СОС

Доп приколы

 Для быстрого получения доступа в интернет на ADMIN-PC, чтобы зайти в интернет в свою методичку

 RTR-L

1. vim /etc/net/sysctl.conf
   1. net.ipv4.ip\_forward = 1
2. cd /etc/net/ifaces
3. cp -r ens19/ ens21
4. vim ens21/options
   1. BOOTPROTO=static
5. vim ens21/ipv4address
   1. 20.20.20.1/24
6. reboot
7. apt-get update && apt-get install nftables -y
8. vim /etc/nftables/nftables.nft
   1. в начало: flush ruleset;
   2. в конец: table ip nat {

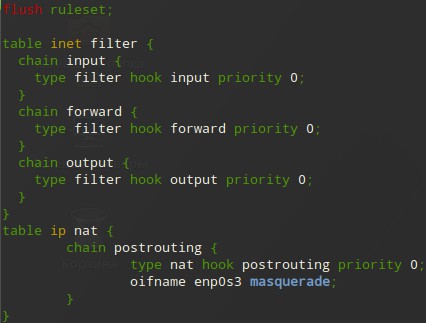
chain postrouting {

type nat hook postrouting priority 0; oifname ens19 masquerade;

}

}

* 1. вот так:



1. systemctl enable --now nftables
2. nft -f /etc/nftables/nftables.nft  ADMIN-PC
3. cd /etc/net/ifaces/ens19
4. vim options
   1. BOOTPROTO=static
5. vim ipv4address
   1. 20.20.20.2.24
6. vim ipv4route
   1. default via 20.20.20.1
7. reboot
8. в /etc/resolv.conf должен быть указан nameserver

94.232.137.104, если нет его, прописываем в начало файла сами

1. все, теперь должен быть интернет, заходите в Firefox на admin- pc и по методичке дальше настриваете

 Конфигурирование RTR-L и L-SRV с ADMIN-PC с помощью SSH подключения (необязательно)

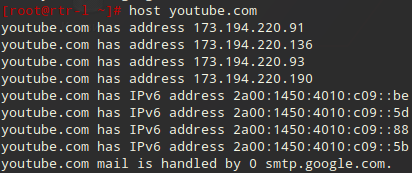
После того, как зашли в интернет на ADMIN-PC, вы можете пожете подключиться по SSH с ADMIN-PC до RTR-L, так как ip адреса пока только на них есть для этого на ADMIN-PC надо написать ssh

[user@20.20.20.2,](mailto:user@20.20.20.2) ответить yes, ввести пароль от user - resu, все, вы зашли на RTR-L с консоли ADMIN-PC, теперь вы можете в браузере открыть свою методичку, копировать оттуда что надо и вставлять в консоль, если что в консоли скопировать вставить через Shift (Ctrl + Shift + C и Ctrl + Shift + V). Чтобы с ADMIN-PC подключиться по ssh до L-SRV, надо настроить dhcp на rtr-l и получить адрес на srv по dhcp.

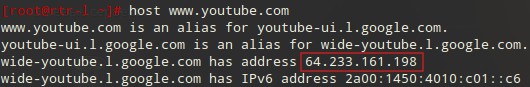
Экзамен

Делаем последовательно, начиная с RTR-L  RTR-L

1. hostnamectl set-hostname rtr-l.au.team
2. vim /etc/net/sysctl.conf
   1. net.ipv4.ip\_forward = 1
3. cd /etc/net/ifaces
4. cp -r ens19/ ens20
5. vim ens20/options
   1. BOOTPROTO=static
6. cp -r ens20/ enp0s21
7. vim ens20/ipv4address
   1. 10.10.10.1/24
8. vim ens21/ipv4address
   1. 20.20.20.1/24
9. systemctl restart network
10. reboot
11. apt-get update && apt-get install nftables dhcp-server bind-utils -y
12. host youtube.com
13. смотрим ip адреса ютуба для написания правил блокировки в nftables, которые получим, IPv6 адреса не нужно запоминать



