Инструкция по настройке L2TP/IPsec VPN-подключения ОС Linux

НАВИГАЦИЯ

Данная инструкция описывает пошаговую настройку VPN-подключения по протоколу **L2TP/IPsec** для доступа к тестовым сервисам Московской Биржи через интернет.

Подробнее об услуге «Доступ через интернет» см. в документе «Доступ через интернет / подключение к тестовому контуру».

НАСТРОЙКА ЧЕРЕЗ ГРАФИЧЕСКИЙ ИНТЕРФЕЙС LINUX

НАЗНАЧЕНИЕ НЕОБХОДИМЫХ ПАКЕТОВ

ПАКЕТ	НАЗНАЧЕНИЕ
`network-manager-l2tp`	Плагин Network Manager для поддержки L2TP-подключений
`network-manager-l2tp-gnome`	Графический интерфейс для настройки L2TP в GNOME
`net-tools`	Утилиты для работы с сетью (route, ifconfig и др.)
`strongswan`	Реализация IPSec для шифрования L2TP-трафика
`xl2tpd`	Демон для работы с L2TP-протоколом (при настройке без Network Manager)

1. Установите пакеты для поддержки VPN L2TP/IPSEC:

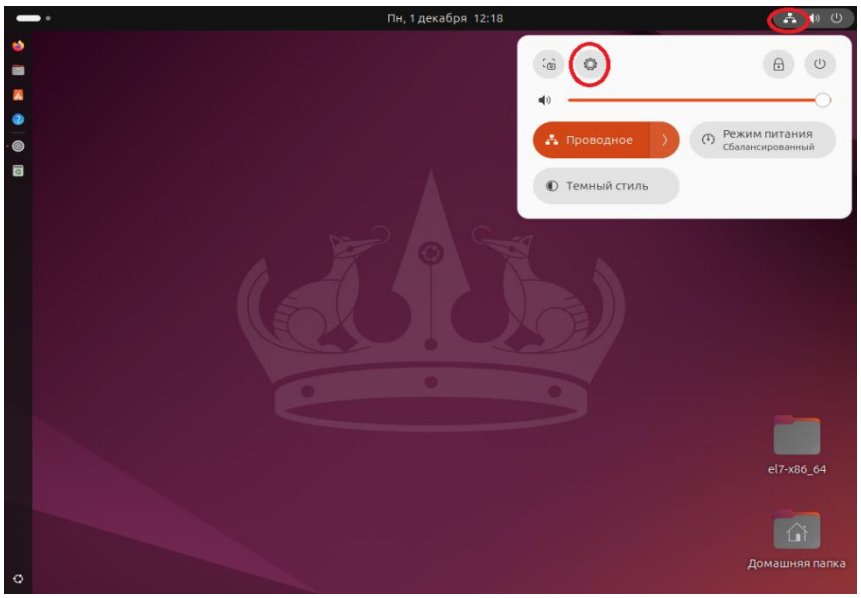
- Ubuntu:

```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt-get update
sudo apt-get install network-manager-l2tp network-manager-l2tp-gnome net-tools
```

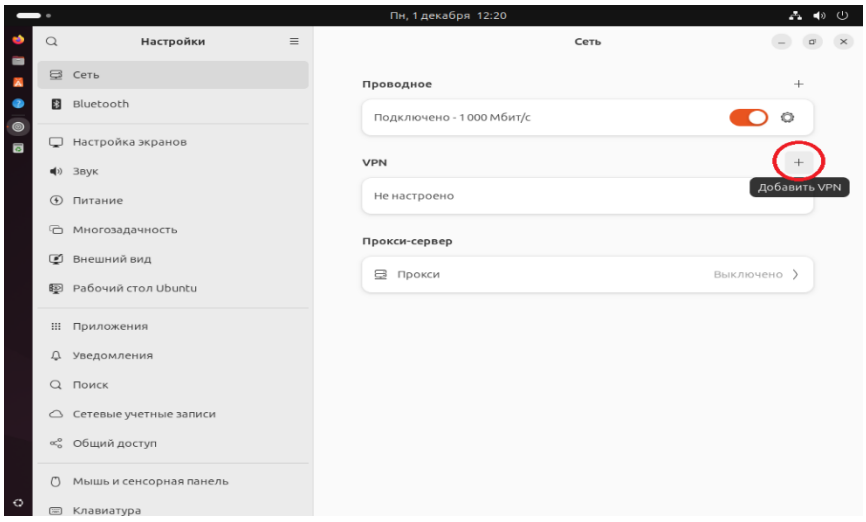
- RHEL/CentOS:

```
sudo dnf install xl2tpd NetworkManager-l2tp NetworkManager-l2tp-gnome net-tools
sudo rpm -e libreswan
sudo dnf install strongswan
```

