

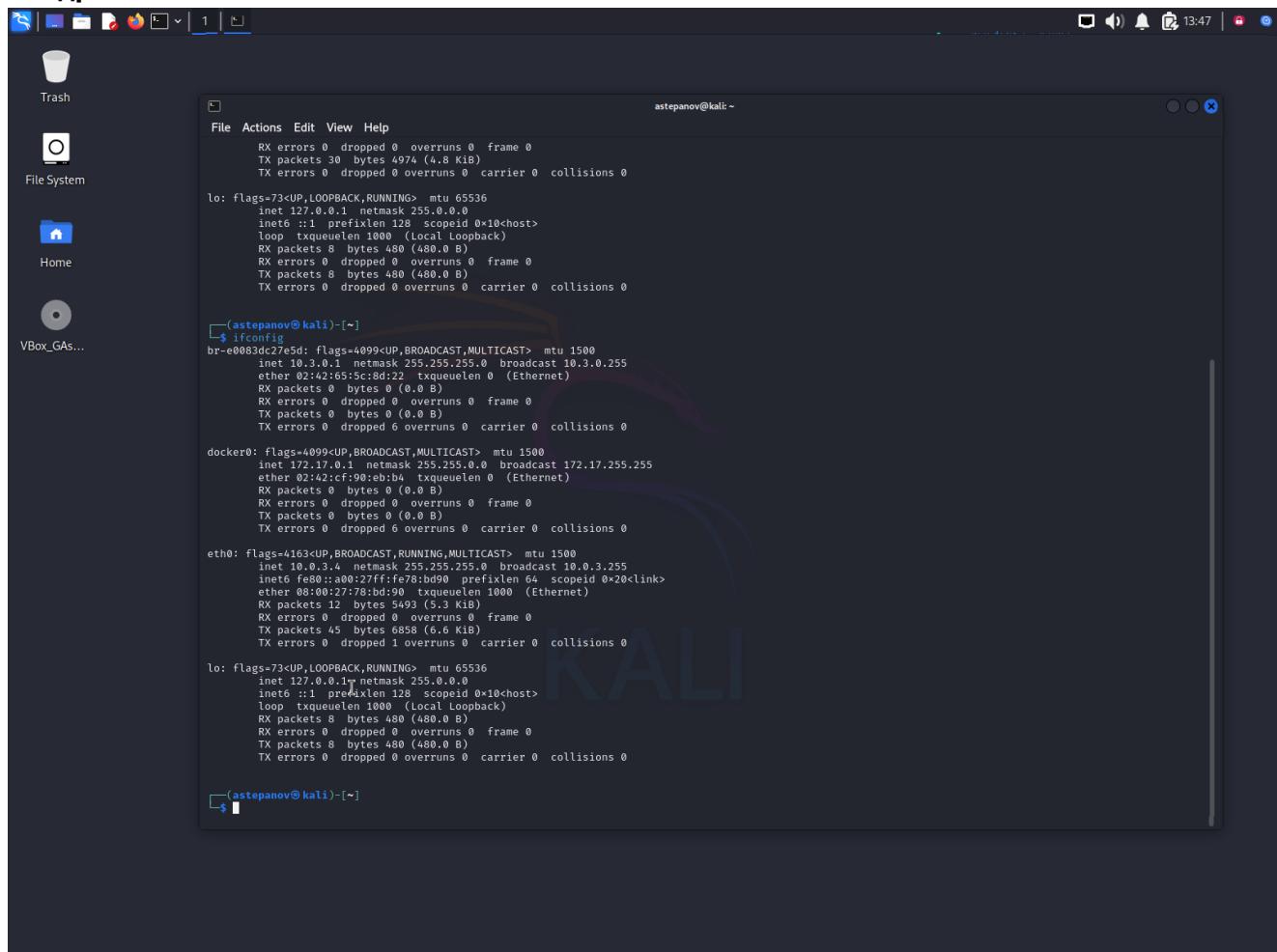
Модуль 3. Виртуальные защищенные каналы связи, DMZ, Wi-Fi (HW)

Лабораторная работа №1 (HW)

Шаг 1. Подготовьте две виртуальные машины

В качестве сервера подготавливаем машину с Kali Linux:

IP-адрес: 10.0.3.4



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "astepanov@kali: ~". The command "ifconfig" is being run, displaying network interface statistics. The output includes information for interfaces like "lo", "br-e008", "eth0", and "docker0". The "KALI" logo is visible in the background of the desktop.

```
astepanov@kali: ~
$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        ether 00:0c:29:14:dc:8d txqueuelen 0 (Ethernet)
        RX packets 30 bytes 4974 (4.8 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-e008: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.0.3.1 netmask 255.255.255.0 broadcast 10.0.3.255
        ether 02:42:65:5c:8d:22 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:c9:90:eb:ba txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

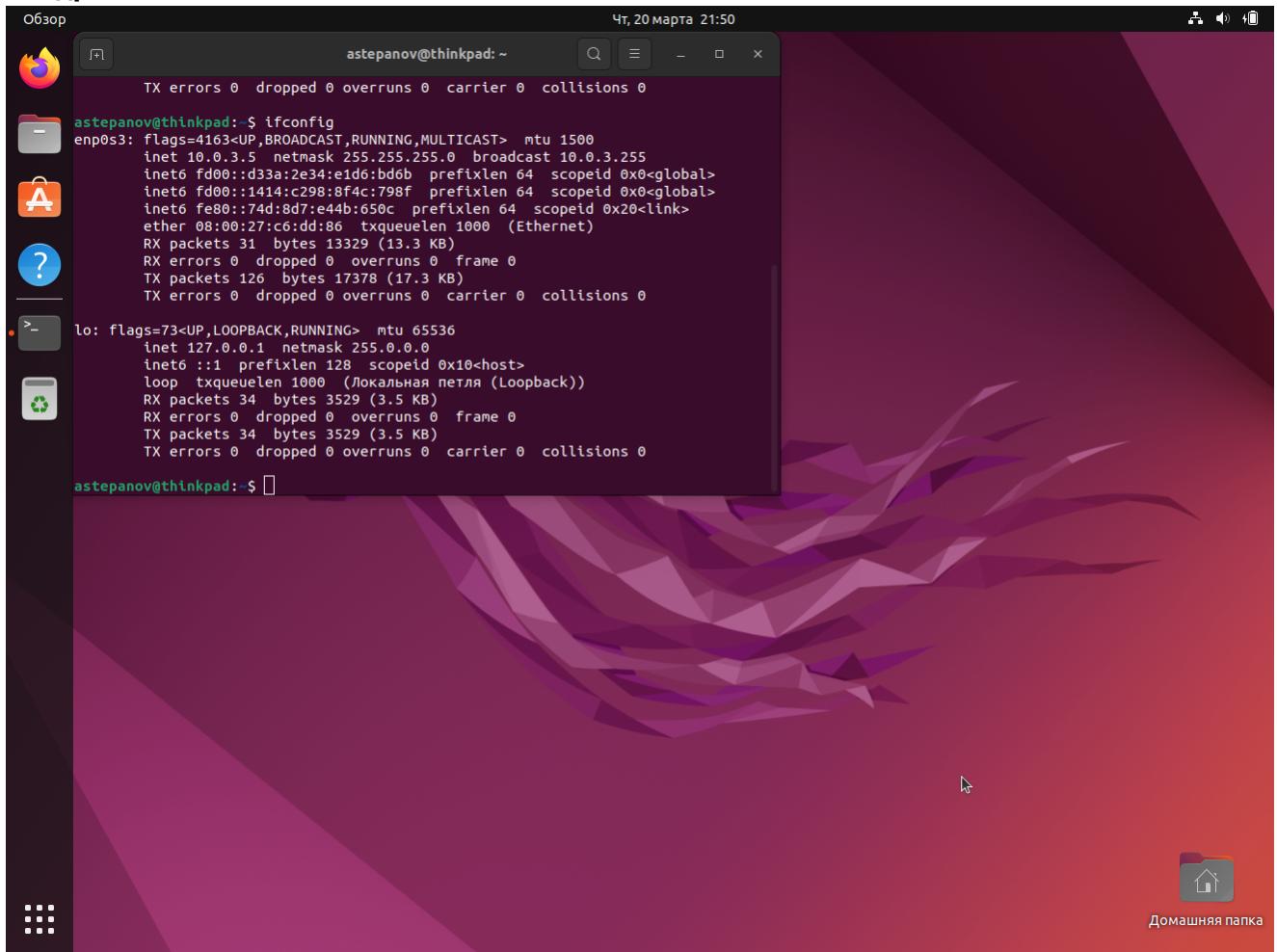
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.4 netmask 255.255.255.0 broadcast 10.0.3.255
        ether fe:80::a0:27ff:fe78:bd90 txqueuelen 64 scopeid 0x20<link>
        ether 08:00:27:78:bd:90 txqueuelen 1000 (Ethernet)
        RX packets 12 bytes 5493 (5.3 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 45 bytes 6858 (6.6 KiB)
        TX errors 0 dropped 1 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        ether 00:0c:29:14:dc:8d txqueuelen 0 (Ethernet)
        RX packets 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

astepanov@kali: ~
```

Для клиентской машины подготовим Ubuntu:

IP-адрес: 10.0.2.5



Шаг 2. Проведите настройку OpenVPN

Устанавливаем пакеты на сервер-хосте

```
astepanov@kali: ~
File Actions Edit View Help
64 bytes from 10.0.3.4: icmp_seq=4 ttl=64 time=0.861 ms
64 bytes from 10.0.3.5: icmp_seq=5 ttl=64 time=1.17 ms
^C
--- 10.0.3.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.861/1.490/2.611/0.595 ms

(asstepanov@kali)-[~]
$ sudo apt install openvpn easy-rsa
[sudo] password for asstepanov:
Upgrading:
    easy-rsa libssl1.3t64 openssl openssl-provider-legacy openvpn

Summary:
  Upgrading: 5, Installing: 0, Removing: 0, Not Upgrading: 1494
  Download size: 4,770 kB
  Space needed: 251 kB / 21.9 GB available

Continue? [Y/n] y
Get:4 http://mirror.amuksa.com/kali kali-rolling/main amd64 easy-rsa all 3.2.2-1 [75.9 kB]
Get:1 http://kali.download/kali Kali-rolling/main amd64 openssl-provider-legacy amd64 3.4.1-1 [302 kB]
Get:2 http://kali.download/kali Kali-rolling/main amd64 libssl1.3t64 amd64 3.4.1-1 [2,304 kB]
Get:3 http://mirror.ourhost.az/kali Kali-rolling/main amd64 openssl amd64 3.4.1-1 [1,427 kB]
Get:5 http://kali.download/kali Kali-rolling/main amd64 openvpn amd64 2.6.13-1 [662 kB]
Fetched 4,770 kB in 1s (493 kB/s)
Preconfiguring packages ...
(Reading database ... 402285 files and directories currently installed.)
Preparing to unpack .../openssl-provider-legacy_3.4.1-1_amd64.deb ...
Unpacking openssl-provider-legacy (3.4.1-1) over (3.3.2-2) ...
Setting up openssl-provider-legacy (3.4.1-1)
(Reading database ... 402285 files and directories currently installed.)
Preparing to unpack .../libssl1.3t64_amd64_3.4.1-1_amd64.deb ...
Unpacking libssl1.3t64_amd64 (3.4.1-1) over (3.3.2-2) ...
Setting up libssl1.3t64_amd64 (3.4.1-1) ...
(Reading database ... 402285 files and directories currently installed.)
Preparing to unpack .../openssl_3.4.1-1_amd64.deb ...
Unpacking openssl (3.4.1-1) over (3.3.2-2) ...
Preparing to unpack .../easy-rsa_3.2.2-1_all.deb ...
Unpacking easy-rsa (3.2.2-1) over (3.2.1-1) ...
Preparing to unpack .../openvpn_2.6.13-1_amd64.deb ...
Unpacking openvpn (2.6.13-1) over (2.6.12-1) ...
Setting up openvpn (2.6.13-1) ...
openvpn-service is already enabled or a static unit, not starting it.
Setting up openssl (3.4.1-1) ...
Setting up easy-rsa (3.2.2-1) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.
```

а: Создание инфраструктуры открытых ключей (PKI), центра сертификации;

