Prvo skinem virtualnu masinu sa ucilnice(desni klik save as i izaberem particiju dje moze), skinem je u neki folder i ekstrakujem. Udjem u VM Box i idem na +(open) nadjem folder dje sam ekstrakovao i onda kliknem na plavu .vbox file. Startujem masinu i odem u Devices->shared clipboard-> bidirectional da omogucim copy paste.

Vazda uzeti NAT network, odem u Network pa u NAT i dodam na + novu. Obavezno refresh mac adresu. Kada kliknem desni klik na image dodam u network NAT network i izaberem kreirani.

Prvo da ugasim IPv6 jer smeta, udjem sudo nano /etc/sysctl.conf i unesem ove komande:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Da bih aktivirao promjene unesem sudo sysctl -p, da provjerim je li dobro unijeto unosim komandu cat /proc/sys/net/ipv6/conf/all/disable_ipv6, dobicu 1 kao rezultat ako je dobro.

Da vidimo ip adresu kucam komandu ip addr.

Za skidanje fajlova koristim komandu sudo apt install <ime fajla>, a za azuriranje sudo apt update.

Da ugasim masinu koristim sudo poweroff.

Kad ocu da kloniram fajl kucam git clone #link

Da aktiviram firewall rules sudo ./iptables1.sh start

Da resetujem na default: sudo ./iptables1.sh reset

Da vidim aktivne rules: sudo iptables --list -vn

Kada imam neke podmreze, na ruteru stavim Adapter1 NAT, a npr ako imam jos 2 podmreze aktiviram Adapter2 i Adapter3 i stavim ih na Internal Network i dam im odgovarajuca imena. Onda udjem na ruteru u sudo nano /etc/netplan/01-network-manager-all.yaml i stavim vrijednosti za enp0s8 itd respektivno kako je zadato npr addresses: [10.0.0.1/24]. Da bih sacuvao te postavke pokrenem sudo netplan apply.

Omoguciti rutiranje za IPv4, da ruter moze da se ponasa kao ruter sa komandom: echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward.

Da omogucim rutiranje iz private mreze ka internet pokrenem sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE.

Kada trebam da podesim ip adresu itd u racunaru u podmrezi udjem u: sudo nano /etc/netplan/01-network-manager-all.yaml. I dopunim ovako, samo stavim podatke koji mi tacno trebaju:

```
network:

  version: 2
  ethernets:
    enp0s3:
      # assign the IP address
      addresses: [10.0.0.2/24]
      # set the default route through isp
      routes:
        - to: default
          via: 10.0.0.1
      # use Google's DNS
      nameservers:
        addresses: [8.8.8.8]
```

SSH PROTOCOL

Odradim `sudo apt update` da azuriram pakete, a da instaliram nove kucam `sudo apt install <list-the-packages>,` na ucilnici je spisak komandi

Uzmem kloniram tu masinu i dobijem 2 masine, ugasim sve adaptere osim prvog koji je na NAT network.

SSH SERVER:

Otvorim fajl `/etc/hosts` i dodam ovu liniju `127.0.1.1 ssh-server,` sacuvam fajl i odradim komandu `sudo hostnamectl set-hostname ssh-server.` Restartujem terminal, i sada sam promijenio hostname masine.

Sad regenerate SSH server keys, prazne passphrase ostavljam.

```
sudo ssh-keygen -t ecdsa -f /etc/ssh/ssh_host_ecdsa_key
sudo ssh-keygen -t rsa   -f /etc/ssh/ssh_host_rsa_key
sudo ssh-keygen -t dsa   -f /etc/ssh/ssh_host_dsa_key
sudo ssh-keygen -t ed25519 -f /etc/ssh/ssh_host_ed25519_key
```

Na SSH CLIENT udjem i ukucam isp@IpAdresaServera, pritisnem yes i ukucam password. Logout radim sa exit ili logout ili ctrl+d.

Za ostatak uci na ucilnicu pa ici korak po korak, ne vjerujem da ce doci na kolokvijumu.

