Set up a company's internal network, its gateway, and an example road warrior according to the specifications.

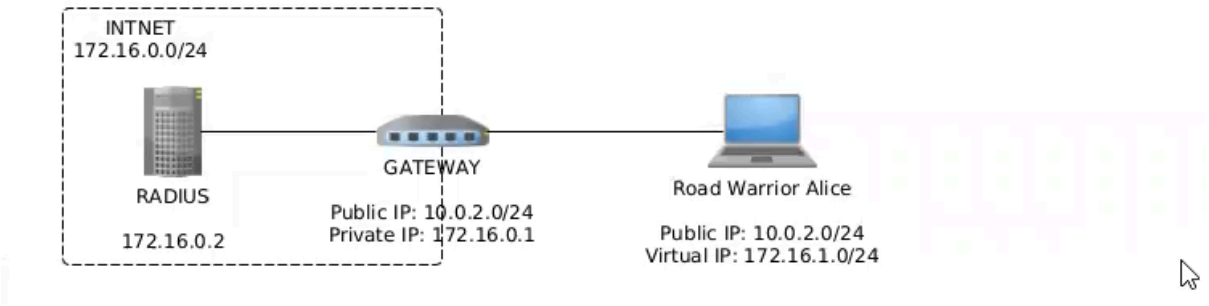


Figure 1: The specification diagram

1 Gateway network [7 points]

Computer `gateway` is connected to the *public* (IP `10.0.2.0/24`) and the private network (IP `172.16.0.1/24`). Both IPs are fixed: they do not change. The gateway acts as a **router** and performs **masquerading** (network address translation) for all traffic that is bound to the Internet. For instance, Radius machine (configured next) should be able to `ping google.com`. You can simulate the public IP network either with a `NAT network` or with `Bridged network` adapter; note that in this case, your *public* IP addresses will be different.

2 Radius [11 points]

The Radius machine is connected to the private network with static IP `172.16.0.2`.

- Machine is running a Freeradius server. Configure it to allow NAS requests from `172.16.0.1`. Authenticate NAS clients with PSK `radiuspassword`.
- Add a user `alice` with password `alice` to the local Freeradius (file-based) database.

3 Gateway firewall [12 points]

Set up a firewall on `gateway` that allows all routed traffic to pass through, but imposes strict limitations on the Internet bound interface regarding the incoming and outgoing traffic. In particular, the following is the only traffic that should be allowed on the Internet bound interface:

- Incoming: ICMP, ISAKMP, IPsec (ESP) and NAT-T.
- Outgoing: ICMP, DNS.

Hints:

- Write stateful firewall rules, they will make your task much easier.
- Once you're done with the rules, disable the firewall. (If you configure it incorrectly, it could interfere with the rest of the assignments. However, once y

1 Gateway network log

nardim glavno virtualko namestim vse potrebno
--- VPN StrongSwan ---
sudo apt update
sudo apt install strongswan strongswan-pki libcharon-extra-plugins apache2 wireshark net-tools

--- AAA with Free RADIUS ---

sudo apt update
sudo apt install freeradius freeradius-utils apache2 libapache2-mod-auth-radius wireshark

naredim nov nat v virtualboxu poimenujem ga old nat midterm

na gateway virtualki nastavim prvi adapter na nat network old nat midterm katerega sem prej naredil, drugi adapter pa na INTNET internal netwrok. Ali tukaj manjka še 3 network??

tako tudi na rw alice dam nat network in old nat midterm na adapter 1, na adapter 2 dam nek internal network (RW_internal)

RADIUS dam samo internal INTNET na adapter 1

Na RADIUS nastavim network

sudo vim /etc/netplan/01-network-manager-all.yaml

```
network:
        version: 2
        ethernets:
                enp0s3:
                addresses: [172.16.0.2/24]
                gateway4: 172.16.0.1
```

potrdim nastavitve
sudo netplan apply

grem na GATEWAY in nastavim network

pri gatewayu se rabi še nastavit:
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

da enableaš routing

sudo vim /etc/netplan/01-network-manager-all.yaml

```
network:
version: 2
ethernets:
enp0s3:
addresses: [10.0.2.0/24]
enp0s8:
addresses: [172.16.0.1/24]
```

Dodam se iptable pravilo za routanje na internet:
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

potrdim nastavitve
sudo netplan apply

preverim ce dela ping gateway na radius in obratno, deluje

preverim ce dela ping radius na google in deluje

grem nastavit še rw alice

sudo vim /etc/netplan/01-network-manager-all.yaml

```
network:
        version: 2
        ethernets:
                enp0s3:
                dhcp4: true
                dhcp-identifier: mac
                enp0s8:
                addresses: [172.16.1.0/24]
```

potrdim nastavitve
sudo netplan apply

2 Radius log

Dodam vnos za 172.16.0.2

sudo vim /etc/freeradius/3.0/clients.conf

```
client RADIUS {
        ipaddr = 172.16.0.2
        secret = radiuspassword
        require_message_authenticator = no
        nas_type = other
}
```

Dodam uporabnika alice:
dodam v /etc/freeradius/3.0/users

sudo vim /etc/freeradius/3.0/users
dodam:

"alice" Cleartext-Password := "alice"