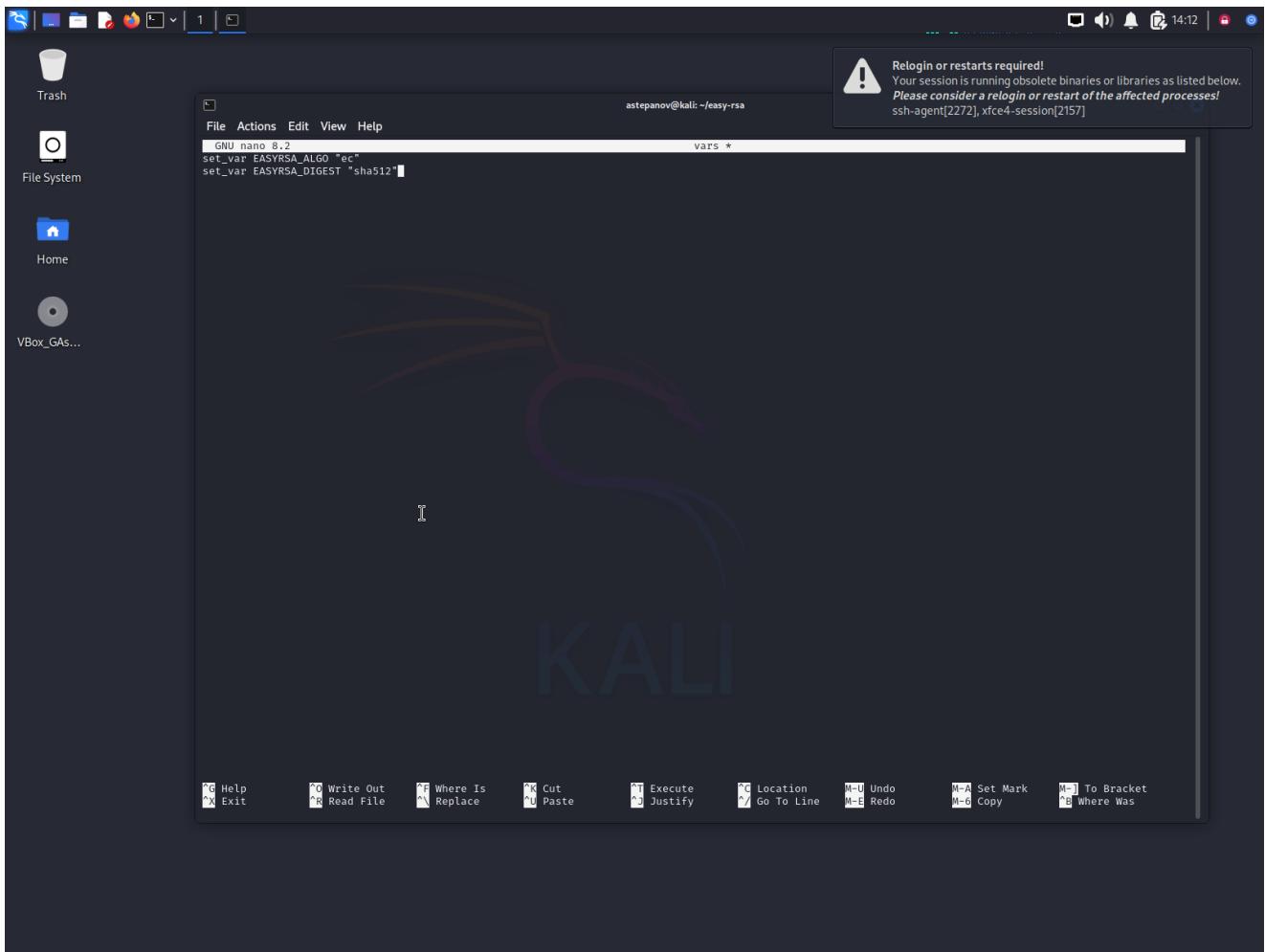
Создаем директорию для инфраструктуры публичных ключей и копируем туда все файлы пакета easy-rsa

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of a package manager (likely apt) performing an upgrade. The logs show various packages being unpacked and upgraded, including openssl, libssl1.3, and openvpn. The terminal session is owned by user 'astepanov'.

```
(Reading database ... 402285 files and directories currently installed.)  
Preparing to unpack .../openssl-provider-legacy_3.4.1-1_amd64.deb ...  
Unpacking openssl-provider-legacy (3.4.1-1) over (3.3.2-2) ...  
Setting up openssl-provider-legacy (3.4.1-1) ...  
(Reading database ... 402285 files and directories currently installed.)  
Preparing to unpack .../libssl1.3_1.3.1-1_amd64.deb ...  
Unpacking libssl1.3_1.3.1-1_amd64 (1.3.1-1) over (1.3.2-2) ...  
Setting up libssl1.3_1.3.1-1_amd64 (1.3.1-1) ...  
(Reading database ... 402285 files and directories currently installed.)  
Preparing to unpack .../openssl_3.4.1-1_amd64.deb ...  
Unpacking openssl (3.4.1-1) over (3.3.2-2) ...  
Preparing to unpack .../easy-rsa_3.2.2-1_all.deb ...  
Unpacking easy-rsa (3.2.2-1) over (3.2.1-1) ...  
Preparing to unpack .../openvpn_2.6.13-1_amd64.deb ...  
Unpacking openvpn (2.6.13-1) over (2.6.12-1) ...  
Setting up openvpn (2.6.13-1) ...  
openvpn.service is a disabled or a static unit, not starting it.  
Setting up openssl (3.4.1-1) ...  
Setting up easy-rsa (3.2.2-1) ...  
Processing triggers for libc-bin (2.40-3) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for kali-menu (2024.4.0) ...  
Scanning processes ...  
Scanning candidates ...  
Scanning linux images ...  
  
Running kernel seems to be up-to-date.  
  
Restarting services ...  
/etc/needrestart/restart.d/systemd-manager  
systemctl restart apache2.service systemd-journald.service systemd-udevd.service upower.service vsftpd.service  
Service restarts being deferred:  
systemctl restart NetworkManager.service  
systemctl restart systemd-logind.service  
  
No containers need to be restarted.  
  
User sessions running outdated binaries:  
astepanov @ session #2: ssh-agent[2272], xfce4-session[2157]  
astepanov @ user manager service: systemd[2111]  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
  
[astepanov@kali:~]  
└$ mkdir ~easy-rsa  
[astepanov@kali:~]  
└$ ln -s /usr/share/easy-rsa/* ~easy-rsa  
[astepanov@kali:~easy-rsa]  
[1] + done ln -s /usr/share/easy-rsa/* ~easy-rsa  
[astepanov@kali:~easy-rsa]  
└$
```

A warning dialog box is visible in the top right corner, stating: "Relogin or restarts required! Your session is running obsolete binaries or libraries as listed below. Please consider a relogin or restart of the affected processes! ssh-agent[2272], xfce4-session[2157]".

Указание криптографических алгоритмов, которые будут использоваться при генерации ключей и подписей



Инициализация PKI

Relogin or restarts required!
Your session is running obsolete binaries or libraries as listed below.
Please consider a relogin or restart of the affected processes!
sshd-agent[2272], xfce4-session[2157]

```
(astepanov㉿kali)-[~]
$ mkdir ~/easy-rsa
(astepanov㉿kali)-[~]
$ ln -s /usr/share/easy-rsa/* ~/easy-rsa & cd ~/easy-rsa
[1] 15142
[1] + done    ln -s /usr/share/easy-rsa/* ~/easy-rsa
(astepanov㉿kali)-[~/easy-rsa]
$ nano vars
(astepanov㉿kali)-[~/easy-rsa]
$ ./easyrsa init-pki
Using Easy-RSA 'vars' configuration:
* /home/astepanov/easy-rsa/vars

Notice
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /home/astepanov/easy-rsa/pki

Using Easy-RSA configuration:
* /home/astepanov/easy-rsa/vars

(astepanov㉿kali)-[~/easy-rsa]
$ ./easyrsa build-ca nopass
Using Easy-RSA 'vars' configuration:
* /home/astepanov/easy-rsa/vars
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 (e.g: your user, host, or server name) [Easy-RSA CA]:kali
Notice
CA creation complete. Your new CA certificate is at:
* /home/astepanov/easy-rsa/pki/ca.crt

Create an OpenVPN TLS-AUTH|TLS-CRYPT-V1 key now: See 'help gen-tls'

Build-ca completed successfully.

(astepanov㉿kali)-[~/easy-rsa]
$
```

b: Создание запроса сертификата и закрытого ключа сервера OpenVPN

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running a command-line interface for generating an SSL/TLS certificate request using the 'easyrsa' tool. A warning message at the top right of the terminal window states: 'Relogin or restarts required! Your session is running obsolete binaries or libraries as listed below. Please consider a relogin or restart of the affected processes! ssh-agent[2272], xice4-session[2157]'. The terminal history is as follows:

```
astepanov@kali: ~/easy-rsa
-rw-rw-r-- 1 astepanov astepanov 118 Mar 10 15:30 .xsessionrc
-rw-r--r-- 1 astepanov astepanov 336 Mar 2 07:49 .zprofile
-rw-r----- 1 astepanov astepanov 5762 Mar 18 18:18 .zsh_history
-rw-r--r-- 1 astepanov astepanov 10868 Mar 2 07:49 .zshrc
(asteponov@kali) [~]
$ cd easy-rsa
(asteponov@kali) [~/easy-rsa]
$ ls
easyrsa openssl-easyrsa.cnf pki vars vars.example x509-types
(asteponov@kali) [~/easy-rsa]
$ cd easy-rsa/
(asteponov@kali) [~/easy-rsa]
$ cd pki/private
(asteponov@kali) [~/easy-rsa/pki/private]
$ ls
ca.key
(asteponov@kali) [~/easy-rsa/pki/private]
$ cd ../..
(asteponov@kali) [~/easy-rsa]
$ ./easyrsa gen-req kali nopass
Using Easy-RSA 'vars' configuration:
* /home/asteponov/easy-rsa/vars
_____
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) [kali]:kali
Notice
_____
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /home/asteponov/easy-rsa/pki/reqs/kali.req
* key: /home/asteponov/easy-rsa/pki/private/kali.key
(asteponov@kali) [~/easy-rsa]
$
```

c: Подпись запроса сертификата сервера OpenVPN

Копируем ключ сервера в директорию конфигурации OpenVpn и подписываем запрос центром сертификации. Подписанный сертификат сервера kali.crt вместе с сертификатом центра

сертификации копируем в директорию конфигурации OpenVPN**

```
(astepanov㉿kali)-[~/easy-rsa]
$ sudo cp ~/easy-rsa/pki/private/kali.key /etc/openvpn/server

(astepanov㉿kali)-[~/easy-rsa]
$ ./easyrsa sign-req server Kali
Using Easy-RSA 'vars' configuration
* ./home/astepanov/easy-rsa/vars
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
source or that you have verified the request checksum with the sender.
You are about to sign the following certificate:

Requested CN: 'kali'
Requested type: 'server'
Valid for: '825' days

subject=
commonName = kali
Type the word 'yes' to continue, or any other input to abort.
Confirm requested details: yes

Using configuration from /home/astepanov/easy-rsa/pki/45f3e980/temp.2.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'kali'
Certificate is to be certified until Jun 23 18:21:49 2027 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
_____
Inline file created:
* /home/astepanov/easy-rsa/pki/inline/private/kali.inline

Notice
_____
Certificate created at:
* /home/astepanov/easy-rsa/pki/issued/kali.crt

(astepanov㉿kali)-[~/easy-rsa]
$ sudo cp ~/easy-rsa/pki/issued/kali.crt /etc/openvpn/server
I
(astepanov㉿kali)-[~/easy-rsa]
$ sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server
I
(astepanov㉿kali)-[~/easy-rsa]
$
```

d: Настройка криптографических материалов OpenVPN

Создаем ta.key и копируем его в директорию сервера openvpn

```
(astepanov㉿kali)-[~/easy-rsa]
$ openvpn --genkey secret ta.key
I
(astepanov㉿kali)-[~/easy-rsa]
$ ls
easyrsa openssl-easyrsa.cnf pki ta.key vars vars.example x509-types

(astepanov㉿kali)-[~/easy-rsa]
$ sudo cp ta.key /etc/openvpn/server
[sudo] password for astepanov:
```

