Openvpn

Last edited time: June 27, 2022 18:58 AM
Reviewed: No

VYOS

VYOS portforward

```
configure
set nat destination rule 10 description 'Port Forward: OpenVPN'
set nat destination rule 10 destination port '1194'
set nat destination rule 10 inbound-interface 'eth3' #WAN poort
set nat destination rule 10 protocol 'udp'
set nat destination rule 10 translation address '10.13.14.1' #IP VPN-server
commit
save
```

Server

Installeren Openvpn

voer de volgende commando's uit op de REHL machine met het IP waarnaartoe de portforward staat.

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
sudo dnf update
sudo dnf install openvpn easy-rsa
```

Configureren Openvpn

kopieer de easyrsa scripts naar de openvpnmap

```
sudo cp -rp /usr/share/easy-rsa/3.0/ /etc/openvpn/server/easyrsa3.0
sudo cp -p /usr/share/doc/easy-rsa/vars.example
```

```
/etc/openvpn/server/easyrsa3.0/vars
```

bewerk het `/etc/openvpn/server/easyrsa3.0/vars` bestand en wijzig de onderstaande data

```
set_var EASYRSA_REQ_COUNTRY     "NL"
set_var EASYRSA_REQ_PROVINCE    "Utrecht"
set_var EASYRSA_REQ_CITY                "Utrecht"
set_var EASYRSA_REQ_ORG                 "Heel Goedkoop Bellen organisatie"
set_var EASYRSA_REQ_EMAIL               "security@hgb.nl"
```

ga naar de volgende map `/etc/openvpn/server/easyrsa3.0/` en voer onderstaande commando's uit

```
./easyrsa clean-all ;# directories klaar maken
./easyrsa gen-dh ;# Diffie-Helman seeds genereren (duurt even)
./easyrsa build-ca ;# CA key en cert. aanmaken
./easyrsa build-server-full server1 nopass ;# server key en cert zonder ww.
./easyrsa build-client-full client1 ;# client key en cert met ww.
```

`openvpn --genkey --secret /etc/openvpn/server/ta.key`

maak tenslotte op de server het .ovpn bestand aan en plak onderstaande data daarin
`nano /etc/openvpn/server/server.ovpn`

```
port 1194
proto udp
dev tun
ca easyrsa3.0/pki/ca.crt
cert easyrsa3.0/pki/issued/server1.crt
key easyrsa3.0/pki/private/server1.key
dh easyrsa3.0/pki/dh.pem
tls-auth ta.key 0
server 10.31.33.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
# optioneel een DNS server: push "dhcp-option DNS 1.1.1.1"
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 2
user nobody
```

```
group nobody
persist-key
persist-tun
status openvpn-status.log
verb 3
mute 20
```

Starten Openvpnserver

voeg onderstaande firewall rules toe

```
sudo firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i tun+ -j ACCEPT
sudo firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -o tun+ -j ACCEPT
sudo firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -o ens160 -j
MASQUERADE
sudo firewall-cmd --permanent --direct --add-rule ipv4 filter FORWARD 0 -i
tun+ -j ACCEPT
sudo firewall-cmd --permanent --direct --add-rule ipv4 filter FORWARD 0 -o
tun+ -j ACCEPT
sudo firewall-cmd --permanent --direct --add-rule ipv4 nat POSTROUTING 0 -o
ens160 -j MASQUERADE
firewall-cmd --permanent --add-masquerade
firewall-cmd --add-masquerade
sudo firewall-cmd --add-port=1194/udp --zone=public --permanent; sudo
firewall-cmd --reload
```

Om de client toegang te geven tot het interne netwerk moet je het `/etc/sysctl.conf` bestand bewerken en onderstaande regel plakken.
`net.ipv4.ip_forward=1`

Ga naar de servermap op de openvpnserver
`cd /etc/openvpn/server/`
Start de server met onderstaand commando
`sudo openvpn --config server.ovpn`

Client

Je dient op de server verschillende bestanden naar de client te sturen (kan met copy-paste in VMWare, maar wij doen via ssh)
Voer onderstaande commando uit op de server

```
sudo scp -p /etc/openvpn/server/ta.key /etc/openvpn/server/easyrsa3.0/pki/ca.crt
/etc/openvpn/server/easyrsa3.0/pki/*/client1.{crt,key} <user>@<client>:/tmp
```

hiermee kopieer je 4 bestanden van de server naar de /tmp map van de client

1. ta.key
2. ca.crt
3. client1.crt
4. client1.key

Plaats nu de client in hetzelfde netwerk als de WANpoort van de vyos-router

Voeg het WAN-IP van de router toe in de hostsfile van de vpn-client (in ons geval noemen wij de de vpnserver vpn.hgb.nl.

`nano /etc/hosts`

`192.168.192.10 vpn.hgb.nl`

installeer openvpn op de client:

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
8.noarch.rpm
sudo dnf update
sudo dnf install openvpn
```

verplaats nu de 4 gekopieerde bestanden van de /tmp map naar de openvpn map

`sudo mv /tmp/ta.key /tmp/ca.crt /tmp/client1.* /etc/openvpn/client`

zet de goede rechten op de bestanden:

`sudo chown root:root /etc/openvpn/client/{ta.key,ca.crt,client1.key,client1.crt}`

`sudo chmod u=r,o-rwx /etc/openvpn/client/{ta.key,ca.crt,client1.key,client1.crt}`

maak nu het .ovpn bestand aan op de client

`nano /etc/openvpn/client/client1.ovpn`

en plak onderstaande tekst in het bestand **(in ons geval heet de hostfile regel vpn.hgb.nl)**

```
client
dev tun
proto udp
remote vpn.hgb.nl 1194 ;# check hosts-file!
resolv-retry infinite
nobind
user nobody
```

```
group nobody
persist-key
persist-tun
mute-replay-warnings
ca ca.crt
cert client1.crt
key client1.key
remote-cert-tls server
tls-auth ta.key 1
cipher BF-CBC
comp-lzo
verb 3
mute 20
```

Starten openvpn client

Ga naar de map `/etc/openvpn/client` en voer het onderstaande commando uit: `openvpn --config ./client1.ovpn` je moet nu het wachtwoord opgeven waarmee je de certificaten heb aangemaakt op de server.