# RemoteAccess VPN configuration-Debian

-Setup

-Public subnet: 10.10.10.0/24

Debian server: 10.10.10.1/24

Windows client: 10.10.10.10/24

Debian client: 10.10.10.100/24

-Private subnet: 192.168.100.0/24

Debian server: 192.168.100.100/24

-VPN private IP pool: 192.168.3.0/24

-Install strongswan and strongswan-pki

apt install strongswan strongswan-pki

-Create a CA and create the certs

-Create the directories

mkdir -p ~/pki/{cacerts,certs,private}

chmod 700 ~/pki

-Generate the key

pki --gen --type rsa --size 4096 --outform pem > ~/pki/private/ca-key.pem

-Sign the root cert

pki --self --ca --lifetime 3650 --in ~/pki/private/ca-key.pem --type rsa --dn "CN=vpn.wsc2022.kr" --outform pem > ~/pki/cacerts/ca-cert.pem

-Generate a private key for the VPN server

pki --gen --type rsa --size 4096 --outform pem > ~/pki/private/server-key.pem

-Create and sign the VPN server cert. If you the DNS name of the server in the CN and SAN fields you’ll only need one SAN field

pki –pub –in ~/pki/private/server-key.pem –type rsa | pki –issue –lifetime 1825 –cacert ~/pki/cacerts/ca-cert.pem –cakey ~/pki/private/ca-key.pem –dn „CN=10.10.10.1” –san @10.10.10.1 –san 10.10.10.1 –flag serverAuth –flag ikeIntermediate –outform pem > ~/pki/certs/server-cert.pem

-Copy the certs and keys to /etc/ipsec.d

cp -r ~/pki/\* /etc/ipsec.d

-Configure Strongswan-

-Edit /etc/ipsec.conf

config setup

uniqueids = no

charondebug = „ike 1, knl 1, cfg 0”