Создаем и подписываем клиентский ключ и копируем все в директорию ключей клиентского конфига

```
(astepanov㉿kali)-[~/easy-rsa]
$ ./easyrsa sign-req client ubuntu
Using Easy-RSA 'vars' configuration:
* ./home/astepanov/easy-rsa/vars
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
source or that you have verified the request checksum with the sender.
You are about to sign the following certificate:

    Requested CN: 'ubuntu'
    Requested type: 'client'
    Valid for: '825' days

    subject=
        commonName = Ubuntu
Type the word 'yes' to continue, or any other input to abort.
Confirm requested details: yes
Using configuration from /home/astepanov/easy-rsa/pki/da4a787a/temp.2.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'ubuntu'
Certificate is to be certified until Jun 23 18:48:41 2027 GMT (825 days)
Write out database with 1 new entries
Database updated
Notice
_____
Inline file created:
* /home/astepanov/easy-rsa/pki/inline/private/ubuntu.inline

Notice
_____
Certificate created at:
* /home/astepanov/easy-rsa/pki/issued/ubuntu.crt

$ cp ./easy-rsa/pki/issued/ubuntu.crt ~/client-configs/keys
$ sudo cp /etc/openvpn/server/ca.crt ~/client-configs/keys
$ sudo ta.key ~/client-configs/keys
$ sudo ta.key ~/client-configs/keys
$ sudo cp ta.key ~/client-configs/keys
$
```

f: Настройка OpenVPN

Настраиваем конфиг openvpn, добавляем параметры шифрования

Network security - Thunar

File Edit View File Actions Edit View Help

GNU nano 8.2 /etc/openvpn/server/server.conf

```
local a.b.c.d
port 1194
proto udp
dev tun
;dev tap
;dev-node MyTap
ca ca.crt
cert kali.crt
key kali.key # This file should be kept secret
dh dh2048.pem
;data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
;learn-address ./script
;push "redirect-gateway def1 bypass-dhcp"
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
;client-to-client
;duplicate-cn

keepalive 10 120
;tls-auth ta.key 0 # This file is secret
tls-crypt ta.key
;cipher AES-256-GCM
cipher AES-256-CBC
auth SHA256
;dh dh2048.pem
dh none
port 1194
proto tcp

;max-clients 100

# Разрешаем входящие соединения на порт OpenVPN (UDP или TCP)
sudo iptables -I INPUT -i eth0 -m state --state NEW -p udp --dport 1194 -j ACCEPT
#
# Разрешаем форвардинг трафика между клиентами
sudo iptables -I FORWARD -i tun+ -j ACCEPT
#
# Разрешаем форвардинг с основного интерфейса на тун+ (входящий трафик)
sudo iptables -I FORWARD -i eth0 -o tun+ -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# Настраиваем NAT для VPN-клиентов (заменило на eth0, если клиенты должны выходить в интернет)
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/14 -o eth0 -j MASQUERADE
#
# Разрешаем исходящий трафик через VPN
sudo iptables -A OUTPUT -o tun+ -j ACCEPT
```

File Edit View Document Help

Help Write Out Where Is Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark To Bracket Where Was Previous Next Back Forward

g: Настройка конфигурации сети сервера OpenVPN

The screenshot shows a terminal window titled "astepanov@kali: /etc". The terminal displays a series of commands being run in a terminal window:

```
(astepanov@kali)-[/etc]
$ sudo nano /etc/sysctl.conf
(astepanov@kali)-[/etc]
$ nano /etc/sysctl.conf
(astepanov@kali)-[/etc]
$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
(astepanov@kali)-[/etc]
$ sudo sysctl -p
net.ipv4.ip_forward = 1
(astepanov@kali)-[/etc]
```

The terminal window is part of a desktop environment, with a sidebar visible on the left containing icons for Trash, File System, Home, and VBox_GAs... The desktop background features the Kali Linux logo.

h: Настройка межсетевого экрана

```
[astepanov@kali]:~$ sudo iptables -I INPUT -i eth0 -m state --state NEW -p tcp --dport 1194 -j ACCEPT
[astepanov@kali]:~$ sudo iptables -I FORWARD -i tun+ -j ACCEPT
[astepanov@kali]:~$ sudo iptables -I FORWARD -i tun+ -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
[astepanov@kali]:~$ sudo iptables -I FORWARD -i eth0 -o tun+ -m state --state ESTABLISHED,RELATED -j ACCEPT
[astepanov@kali]:~$ sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
[astepanov@kali]:~$ sudo iptables -A OUTPUT -o tun+ -j ACCEPT
[astepanov@kali]:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source         destination
  0   0 ACCEPT      tcp  --  eth0   *       0.0.0.0/0      0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source         destination
  0   0 ACCEPT      all  --  eth0   tun+   0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  tun+   eth0   0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  tun+   *       0.0.0.0/0      0.0.0.0/0
  0   0 DOCKER-USER all  --  *       *       0.0.0.0/0      0.0.0.0/0
  0   0 DOCKER-ISOLATION-STAGE-1 all  --  *       *       0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  *       docker0 0.0.0.0/0      0.0.0.0/0
  0   0 DOCKER      all  --  *       docker0 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  docker0 !docker0 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  docker0 docker0 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  *       br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
  0   0 DOCKER      all  --  *       br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  br-e0083dc27e5d !br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      all  --  br-e0083dc27e5d br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source         destination
  0   0 ACCEPT      all  --  *       tun+   0.0.0.0/0      0.0.0.0/0
Chain DOCKER (2 references)
pkts bytes target     prot opt in     out    source         destination
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
pkts bytes target     prot opt in     out    source         destination
  0   0 DOCKER-ISOLATION-STAGE-2 all  --  docker0 !docker0 0.0.0.0/0      0.0.0.0/0
  0   0 DOCKER-ISOLATION-STAGE-2 all  --  br-e0083dc27e5d !br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
  0   0 RETURN      all  --  *       *       0.0.0.0/0      0.0.0.0/0
Chain DOCKER-ISOLATION-STAGE-2 (2 references)
pkts bytes target     prot opt in     out    source         destination
  0   0 DROP        all  --  *       docker0 0.0.0.0/0      0.0.0.0/0
  0   0 DROP        all  --  *       br-e0083dc27e5d 0.0.0.0/0      0.0.0.0/0
```

```
/mnt/shared/2.vnc
File Edit Search View Document Help
1 # Разрешаем входящие соединения на порт 0
2 sudo iptables -t INPUT -i eth0 -m state --state NEW tcp dpt:1194
3
4 # Разрешаем форвардинг трафика между клиентом и сервером
5 sudo iptables -I FORWARD -i tun+ -j ACCEPT
6
7 # Разрешаем соединения на основной интерфейс
8 sudo iptables -I FORWARD -i tun+ -o eth0 -
9
10 # Разрешаем форвардинг трафика с основного интерфейса на туннель
11 sudo iptables -I FORWARD -o eth0 -i tun+ -
12
13 # Настраиваем NAT для VPN-клиентов (замена IP)
14 sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
15
16 # Разрешаем выходящий трафик через VPN
17 sudo iptables -A OUTPUT -o tun+ -j ACCEPT
```

i: Запуск OpenVPN

```
Mar 20 15:31:19 kali openvpn[57099]: Note: Kernel support for ovpn-dco missing, disabling data channel offload.
Mar 20 15:31:19 kali openvpn[57099]: Options error: --cert fails with 'server.crt': No such file or directory (errno=2)
Mar 20 15:31:19 kali openvpn[57099]: WARNING: cannot stat file 'server.key': No such file or directory (errno=2)
Mar 20 15:31:19 kali openvpn[57099]: Options error: --key fails with 'server.key': No such file or directory (errno=2)
Mar 20 15:31:19 kali openvpn[57099]: Options error: Please correct these errors.
Mar 20 15:31:19 kali systemd[1]: openvpn-server@server.service: Main process exited, code=exited, status=1/FAILURE
Subject: Unit process exited
Defined-By: systemd
Support: https://www.debian.org/support
An ExecStart= process belonging to unit openvpn-server@server.service has exited.
The process' exit code is 'exited' and its exit status is 1.
Mar 20 15:31:19 kali systemd[1]: openvpn-server@server.service: Failed with result 'exit-code'.
Subject: Unit failed
Defined-By: systemd
Support: https://www.debian.org/support
The unit openvpn-server@server.service has entered the 'failed' state with result 'exit-code'.
Mar 20 15:31:19 kali systemd[1]: Failed to start openvpn-server@server.service - OpenVPN service for server.
Subject: A start job for unit openvpn-server@server.service has failed
Defined-By: systemd
Support: https://www.debian.org/support
A start job for unit openvpn-server@server.service has finished with a failure.
Device
File System
VBox_GAs_ Network
Places Computer
astepanov Desktop
Recent Trash
shared Documents
Music Pictures
Videos Downloads
Devices File System
VBox_GAs_ Network
Brows Net
astepanov@kali:[/etc]
$ sudo nano /etc/openvpn/server/server.conf
astepanov@kali:[/etc]
$ sudo systemctl -f enable openvpn-server@server.service
astepanov@kali:[/etc]
$ sudo systemctl start openvpn-server@server.service
astepanov@kali:[/etc]
$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
  Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; preset: disabled)
  Active: active (running) since Thu 2025-03-20 15:33:35 EDT; 21s ago
    Invocation: /usr/bin/openvpn --config /etc/openvpn/server/server.conf
  Docs: man:openvpn(8)
         https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/
         https://openvpn.net/openvpn/wiki/HOWTO
 Main PID: 58340 (openvpn)
 Status: "Initialization Sequence Completed"
   Tasks: 1 (limit: 4555)
  Memory: 1.9M (peak: 2M)
     CPU: 26ms
    CGroup: /system.slice/system-openvpn@x2dserver.slice/openvpn-server@server.service
           └─58340 /usr/sbin/openvpn --status /run/openvpn/server/status-server.log --status-version 2 --suppress-timestamps --config server.conf

Mar 20 15:33:35 kali openvpn[58340]: Could not determine IP4/IP6 protocol. Using AF_INET
Mar 20 15:33:35 kali openvpn[58340]: Socket Buffers: R:[131072->131072] S:[16384->16384]
Mar 20 15:33:35 kali openvpn[58340]: Listening for incoming TCP connection on [AF_INET][undef]:1194
Mar 20 15:33:35 kali openvpn[58340]: TCPv4_SERVER link local (bound): [AF_INET][undef]:1194
Mar 20 15:33:35 kali openvpn[58340]: TCPv4_SERVER link remote: [AF_UNSPEC]
Mar 20 15:33:35 kali openvpn[58340]: MULTI: multi_init called, r=256 v=256
Mar 20 15:33:35 kali openvpn[58340]: IFCONFIG POOL IPv4: base=10.8.0.2 size=253
Mar 20 15:33:35 kali openvpn[58340]: IFCONFIG POOL LIST
Mar 20 15:33:35 kali openvpn[58340]: MULTI: TCP INIT maxclients=1024 maxevents=1029
Mar 20 15:33:35 kali openvpn[58340]: Initialization Sequence Completed
astepanov@kali:[/etc]
```

j: Создание инфраструктуры конфигурации клиентских систем

Копируем шаблон для создания клиентского конфига

```
astepanov@kali:[/etc]
$ mkdir -p ~/client-configs/files

astepanov@kali:[/etc]
$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
[sudo] password for astepanov:
```

Редактируем шаблон клиентского конфига

```
File Actions Edit View Help
└─(astepanov㉿kali)-[~]
$ cat ~/client-configs/base.conf
client
dev tun
proto tcp
remote 10.0.3.4 1194

resolv-retry infinite
nobind

persist-key
persist-tun

cipher AES-256-GCM
auth SHA256
key-direction 1
remote-cert-tls server

script-security 2
up /etc/openvpn/update-systemd-resolved
down /etc/openvpn/update-systemd-resolved
down-pre
dhcp-option DOMAIN-ROUTE

└─(astepanov㉿kali)-[~]
$ █
```

Создаем скрипт для создания .ovpn конфига из base.conf

```
cat ./make_config.sh
#!/bin/bash

KEY_DIR=keys
OUTPUT_DIR=files
BASE_CONFIG=base.conf

CLIENT_NAME=$1

cat ${BASE_CONFIG} \
<(echo -e '<ca>' ) \
${KEY_DIR}/ca.crt \
<(echo -e '</ca>\n<cert>' ) \
${KEY_DIR}/${CLIENT_NAME}.crt \
<(echo -e '</cert>\n<key>' ) \
${KEY_DIR}/${CLIENT_NAME}.key \
<(echo -e '</key>\n<tls-crypt>' ) \
${KEY_DIR}/ta.key \
<(echo -e '</tls-crypt>' ) \
> ${OUTPUT_DIR}/${CLIENT_NAME}.ovpn
```

k: создание конфигураций клиентов

Запускаем скрипт make_config.sh и генерируем файл конфига ubuntu.ovpn

```

astepanov@kali: ~/client-configs $ sudo ./make_config.sh
cat: keys./make_config.sh.crt: No such file or directory
cat: keys./make_config.sh.key: No such file or directory
astepanov@kali: ~/client-configs $ sudo ./make_config.sh
cat: keys./make_config.sh.crt: No such file or directory
cat: keys./make_config.sh.key: No such file or directory
astepanov@kali: ~/client-configs $ ls
astepanov@kali: ~/client-configs $ sudo nano ./make_config.sh
astepanov@kali: ~/client-configs $ sudo ./make_config.sh ubuntu
astepanov@kali: ~/client-configs $ cd files
astepanov@kali: ~/client-configs/files $ ls
astepanov@kali: ~/client-configs/files $ cat ubuntu.ovpn
client
dev tun
proto tcp
remote 10.0.3.4 1194
resolv-retry infinite
nobind
persist-key
persist-tun
cipher AES-256-GCM
auth SHA256
key-direction 1
remote-cert-tls server
script-security 2
up /etc/openvpn/update-systemd-resolved
down /etc/openvpn/update-systemd-resolved
down-pre
dhcp-option DOMAIN=ROUTE
<ca>
-----BEGIN CERTIFICATE-----
MIIB5CCAN2SAwIBAgTUb1kUVAZi5Xvn
DzENMASGAUEAwEzFsaTAeFw0vNTAz
MA8xDTALBgNVBAMBGthbGkwIJAQBccq
+dRqJ59EBgatjGRPVrEW9SE4K8cA1zI
<C3kCyHnwsgqrA4ig4NW1/ekUSM4jjb/
-----END CERTIFICATE-----