1. Получили 173.194.220.91 (у вас может быть другой адрес!) и еще 3 других адреса, надо для правил в nftables запомнить 173.194.0.0/16, то есть первые два числа
2. host [www.youtube.com](http://www.youtube.com/)
3. Смотрим этот адрес для написания правил блокировки в nftables



1. Получили 64.233.161.198 (у вас может быть другой адрес!), надо

для правил в nftables запомнить 64.233.0.0/16, то есть первые два числа

1. vim /etc/nftables/nftables.nft
   1. в начало: flush ruleset;
   2. в chain input:

ip saddr 10.10.10.100 icmp type echo-request drop; ip saddr 10.10.10.100 tcp dport 65000 drop;

* 1. в chain forward:

ip daddr 64.233.0.0/16 drop; (здесь 64.233.0.0/16 адрес, который мы запомнили ранее)

ip daddr 173.194.0.0/16 drop; (здесь 173.194.0.0/16 адрес, который мы запомнили ранее)

* 1. в chain output:

ip daddr 10.10.10.100 icmp type echo-request drop;

ip daddr 64.233.0.0/16 drop; (здесь 64.233.0.0/16 адрес, который мы запомнили ранее)

ip daddr 173.194.0.0/16 drop; (здесь 173.194.0.0/16 адрес, который мы запомнили ранее)

* 1. в конец: table ip nat {

chain postrouting {

type nat hook postrouting priority 0; oifname ens19 masquerade;

}

chain prerouting {

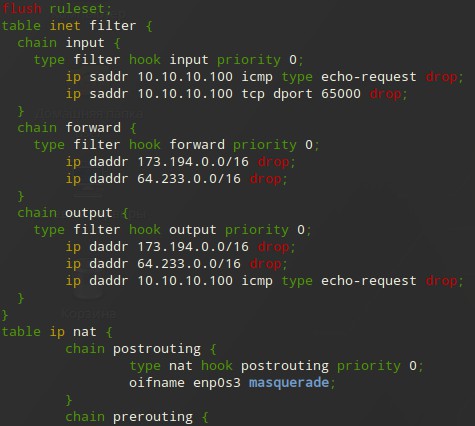
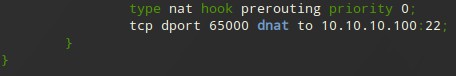
type nat hook prerouting priority 0;

tcp dport 65000 dnat to 10.10.10.100:22;

}

}

* 1. вот так:



1. systemctl enable --now nftables
2. nft -f /etc/nftables/nftables.nft
3. vim /etc/dhcp/dhcpd.conf
   1. вписываем это:

option subnet-mask 255.255.255.0; option domain-name "au.team";

option domain-name-servers 10.10.10.100;

subnet 10.10.10.0 netmask 255.255.255.0 {

range 10.10.10.100 10.10.10.120;

option routers 10.10.10.1;

}

subnet 20.20.20.0 netmask 255.255.255.0 {

range 20.20.20.150 20.20.20.200;

option routers 20.20.20.1;

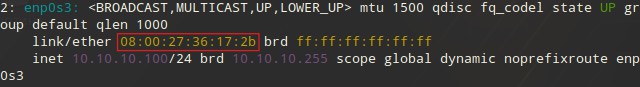
}

host l-srv {

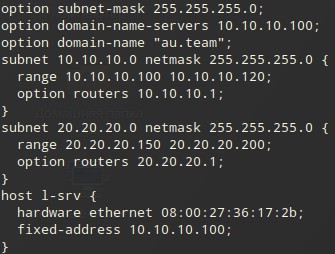
hardware ethernet (MAC-адрес l-srv см. пункт b); fixed-address 10.10.10.100;

}

* 1. Чтобы узнать MAC-адрес l-srv, пишем на l-srv команду ip -c a, ищем строку link/ether xx:xx:xx:xx:xx:xx, вот здесь, тут написан MAC-адрес, его записываем в hardware ethernet в пункте выше **БЕЗ СКОБОК**:

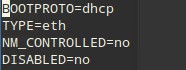


* 1. вот так:



1. vim /etc/sysconfig/dhcpd
   1. DHCPDARGS="ens20 ens21"
2. systemctl enable --now dhcpd
3. vim /etc/openssh/sshd\_config
   1. расскоментируем Port 22
   2. расскоментируем PasswordAuthentication yes
4. systemctl restart sshd  ADMIN-PC
5. hostnamectl set-hostname admin-pc.au.team
6. vim /etc/net/ifaces/ens19/options
   1. BOOTPROTO=dhcp
   2. TYPE=eth
   3. NM\_CONTROLLED=no
   4. DISABLED=no

# вот так и больше ничего:



1. reboot
2. Так как DNS на SRV еще не настроили, а интернет нужен, то в vim /etc/resolv.conf пишем:
   1. добавить в начало: nameserver 94.232.137.104
   2. после того, как мы настроили свой DNS сервер в лице L-SRV и он работает, а именно после 15 пунтка в L-SRV, надо в

/etc/resolv.conf указать только domain au.team и nameserver 10.10.10.100, больше ничего.

1. Теперь на ADMIN-PC должен быть выход в интернет, заходим в Firefox куда надо
2. apt-get update && apt-get install samba-client krb5-kdc task-auth-ad- sssd -y
3. (После настройки L-SRV)
4. system-auth write ad au.team admin-pc AU ‘administratorʼ ‘P@ssw0rdʼ
5. net ads testjoin
6. reboot
7. заходим под user пароль resu
8. su-
9. mkdir /mnt/Adsamba
10. vim /etc/fstab
    1. добавляем в конец:

 пишем не через пробел, а через Tab:

//l-srv.au.team/public /mnt/Adsamba cifs user=user1.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user2.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user3.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user4.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user5.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user6.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user7.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user8.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user9.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user10.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user11.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user12.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user13.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user14.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user15.userl,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user1.admin,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user2.admin,password=P@ssw0rd,rw 0 0

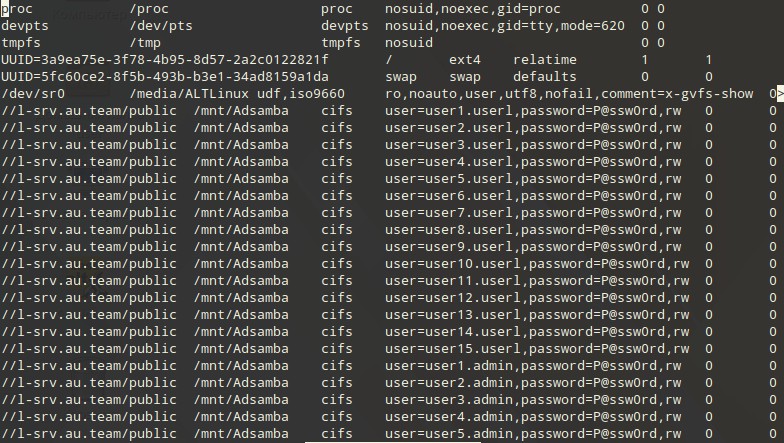
//l-srv.au.team/public /mnt/Adsamba cifs user=user3.admin,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs user=user4.admin,password=P@ssw0rd,rw 0 0

//l-srv.au.team/public /mnt/Adsamba cifs

user=user5.admin,password=P@ssw0rd,rw 0 0

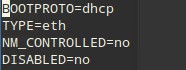
Должно получиться так:



L-SRV

1. hostnamectl set-hostname l-srv.au.team
2. vim /etc/net/ifaces/ens19/options
   1. BOOTPROTO=dhcp
   2. TYPE=eth
   3. NM\_CONTROLLED=no
   4. DISABLED=no

