



Technik12345

30 июн 2023 в 11:17

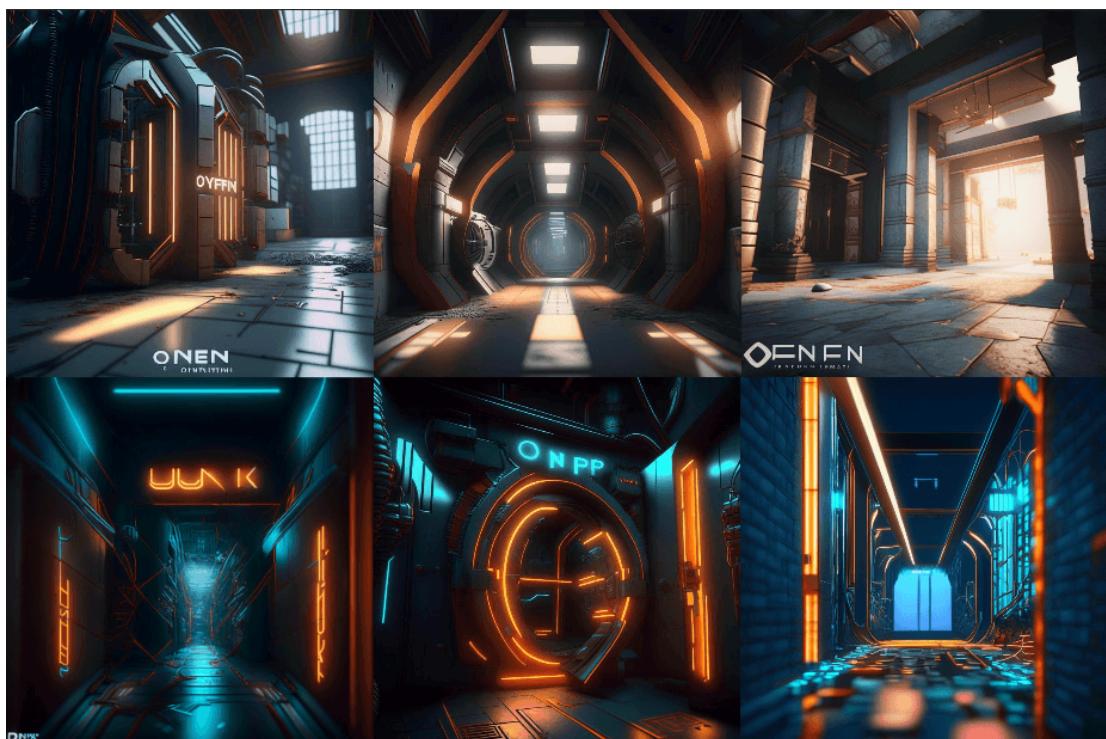
Как поднять OpenVPN сервер на Ubuntu 22.04?

Средний5 мин181K

Настройка Linux*, Облачные сервисы*, Сетевые технологии*

Из песочницы

В эпоху массовых блокировок и ограничений в сети, сохранение своей онлайн приватности становится все более актуальным. И здесь вам на помощь приходит OpenVPN – одно из самых популярных и надежных решений для создания безопасного туннеля в интернет. Если вы хотите обойти географические ограничения, обеспечить защиту своих данных или просто настроить собственный сервер для удаленного доступа к локальным ресурсам, то данная статья именно для вас! Мы рассмотрим этапы создания и настройки своего собственного OpenVPN сервера, чтобы вы могли насладиться свободным и безопасным интернетом, не зависимо от места нахождения. Присоединяйтесь к нам и давайте начнем этот увлекательный путь в мир безграничной свободы в онлайне!



Где взять VPS(виртуальную машину) и как к ней подключится?

Я лично использовал justhost([тык!](#)) и брал самую дешёвую виртуалку в Нидерландах.