```

i: установка клиентской конфигурации

Копируем .ovpn файл на клиентскую машину

```

astepanov@thinkpad: ~$ ls -la
astepanov@thinkpad: ~$ scp ubuntu.ovpn astepanov@10.0.3.5:~
astepanov@thinkpad: ~$ ls -l /etc/ssl/private/vsftpd.pem
astepanov@thinkpad: ~$ 

```

Устанавливаем openvpn клиентскую службу

```

astepanov@thinkpad:~$ sudo apt install -y openvpn-systemd-resolved
[sudo] пароль для астепанов:
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libnss-resolve

Следующие НОВЫЕ пакеты будут установлены:
  libnss-resolve openvpn-systemd-resolved

Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 3 пакетов не обновлено.
Необходимо скачать 76,9 kB архивов.

После данной операции объем занятого дискового пространства возрастёт на 352 kB.
Пол:1 http://ru.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libnss-resolve amd64 249.11-0ubuntu3.12 [64,5 kB]
Пол:2 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 openvpn-systemd-resolved amd64 1.3.0-3.1 [12,4 kB]
Получено 76,9 kB за 11с (6 818 B/s)
Выбор ранее не выбранного пакета libnss-resolve:amd64.
(Чтение базы данных -- на данный момент установлено 194568 файлов и каталогов.)
Подготовка к распаковке .../libnss-resolve_249.11-0ubuntu3.12_amd64.deb ...
Распаковывается libnss-resolve:amd64 (249.11-0ubuntu3.12) ...
Выбор ранее не выбранного пакета openvpn-systemd-resolved.
Подготовка к распаковке .../openvpn-systemd-resolved_1.3.0-3.1_amd64.deb ...
Распаковывается openvpn-systemd-resolved (1.3.0-3.1) ...
Настраивается пакет libnss-resolve:amd64 (249.11-0ubuntu3.12) ...
First installation detected...
Checking NSS setup...
Настраивается пакет openvpn-systemd-resolved (1.3.0-3.1) ...
Обрабатываются триггеры для libc-bin (2.35-0ubuntu3.9) ...
Обрабатываются триггеры для man-db (2.10.2-1) ...

```

Шаг 3. Проведите настройку WireGuard

Устанавливаем Wireguard на сервере

```

astepanov@kali:~/client-configs$ sudo apt install wireguard
[sudo] пароль для астепанов:
Installing:
  wireguard
Installing dependencies:
  wireguard-tools

Suggested packages:
  openresolv | resolvconf

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1544
  Download size: 90.1 kB
  Space needed: 343 kB / 21.9 GB available

Continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 wireguard-tools amd64 1.0.20210914-1.1 [84.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 wireguard-all 1.0.20210914-1.1 [5,472 B]
Fetched 90.1 kB in 15s (5,864 B/s)
Selecting previously unselected package wireguard-tools.
(Reading database ... 402312 files and directories currently installed.)
Preparing to unpack .../wireguard-tools_1.0.20210914-1.1_amd64.deb ...
Unpacking wireguard-tools (1.0.20210914-1.1) ...
Selecting previously unselected package wireguard.
Preparing to unpack .../wireguard_1.0.20210914-1.1_all.deb ...
Unpacking wireguard (1.0.20210914-1.1) ...
Setting up wireguard-tools (1.0.20210914-1.1) ...
wg-quick.target is a disabled or a static unit, not starting it.
Setting up wireguard (1.0.20210914-1.1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Scanning processes ...
Scanning candidates...
Scanning linux images...
Running kernel seems to be up-to-date.

Restarting services...
Service restarts being deferred:
  systemctl restart NetworkManager.service
No containers need to be restarted.

User sessions running outdated binaries:
astepanov @ session #2: ssh-agent[2272], xfce4-session[2157]
astepanov @ user manager service: systemd[2111]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

astepanov@kali:~/client-configs$ 

```

а. генерация пары ключей для сервера Wireguard

```

astepanov@kali:~/client-configs$ wg genkey | sudo tee /etc/wireguard/private.key
4MPKL+PA9t4DBKQgSv74edS0YSVYzZxWhvQ8jxHBUVm=

astepanov@kali:~/client-configs$ sudo chmod go= /etc/wireguard/private.key

astepanov@kali:~/client-configs$ sudo cat /etc/wireguard/private.key | wg pubkey | sudo tee /etc/wireguard/public.key
l050Y4etv+UxNj1EEHQV9Y5tkQ5HNL4V3L48DTFKNiM=


astepanov@kali:~/client-configs$ 

```

b. создание файла конфигурации сервера

```
astepanov@kali: ~/client-configs/files  x  astepanov@kali: ~/client-  
GNU nano 8.2  
[Interface]  
PrivateKey = 4MPKL+PA9t4DBKQgSv74eds0YSVYzZxWhvQ8jxH8UVw=  
Address = 10.8.0.1/24  
ListenPort = 51820  
SaveConfig = true  
Module 1  Module 2  Module 3  buffer  
Recent
```

c. настройка межсетевого экрана

Добавляем необходимые настройки в iptables

```
(astepanov@kali)-[~/client-configs]  $ sudo iptables -L -v -n  
Chain INPUT (policy ACCEPT 54041 packets, 1802M bytes)  0: ACCEPT [54041/1802M] --> [0/0] 链表 INPUT 表达式: 从 eth0 到 eth0, 通过 POSTROUTING 1 -> 10.8.1.0/24 -o eth0 -j MASQUERADE  
pkts bytes target prot opt in     out    source      destination  
  0   0  ACCEPT   udp  --  eth0   *      0.0.0.0/0  [0/0]  赋予权限: 从 eth0 到 eth0, 通过 POSTROUTING 1 -> 10.8.1.0/24 -o eth0 -j MASQUERADE  
  0   0  ACCEPT   all  --  wg0    *      0.0.0.0/0  [0/0]  赋予权限: 从 wg0 到 eth0, 通过 ipTables FORWARD 1 -> 1 -i eth0 -o wg0 -j ACCEPT  
  1   60  ACCEPT  tcp  --  eth0   *      0.0.0.0/0  [0/0]  state NEW tcp dpt:1194  
  0   0  ACCEPT   udp  --  eth0   *      0.0.0.0/0  [0/0]  赋予权限: 从 eth0 到 eth0, 通过 ipTables FORWARD 1 -> 1 -i eth0 -o eth0 -j ACCEPT  
Chain FORWARD (policy DROP 0 packets, 0 bytes)  0: ACCEPT [0/0]  表达式: 从 eth0 到 wg0, 通过 ipTables FORWARD 1 -> 1 -i eth0 -o wg0 -j ACCEPT  
pkts bytes target prot opt in     out    source      destination  
  0   0  ACCEPT   all  --  wg0    eth0  0.0.0.0/0  [0/0]  赋予权限: 从 wg0 到 eth0, 通过 FORWARD 1 -> 1 -i eth0 -o wg0 -j ACCEPT  
  0   0  ACCEPT   all  --  eth0    wg0  0.0.0.0/0  [0/0]  赋予权限: 从 eth0 到 wg0, 通过 FORWARD 1 -> 1 -i wg0 -o eth0 -j ACCEPT  
  0   0  ACCEPT   all  --  eth0   tun+  0.0.0.0/0  [0/0]  state RELATED,ESTABLISHED  
  0   0  ACCEPT   all  --  tun+   eth0  0.0.0.0/0  [0/0]  state RELATED,ESTABLISHED  
  0   0  ACCEPT   all  --  tun+   *      0.0.0.0/0  [0/0]  赋予权限: 从 tun+ 到 本地端口, 通过 FORWARD 1 -> 1 -i tun+ -o * -j ACCEPT  
  0   0  DOCKER-USER all  --  *      *      0.0.0.0/0  [0/0]  赋予权限: 从 * 到 * 本地端口, 通过 FORWARD 1 -> 1 -i * -o * -j ACCEPT  
  0   0  DOCKER-ISOLATION-STAGE-1 all  --  *      *      0.0.0.0/0  [0/0]  赋予权限: 从 * 到 * 本地端口, 通过 FORWARD 1 -> 1 -i * -o * -j ACCEPT  
  0   0  ACCEPT   all  --  docker0 0.0.0.0/0  [0/0]  ctstate RELATED,ESTABLISHED  
  0   0  DOCKER   all  --  *      docker0 0.0.0.0/0  [0/0]  赋予权限: 从 docker0 到 * 本地端口, 通过 FORWARD 1 -> 1 -i * -o docker0 -j ACCEPT  
  0   0  ACCEPT   all  --  docker0 !docker0 0.0.0.0/0  [0/0]  赋予权限: 从 docker0 到 docker0 本地端口, 通过 FORWARD 1 -> 1 -i docker0 -o docker0 -j ACCEPT  
  0   0  ACCEPT   all  --  docker0 docker0 0.0.0.0/0  [0/0]  赋予权限: 从 docker0 到 docker0 本地端口, 通过 FORWARD 1 -> 1 -i docker0 -o docker0 -j ACCEPT  
  0   0  ACCEPT   all  --  *      br-e0083dc27e5d 0.0.0.0/0  [0/0]  赋予权限: 从 br-e0083dc27e5d 到 * 本地端口, 通过 FORWARD 1 -> 1 -i br-e0083dc27e5d -o * -j ACCEPT  
  0   0  DOCKER   all  --  *      br-e0083dc27e5d br-e0083dc27e5d 0.0.0.0/0  [0/0]  赋予权限: 从 br-e0083dc27e5d 到 br-e0083dc27e5d 本地端口, 通过 FORWARD 1 -> 1 -i br-e0083dc27e5d -o br-e0083dc27e5d -j ACCEPT  
  0   0  ACCEPT   all  --  br-e0083dc27e5d br-e0083dc27e5d br-e0083dc27e5d 0.0.0.0/0  [0/0]  赋予权限: 从 br-e0083dc27e5d 到 br-e0083dc27e5d 本地端口, 通过 FORWARD 1 -> 1 -i br-e0083dc27e5d -o br-e0083dc27e5d -j ACCEPT  
Chain OUTPUT (policy ACCEPT 41325 packets, 2168K bytes)  
pkts bytes target prot opt in     out    source      destination  
  18 10200  ACCEPT   all  --  *      tun+  0.0.0.0/0  [0/0]  赋予权限: 从 * 到 tun+, 通过 OUTPUT 1 -> 1 -i * -o tun+ -j ACCEPT  
Chain DOCKER (2 references)  
pkts bytes target prot opt in     out    source      destination  
Chain DOCKER-ISOLATION-STAGE-1 (1 references)  
pkts bytes target prot opt in     out    source      destination  
  0   0  DOCKER-ISOLATION-STAGE-2 all  --  docker0 !docker0 0.0.0.0/0  [0/0]  赋予权限: 从 docker0 到 docker0 本地端口, 通过 FORWARD 1 -> 1 -i docker0 -o docker0 -j ACCEPT  
  0   0  DOCKER-ISOLATION-STAGE-2 all  --  br-e0083dc27e5d !br-e0083dc27e5d 0.0.0.0/0  [0/0]  赋予权限: 从 br-e0083dc27e5d 到 br-e0083dc27e5d 本地端口, 通过 FORWARD 1 -> 1 -i br-e0083dc27e5d -o br-e0083dc27e5d -j ACCEPT  
  0   0  RETURN   all  --  *      *      0.0.0.0/0  [0/0]  赋予权限: 从 * 到 *, 通过 FORWARD 1 -> 1 -i * -o * -j ACCEPT  
Chain DOCKER-ISOLATION-STAGE-2 (2 references)  
pkts bytes target prot opt in     out    source      destination  
  0   0  DROP     all  --  *      docker0 0.0.0.0/0  [0/0]  赋予权限: 从 docker0 到 *, 通过 FORWARD 1 -> 1 -i * -o docker0 -j ACCEPT  
  0   0  DROP     all  --  *      br-e0083dc27e5d 0.0.0.0/0  [0/0]  赋予权限: 从 br-e0083dc27e5d 到 *, 通过 FORWARD 1 -> 1 -i * -o br-e0083dc27e5d -j ACCEPT  
  0   0  RETURN   all  --  *      *      0.0.0.0/0  [0/0]  赋予权限: 从 * 到 *, 通过 FORWARD 1 -> 1 -i * -o * -j ACCEPT  
Chain DOCKER-USER (1 references)  
pkts bytes target prot opt in     out    source      destination  
  0   0  RETURN   all  --  *      *      0.0.0.0/0  [0/0]  赋予权限: 从 * 到 *, 通过 FORWARD 1 -> 1 -i * -o * -j ACCEPT  
(astepanov@kali)-[~/client-configs]
```

