БАЗОВАЯ НАСТРОЙКА

Смена имени хоста:

```
echo ИМЯ > /etc/hostname
```

Настройка сети.

1) Открываем конфиг:

```
nano /etc/network/interfaces
```

2) Прописываем параметры:

```
auto ensXX
iface ensXX inet static
address XXX.XXX.XXX.XXX/XX
gateway XXX.XXX.XXX.XXX
```

3) Добавляем маршруты при необходимости:

```
up ip ro add XXX.XXX.XXX.XXX/XX via XXX.XXX.XXX.XXX dev ensXX
```

4) Перезагружаем службу сети после настройки:

```
systemctl restart networking.services
```

УСТАНОВКА ФАЙРВОЛА

1. Устанавливаем службу:

```
apt install ufw -y
```

2. Включаем службу:

```
systemctl enable ufw
ufw enable
```

3. Запрещаем все входящие подключения:

```
ufw default deny incoming
```

Чтобы разрешить работу службы или порта вводим команду:

```
ufw allow СЛУЖБА|ПОРТ
```

Примеры:

```
ufw enable ssh
ufw enable 21
```

Чтобы запретить, вместо «allow» следует написать «deny».

Чтобы разрешить подключения от определённого хоста в сети, вводим команду:

```
ufw allow from XXX.XXX.XXX.XXX
```

Сброс всех правил файрвола:

```
ufw reset
```

После сброса брандмауэра UFW нужно будет снова включить брандмауэр и начать весь процесс добавления правил. По возможности следует использовать команду сброса с осторожностью.

НАСТРОЙКА NAT

Убедитесь, что перед этим вы установили файрвол.

1. Открываем конфиг:

```
nano /etc/sysctl.conf
```

2. Раскомментируем следующую строчку:

```
net.ipv4.ip_forward=1
```

3. Применяем изменения:

```
sysctl -p
```

4. Открываем скрипт:

```
nano /etc/network/if-pre-up.d/nat
```

5. Пишем в нём:

```
#!/bin/sh
/sbin/iptables -A POSTROUTING -t nat -j MASQUERADE
```

6. Делаем этот файл исполняемым:

```
chmod +x /etc/network/if-pre-up.d/nat
```

7. Перезагружаем систему:

```
reboot
```

УСТАНОВКА ТУННЕЛЯ

1. Устанавливаем службу:

```
apt install strongswan -y
```

2. Включаем службу:

```
systemctl enable strongswan-starter
```

3. Открываем конфиг:

```
nano /etc/ipsec.conf
```

4. Прописываем параметры:

```
conn name
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=XXX.XXX.XXX.XXX
        leftsubnet=XXX.XXX.XXX.XXX/XX
        right=XXX.XXX.XXX.XXX
        rightsubnet=XXX.XXX.XXX.XXX/XX
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
```

5. Открываем конфиг:

```
nano /etc/ipsec.secrets
```

6. Пишем нужный ключ:

```
XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX : PSK “ключ” #откуда-куда
```

7. Перезагружаем службу:

```
systemctl restart ipsec
```

УСТАНОВКА SSH

1. Устанавливаем службу:

```
apt install ssh -y
```

2. Включаем службу:

```
systemctl enable ssh
```

3. Открываем конфиг:

```
nano /etc/ssh/sshd_config
```

4. Находим следующую строчку:

```
#permitrootlogin prohibit-password
```

5. Раскомментируем и разрешаем подключение через рута:

```
permitrootlogin yes
```

6. При необходимости меняем порт:

```
Port ПОРТ
```

Перезагружаем службу после настройки:

```
systemctl restart ssh
```

Команда для подключения через SSH:

```
ssh -p ПОРТ root@XXX.XXX.XXX.XXX
```

УСТАНОВКА DHCP

1. Устанавливаем службу:

```
apt install isc-dhcp-server -y
```

2. Открываем конфиг:

```
nano /etc/dhcp/dhcpd.conf
```

3. Прописываем параметры:

```
subnet XXX.XXX.XXX.XXX netmask 255.255.255.0 { #подсеть и маска
        range XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX; #диапазон выдачи от и до
        option subnet-mask 255.255.255.0; #маска
        option broadcast-address XXX.XXX.XXX.255; #широковещательный адрес
        option domain-name-servers XXX.XXX.XXX.XXX, XXX.XXX.XXX.XXX; #DNS
        default-lease-time 7200;
        max-lease-time 480000;
 }
```

4. Открываем конфиг:

```
nano /etc/default/isc-dhcp-server
```

5. Прописываем сетевой интерфейс:

```
INTERFACESv4 = "ensXX"
```

6. Перезапускаем службу:

```
systemctl restart isc-dhcp-server
```

УСТАНОВКА SMB

1. Устанавливаем службу:

```
apt install cifs-utils
```

2. Создаём каталог:

```
mkdir /opt/share
```

3. Открываем конфиг подключения:

```
nano /etc/fstab
```

4. Прописываем параметры:

```
//СЕТЕВАЯ ПАПКА /opt/share cifs user,rw,credentials=/root/.smbclient 0 0
```

5. Открываем конфиг с данными для авторизации:

```
nano /root/.smbclient
```

6. Прописываем логин и пароль:

```
username=ЛОГИН
password=ПАРОЛЬ
```

7. Монтируемся:

```
mount -a
```

НАСТРОЙКА NTP

1. Устанавливаем службу:

```
apt install chrony -y
```

Настройка для сервера:

1. Открываем конфиг:

```
nano /etc/chrony/chrony.conf
```

2. Прописываем:

```
local stratum 4
allow XXX.XXX.XXX.XXX/XX
```

Настройка для клиента:

1. Открываем конфиг:

```
nano /etc/chrony/chrony.conf
```

2. Прописываем после строчки "#Use Debian vendor zone" следующее:

```
pool СЕРВЕР iburst
allow XXX.XXX.XXX.XXX/XX
```

Перезагружаем службу:

```
systemctl restart chrony.service
systemctl restart chronyd.service
```

Проверка синхронизации:

```
chronyc tracking
```

ШПАРГАЛКИ

Монтирование диска:

```
apt-cdrom add
```

Обновление пакетов:

```
apt update
```

Показать список файлов и каталогов в директории:

```
ls
```

Проверка соединения:

```
ping XXX.XXX.XXX.XXX
```

Узнать IP по домену:

```
nslookup ДОМЕН
```

Создание и редактирование конфига или скрипта:

```
nano ПУТЬ К ФАЙЛУ
```

Перезагрузить систему:

```
reboot
```

Выключить систему:

```
poweroff
```