conn ikev2-vpn

auto = add

compress = no

type = tunnel

keyexchange = ikev2

fragmentation = yes

forceencaps = yes

dpdaction = clear

dpddelay = 300s

rekey = no

left = %any

leftid = 10.10.10.1 #you can use a domain name aswell: leftid = @domain.tld

leftcert = server-cert.pem

leftsendcert = always

leftsubnet = 192.168.100.0/24

right = %any

rightid = %any

rightauth = eap-mschapv2

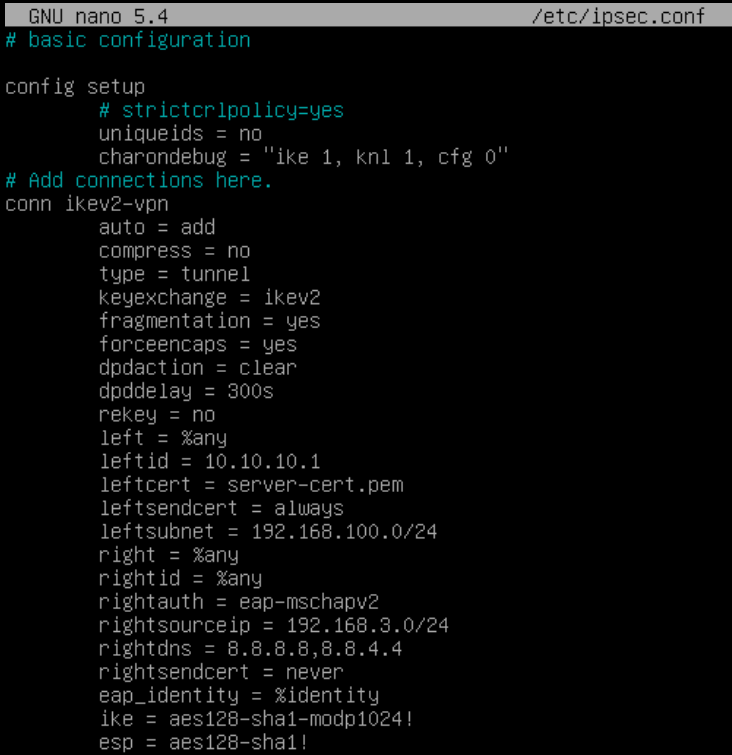
rightsourceip = 192.168.3.0/24

rightdns = 8.8.8.8,8.8.4.4

rightsendcert = never

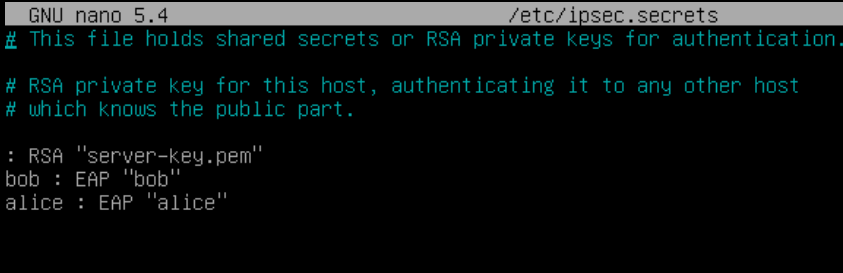
eap\_identity = %identity

ike = aes128-sha1-modp1024!

esp = aes128-sha1!

-Edit /etc/ipsec.secrets

: RSA „server-key.pem”

<username> : EAP „<password>” #Add users to authenticate as

-Enable packet forwarding in /etc/sysctl.conf

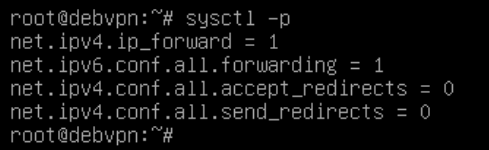
Uncomment the following lines

net.ipv4.ip\_forward = 1

net.ipv6.conf.all.forwarding = 1

net.ipv4.conf.all.accept.redirects = 0

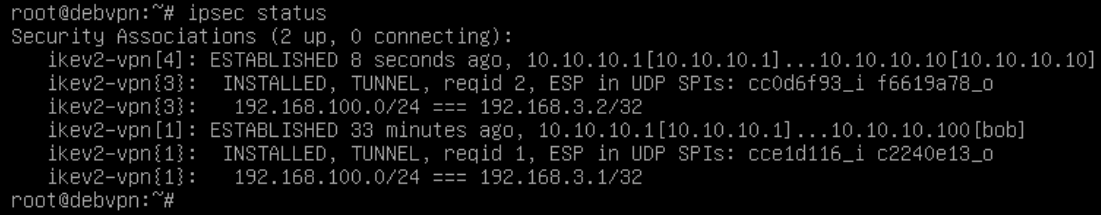
net.ipv4.conf.all.send.redirects = 0

Enable the changes with: sysctl -p

-Restart the service

systemctl restart strongswan-starter

-To check active connections

ipsec status

-Configuring the Debian client-

-Install strongswan on the client aswell

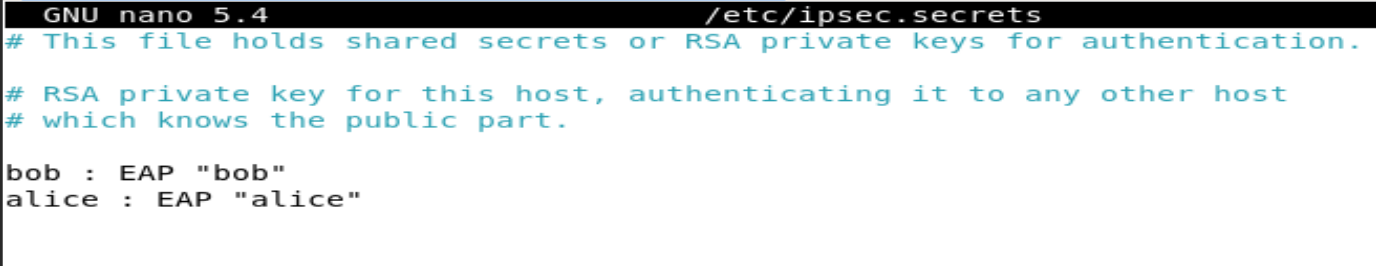
apt install strongswan libcharon-extra-plugins