d. запуск Wireguard

Поднимаем wg-сервер

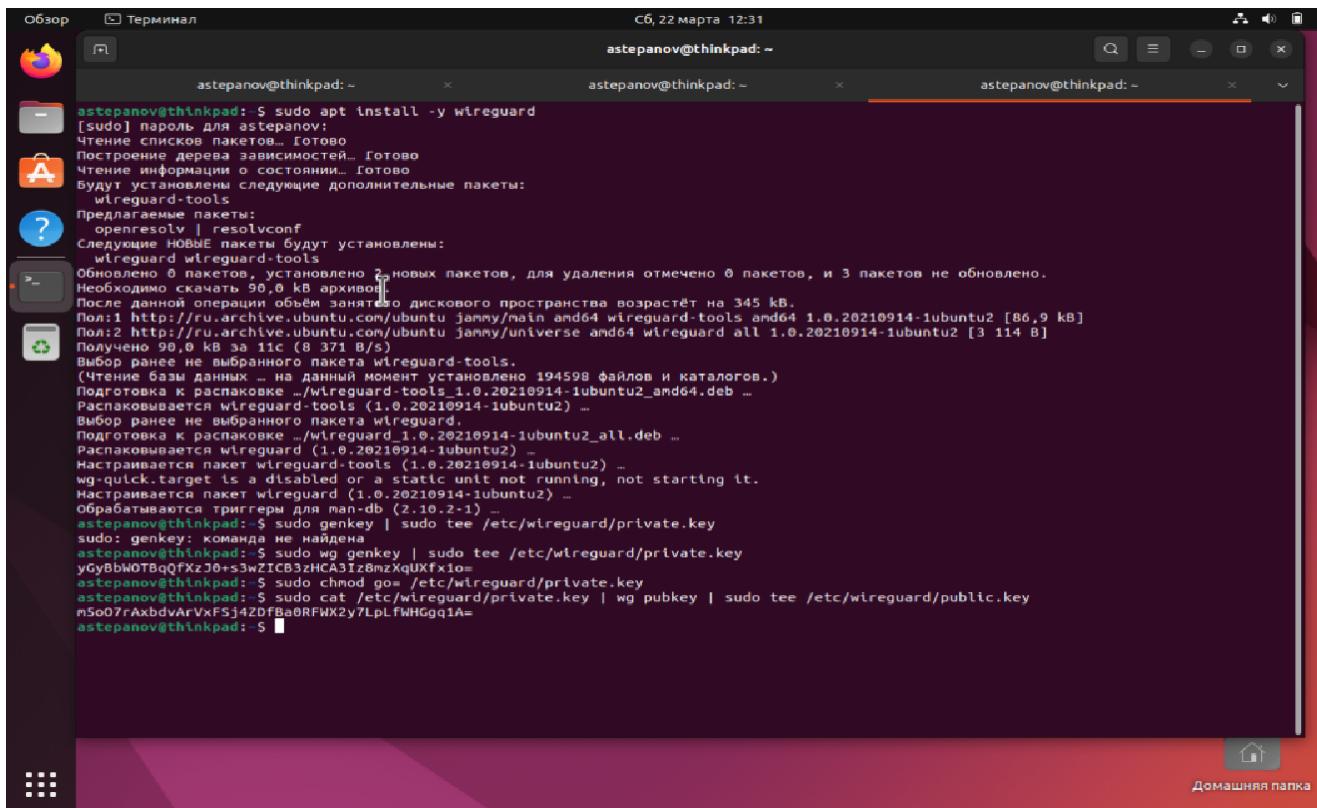
```
(astepanov㉿kali)-[~/client-configs]
$ sudo systemctl enable wg-quick@wg0.service
Created symlink '/etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service' → '/usr/lib/systemd/system/wg-quick@.service'.

(astepanov㉿kali)-[~/client-configs]
$ sudo systemctl start wg-quick@wg0.service

(astepanov㉿kali)-[~/client-configs]
$ sudo systemctl status wg-quick@wg0.service
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
   Loaded: loaded (/usr/lib/systemd/system/wg-quick@.service; enabled; preset: disabled)
     Active: active (exited) since Sat 2025-03-22 04:25:53 EDT; 4s ago
       Docs: man:wg-quick(8)
              man:wg(8)
              https://www.wireguard.com/
              https://www.wireguard.com/quickstart/
              https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
              https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
     Process: 294566 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/SUCCESS)
    Main PID: 294566 (code-exited, status=0/SUCCESS)
      Mem peak: 4.1M
        CPU: 57ms

Mar 22 04:25:53 kali systemd[1]: Starting wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0...
Mar 22 04:25:53 kali wg-quick[294566]: [#] ip link add wg0 type wireguard
Mar 22 04:25:53 kali wg-quick[294566]: [#] wg setconf wg0 /dev/fd/63
Mar 22 04:25:53 kali wg-quick[294566]: [#] ip -4 address add 10.8.0.1/24 dev wg0
Mar 22 04:25:53 kali wg-quick[294566]: [#] ip link set mtu 1420 up dev wg0
Mar 22 04:25:53 kali systemd[1]: Finished wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0.
```

е. генерация пары ключей для клиента Wireguard



```
astepanov@thinkpad:~$ sudo apt install -y wireguard
[sudo] пароль для astepanov:
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состояниях... Готово
Будут установлены следующие дополнительные пакеты:
  wireguard-tools
Предлагаемые пакеты:
  openresolv | resolvconf
Следующие НОВЫЕ пакеты будут установлены:
  wireguard wireguard-tools
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 3 пакетов не обновлено.
Необходимо скачать 90,6 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 345 kB.
Пол:1 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 wireguard-tools amd64 1.0.20210914-1ubuntu2 [86,9 kB]
Пол:2 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 wireguard all 1.0.20210914-1ubuntu2 [3 114 B]
Получено 90,0 kB за 11с (8 371 B/s).
Выбор ранее не выбранного пакета wireguard-tools.
(Чтение базы данных ... – в данный момент установлено 194598 файлов и каталогов.)
Подготовка к распаковке .../wireguard-tools_1.0.20210914-1ubuntu2_amd64.deb ...
Распаковывается wireguard-tools (1.0.20210914-1ubuntu2) ...
Выбор ранее не выбранного пакета wireguard.
Подготовка к распаковке .../wireguard_1.0.20210914-1ubuntu2_all.deb ...
Распаковывается wireguard (1.0.20210914-1ubuntu2) ...
Настраивается пакет wireguard-tools (1.0.20210914-1ubuntu2) ...
wg-quick.target is a disabled or a static unit not running, not starting it.
Настраивается пакет wireguard (1.0.20210914-1ubuntu2) ...
Обрабатываются триггеры для man-db (2.10.2-1) ...
astepanov@thinkpad:~$ sudo genkey | sudo tee /etc/wireguard/private.key
sudo: genkey: команда не найдена
astepanov@thinkpad:~$ sudo wg genkey | sudo tee /etc/wireguard/private.key
у0yBbWOTBqQfxZ0+s3wZICB3zHCA3IZ8mzxqUxfxi0=
astepanov@thinkpad:~$ sudo chmod go= /etc/wireguard/private.key
astepanov@thinkpad:~$ sudo cat /etc/wireguard/private.key | wg pubkey | sudo tee /etc/wireguard/public.key
n5o07rAxbdvArVxF5I4ZDFBa@RFWK2y7LpLfWHggq1A=
astepanov@thinkpad:~$
```

f. создание файла конфигурации клиента

g. добавление публичного ключа клиента на сервер Wireguard

```

astepanov@thinkpad:~$ sudo wg set wg0 peer m5o07rAxbdvArVxFSj4ZDFBa0RFWX2y7LpLfWHGqq1A= allowed-ips 10.8.0.2
Unable to modify interface: No such device
astepanov@thinkpad:~$ sudo wg-quick up wg0
wg-quick: '/etc/wireguard/wg0.conf' does not exist
astepanov@thinkpad:~$ sudo wg show
astepanov@thinkpad:~$ sudo wg-quick up --client-configs/wg0.conf
Warning: '/home/astepanov/client-configs/wg0.conf' is world accessible
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.8.0.2/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
astepanov@thinkpad:~$ sudo wg show
Interface: wg0
  public key: m5o07rAxbdvArVxFSj4ZDFBa0RFWX2y7LpLfWHGqq1A=
  private key: (hidden)
  listening port: 51030

peer: l050Y4etv+UxNj1EEHQV9YStkQ5HNL4V3L48DTFKNlM=
  endpoint: 10.0.3.4:51820
  allowed ips: 10.8.0.0/24
astepanov@thinkpad:~$ sudo cat --client-configs/wg0.conf
[Interface]
  PrivateKey = yGyBbW0TBqQfxzJ0+s3wZICB3zHCA3Iz8mzXqUXfx1o=
  Address = 10.8.0.2/24
[Peer]
  PublicKey = l050Y4etv+UxNj1EEHQV9YStkQ5HNL4V3L48DTFKNlM=
  AllowedIPs = 10.8.0.0/24
  Endpoint = 10.0.3.4:51820
astepanov@thinkpad:~$ 

```

Шаг 4. Произведите соединение поочередно каждой из технологий. Замерьте скорость

OpenVPN

Подключаемся через openvpn

```

astepanov@thinkpad:~$ sudo openvpn --config ubuntu.ovpn
2025-03-22 11:47:36 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2025-03-22 11:47:36 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2025-03-22 11:47:36 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-03-22 11:47:36 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.4:1194
2025-03-22 11:47:36 Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194 [nonblock]
2025-03-22 11:47:36 TCP connection established with [AF_INET]10.0.3.4:1194
2025-03-22 11:47:36 TCP_CLIENT link local: (not bound)
2025-03-22 11:47:36 TCP_CLIENT link remote: [AF_INET]10.0.3.4:1194
2025-03-22 11:47:36 [kali] Peer Connection Initiated with [AF_INET]10.0.3.4:1194
2025-03-22 11:47:36 TUN/TAP device tun0 opened
2025-03-22 11:47:36 net_iface_mtu_set: mtu 1500 for tun0
2025-03-22 11:47:36 net_iface_up: set tun0 up
2025-03-22 11:47:36 net_addr_v4_add: 10.8.0.2/24 dev tun0
2025-03-22 11:47:36 /etc/openvpn/update-systemd-resolved tun0 1500 1626 10.8.0.2 255.255.255.0 init
<14>Mar 22 11:47:36 update-systemd-resolved: Link 'tun0' coming up
<14>Mar 22 11:47:36 update-systemd-resolved: Adding DNS Routed Domain DOMAIN-ROUTE
<14>Mar 22 11:47:36 update-systemd-resolved: SetLinkDomains(3 1 DOMAIN-ROUTE true)
2025-03-22 11:47:36 Initialization Sequence Completed
^[[

```

Соединение успешно установлено...

