??????

Установка sudo

```
apt-get install sudo
usermod -aG sudo username
```

Шаблон /etc/network/interfaces

```
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.1.10
gateway 192.168.1.1
netmask 255.255.255.0
dns-nameservers 8.8.8.8 8.8.4.4
```

Узнать текущий dhcp сервер:

```
sudo dhclient -v
```

Оставить только один шлюз по умолчанию при двух серверах dhcp

```
cat /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 enp0s3
iface enp0s3 inet dhcp
    post-up ip route add default via $(ip route | grep 'default via' | awk '{print $3}') dev
enp0s3 2>/dev/null || true
```

```
allow-hotplug enp0s8
iface enp0s8 inet dhcp
    post-up ip route add 192.168.0.0/16 via 192.168.51.1
    post-up ip route del default dev enp0s8 2>/dev/null || true
```

Архивация папки рекурсивно

```
zip -r archive.zip myfolder/
```

Копирование файла по scp

```
scp /home/sergey/file sergey@192.168.1.10:~/
scp sergey@192.168.1.10:~/file ~/
```

Закодировать строку в Base64

```
echo "My string" | base64
```

openVPN

```
sudo openvpn <файл_конфига>
```

Временный socks5 VPN

```
ssh -D 8081 -N -f username@your-vpn-server.com
#в случае ключа
ssh -D 8081 -N -f -i ~/.ssh/your_private_key username@your-vpn-server.com
# завершение фонового процесса
ps aux | grep ssh
kill <pid>
```

Запуск сетевого взаимодействия через proxy без изменения настроек приложения

```
sudo apt install tsocks
# в файле /etc/tsocks.conf path полностью убрал, чтобы весь трафик шел в proxy
local = 192.168.1.0/255.255.255.0
server = 127.0.0.1
server_type = 5
server_port = 1080
#
sudo -s
```

```
tsocks apt update
tsocks apt upgrade
exit
```

Авторизация по ключу

Шаг 1. Вариант 1. Клиент Windows + Putty на Linux Генерим ключ через PuTTYgen. Сохраняем закрытый ключ, для открытого ключа на сервере Шаг 2. Добавляем закрытый ключ к нужной сессии.

Шаг 1. Вариант 2. Клиент Linux. Ключи будут расположены в .ssh/ Нужен id_rsa.pub

```
ssh-keygen -t rsa -b 4096
```

Шаг 2. На сервере.

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
nano ~/.ssh/authorized_keys
#вставить открытый ключ из PuttyGen
chmod 600 ~/.ssh/authorized_keys
```

Дополнительно на сервере можно закрыть доступ по паролю

```
sudo nano /etc/ssh/sshd_config
PubkeyAuthentication yes
PasswordAuthentication no
```

Добавить отображение ip адреса в строку приглашения tty

Создаем службу. sudo nano /etc/systemd/system/update-issue.service

```
[Unit]
Description=Update /etc/issue with current IP
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
# ExecStartPre: ждать IP до 60 секунд
ExecStartPre=/bin/bash -c 'for i in $(seq 1 60); do ip=$(hostname -I | awk "{print \$1}"); [ -
n "$ip" ] && exit 0; sleep 1; done; exit 1'
```

```
ExecStart=/bin/bash -c 'ip=$(hostname -I | awk "{print \$1}"); echo "Debian server — IP: $ip"
> /etc/issue;'
TimeoutStartSec=120

[Install]
WantedBy=multi-user.target
```

Создаем и запускаем службу

```
sudo systemctl daemon-reload
sudo systemctl enable --now update-issue.service
```

Revision #13
Created 13 March 2025 08:00:24 by Admin
Updated 20 March 2026 12:25:04 by Admin