VPN IPsec

Znaci imam dvije privatne mreze koje treba spojiti sa IPsec, znaci imam 2 rutera i dva racunara. Uzmem base image i instaliram sve potrebno

```
sudo apt install \

    charon-systemd \
    strongswan-swanctl \
    strongswan-pki \
    libstrongswan-extra-plugins \
    apache2 \
    wireshark
```

Prvo provjeriti je li strongswan upaljen sa `sudo systemctl status strongswan` ako pise running onda je ok, ako ne pise unesem komandu `sudo systemctl enable --now strongswan`

Ugasim masinu i podesim Adapter1 na NAT Network, a Adapter2 na Internal network i stavim bilo sta. Sad to kloniram 4 puta, i onda tu podesavam na Adapter2 imena. Na ruterima kreiram te subnet u Internal Network, a na racunarima izaberem te odgovarajuce. Onda udjem da konfigurisem ruter, prvo sam uzeo hq_ruter. Otvorim /`etc/netplan/01-network-manager-all.yaml` i konfigurisem po zadatku, dodam adresu podmreze, npr:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp-identifier: mac
    enp0s8:
      addresses: [10.1.0.1/16] #adresa podmreze
```

Da aktiviram promjene sudo netplan apply, i za ruter ovo vazda da pokrenem da ne zaboravim !!!! echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward da bi mogao rutirati

Sad podesavam racunar u ovoj mrezi, dajem mu staticku konfiguraciju kao sto je trazeno, otvorim /etc/netplan/01-network-manager-all.yaml

```
network:

  version: 2
  ethernets:
    enp0s3:
      addresses: [10.1.0.2/16] #adresa staticna
      routes:
        - to: default
          via: 10.1.0.1
      nameservers:
        addresses: [8.8.8.8]
```

Da aktiviram promjene sudo netplan apply

Sad predjem na drugi ruter i sve isto uradim:

```
network:

  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp-identifier: mac
    enp0s8:
      addresses: [10.2.0.1/16] #adresa podmreze
```

Da aktiviram promjene sudo netplan apply, i za ruter ovo vazda da pokrenem da ne zaboravim !!!! echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward da bi mogao rutirati

I za racunar u ovoj podmrezi, otvorim /etc/netplan/01-network-manager-all.yaml

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [10.2.0.2/16]
      routes:
        - to: default
          via: 10.2.0.1
      nameservers:
        addresses: [8.8.8.8]
```

Da aktiviram promjene sudo netplan apply

Da bi kreirao IPsec tunel na jednom ruteru npr hq_ruter otvorim /etc/swanctl/swanctl.conf i na vrhu dodam:

```
connections {

    net-net {
        # Use IKEv2
        version = 2

        # Remote "public" address: the IP of branch_router on enp0s3
        # Replace $BRANCH_IP with the actual address you see on branch_router.
        remote_addrs = $BRANCH_IP
        # IKE authentication: pre-shared key (PSK)
        local {
            auth = psk
            id   = hq
        }
        remote {
            auth = psk
            id   = branch
        }
        children {
            net-net {
                # Local HQ subnet behind hq_router
                local_ts  = 10.1.0.0/16
                # Remote branch subnet behind branch_router
                remote_ts = 10.2.0.0/16
                # We will initiate the tunnel manually via swanctl,
                # so we keep the default start_action = none.
                # (You could also use "trap" to start on demand.)
                start_action = none
            }
        }
    }
}
secrets {
    # IKE pre-shared key shared between @hq and @branch
    ike-hq-branch {
        id-hq     = hq
        id-branch = branch
        secret    = "secret"
    }
}
```

Sad reloadujem sa sudo swanctl --load-all

Sada na drugom ruteru otvorim /etc/swanctl/swanctl.conf, i dodam:

```
connections {

    net-net {
        version = 2

        # Remote "public" address: the IP of hq_router on enp0s3
        # Replace $HQ_IP with the actual address you see on hq_router.
        remote_addrs = $HQ_IP

        local {
            auth = psk
            id   = branch
        }
        remote {
            auth = psk
            id   = hq
        }

        children {
            net-net {
                # Local branch subnet behind branch_router
                local_ts  = 10.2.0.0/16

                # Remote HQ subnet behind hq_router
                remote_ts = 10.1.0.0/16

                start_action = none
            }
        }
    }
}

secrets {
    ike-hq-branch {
        id-hq     = hq
        id-branch = branch
        secret    = "secret"
    }
```