Пингуем адрес сервера, для проверки работы vpn

```

astepanov@thinkpad:~$ ping 10.0.3.5
PING 10.0.3.5 (10.0.3.5) 56(84) bytes of data.
64 bytes from 10.0.3.5: icmp_seq=1 ttl=64 time=0.205 ms
64 bytes from 10.0.3.5: icmp_seq=2 ttl=64 time=0.386 ms
^C
--- 10.0.3.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.205/0.295/0.386/0.090 ms
astepanov@thinkpad:~$ ^C
astepanov@thinkpad:~$ ping 10.0.3.4
PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.
64 bytes from 10.0.3.4: icmp_seq=1 ttl=64 time=2.17 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=64 time=3.25 ms
64 bytes from 10.0.3.4: icmp_seq=3 ttl=64 time=0.791 ms
64 bytes from 10.0.3.4: icmp_seq=4 ttl=64 time=0.802 ms
^C
--- 10.0.3.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3236ms
rtt min/avg/max/mdev = 0.791/1.752/3.246/1.028 ms
astepanov@thinkpad:~$ 

```

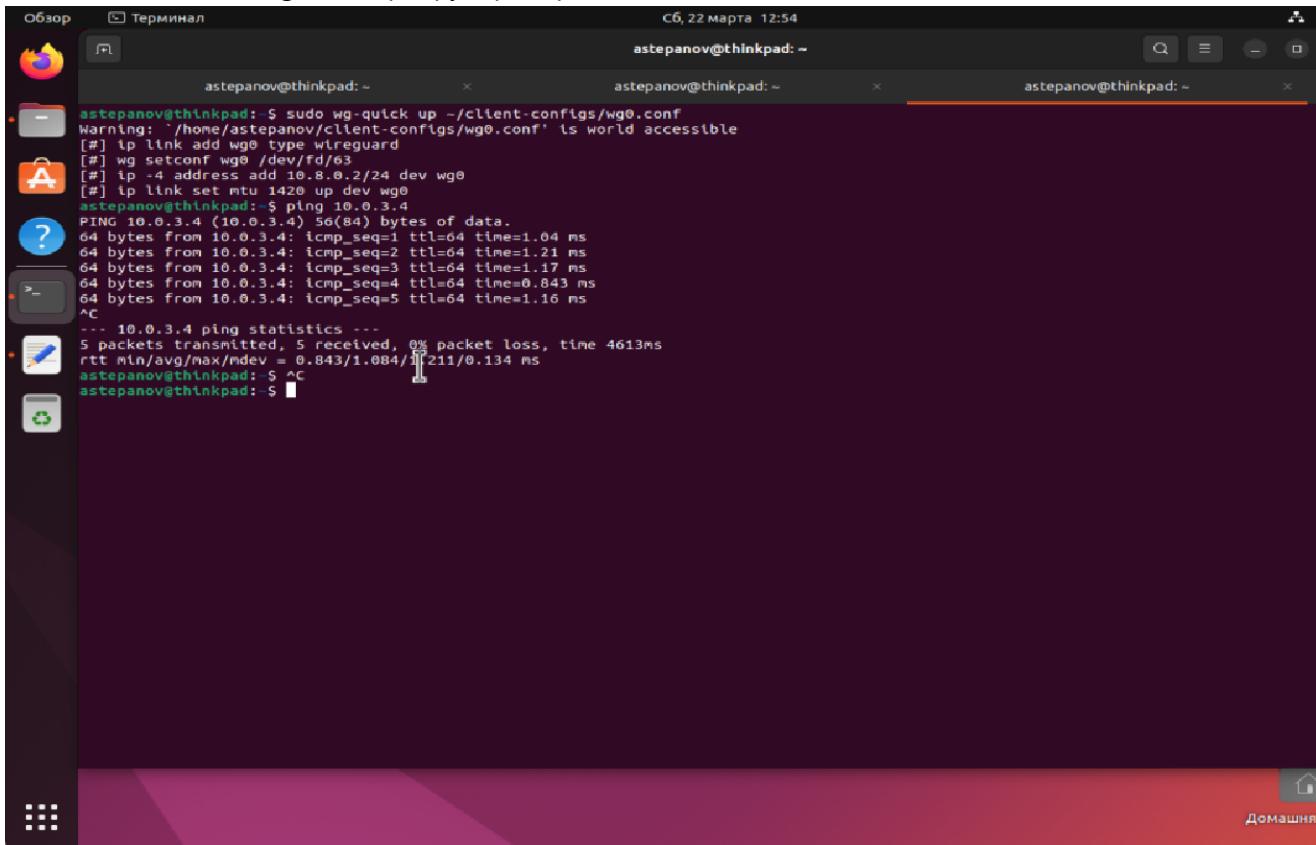
Сервер пингуется успешно...

Замеряем скорость соединения с помощью утилиты iperf

```
Обрабатываются триггеры для libc-bin (2.35-0ubuntu3.9) ...
astepanov@thinkpad:~$ iperf3 -c 10.0.3.4
Connecting to host 10.0.3.4, port 5201
[ 5] local 10.0.3.5 port 60562 connected to 10.0.3.4 port 5201
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 5] 0.00-1.00 sec 167 MBytes 1.40 Gbits/sec 274 286 KBytes
[ 5] 1.00-2.00 sec 168 MBytes 1.41 Gbits/sec 228 223 KBytes
[ 5] 2.00-3.00 sec 181 MBytes 1.51 Gbits/sec 180 233 KBytes
[ 5] 3.00-4.00 sec 184 MBytes 1.54 Gbits/sec 90 446 KBytes
[ 5] 4.00-5.00 sec 167 MBytes 1.40 Gbits/sec 90 413 KBytes
[ 5] 5.00-6.00 sec 166 MBytes 1.39 Gbits/sec 101 420 KBytes
[ 5] 6.00-7.00 sec 154 MBytes 1.29 Gbits/sec 218 238 KBytes
[ 5] 7.00-8.00 sec 155 MBytes 1.38 Gbits/sec 134 318 KBytes
[ 5] 8.00-9.00 sec 166 MBytes 1.39 Gbits/sec 135 329 KBytes
[ 5] 9.00-10.00 sec 144 MBytes 1.21 Gbits/sec 225 253 KBytes
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 5] 0.00-10.00 sec 1.61 GBytes 1.38 Gbits/sec 1675 sender
[ 5] 0.00-10.01 sec 1.61 GBytes 1.38 Gbits/sec receiver
iperf Done.
```

WireGuard

Подключаемся к wireguard серверу, проверяем пинг



Соединение успешно, пинг проходит...

Перед тем как замерить скорость - следует отключить ранее запущенный openvpn, проверяя что сервис openvnp выключен

```

astepanov@kali: ~/client-configs/files × astepanov@kali: ~/client-configs × astepanov@kali: ~/client-configs ×
└─(astepanov㉿kali)-[~/client-configs]
$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; preset: disabled)
   Active: inactive (dead) since Sat 2025-03-22 04:56:22 EDT; 2min 17s ago
     Duration: 16h 30min 39.543s
   Invocation: 6cfdb8788450f4d0eb5ede927592cabdf
     Docs: man:openvpn(8)
           https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Process: 110726 ExecStart=/usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --supp
 Main PID: 110726 (code=exited, status=0/SUCCESS)
   Status: "Initialization Sequence Completed"
    Mem peak: 2.4M
      CPU: 735ms

Mar 22 04:42:31 kali openvpn[110726]: ubuntu/10.0.3.5:46984 peer info: IV_TCPNL=1
Mar 22 04:42:31 kali openvpn[110726]: ubuntu/10.0.3.5:46984 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA
Mar 22 04:55:42 kali openvpn[110726]: ubuntu/10.0.3.5:46984 Connection reset, restarting [0]
Mar 22 04:55:42 kali openvpn[110726]: ubuntu/10.0.3.5:46984 SIGUSR1[soft,connection-reset] received, client-instance res
Mar 22 04:56:22 kali systemd[1]: Stopping openvpn-server@server.service - OpenVPN service for server ...
Mar 22 04:56:22 kali openvpn[110726]: Closing TUN/TAP interface
Mar 22 04:56:22 kali openvpn[110726]: net_addr_v4_del: 10.8.0.1 dev tun0
Mar 22 04:56:22 kali openvpn[110726]: SIGTERM[hard,] received, process exiting
Mar 22 04:56:22 kali systemd[1]: openvpn-server@server.service: Deactivated successfully.
Mar 22 04:56:22 kali systemd[1]: Stopped openvpn-server@server.service - OpenVPN service for server.

└─(astepanov㉿kali)-[~/client-configs]
$ 
└─(astepanov㉿kali)-[~/client-configs]
$ sudo wg show
interface: wg0
  public key: lo50Y4etv+UxNJ1EEHQV9YStlkQ5HNL4V3L48DTFKNiM=
  private key: (hidden)
  listening port: 51820

└─(astepanov㉿kali)-[~/client-configs]
$ 

```

Замеряем скорость соединения с помощью утилиты iperf

```

astepanov@thinkpad:~$ iperf3 -c 10.0.3.4
Connecting to host 10.0.3.4, port 5201
[  5] local 10.0.3.5 port 44188 connected to 10.0.3.4 port 5201
[ ID] Interval          Transfer       Bitrate
[  5]  0.00-1.00  sec  202 MBytes  1.69 Gbits/sec  90  420 KBytes
[  5]  1.00-2.00  sec  193 MBytes  1.62 Gbits/sec  161  416 KBytes
[  5]  2.00-3.00  sec  202 MBytes  1.70 Gbits/sec  123  414 KBytes
[  5]  3.00-4.00  sec  199 MBytes  1.67 Gbits/sec  180  474 KBytes
[  5]  4.00-5.00  sec  200 MBytes  1.68 Gbits/sec  180  421 KBytes
[  5]  5.00-6.00  sec  197 MBytes  1.66 Gbits/sec  172  445 KBytes
[  5]  6.00-7.00  sec  189 MBytes  1.58 Gbits/sec  135  426 KBytes
[  5]  7.00-8.00  sec  180 MBytes  1.51 Gbits/sec  234  362 KBytes
[  5]  8.00-9.00  sec  187 MBytes  1.57 Gbits/sec  270  304 KBytes
[  5]  9.00-10.00 sec  181 MBytes  1.52 Gbits/sec  180  362 KBytes
[  5]  10.00-10.01 sec  1.88 GBytes  1.62 Gbits/sec  1725
                                         sender
                                         receiver

iperf Done.

```

Шаг 5. Сделайте выводы в соответствии с полученными результатами, основываясь на тонкостях двух изучаемых протоколов

Результатам сравнения скорости передачи данных с помощью утилиты **iperf** показали следующие результаты:

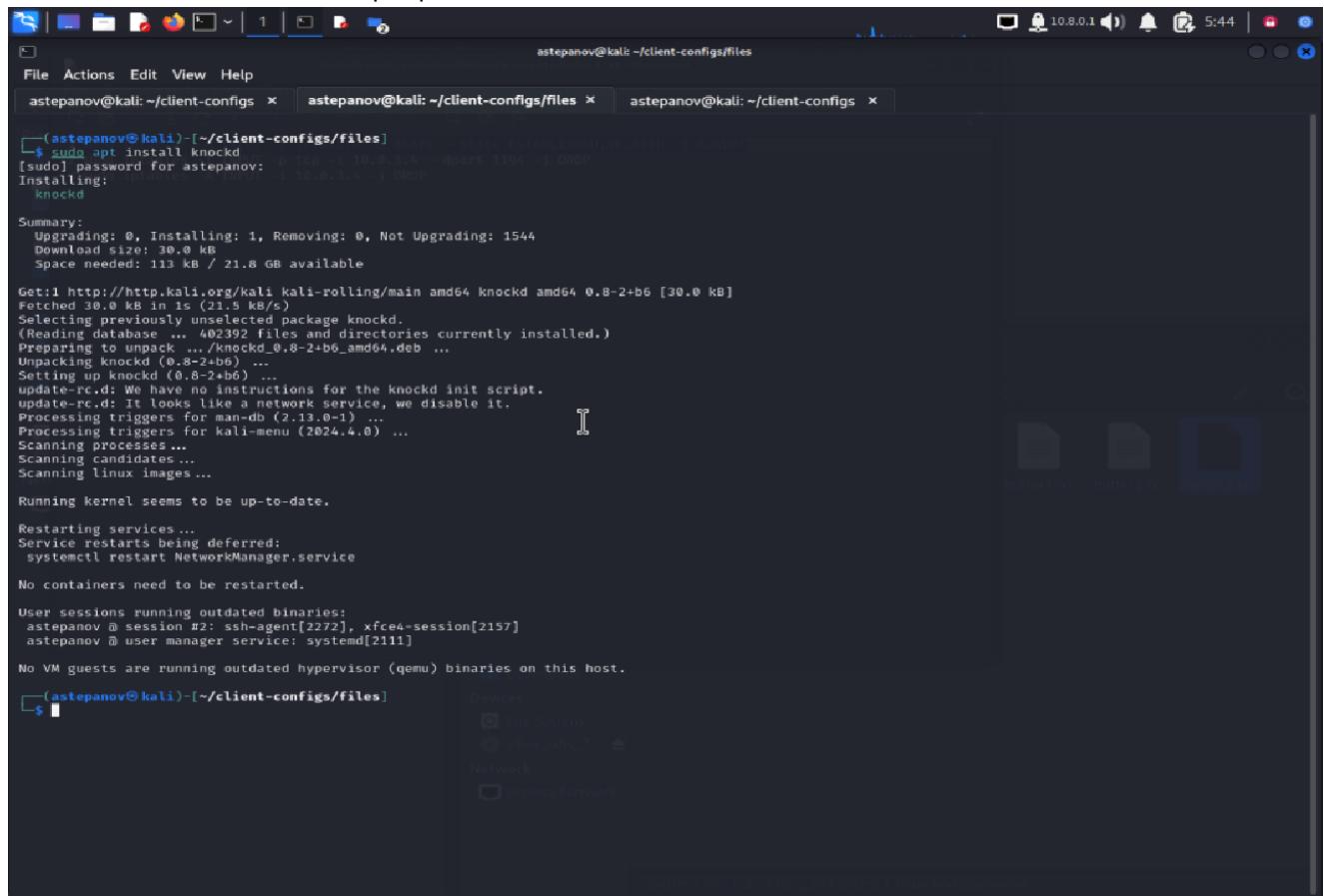
- Средняя скорость передачи данных через OpenVPN составила 1,38 Gb/sec
- Средняя скорость передачи данных через WireGuard составила 1,62 Gb/sec

Таким образом, практический замер скорости VPN-соединений данных протоколов подтверждает теоретическую информацию о том, что скорость передачи данных через WireGuard несколько выше.