-Copy the CA certificate from the server to /etc/ipsec.d/cacerts

-To ensure the VPN only runs on demand, disable it from running automatically

systemctl disable –now strongswan-starter

-Edit the /etc/ipsec.secrets file

<username> : EAP „<password>” #Same config as the server

-Edit the /etc/ipsec.conf

conn ikev2-rw

right = 10.10.10.1 #You can use domain name

rightid = 10.10.10.1 #You can use domain name

rightsubnet = 0.0.0.0/0

rightauth = pubkey

leftsourceip = %config

leftid = <username> #Enter a username from /etc/ipsec.secrets

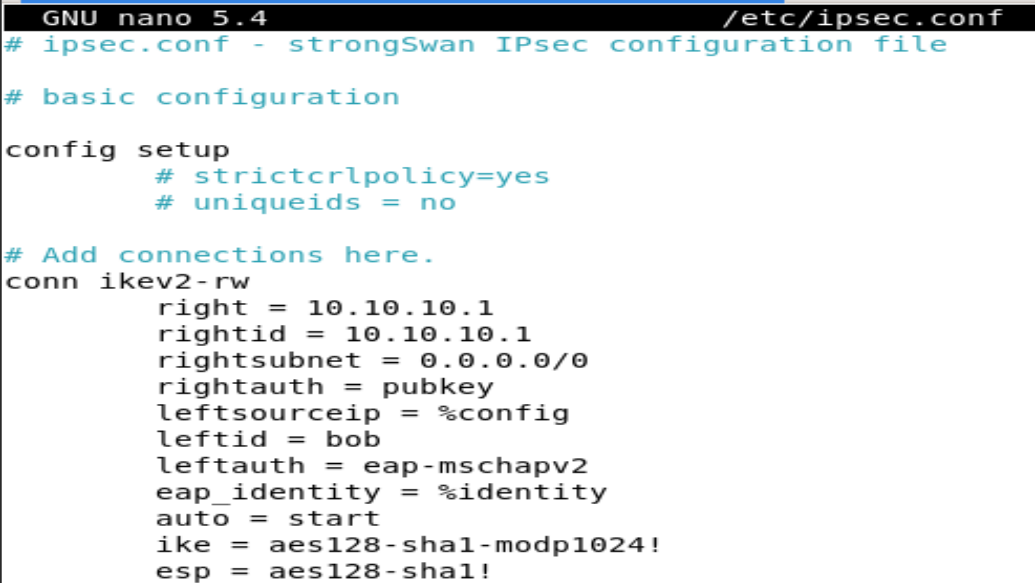
leftauth = eap-mschapv2

eap\_identity = %identity

auto = start

ike = aes128-sha1-modp1024! #Needs to be same as it’s on the server

esp = aes128-sha1! #Needs to be the same as it’s on the server



-To connect to the VPN

systemctl start strongswan-starter

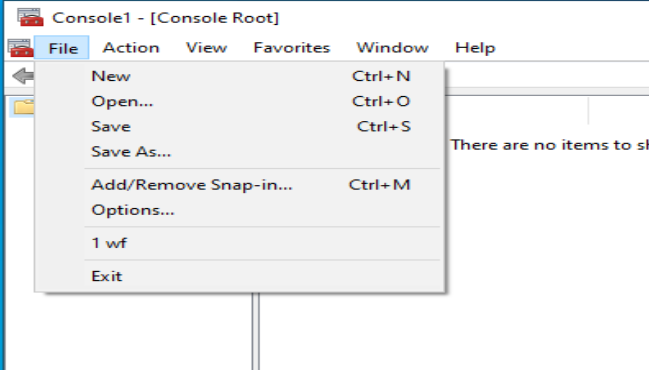
-To disconnect

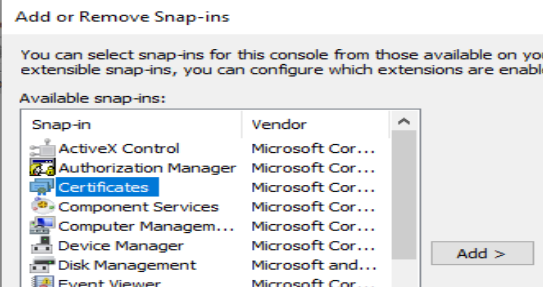
systemctl stop strongswan-starter

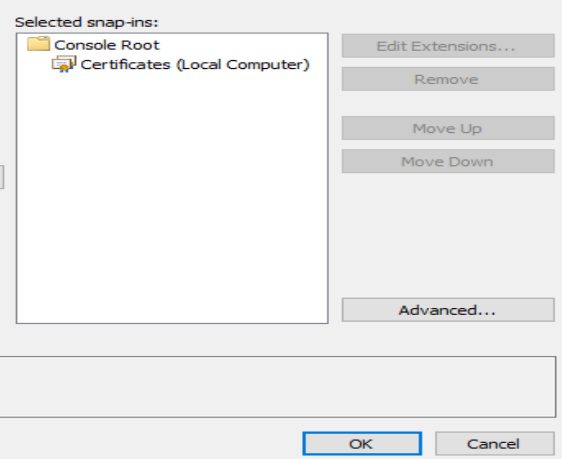
-Configuring the Windows client-

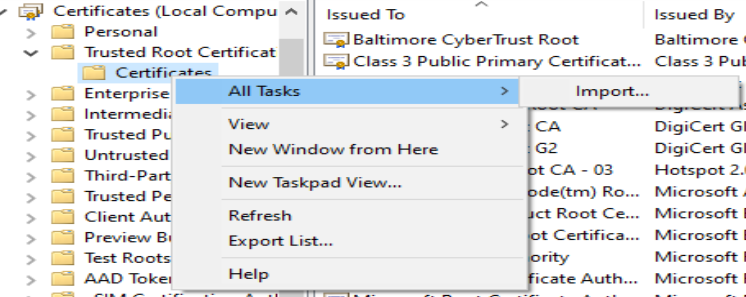
-Copy the CA certificate from the server