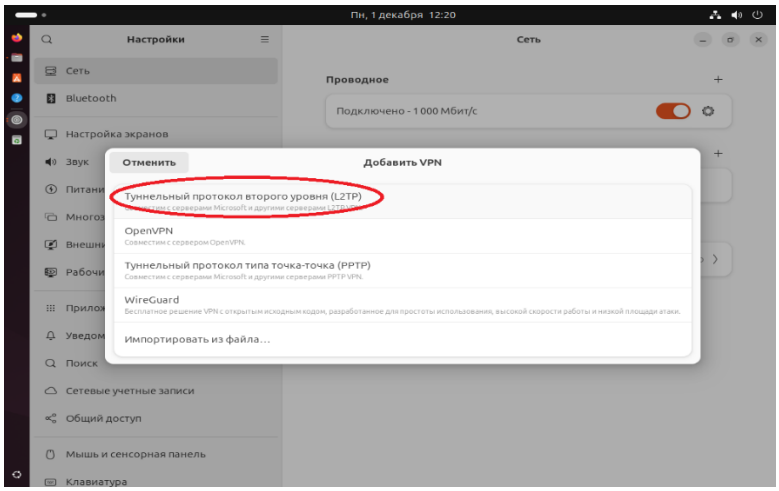
2. Зайдите в **Настройка сети** → **Параметры**:



3. Нажмите **Добавить VPN**:

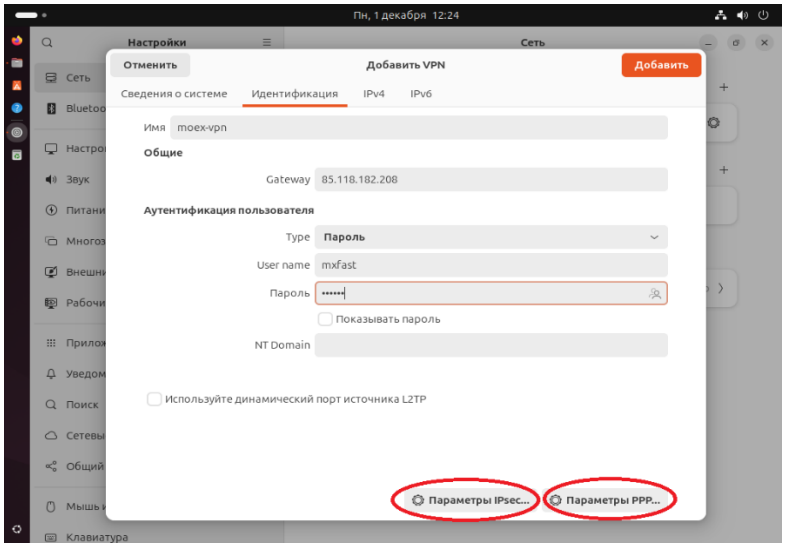


4. Выберите **Туннельный протокол второго уровня (L2TP)**:

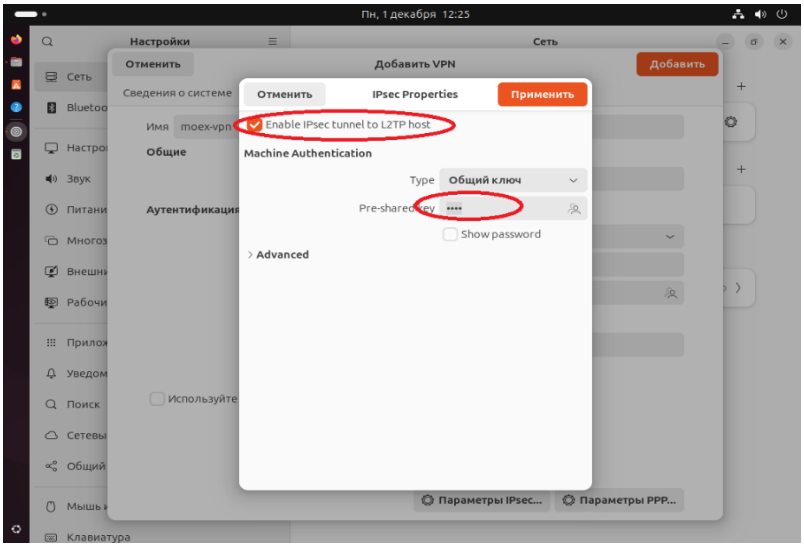


5. Введите следующие настройки:

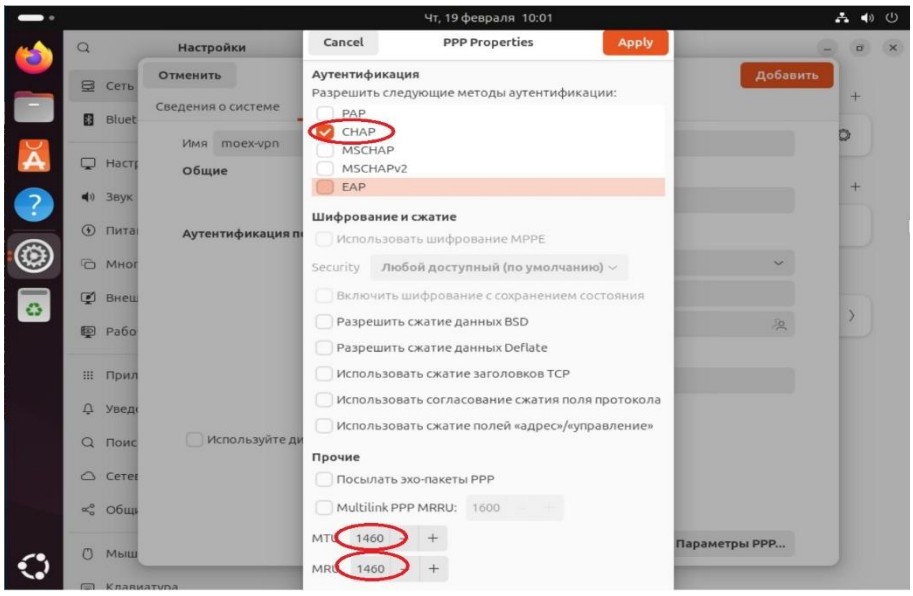
- Имя: moex-vpn;
- Адрес сервера (Gateway): 85.118.182.208;
- Имя (User name) и пароль: mxfast.



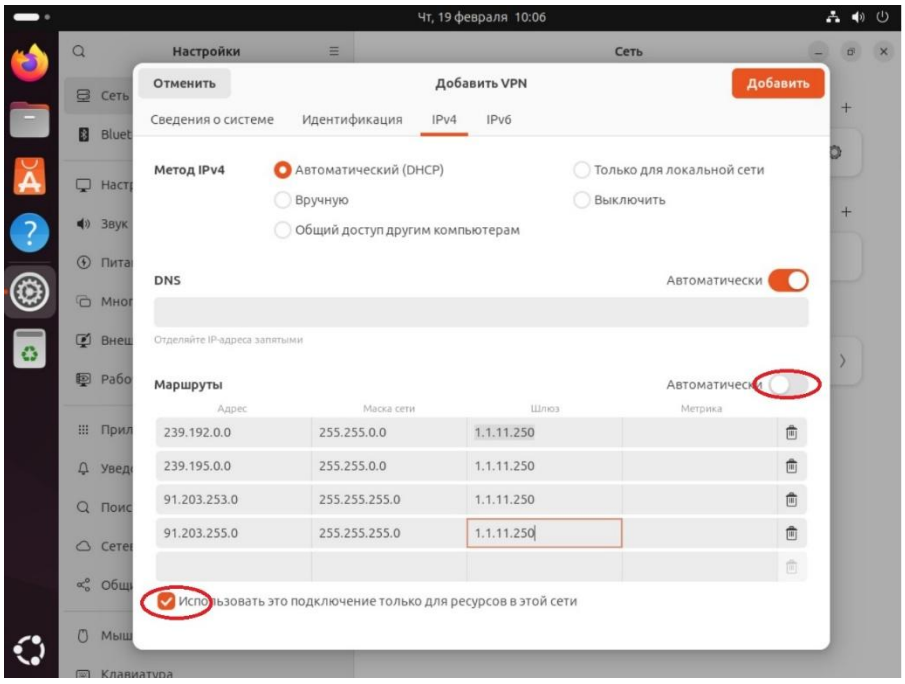
6. Введите общий ключ (**moex**) в параметрах IPSEC:



7. В параметрах PPP выберите **CHAP** и установите значения **MTU** и **MRU** на 1460:



8. Пропишите маршруты во вкладке **IPv4**:



9. (Опционально) Добавьте маршруты через командную строку:

```
sudo route add -net 239.192.0.0 netmask 255.255.0.0 gw 1.1.11.250
sudo route add -net 239.195.0.0 netmask 255.255.0.0 gw 1.1.11.250
sudo route add -net 91.203.253.0 netmask 255.255.255.0 gw 1.1.11.250
sudo route add -net 91.203.255.0 netmask 255.255.255.0 gw 1.1.11.250
```

НАСТРОЙКА ЧЕРЕЗ КОМАНДНУЮ СТРОКУ LINUX (NETWORK MANAGER)

НАЗНАЧЕНИЕ НЕОБХОДИМЫХ ПАКЕТОВ

ПАКЕТ	НАЗНАЧЕНИЕ
`network-manager-l2tp`	Плагин Network Manager для поддержки L2TP-подключений
`network-manager-l2tp-gnome`	Графический интерфейс для настройки L2TP в GNOME
`net-tools`	Утилиты для работы с сетью (route, ifconfig и др.)
`strongswan`	Реализация IPSec для шифрования L2TP-трафика
`xl2tpd`	Демон для работы с L2TP-протоколом (при настройке без Network Manager)

1. Установите пакеты:

- CentOS/RHEL/Fedora/RedOS:

```
sudo yum -y install NetworkManager-l2tp-gnome
sudo dnf -y install NetworkManager-l2tp-gnome
```

- Ubuntu/Debian:

```
apt-get install network-manager-l2tp-gnome
```

2. Если в дистрибутиве установлен libreswan, замените его на strongswan:

```
sudo rpm -e libreswan
sudo dnf install strongswan
```

3. Добавьте VPN-подключение:

```
sudo nmcli connection add connection.id moex con-name moex type VPN vpn-type l2tp
ifname -- connection.autoconnect no ipv4.method auto vpn.data "gateway =
85.118.182.208, ipsec-enabled = yes, ipsec-psk = moex, machine-auth-type = psk, mru =
1460, mtu = 1460, no-vj-comp = yes, noaccomp = yes, nobsdcomp = yes, nodeflate = yes,
nopcomp = yes, password-flags = 0, refuse-eap = yes, refuse-mschap = yes, refuse-
mschapv2 = yes, refuse-pap = yes, user = mxfast" vpn.secrets password=mxfast
```

4. Добавьте маршруты к VPN-подключению:

```
nmcli connection modify moex +ipv4.routes "239.192.0.0/16 1.1.11.250, 239.195.0.0/16
1.1.11.250, 91.203.253.0/24 1.1.11.250, 91.203.255.0/24 1.1.11.250"
```

5. Перезапустите службы:

```
sudo systemctl restart NetworkManager
```

6. Проверьте настройки VPN-подключения:

- Настройки хранятся в папке:
  /etc/NetworkManager/system-connections/.
- Выведите данные обо всех подключениях:
  `nmcli con`

```
[root@localhost ~]# nmcli con
NAME  UUID                                  TYPE      DEVICE
eth0  0ea97d44-1ecc-3d69-8ad2-a56c688e3ae5  ethernet  eth0
lo    bcdeab6c-5069-46c0-9e64-5260a9bc0361  loopback  lo
moex  c74812c7-ab50-481a-98b2-aee7a4bac105  vpn       --
[root@localhost ~]#
```

- Выведите данные о созданном подключении:
  `nmcli c show id moex`

7. Подключитесь к VPN-серверу через командную строку:

```
nmcli c up moex
```

8. Для завершения сессии выполните команду ниже:

```
nmcli c down moex
```

НАСТРОЙКА ЧЕРЕЗ КОМАНДНУЮ СТРОКУ LINUX (БЕЗ NETWORK MANAGER, НА ПРИМЕРЕ UBUNTU)