WireGuard обычно быстрее, чем OpenVPN, благодаря меньшему коду, использованию современных криптографических алгоритмов и меньшему потреблению ресурсов. Он быстрее устанавливает соединение, имеет меньшие задержки и эффективнее работает на слабых устройствах

Шаг 6. Произведите настройку технологии Port Knocking для порта OpenVPN

Устанавливаем knockd на сервер



```
(astepanov㉿kali)-[~/client-configs/files] $ sudo apt install knockd
[sudo] password for astepanov: 
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  knockd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 30.0 kB of archives.
After this operation, 113 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 knockd amd64 0.8-2+b6 [30.0 kB]
Fetched 30.0 kB in 0s (21.5 kB/s)
Selecting previously unselected package knockd.
(Reading database ... 402392 files and directories currently installed.)
Preparing to unpack .../knockd_0.8-2+b6_amd64.deb ...
Unpacking knockd (0.8-2+b6) ...
Setting up knockd (0.8-2+b6) ...
update-rc.d: We have no instructions for the knockd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Scanning processes ...
Scanning candidates ...
Scanning linux images ...

Running kernel seems to be up-to-date.

Restarting services ...
Service restarts being deferred:
systemctl restart NetworkManager.service

No containers need to be restarted.

User sessions running outdated binaries:
astepanov @ session #2: ssh-agent[2272], xfce4-session[2157]
astepanov @ user manager service: systemd[2111]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

(astepanov㉿kali)-[~/client-configs/files]
```

Производим настройку пакетного фильтра

После некоторых неудачных попыток настроить пакетный фильтр, окончательный **iptables** выглядит следующим образом:

```

[astepanov@kali] -[~/client-configs]
$ sudo iptables -I INPUT -p tcp --dport 1194 -j DROP
[astepanov@kali] -[~/client-configs]
$ sudo iptables -I INPUT -p udp --dport 1194 -j DROP
[astepanov@kali] -[~/client-configs]
$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 211K packets, 7624M bytes) 0:0
    pkts bytes target     prot opt in     out    source        destination
      0   0 DROP       udp  --  *     *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0
      0   0 DROP       tcp  --  *     *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0
      0   0 ACCEPT    udp  --  eth0   *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0
      0   0 ACCEPT    all   --  w提醒  *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0
  16  960 ACCEPT    tcp  --  eth0   *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0      state NEW tcp dpt:1194
      0   0 ACCEPT    udp  --  eth0   *     0.0.0.0/0  0.0.0.0/0          0.0.0.0/0      state NEW udp dpt:51820

```

Где первые две строчки блокируют входящие tcp и udp пакеты на порт OpenVpn, в результате чего ни один ip-адрес не сможет установить соединение с OpenVpn сервером

Настраиваем конфиг knockd

```

File Actions Edit View Help
astepanov@kali: ~/client-configs × astepanov@kali: ~/client-configs/files × astepanov@kali: /etc/knockd.conf
GNU nano 8.2
[options]
UseSyslog
Interface = eth0

[openClosePort]
sequence = 7000,8000,9000
seq_timeout = 5
start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 1194 -j ACCEPT
cmd_timeout = 60
stop_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 1194 -j ACCEPT
tcpflags = syn +
TCP      all   -- br-e0083dc27e5d !br-e0083dc27e5d  0.0.0.0/0          0.0.0.0/0
TCP      all   -- br-e0083dc27e5d br-e0083dc27e5d  0.0.0.0/0          0.0.0.0/0

policy ACCEPT 163K packets, 8574K bytes)
reet      prot opt in     out    source        destination

```

Конфиг открывает порт 1194 для ip-адреса, с которого поступил запрос на tcp-соединение при правильном "простукивании" портов с таймаутом закрытия порта в 60 секунд.

Запускаем службу knockd и проверяем статус

```

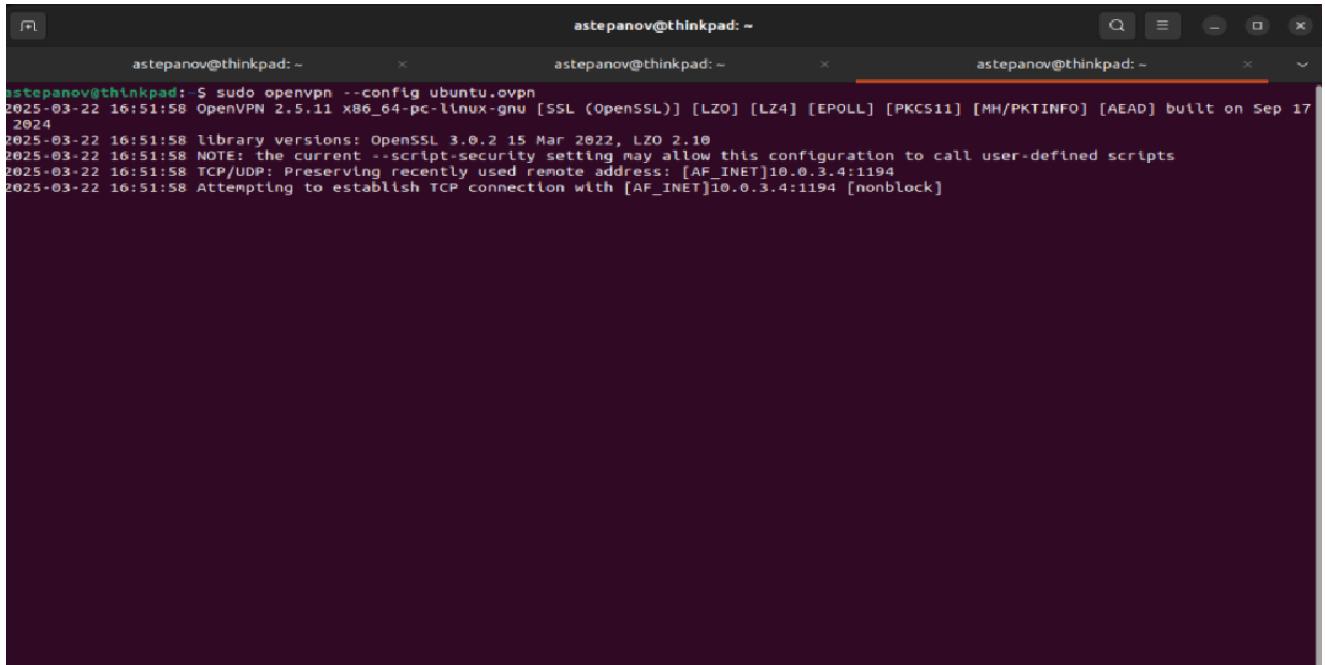
[astepanov@kali] -[~/client-configs]
$ sudo systemctl status knockd.service
● knockd.service - Port-Knock Daemon
   Loaded: loaded (/usr/lib/systemd/system/knockd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-03-22 08:40:27 EDT; 4s ago
     Invocation: c10f1c2f31b0441d8ca049a0ffa06721
     Docs: man:knockd(1)
   Main PID: 378213 (knockd)
     Tasks: 1 (limit: 4555)
    Memory: 392K (peak: 1.8M)
      CPU: 79ms
     CGroup: /system.slice/knockd.service
           └─378213 /usr/sbin/knockd
Mar 22 08:40:27 kali systemd[1]: knockd.service: Deactivated successfully.
Mar 22 08:40:27 kali systemd[1]: Stopped knockd.service - Port-Knock Daemon.
Mar 22 08:40:27 kali systemd[1]: Started knockd.service - Port-Knock Daemon.
Mar 22 08:40:27 kali (knockd)[378213]: knockd.service: Referenced but unset environment variable evaluates to an empty string: K
Mar 22 08:40:27 kali knockd[378213]: starting up, listening on eth0

```

Шаг 7. Произведите подключение по OpenVPN с технологией Port Knocking, проверьте работоспособность

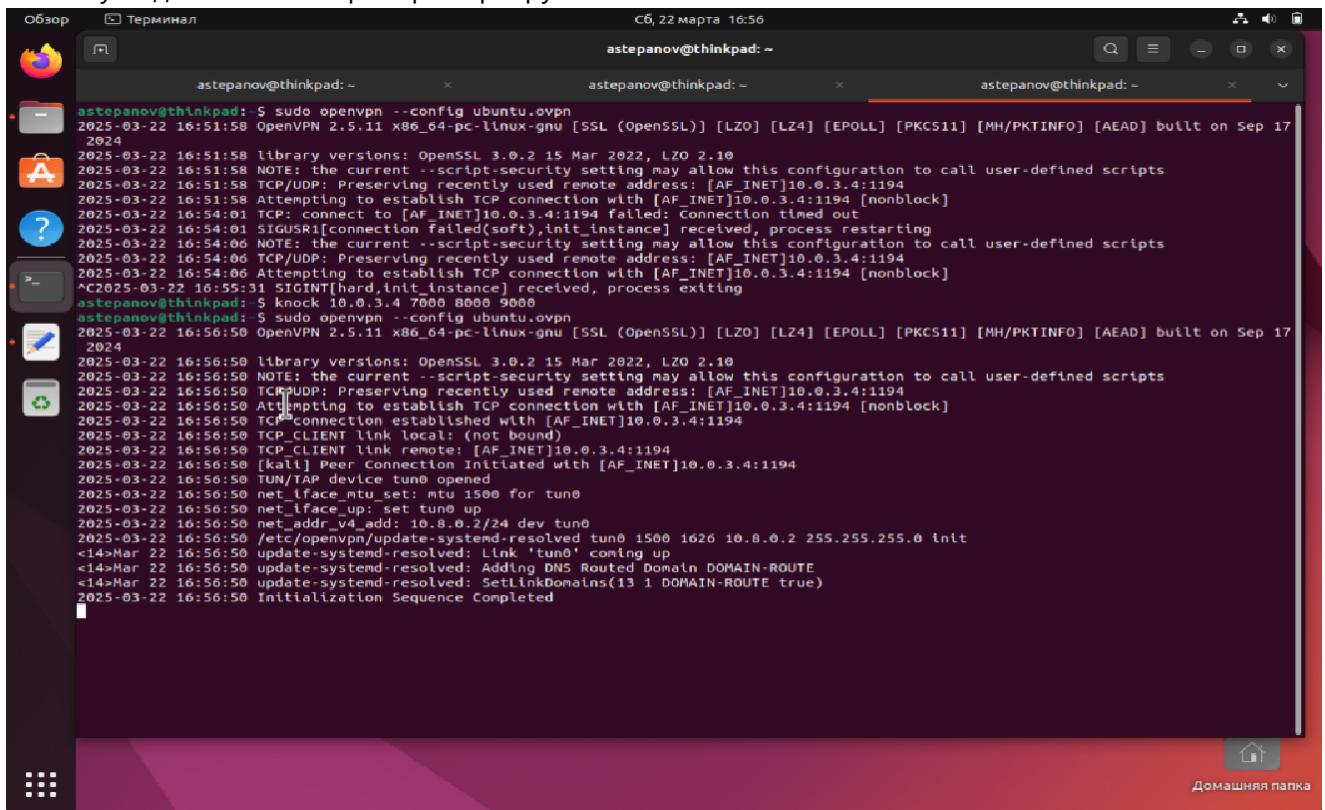
Для начала проверим что без простояивания портов VPN-соединение не сможет быть установлено. Для этого пробуем подключиться с VPN-серверу и видим, что статус нашего соединения "зарывает" в состоянии **Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194**

