# VPN!

# Πίνακας περιεχομένων



# 1. Install docker (Home PC)

HowTo: See How to

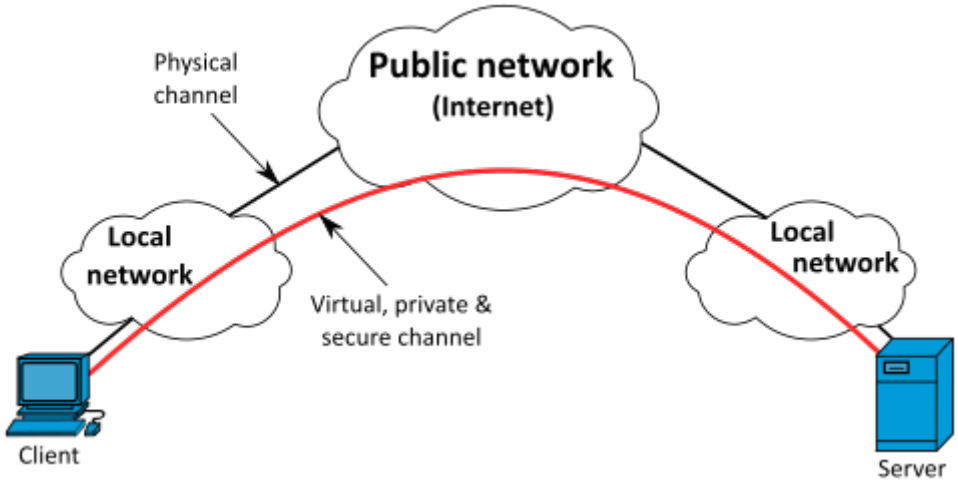
*NOTE*

Assuming you're already logged in

# 2. VPN

A **virtual private network (VPN)** extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, though not an inherent, part of a VPN connection

More: wikipedia




*NOTE*

**OpenVPN** is an open-source software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

More: wikipedia

# 3. Create VPN

*create-vpn.sh*

```
#!/bin/bash
IP=127.0.0.1                                          # Server IP       ①
P=1194                                                # Server Port     ②
OVPN_SERVER='10.80.0.0/16'                            # VPN Network     ③

#vpn_data=/var/lib/swarmlab/openvpn/openvpn-services/   # Dir to save data ** this
must exist **
vpn_data=$PWD/openvpn-services/                                           ④
if [ ! -d $vpn_data ]; then
 mkdir -p $vpn_data
fi

NAME=swarmlab-vpn-services                            # name of docker service ⑤
DOCKERnetwork=swarmlab-vpn-services-network           # docker network
docker=registry.vlabs.uniwa.gr:5080/myownvpn          # docker image

docker stop  $NAME                        #stop container
sleep 1
docker container rm  $NAME              #rm container

# rm config files
rm -f $vpn_data/openvpn.conf.*.bak
```

```
rm -f $vpn_data/openvpn.conf
rm -f $vpn_data/ovpn_env.sh.*.bak
rm -f $vpn_data/ovpn_env.sh

# create network
sleep 1
docker network create --attachable=true --driver=bridge --subnet=172.50.0.0/16
--gateway=172.50.0.1 $DOCKERnetwork

#run container        see ovpn_genconfig
docker run --net=none -it -v $vpn_data:/etc/openvpn  -p 1194:1194 --rm $docker
ovpn_genconfig  -u udp://$IP:1194 \
-N -d -c -p "route 172.50.20.0 255.255.255.0" -e "topology subnet" -s $OVPN_SERVER
⑥

# create pki          see ovpn_initpki
docker run --net=none -v $vpn_data:/etc/openvpn  --rm -it $docker ovpn_initpki     ⑦

#                     see ovpn_copy_server_files
#docker run --net=none -v $vpn_data:/etc/openvpn  --rm $docker ovpn_copy_server_files

#create vpn           see --cap-add=NET_ADMIN
sleep 1
docker run --detach --name $NAME -v $vpn_data:/etc/openvpn --net=$DOCKERnetwork
--ip=172.50.0.2 -p $P:1194/udp --cap-add=NET_ADMIN $docker  ⑧

sudo sysctl -w net.ipv4.ip_forward=1

#show created
docker ps
```

① **localhost** inside of a container will resolve to the network stack of this container

② Port

③ Specify Addresses and Netmasks for VPN Clients

④ Directory to mount data

⑤ Name of docker services

⑥ Create config

⑦ keys

⑧ Run docker vpn service

# 4. Create user

*create-user.sh*

```
USERNAME=test1
vpn_data=$PWD/openvpn-services/
docker=registry.vlabs.uniwa.gr:5080/myownvpn

docker run -v $vpn_data:/etc/openvpn --rm -it $docker easyrsa build-client-full
$USERNAME nopass
docker run -v $vpn_data:/etc/openvpn --log-driver=none --rm $docker ovpn_getclient
$USERNAME  > $USERNAME.ovpn
```

*add to $USERNAME.ovpn file*

```
client
nobind
dev tun
comp-lzo
resolv-retry infinite
keepalive 15 60

remote-cert-tls server
remote 192.168.1.5 1194 udp ①
float
```

① Host machine's IP. Not Docker Container IP Address

# 5. rm vpn user

*rm-user.sh*

```
#!/bin/bash

CLIENTNAME=test1
U=$CLIENTNAME

vpn_data=$PWD/openvpn-services/
docker=registry.vlabs.uniwa.gr:5080/myownvpn

rm -f $vpn_data/pki/reqs/$CLIENTNAME.req
rm -f $vpn_data/pki/private/$CLIENTNAME.key
rm -f $vpn_data/pki/issued/$CLIENTNAME.crt
rm -f $vpn_data/server/ccd/$CLIENTNAME
rm -f $vpn_data/ccd/$CLIENTNAME
pem=$(sudo grep "CN=$U$"  $vpn_data/pki/index.txt | cut  -f4)

rm -f $vpn_data/pki/certs_by_serial/$pem.pem
sed -i "/CN=$U$/d"  $vpn_data/pki/index.txt
echo $pem
docker run -v $vpn_data:/etc/openvpn --log-driver=none --rm -it $docker
ovpn_revokeclient  $CLIENTNAME remove

rm -f $vpn_data_user_config/$CLIENTNAME.ovpn
rm -f $vpn_data_user_config1/$CLIENTNAME.ovpn
```

# 6. show all vpn users

*show-user.sh*

```
NAME=swarmlab-vpn-services                              # name of docker service
docker exec -it  $NAME ovpn_listclients
```

# 7. show all connected vpn users

*show-conn-user.sh*

```
NAME=swarmlab-vpn-services                              # name of docker service
docker exec -it  $NAME  cat /tmp/openvpn-status.log
```

# 8. client connect

*client connect*

```
openvpn --config ./clientfile.vpn
```

*Reminder*

Caminante, no hay camino,
se hace camino al andar.

Wanderer, there is no path,
the path is made by walking.

**Antonio Machado** Campos de Castilla