НАЗНАЧЕНИЕ НЕОБХОДИМЫХ ПАКЕТОВ

ПАКЕТ	НАЗНАЧЕНИЕ
`network-manager-l2tp`	Плагин Network Manager для поддержки L2TP-подключений
`network-manager-l2tp-gnome`	Графический интерфейс для настройки L2TP в GNOME
`net-tools`	Утилиты для работы с сетью (route, ifconfig и др.)
`strongswan`	Реализация IPSec для шифрования L2TP-трафика
`xl2tpd`	Демон для работы с L2TP-протоколом (при настройке без Network Manager)

1. Установите необходимое ПО:

```
apt-get update
apt-get install strongswan xl2tpd net-tools
```

2. Зайдите в настройки IPSec:

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

3. Скопируйте конфигурацию ниже и вставьте в командную строку:

```
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
  # nat_traversal=yes - depricated ubuntu
  # strictcrlpolicy=yes
  # uniqueids = no

# Add connections here.

# Sample VPN connections

conn %default
  ikelifetime=60m
  keylife=20m
  rekeymargin=3m
  keyingtries=1
  keyexchange=ikev1
  authby=secret
  ike=3des-sha1-modp1024!
  esp=3des-sha1!
```

```
conn moex
  keyexchange=ikev1
  left=%defaultroute
  auto=add
  authby=secret
  type=transport
  leftprotoport=17/1701
  rightprotoport=17/1701
  right=85.118.182.208
  rightid=10.50.141.242
```

4. Зайдите в настройки IPSec Pre-Shared Key:

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

5. Укажите ключ:

```
PSK moex
```

6. Смените права на файл ipsec.secrets:

```
chmod 600 /etc/ipsec.secrets
```

7. Зайдите в настройки xl2tpd:

```
nano /etc/xl2tpd/xl2tpd.conf
```

8. Скопируйте конфигурацию ниже и вставьте в командную строку:

```
[lac moex]
lns = 85.118.182.208
ppp debug = yes
pppoptfile = /etc/ppp/options.l2tpd.client
length bit = yes
EOF
```

9. Зайдите в настройки l2tpd.client:

```
nano /etc/ppp/options.l2tpd.client
```

10. Скопируйте конфигурацию ниже и вставьте в командную строку:

```
ipcp-accept-local
ipcp-accept-remote
refuse-eap
require-chap
noccp
noauth
mtu 1460
mru 1460
noipdefault
```

```
defaultroute

usepeerdns

connect-delay 5000

name mxfast

password mxfast
```

11. Смените права на файл options.l2tpd.client:

```
chmod 600 /etc/ppp/options.l2tpd.client
```

12. Создайте каталог и файл:

```
mkdir -p /var/run/xl2tpd

touch /var/run/xl2tpd/l2tp-control
```

13. Перезапустите службы xl2tpd и strongswan:

```
service strongswan restart
```

- На Ubuntu, если сервис strongswan не обнаружен:

```
ipsec restart

service xl2tpd restart
```

14. Проверьте статус:

```
systemctl status xl2tpd

 systemctl status strongswan
```

- На Ubuntu, если сервис strongswan не обнаружен:

```
 systemctl status ipsec
```

15. Подключитесь к VPN-серверу:

- Ubuntu/Debian:

```
ipsec up moex
```

- CentOS/Fedora:

```
strongswan up moex
```

16. Установите L2TP-соединение:

```
echo "c moex" > /var/run/xl2tpd/l2tp-control
```

17. Проверьте, что появился сетевой интерфейс ppp:

```
$ ip a
```

ОТКЛЮЧЕНИЕ VPN-СОЕДИНЕНИЯ

1. Отключите L2TP:

```
echo "d moex" | sudo tee /var/run/xl2tpd/l2tp-control
```

2. Отключите IPSec:

```
sudo strongswan down moex
```

- На Ubuntu, если сервис strongswan не обнаружен:

```
sudo ipsec down moex
```

ПЕРЕЗАГРУЗКА VPN-СОЕДИНЕНИЯ

1. Введите команды:

```
service ipsec restart

service strongswan restart

service xl2tpd restart
```