Дальше ничего не происходит, сообщения об успешном подключении к VPN-серверу нету, так как на стороне сервера tcp-пакеты фильтруются.



```
astepanov@thinkpad:~$ sudo openvpn --config ubuntu.ovpn
2025-03-22 16:51:58 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2025-03-22 16:51:58 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2025-03-22 16:51:58 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-03-22 16:51:58 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.4:1194
2025-03-22 16:51:58 Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194 [nonblock]
```

Дальше "простукиваем" сервер заданной последовательностью **7000 8000 9000" и повторяем попытку подключения к OpenVpn серверу.



```
astepanov@thinkpad:~$ sudo openvpn --config ubuntu.ovpn
2025-03-22 16:51:58 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2025-03-22 16:51:58 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2025-03-22 16:51:58 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-03-22 16:51:58 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.4:1194
2025-03-22 16:51:58 Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194 [nonblock]
2025-03-22 16:54:01 TCP: Connect to [AF_INET]10.0.3.4:1194 failed: Connection timed out
2025-03-22 16:54:01 SIGUSR1[connection failed(soft).init_instance] received, process restarting
2025-03-22 16:54:06 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-03-22 16:54:06 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.4:1194
2025-03-22 16:54:06 Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194 [nonblock]
^C2025-03-22 16:55:31 SIGINT[hard,init_instance] received, process exiting
astepanov@thinkpad:~$ knock 10.0.3.4 7000 8000 9000
astepanov@thinkpad:~$ sudo openvpn --config ubuntu.ovpn
2025-03-22 16:56:50 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2025-03-22 16:56:50 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2025-03-22 16:56:50 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-03-22 16:56:50 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.4:1194
2025-03-22 16:56:50 Attempting to establish TCP connection with [AF_INET]10.0.3.4:1194 [nonblock]
2025-03-22 16:56:58 TCP connection established with [AF_INET]10.0.3.4:1194
2025-03-22 16:56:58 TCP_CLIENT link local: (not bound)
2025-03-22 16:56:58 TCP_CLIENT link remote: [AF_INET]10.0.3.4:1194
2025-03-22 16:56:58 [kali] Peer Connection Initiated with [AF_INET]10.0.3.4:1194
2025-03-22 16:56:58 TUN/TAP device tun0 opened
2025-03-22 16:56:58 net_iface_mtu set: mtu 1500 for tun0
2025-03-22 16:56:58 net_iface_up: set tun0 up
2025-03-22 16:56:58 net_addr_v4_add: 10.8.0.2/24 dev tun0
2025-03-22 16:56:58 /etc/openvpn/update-systemd-resolved tun0 1500 1626 10.8.0.2 255.255.255.0 init
<14>Mar 22 16:56:58 update-systemd-resolved: Link 'tun0' coming up
<14>Mar 22 16:56:58 update-systemd-resolved: Adding DNS Routed Domain DOMAIN-ROUTE
<14>Mar 22 16:56:58 update-systemd-resolved: SetLinkDomains(13 1 DOMAIN-ROUTE true)
2025-03-22 16:56:58 Initialization Sequence Completed
```

Видим, что соединение моментально установлено.

Шаг 8. Просканируйте порт с помощью nmap до отправки последовательности и после, сравните результаты

Результаты сканирования порта 1194 с помощью TCP SCAN

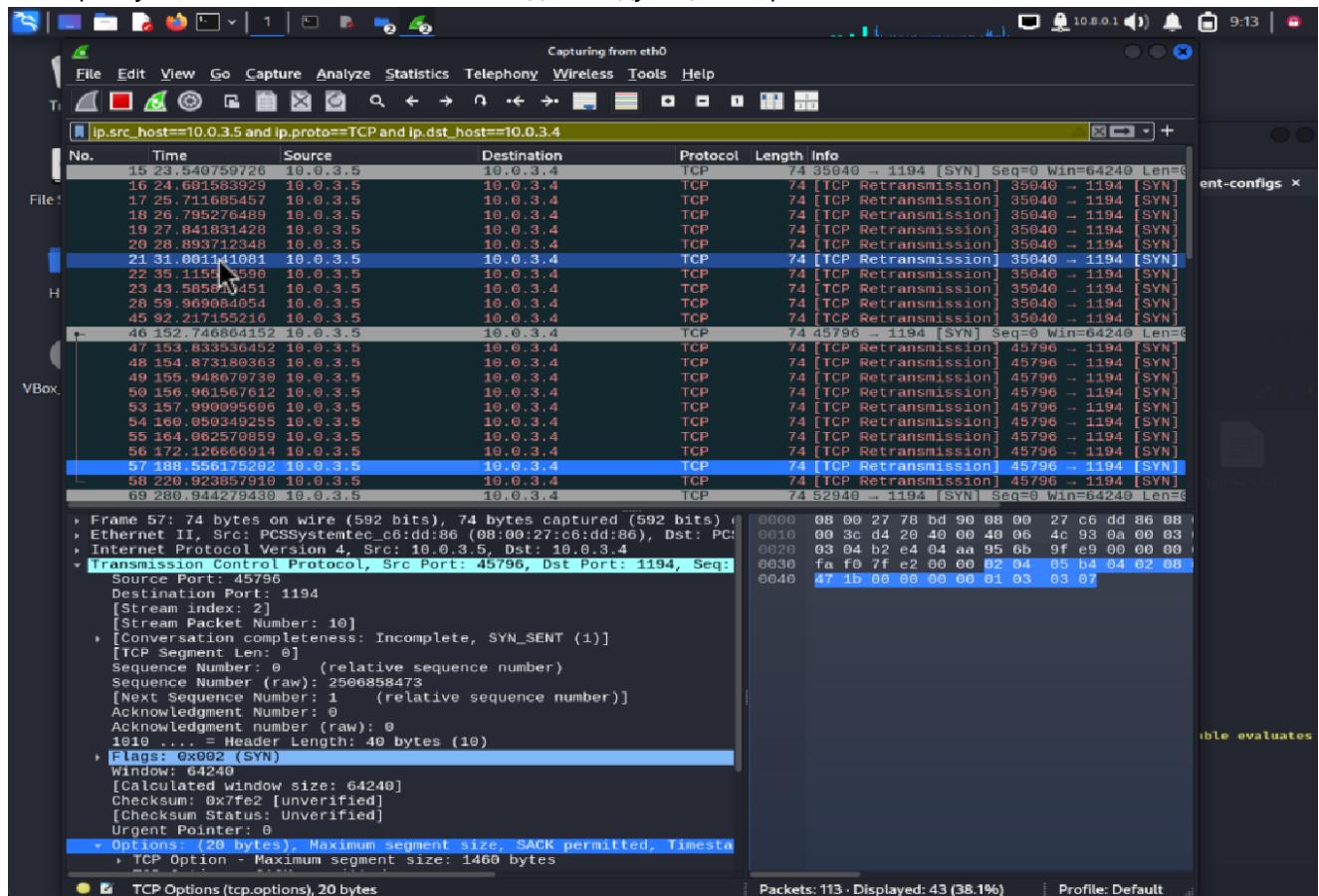


Как видим, до простукивания состояние порта "filtered", что говорит нам о том, что порт блокируется межсетевым фильтром и ответные пакеты от сканируемого хоста не возвращаются обратно.

После простукивания состояние порта "open", что говорит нам о том, что порт открыт и пакеты успешно перемещаются между хостами

Шаг 9. Посмотрите в Wireshark, как отправляются пакеты при подключении через Port Knocking

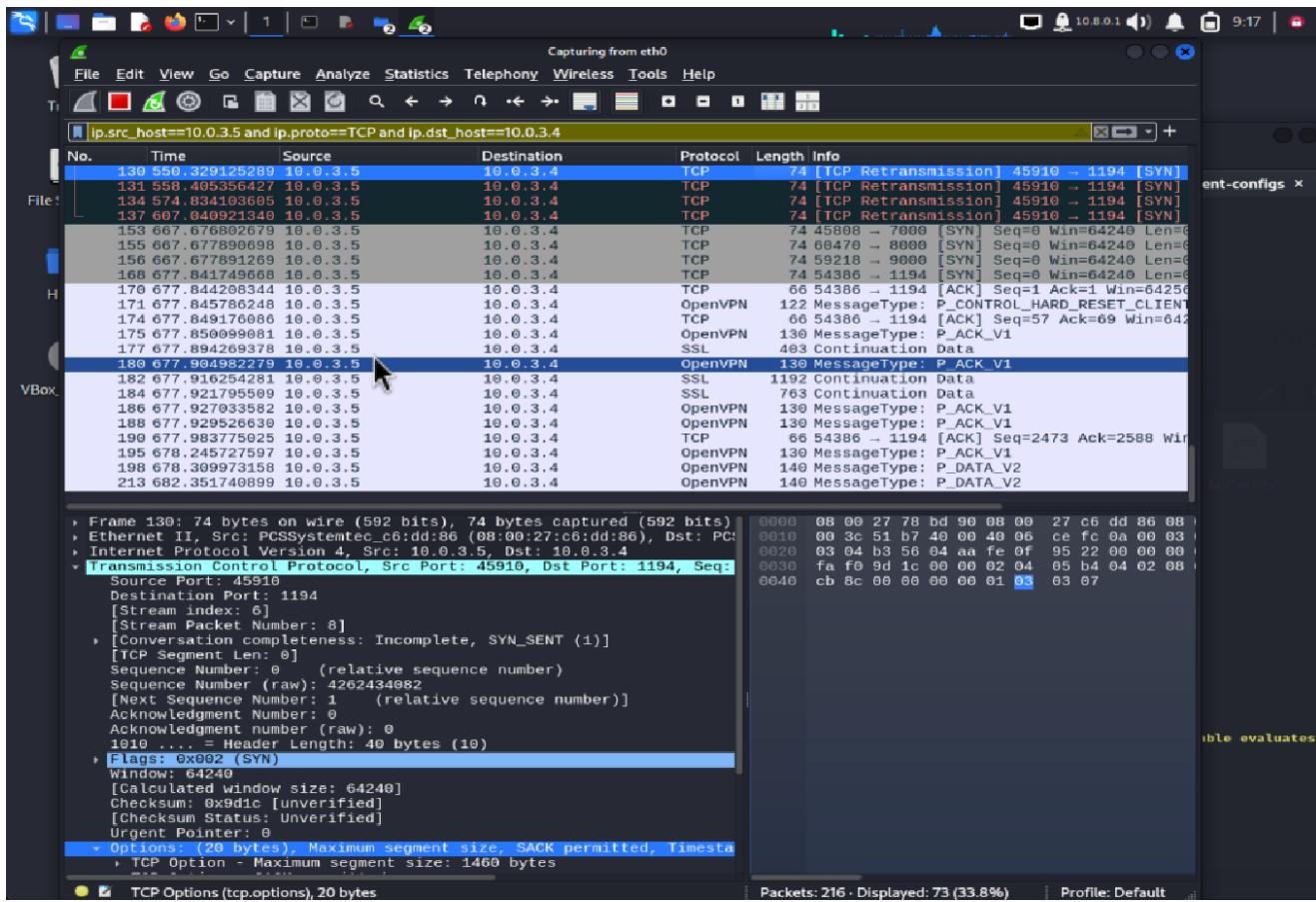
До "простукивания" пакеты в сети выглядят следующим образом



Wireshark screenshot showing network traffic captured from eth0. The filter is set to `ip.src_host==10.0.3.5 and ip.proto==TCP and ip.dst_host==10.0.3.4`. The list of captured frames shows numerous TCP SYN packets (flag `S`) from source 10.0.3.5 to destination 10.0.3.4. These are labeled as `[TCP Retransmission]`. The details pane for frame 57 shows the SYN flag is set, and the sequence number is 0. The bytes pane shows the raw hex and ASCII data for the SYN packet.

- Клиент отправляет SYN (первый пакет TCP handshake) на сервер.
- Сервер не отвечает (firewall его просто дропает).
- Клиент ждёт таймаут и повторяет SYN (TCP Retransmission).
- Повторные SYN продолжаются несколько раз

А вот как выглядит "простукивание" портов с помощью port-knocking



До установления соединения с OpenVpn сервером идут 3 TCP-пакета на порты 7000, 8000 и 9000 соответственно.

После этого мы видим успешное tcp-соединение и дальше пакеты по протоколу OpenVPN передаются между клиентом и сервером