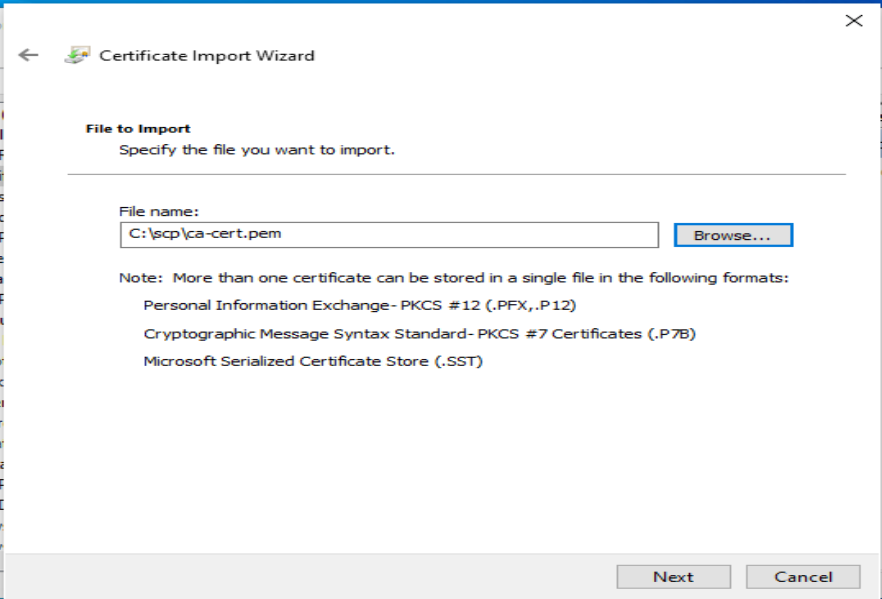
-Import the root cert

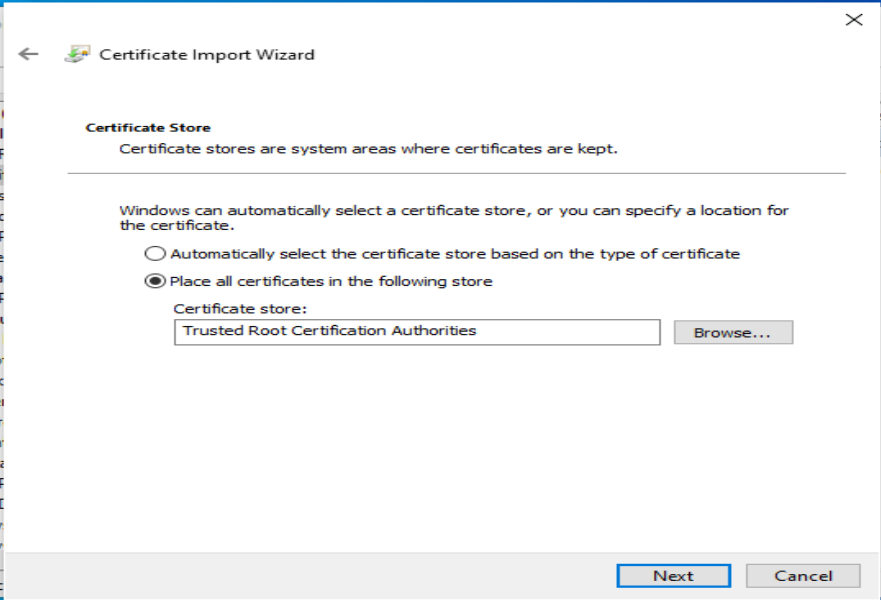
-Open mmc.exe -> click on File > Add/Remove Snap-in…

