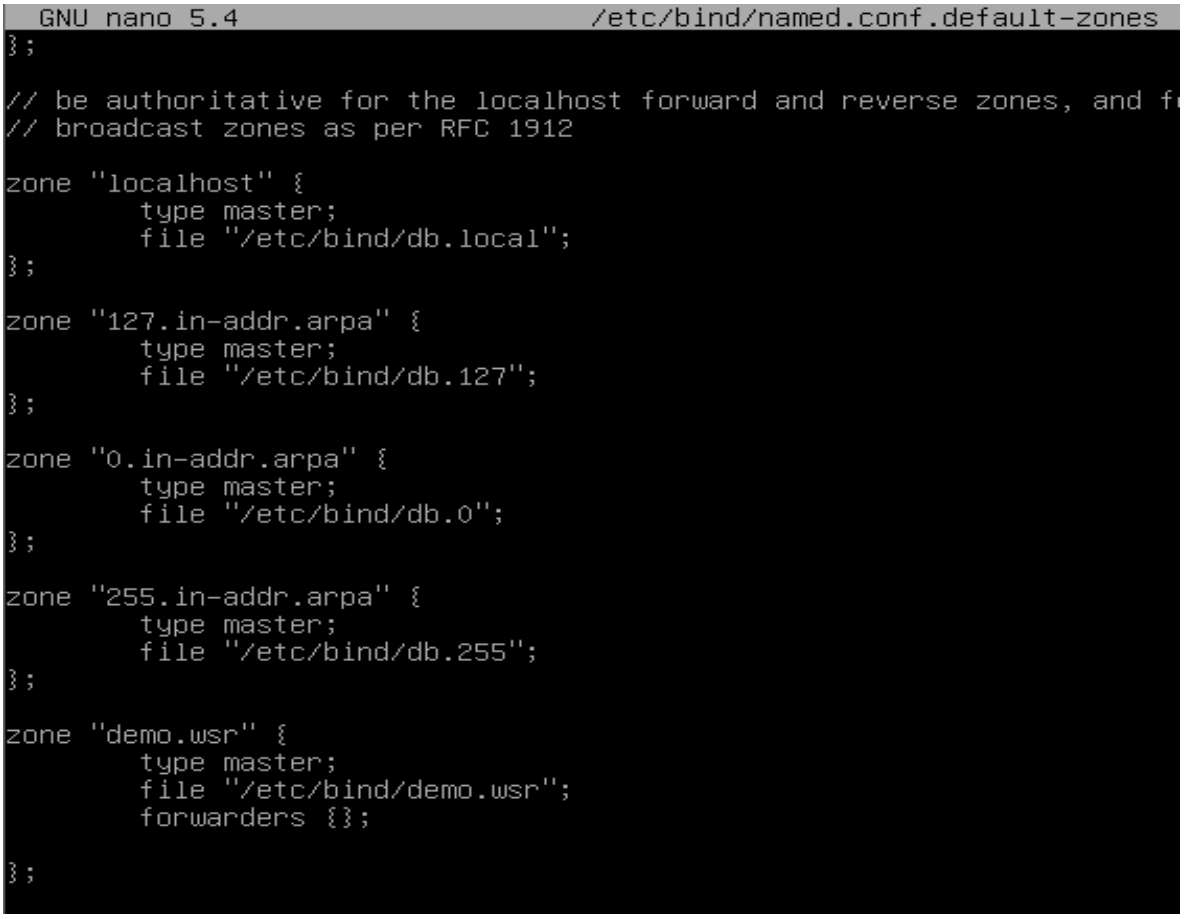
1. Устанавливаем на ISP - **apt install bind9**
2. В конфиге **/etc/bind/named.conf.options** прописать следующие строки:




```
forwarders {
        8.8.8.8
};
        dnssec-validation no;
        allow-query {any;};
        recursion yes;
        listen-on { any; };
};
```

3. Далее в конфиге - **/etc/bind/named.conf.default-zones** пишем :

```
zone "demo.wsr" {
        type master;
        file "/etc/bind/demo.wsr";
        forwarders {};
};
```