3 Gateway firewall log

Vzamemo datoteko iz vaj iptables1.sh in dodamo:

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

#da potem ni treba pisati dvojnih pravil za incomig ali outgoing traffic ->stateful firewall
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#allow all routed traffic to pass through
iptables -A FORWARD -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#incoming ping
iptables -A OUTPUT -p icmp -m state --state NEW -j ACCEPT

#outgoing ping
iptables -A INPUT -p icmp -m state --state NEW -j ACCEPT

#dns outgoing
iptables -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

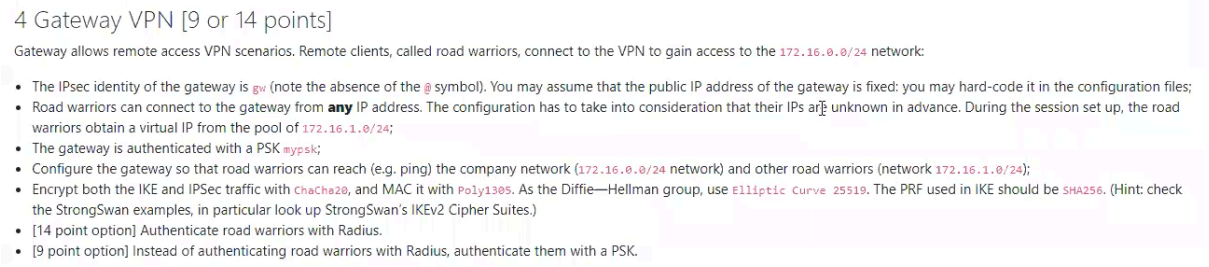
#ISAKMP incoming
iptables -A INPUT -p udp --dport 500 -m state --state NEW -j ACCEPT

#IPsec(ESP) incoming
iptables -A INPUT -p esp -m state --state NEW -j ACCEPT

#NAT-T
iptables -A INPUT -p udp --dport 4500 -m state --state NEW -j ACCEPT

za ISAKMP, ESP in NAT-T sem nadu tole:
https://gist.github.com/dunkelstern/07b3e0185467cfdbbfb224e9f01967da

OUTGOING ISAKMP
iptables -A OUTPUT -p tcp --dport 500 -j ACCEPT
iptables -A INPUT -p tcp ! --syn --sport 500 -j ACCEPT



4 Gateway VPN [9 or 14 points]

Gateway allows remote access VPN scenarios. Remote clients, called road warriors, connect to the VPN to gain access to the `172.16.0.0/24` network:

- The IPsec identity of the gateway is `gw` (note the absence of the `@` symbol). You may assume that the public IP address of the gateway is fixed: you may hard-code it in the configuration files;
- Road warriors can connect to the gateway from **any** IP address. The configuration has to take into consideration that their IPs are unknown in advance. During the session set up, the road warriors obtain a virtual IP from the pool of `172.16.1.0/24`;
- The gateway is authenticated with a PSK `mypsk`;
- Configure the gateway so that road warriors can reach (e.g. ping) the company network (`172.16.0.0/24` network) and other road warriors (network `172.16.1.0/24`);
- Encrypt both the IKE and IPSec traffic with `ChaCha20`, and MAC it with `Poly1305`. As the Diffie—Hellman group, use `Elliptic Curve 25519`. The PRF used in IKE should be `SHA256`. (Hint: check the StrongSwan examples, in particular look up StrongSwan's IKEv2 Cipher Suites.)
- [14 point option] Authenticate road warriors with Radius.
- [9 point option] Instead of authenticating road warriors with Radius, authenticate them with a PSK.

4 Gateway VPN log

Na gateway uredim VPN.

Konfiguriram config file:
sudo vim /etc/ipsec.conf

Notri dodam:
config setup

conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev2
authby=secret

conn VPN
leftsubnet=172.16.0.0/24
leftfirewall=yes
leftid=gw
right=%any
auto=add

resetiram
sudo ipsec restart

na rw alice uredim:
Konfiguriram config file:
sudo vim /etc/ipsec.conf

config setup

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2
    authby=secret

conn net-net
    leftsubnet=10.2.0.0/16

leftid=%any
leftfirewall=yes
right=10.0.2.5
rightsubnet=10.0.2.0/24
rightid=gw
auto=add

resetiram
sudo ipsec restart

na gateway dodam psk:
sudo vim /etc/ipsec.secrets

v datoteko dodam
@gw: PSK "secret"

resetiram
sudo ipsec restart

Tudi na rwarior dodam psk:
sudo vim /etc/ipsec.secrets

v datoteko dodam
@gw: PSK "secret"

resetiram
sudo ipsec restart

5 Road warrior [6 points]

- The Road warrior (`rw`) is connected to the public network (`10.0.2.0/24`, or equivalent if you are using the `Bridged adapter`);
- Her identity is `alice`, her password depends on whether you are using the Radius as the authenticator (password is `alice`) or PSK (password is `mypsk`);
- Road warriors should be able to reach all nodes in the `172.16.0.0/24` network via the Gateway.
- Similarly, the Road warrior should be able to reach other road warriors in the `172.16.1.0/24` network via the Gateway.

5 RoadWarrior log

RW je povezan na public.

password je alice, ker smo tako nastavili pri Radius kot authenticator