Далее будет инструкция по подключению:

1. Зарегистрироваться, оплатить VPS
2. Пока Вы ждёте её включение, скачайте PuTTy([тык!](#), [тык!](#))
3. Когда VPS запустилась, Вам на почту по которой вы зарегистрировались приходит письмо, в котором есть пароль от пользователя root, и IPv4 адрес, запоминаем их
4. Открываем PuTTy и в поле Host Name вводим IP-адрес из письма, запомнили из письма и нажимаем Connect
5. Соглашаемся(Accept) с предупреждением о безопасности(оно появляется 1 раз)



Как мы строим S3

Онлайн-вебинар в Selectel

РЕКЛАМА

6. Если вы увидели надпись *login as:*, то Вы подключились
7. Вводим root и при запросе пароля вводим пароль из письма

```
root@vm549021:~# login as: root
root@194.58.68.46's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-57-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
Last login: Tue Jun 27 10:24:05 2023 from 77.37.184.204
root@vm549021:~#
```

Создание нового пользователя и вход под ним(по соображениям безопасности)

1. useradd -m <любое имя пользователя>
2. passwd <имя созданного ранее пользователя>
3. usermod -aG sudo <имя созданного ранее пользователя>

```
root@vm549021:~# sudo useradd -m Technik12345
root@vm549021:~# sudo passwd Technik12345
New password:
Retype new password:
passwd: password updated successfully
```

```
root@vm549021:~# usermod -aG sudo Technik12345
```

1. sudo chsh -s /bin/bash <имя созданного ранее пользователя>

Подключаемся заново и входим под ранее созданным пользователем (предыдущий пункт, всё с 3 шага)

Предварительная подготовка

Установка пакетов

1. sudo apt install easy-rsa
2. sudo apt install openvpn
3. sudo apt install iptables-persistent

Настройка FireWall

1. sudo iptables -I INPUT -p udp --dport 1194 -j ACCEPT
2. sudo netfilter-persistent save

Настройка директорий VPN

1. sudo mkdir -p /etc/openvpn/keys
2. sudo mkdir /etc/openvpn/easy-rsa
3. cd /etc/openvpn/easy-rsa
4. sudo cp -r /usr/share/easy-rsa/



Как мы строим S3
Онлайн-вебинар в Selectel

```
Technik12345@vm549021:~$ sudo mkdir -p /etc/openvpn/keys
Technik12345@vm549021:~$ sudo mkdir /etc/openvpn/easy-rsa
Technik12345@vm549021:~$ cd /etc/openvpn/easy-rsa
Technik12345@vm549021:/etc/openvpn/easy-rsa$ sudo cp -r /usr/share/easy-rsa/* .
Technik12345@vm549021:/etc/openvpn/easy-rsa$
```

1. `sudo mkdir /etc/openvpn/ccd`

Настройка VPN

Конфигурируем конфиги

Настройка vars

1. `sudo nano vars`

2. В открывшийся интерфейс вставляем:

```
export KEY_COUNTRY=<<RU>>
export KEY_PROVINCE=<<Moscow>>
export KEY_CITY=<<Moscow>>
export KEY_ORG=<<sten>>
export KEY_ORG=<<fdjgbi@sten.com>>
export KEY_CN=<<sten>>
export KEY_OU=<<sten>>
export KEY_NAME=<<vpn.StenLi.com>>
export KEY_ALTNAMES=<<vpn2.StenLi.com>>
```

KEY_ORG, KEY_ORG, KEY_CN, KEY_OU, KEY_NAME, KEY_ALTNAMES — можно указывать всё, что угодно

1. нажимаем по порядку: `ctrl+x, y, enter`

```
export KEY_COUNTRY="RU"
export KEY_PROVINCE="Moscow"
export KEY_CITY="Moscow"
export KEY_ORG="sten"          #Любое слово
export KEY_EMAIL="fdjgbi@sten.com"    #Любая почта
export KEY_CN="sten"            #Любое слово
export KEY_OU="sten"            #Любое слово
export KEY_NAME="vpn.StenLi.com"  #Любой домен
export KEY_ALTNAMES="vpn2.StenLi.com" #Любой домен
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

Настройка /etc/nat(FireWall)



Как мы строим S3
Онлайн-вебинар в Selectel

1. `sudo nano /etc/nat`

2. В открывшийся интерфейс вставляем:

```
#!/bin/sh

# Включаем форвардинг пакетов
echo 1 > /proc/sys/net/ipv4/ip_forward

# Сбрасываем настройки брандмауэра
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X

# Разрешаем инициированные нами подключения извне
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Разрешаем подключения по SSH
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT

# Разрешаем подключения к OpenVPN
iptables -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT

# Разрешает входящий трафик из tun0
iptables -A INPUT -i tun0 -j ACCEPT

# Разрешает транзитный трафик между eth0 и tun0:
iptables -A FORWARD -i eth0 -o tun0 -j ACCEPT
iptables -A FORWARD -i tun0 -o eth0 -j ACCEPT