-Add the Certificates snap-in

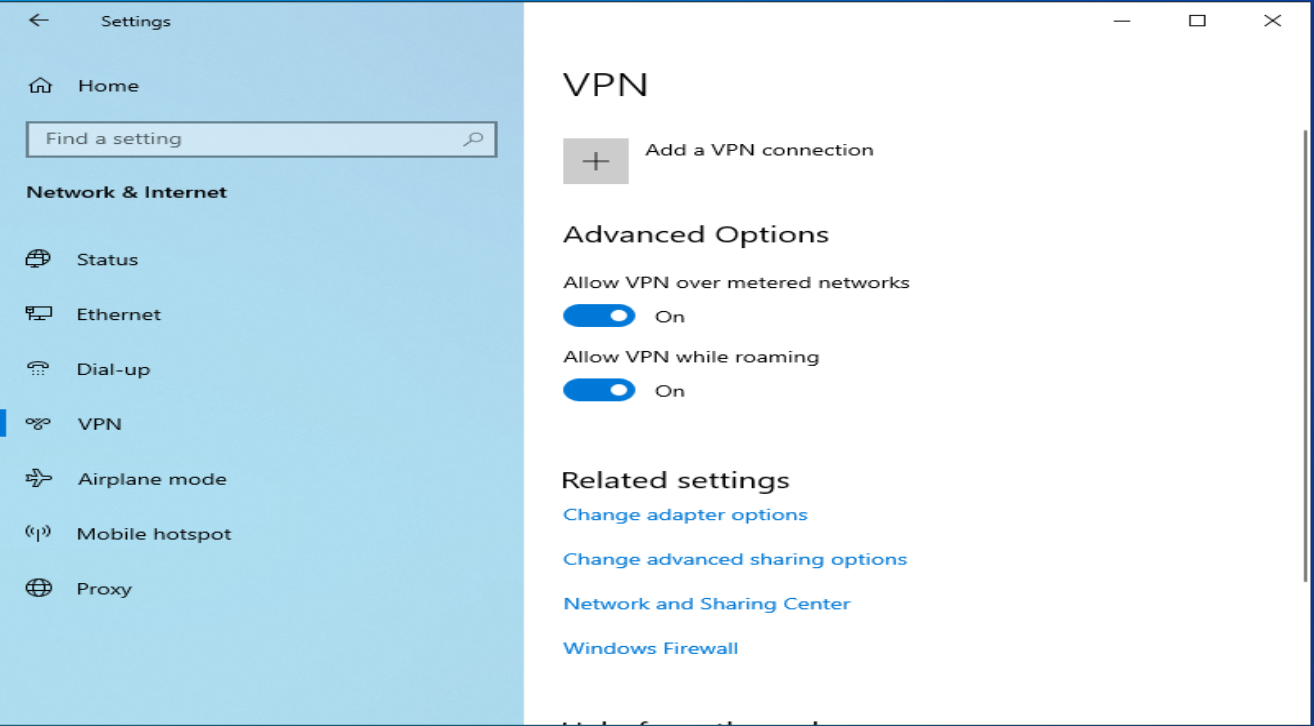
-Select Computer Account, then Local Computer, then OK