Sad reloadujem sa `sudo swanctl --load-all,` da provjerim ipsec podesavanja ukucam `sudo swanctl --list-conns`

Da pokrenem tunel kucam `sudo swanctl --initiate --child net-net` a da ga ugasim `sudo swanctl --terminate --ike net-net.`

RADIUS AAA

Prvo instaliram sve sto treba, `sudo apt install freeradius freeradius-utils apache2 libapache2-mod-auth-radius wireshark`

Verzija dje se pravi server i pokazuje da radi, otvorim `sudo nano /etc/freeradius/3.0/clients.conf` i unosim da registrujem NAS

```
client localhost {
    ipaddr = 127.0.0.1
    secret = testing123
    require_message_authenticator = no
    nas_type = other
}
```

Da dodam end usera otvaram `sudo nano /etc/freeradius/3.0/users,` i dodam tekst

```
"alice" Cleartext-Password := "password"
```

Prvo ugasim server sa `sudo service freeradius stop` otvorim novi terminal i pokrenem `sudo freeradius -X -d /etc/freeradius/3.0`

Da vidim radi li kucam `echo "User-Name=alice, User-Password=password" | radclient 127.0.0.1 auth testing123 –x`

PRIMJER SA WEB SERVEROM I RADIUS NA UCILNICI

ROAD WARRIOR IPSEC

Na road warrioru u swanctl.conf stavim novu konekciju:

```
connections {

   rw {
      version = 2
      remote_addrs = #adresa rutera
      vips = 0.0.0.0

      local {
         auth = psk
         id = “adresa roadwarriora” #ako je zadato neko ime stavim ime npr 
alice, ako dobijem psk koji treba stavim #”sifra” dolje u connections
      }
      remote {
         auth = psk
         id = “adresa rutera” #ili ime
      }
      children {
         rw {
            remote_ts = “subnet rutera”
            start_action = none
         }
      }
   }
}
secrets {

   ike-rw {
      secret = “secret”
   }
}
```

A na ruteru dodam konekciju u swanctlconf:

```
connections {

   rw {
      version = 2
      local_addrs  = #adresa rutera
      pools = rw_pool

      local {
         auth = psk
         id = #adresa rutera
      }
      remote {
         auth = psk
         id = ime #ako imam zadato ime, a u secrets dolje kucam psk koji je
zadat
      }
      children {
         rw {
            local_ts  = #lokalni subnet


         }
      }

   }
}
secrets {

   ike-rw {
      secret = "secret"
   }
}


pools {
   rw_pool {
      addrs = 10.3.0.0/28
   }
}
```

----

zabrani input output saobracaj, samo forward dozvoljen

```
iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD ACCEPT
```

Omoguci vec postavljene konekcije

```
iptables -A INPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

LOOP BACK OBAVEZNO

```
iptables -A INPUT  -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT
```

Incoming pravila sa internet:

```
ICMP - iptables -A INPUT -i enp0s3 -p icmp -m state --state NEW -j ACCEPT

ISAKMP - iptables -A INPUT -i enp0s3 -p udp --dport 500 -m state --state NEW
-j ACCEPT

NAT-T- iptables -A INPUT -i enp0s3 -p udp --dport 4500 -m state --state NEW -
j ACCEPT
```

ESP - iptables -A INPUT -i enp0s3 -p esp -m state --state NEW -j ACCEPT

Izlazni saobracaj:

ICMP - iptables -A OUTPUT -o enp0s3 -p icmp -m state --state NEW -j ACCEPT

DNS - iptables -A OUTPUT -o enp0s3 -p udp --dport 53 -m state --state NEW -j ACCEPT

Kada imam freeradius i treba dodati neki NAS, otvaram sudo nano /etc/freeradius/3.0/clients.conf i unosim

```
client nas-gateway {
    ipaddr = #ipaddr
    secret = #password
}
```

Korisnika dodajem tako sto otvorim fajl sudo nano /etc/freeradius/3.0/users

it u unesem alice(username bez navodnika) Cleartext-Password := "alice"(password)

FORWARD PRAVILA

```
iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state ESTABLISHED,RELATED -j ACCEPT
```