# Запрещаем входящие извне
iptables -A INPUT -i eth0 -j DROP

# Разрешаем инициированные нами транзитные подключения извне
iptables -A FORWARD -i eth0 -o tun0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Запрещаем транзитный трафик извне
iptables -A FORWARD -i eth0 -o tun0 -j DROP

# Включаем маскарадинг для локальной сети
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j MASQUERADE
```

3. нажимаем по порядку: **ctrl+x, y, enter**

4. **sudo chmod 755 /etc/nat**



Как мы строим S3
Онлайн-вебинар в Selectel

```
GNU nano 6.2                               /etc/nat
/bin/sh

# Включаем форвардинг пакетов
echo 1 > /proc/sys/net/ipv4/ip_forward

# Сбрасываем настройки брандмауэра
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X

# Разрешаем инициированные нами подключения извне
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
# Разрешаем подключения по SSH
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT

# Разрешаем подключения к OpenVPN
iptables -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT

# Разрешает входящий трафик из tun0
iptables -A INPUT -i tun0 -j ACCEPT

# Разрешает транзитный трафик между eth0 и tun0:
iptables -A FORWARD -i eth0 -o tun0 -j ACCEPT
iptables -A FORWARD -i tun0 -o eth0 -j ACCEPT

# Запрещаем входящие извне
iptables -A INPUT -i eth0 -j DROP

# Разрешаем инициированные нами транзитные подключения извне
iptables -A FORWARD -i eth0 -o tun0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Запрещаем транзитный трафик извне
iptables -A FORWARD -i eth0 -o tun0 -j DROP

# Включаем маскарадинг для локальной сети
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j MASQUERADE
```

**^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line**

Создание ключей сервера

1. sudo ./easyrsa init-pki
2. sudo ./easyrsa build-ca
3. вводим пароль и запоминаем его(Enter New CA Key Passphrase)



Как мы строим S3
Онлайн-вебинар в Selectel

```
Technik12345@vm549021:/etc/openvpn/easy-rsa$ sudo ./easyrsa init-pki
Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/pki

Technik12345@vm549021:/etc/openvpn/easy-rsa$ sudo ./easyrsa build-ca
Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:StenLi

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/pki/ca.crt

Technik12345@vm549021:/etc/openvpn/easy-rsa$
```

```
4. sudo ./easyrsa gen-req server nopass
```

```
5. sudo ./easyrsa sign-req server server
```

После ввода команды подтверждаем правильность данных, введя yes.

и вводим пароль, который указывали при создании корневого сертификата.

```
Technik12345@vm549021:/etc/openvpn/easy-rsa$ sudo ./easyrsa sign-req server server
Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
```

1. sudo ./easyrsa gen-dh
2. sudo openvpn --genkey secret pki/ta.key
3. sudo cp pki/ca.crt /etc/openvpn/keys/
4. sudo cp pki/issued/server.crt /etc/openvpn/keys/
5. sudo cp pki/private/server.key /etc/openvpn/keys/
6. sudo cp pki/dh.pem /etc/openvpn/keys/
7. sudo cp pki/ta.key /etc/openvpn/keys/

Настройка сервера

1. sudo nano /etc/openvpn/server.conf
2. В открывшийся интерфейс вставляем:

```
local 999.999.999.999
port 1194
proto udp
dev tun
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
```



Как мы строим S3

Онлайн-вебинар в Selectel

```
dh keys/dh.pem
tls-auth keys/ta.key 0
server 10.0.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-to-client
client-config-dir /etc/openvpn/ccd
keepalive 10 120
max-clients 32
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 4
mute 20
daemon
mode server
tls-server
comp-lzo
tun-mtu 1500
mssfix 1620
cipher AES-256-GCM
topology subnet

push «redirect-gateway def1»
push «dhcp-option DNS 8.8.8.8»

up /etc/nat
```

- `client-to-client` даёт возможность клиентам видеть и общаться друг с другом в локальной сети
- `client-config-dir /etc/openvpn/ccd` выдаёт статические ip адреса клиентам. Обычно



Как мы строим S3

Онлайн-вебинар в Selectel

- Меняем local 999.999.999.999 на local <внешний ip VPS(IP по которому вы подключались через PuTTY)>

Запуск сервера

Запуск сервера

1. sudo systemctl start openvpn@server
2. sudo systemctl status openvpn@server

3. Вы запустили сервер!!!! УРА!!!!

Генерация сертификатов

Генерация сертификатов

Со 2 по 4 выполняется 1 раз!

После этого запускаем 1, и 5+

1. cd /<Любая удобная вам директория>
 2. sudo nano gen_sert.sh
3. Вставляем в открывшееся окно:

```
#!/bin/bash

if [ $# -ne 1 ]; then
    echo «Usage: $0 --client-name»
    exit 1
fi

client_name=$1
password=<>
rm -r /tmp/keys
mkdir /tmp/keys
cd /etc/openvpn/easy-rsa
export EASYRSA_CERT_EXPIRE=1460
echo «$password» | ./easyrsa build-client-full $client_name nopass
cp pki/issued/client_name.key pki/ca.crt pki/ta.key /tmp/keys/
chmod -R a+r /tmp/keys
cat << EOF > /tmp/keys/$client_name
client
resolv-retry infinite
```



Как мы строим S3

Онлайн-вебинар в Selectel

```
nobind
remote 999.999.999.999 1194
proto udp
dev tun
comp-lzo
ca ca.crt
cert $client_name.crt
key $client_name.key
tls-client
tls-auth ta.key 1
float
keepalive 10 120
persist-key
persist-tun
tun-mtu 1500
mssfix 1620
cipher AES-256-GCM
verb 0

EOF

echo «OpenVPN client configuration file created: /tmp/keys/$client_name.ovpn»
```

1. Заменяем `remote 999.999.999.999 1194` на `remote <IP сервера> 1194`
2. `sudo bash ./gen_sert.sh <Имя сертификата>`
3. `cd /tmp/keys`
4. Например с помощью winscp достаем из этой директории сертификаты([получение файлов, скачать](#))

Задание статических адресов клиентам

1. `cd /etc/openvpn/ccd`
2. `sudo nano <Имя сертификата который вы указали при создании>`
3. Вставляем в открывшееся окно:

```
ifconfig-push 10.0.0.<адрес который не будет меняться, адреса не должны повторяться> ?
```

Теги: [vpn-сервер](#), [vpn](#), [vps/vds](#), [ubuntu](#), [openvpn](#), [linux](#), [bash](#)

Хабы: [Настройка Linux](#), [Облачные сервисы](#), [Сетевые технологии](#)



-2



83



32

Редакторский дайджест

Присыпаем лучшие статьи раз в месяц

Электропочта



Оставляя свою почту, я принимаю [Политику конфиденциальности](#)



Как мы строим S3

Онлайн-вебинар в Selectel



7

0

Карма Общий рейтинг

@Technik12345

Пользователь

Подписаться



Комментарии 32

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ



Catx2

21 час назад

Нижегородское метро: 40 горьких лет

28 мин

19K

+109

30

88



zarazaexe

22 часа назад

Что скрывается за «сертификатами безопасности» от Минцифры?

Средний

6 мин

18K

Из песочницы

+67

86

198



teamfighter

23 часа назад

Как за 5 дней с помощью Claude я создал приложение для кошки с диабетом (и кажется запустил стартап)

Средний

6 мин

5.4K

Кейс

+63

38

45



OlegSivchenko

19 часов назад

На смерть Джеймса Уотсона

14 мин

2.9K

+43

16

27



valisak

21 час назад

Теория неоднородной Вселенной как альтернатива тёмной энергии

Простой

8 мин

2.2K

Обзор

+36



Как мы строим S3

Онлайн-вебинар в Selectel



Dingzhibo

2 часа назад

Как работают ИИ-агенты и кому они на самом деле нужны

🕒 9 мин 🕰 1.1K

+29

9

0

 MishaBucha
18 часов назад

Многопоточность без боли: моя шпаргалка для собесов в Java

🕒 Простой 🕒 8 мин 🕰 6.3K

+23

142

12

 rsashka
3 часа назад

Ищем ошибку в работе WiFi у платы ESP32-C3 SuperMini

⚠ Средний 🕒 5 мин 🕰 844

Кейс

+18

12

6

 RationalAnswer
5 часов назад

Чебурахнувшийся робот, а также ИГРОКУБ от Valve

🕒 9 мин 🕰 5.5K

Дайджест

+17

3

8

 MnsDev
16 часов назад

Как устроена цензура изнутри. На примере слитого китайского фаерволла (блокировки Tor, VPN, анализ трафика)

🕒 Простой 🕒 7 мин 🕰 17K

+17

60

29

Обратный тренд: почему бизнес массово возвращается от облаков к ЦОД

Промо

Показать еще

МИНУТОЧКУ ВНИМАНИЯ



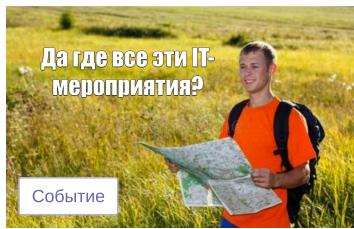
Как мы строим S3

Онлайн-вебинар в Selectel



Промо

Железные корни: итоги опроса об IT-инфраструктуре



Событие

Не знаете, куда идти? Загляните в Календарь IT-мероприятий



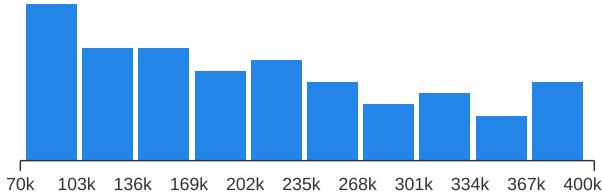
Опрос

Что думают о Heavy Digital: опрос для промышленных айтишников

СРЕДНЯЯ ЗАРПЛАТА В ИТ

211 263 ₽/мес.

— средняя зарплата во всех IT-специализациях по данным из 43 316 анкет, за 2-ое пол. 2025 года. Проверьте «в рынке» ли ваша зарплата или нет!



Проверить свою зарплату

ЧИТАЮТ СЕЙЧАС

Созданный инженером сайт почти сразу вывели из строя боты-парсеры

6.6K 29

Как устроена цензура изнутри. На примере слитого китайского фаерволла (блокировки Tor, VPN, анализ трафика)

17K 29

Нижегородское метро: 40 горьких лет

19K 88

Ты можешь выбрать свою сторону

187K 28

Что скрывается за «сертификатами безопасности» от Минцифры?

18K 198

Обратный тренд: почему бизнес массово возвращается от облаков к ЦОД

Промо

ИСТОРИИ



Как мы строим S3

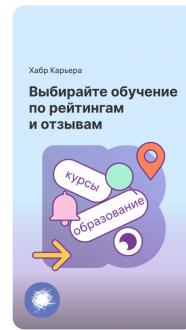
Онлайн-вебинар в Selectel



Как устроен мир по ту сторону карты



Первый карьерный онлайн-фест

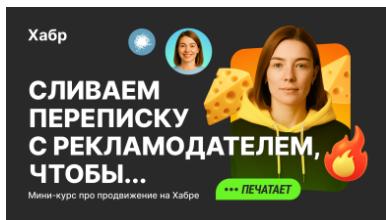


Выбирайте курсы по отзывам



Road to Highload

БЛИЖАЙШИЕ СОБЫТИЯ



23 сентября – 31 декабря

**Бесплатный мини-курс:
как продвигаться на
Хабре, если вы — не IT-
бренд**

Онлайн

Маркетинг



17 – 23 ноября

**Первый карьерный
онлайн-ФЕСТ**

Онлайн

Разработка

Тестирование

Другое

Больше событий в календаре



17 – 19 ноября

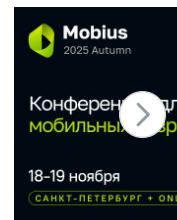
**Конференция «TECH
WEEK 2025»**

Москва

Разработка

Менеджмент

Больше событий в календаре



18 – 19 ноября

**Конференция
мобильной
Mobius 2025**

Санкт-Петербург

Разработка

Больше событий

Больше событий в календаре

Больше событий в календаре

Больше событий

Ваш аккаунт	Разделы	Информация	Услуги
Войти	Статьи	Устройство сайта	Корпоративный блог
Регистрация	Новости	Для авторов	Медийная реклама
	Хабы	Для компаний	Нативные проекты
	Компании	Документы	Образовательные программы
	Авторы	Соглашение	Стартапам
	Песочница	Конфиденциальность	



Настройка языка

Техническая поддержка

© 2006–2025, Habr

Как мы строим S3

Онлайн-вебинар в Selectel