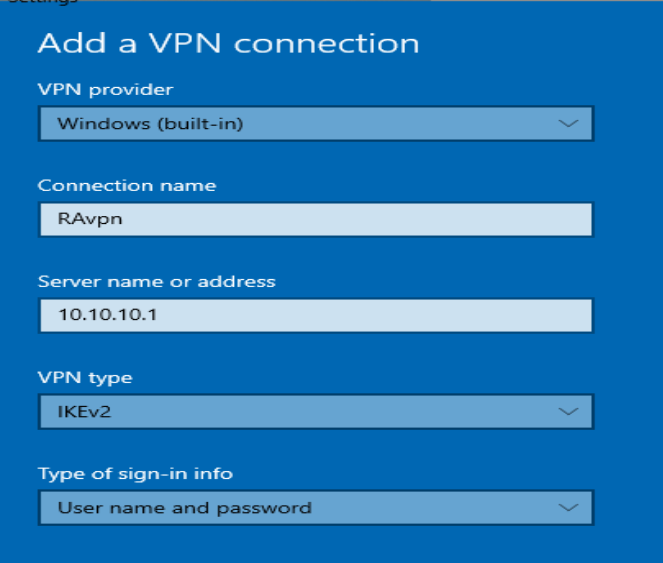
-Open Trusted Root Certification Authorities and right click on Certificates, then click on All tasks > Import

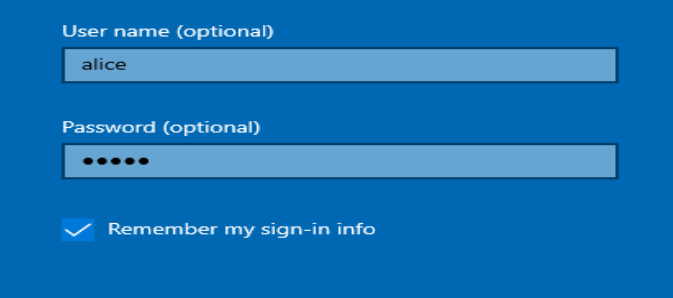
-Specify the cert you copied over

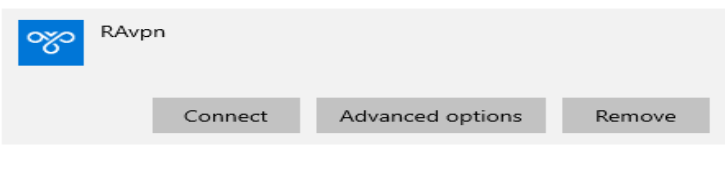
-Make sure it goes to the Trusted Root Certification Authorities

-Add a new VPN connection

-Go to Settings > VPN > Add a VPN connection

-Fill out the fields



-Click on connect on the new VPN connection

-If everything works you should be able to ping stuff in 192.168.100.0/24