4. Нужно поменять директорию и скопировать файл.
   cd /etc/bind; cp db.local demo.wsr
5. Далее нужно отредактировать **demo.wsr**
   (NE CTRL+V)

```
; BIND for demo.wsr
$ORIGIN demo.wsr.
@       IN      SOA   demo.wsr.    root.demo.wsr. (

@       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

$ORIGIN int.demo.wsr.
@       IN      NS    int.demo.wsr.
@       IN      A     4.4.4.100
```

```
 GNU nano 5.4                                  /etc/bind/demo.wsr
;
; BIND data file for demo.wsr interface
;
$TTL    86400
$ORIGIN demo.wsr.
@       IN      SOA     demo.wsr. root.demo.wsr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; 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

$ORIGIN int.demo.wsr.
@       IN      NS      int.demo.wsr.
@       IN      A       4.4.4.100
```

Для проверки надо написать команду **named-checkconf- z**

Для перезапуска службы **systemctl restart bind9**

Для полной проверки нужно с Web-L(R) сделать следующее:

```
root@WEB-L:~# host demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

Host demo.wsr not found: 2(SERVFAIL)
root@WEB-L:~# host demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

demo.wsr has address 3.3.3.1
root@WEB-L:~# host isp.demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

isp.demo.wsr has address 3.3.3.1
root@WEB-L:~# host www.demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

www.demo.wsr has address 5.5.5.100
www.demo.wsr has address 4.4.4.100
```

6. Только на RTR-L нужно в nftables.conf прописать (где tcp dport 2222…) следующую строку
   udp dport 53 dnat to 192.168.100.200:53;
7. На SRV:

   nano /etc/bind/named.conf.options

   uncomment "forwarders" and put there 3.3.3.1;

   ```
   dnssec-validation no;
   allow-query {any;};
   recursion yes;
   listen-on { any; };
   allow-recursion { 172.16.100.0/24; 192.168.100.0/24; };
   ```
8. В nano /etc/bind/named.conf.default-zones прописать

   ```
   zone "demo.wsr" {
   	type master;
   	file "/etc/bind/int.demo.wsr";
   };

   zone "100.168.192.in-addr.arpa" {
   	type master;
   	file "/etc/bind/left.reverse";
   };

   zone "100.16.172.in-addr.arpa" {
   	type master;
   	file "/etc/bind/right.reverse";
   };
   ```
9. cd /etc/bind; cp db.local int.demo.wsr; cp db.local left.reverse; cp db.local right.reverse
10. d

    SRV:

    Nano /etc/bind/named.conf.options

    uncomment "forwarders" and put there 3.3.3.1;

```
        dnssec-validation no;
        allow-query {any;};
        recursion yes;
        listen-on { any; };
        allow-recursion { 172.16.100.0/24; 192.168.100.0/24; };

nano /etc/bind/named.conf.default-zones

zone "int.demo.wsr" {
        type master;
        file "/etc/bind/int.demo.wsr";
};

zone "100.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/left.reverse";
};

zone "100.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/right.reverse";
};

cd /etc/bind;
cp db.local int.demo.wsr
cp db.local left.reverse
cp db.local right.reverse

cd /etc/bind; cp db.local int.demo.wsr; cp db.local left.reverse; cp
db.local right.reverse

nano int.demo.wsr
#First text write by your own (DO NOT CTRL+C - CTRL-V)
; BIND ... for int.demo.wsr ...
@       IN      SOA  int.demo.wsr.       root.int.demo.wsr. (
                        ...
                        ...
```

```
                        ...
;
@       IN      NS      int.demo.wsr.
@       IN      A       192.168.100.200
web-l   IN      A       192.168.100.100
web-r   IN      A       172.16.100.100
srv     IN      A       192.168.100.200
rtr-l   IN      A       192.168.100.254
rtr-r   IN      A       172.16.100.254
ntp     IN      CNAME   srv
dns     IN      CNAME   srv
webapp  IN      CNAME   web-l
```

nano left.reverse

```
; BIND ... for 100.168.192.in-addr.arpa ...
@       IN      SOA     100.168.192.in-addr.arpa.       root.100.168.192.in-addr.arpa. (
                        ...
                        ...
                        ...
;
@       IN      NS      int.demo.wsr.
@       IN      A       192.168.100.200
100     PTR     web-l.int.demo.wsr.
200     PTR     srv.int.demo.wsr.
254     PTR     rtr-l.int.demo.wsr.
```

nano right.reverse

```
; BIND ... for 100.16.172.in-addr.arpa ...
@       IN      SOA     100.16.172.in-addr.arpa.        root.100.16.172.in-addr.arpa. (
                        ...
                        ...
                        ...
;
```

```
@     IN    NS    int.demo.wsr.
@     IN    A     192.168.100.200
100   PTR   web-r.int.demo.wsr.
254   PTR   rtr-r.int.demo.wsr.
```