# вот так и больше ничего:



1. reboot
2. vim /etc/resolv.conf
   1. в начало:

nameserver 94.232.137.104

1. apt-get update && apt-get install task-samba-dc krb5-kdc -y
2. systemctl stop smb nmb krb5kdc slapd bind dnsmasq
3. systemctl disable smb nmb krb5kdc slapd bind dnsmasq
4. rm -f /etc/samba/smb.conf
5. rm -rf /var/lib/samba
6. rm -rf /var/cache/samba
7. mkdir -p /var/lib/samba/sysvol
8. samba-tool domain provision
   1. будут вылезать подсказки для настройки домена, нужно ответить на них вот так:

Realm [AU.TEAM]: //жмем Enter Domain [AU]: //жмем Enter

Server Role (dc, member, standalone) [dc]: //жмем Enter

DNS backend (SAMBA\_INTERNAL, BIND9\_FLATFILE, BIND

9\_DLZ, NONE) [SAMBA\_INTERNAL]: //жмем Enter

DNS forwarder IP address (write 'none' to disable forwarding) [94.232.137.104]: //если в квадратных скобках не указан 94.232.137.104, то пишем 94.23

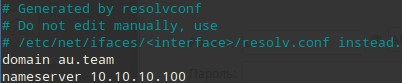
2.137.104 и жмем Enter, если уже указан, то прост о жмем Enter.

Administrator password: //Вводим пароль P@ssw0rd Retype password: //Повторяем пароль P@ssw0rd

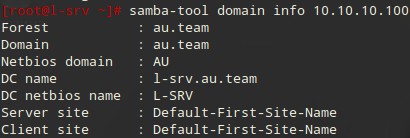
1. systemctl enable --now samba
2. reboot
3. cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
4. vim /etc/resolv.conf
   1. должно быть указано только: domain au.team

nameserver 10.10.10.100

* 1. вот так:



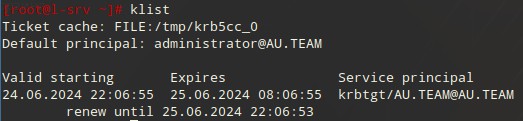
1. systemctl restart network
2. проверяем (на всякий случай):
   1. samba-tool domain info 10.10.10.100



* 1. kinit administrator

вводим пароль P@ssw0rd

* 1. klist



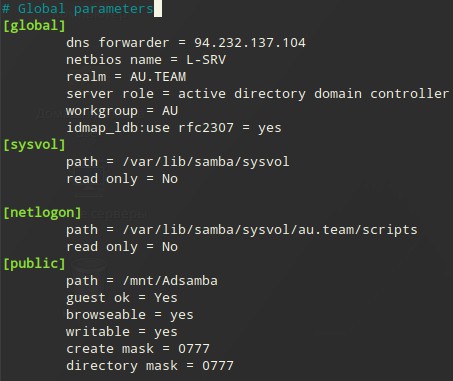
1. for i in {1..15}; do samba-tool user create user$i.userl P@ssw0rd; done;
2. for i in {1..5}; do samba-tool user create user$i.admin P@ssw0rd; done;
3. samba-tool group add left
4. samba-tool group add admin
5. for i in {1..15}; do samba-tool group addmembers left user$i.userl; done;
6. for i in {1..5}; do samba-tool group addmembers admin user$i.admin; done;
7. samba-tool dns zonecreate 10.10.10.100 10.10.10.in-addr.arpa -U administrator
   1. пароль P@ssw0rd
8. samba-tool dns zonecreate 10.10.10.100 20.20.20.in-addr.arpa -U administrator
   1. пароль P@ssw0rd
9. samba-tool dns add 10.10.10.100 au.team admin-pc A 20.20.20.150 -U administrator
   1. пароль P@ssw0rd
10. samba-tool dns add 10.10.10.100 au.team rtr-l A 20.20.20.1 -U administrator
    1. пароль P@ssw0rd
11. samba-tool dns add 10.10.10.100 au.team rtr-l A 10.10.10.1 -U administrator
    1. пароль P@ssw0rd
12. samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 1 PTR rtr- l.au.team -U administrator
    1. пароль P@ssw0rd
13. samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 100 PTR l- srv.au.team -U administrator
    1. пароль P@ssw0rd
14. samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 150 PTR admin- pc.au.team -U administrator
    1. пароль P@ssw0rd
15. samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 1 PTR rtr- l.au.team -U administrator
    1. пароль P@ssw0rd
16. samba-tool dns add 10.10.10.100 au.team dc CNAME l-srv.au.team -U administrator
    1. пароль P@ssw0rd
17. mkdir /mnt/Adsamba/
18. chmod 0777/mnt/Adsamba/
19. vim /etc/samba/smb.conf
    1. добавляем в директиву [global]: idmap-ldb:use rfc2307 = yes
    2. добавляем в конец файла новую директиву [public] и в нее записываем через Tab:

path = /mnt/Adsamba guest ok = yes browseable = yes

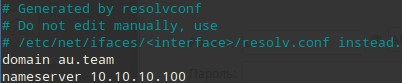
writable = yes

create mask = 0777 directory mask = 0777

* 1. вот так должно быть по итогу:



1. Теперь, так как мы настроили свой DNS сервер и если он работает нормально, надо на всех машинах в /etc/resolv.conf указать domain au.team и nameserver 10.10.10.100, больше ничего, вот так:



Траблшутинг

1. Если есть ping 8.8.8.8, но нет ping ya.ru, то проблема в DNS сервере, заходим в /etc/resolv.conf и добавляем в начало nameserver

94.232.137.104, НО после того, как мы настроили свой DNS сервер в лице L-SRV и он работает нормально, а именно после 15 пунтка в L- SRV, надо в /etc/resolv.conf указать только domain au.team и nameserver 10.10.10.100, больше ничего.

1. Если проблема с Samba на L-SRV, просто systemctl disable --now bind и systemctl restart samba
2. Если host au.team или dig au.team или nslookup au.team не работают, то указываем в /etc/resolv.conf только domain au.team и nameserver

10.10.10.100, больше ничего.

1. Если на L-SRV или ADMIN-PC пропали ip адреса, полученные от dhcp сервера на RTR-L, попробуйте systemctl restart network на них, если не помогло, то на RTR-L пишем systemctl restart dhcpd, systemctl status

dhcpd, если в статусе dhcp нет ошибок, то переходим опять на L-SRV или ADMIN-PC, где пропали адреса и заново пишем systemctl restart network.

1. Если при настройке домена после команды samba-tool domain provision на L-SRV в скобках после Realm написано не au.team, проверьте /etc/hostname, там должно быть l-srv.au.team, если там так, то reboot, если не так, то hostnamectl set-hostname l-srv.au.team и потом reboot
2. Если в /etc/resolv.conf меняется сам по себе и там появляется nameserver 127.0.0.1 и добавляется еще какой-то option, то пишите нужные настройки и chattr +i /etc/resolv.conf
3. Если на L-SRV kinit administrator не работает, то надо на L-SRV написать systemctl disable --now krb5kdc, systemctl stop samba,

systemctl start samba, systemctl restart samba, еще надо проверить systemctl status samba на отсутствие ошибок.

1. Если у ADMIN-PC или L-SRV адрес полученный по DHCP не тот, который нужен по таблице, например у ADMIN-PC 20.20.20.151 или 20.20.20.152, а не 20.20.20.150, то перепроверяем ens19/options на

ADMIN-PC, делаем systemctl restart network, если все равно такой-же адрес, то заходим в RTR-L, открываем файл vim

/var/lib/dhcp/dhcpd/state/dhcpd.leases и комментируем все записи lease **server-duid не трогаем** (см. рисунок ниже), далее systemctl

restart dhcp, потом переходим на ADMIN-PC и пишем systemctl restart network

