Remote Access VPN with Windows AD Auth - Debian&Windows

-Setup

-Domain: wsc2022.kr
-Public subnet: 10.10.10.0/24
Debian server: 10.10.10.1/24
Windows server: 10.10.10.2/24
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
-Users in AD
-Emil
-Frank

-Install strongswan and it's plugins

```
apt install strongswan strongswan-pki libcharon-extra-plugins
```

-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 use 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 and /etc/freeradius/3.0

```
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-radius
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!

```
  GNU nano 5.4                                  /etc/ipsec.conf *
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        uniqueids = no
        charondebug = "ike 1, knl 1, cfg 0"
# Add connections here.
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
        leftcert = server-cert.pem
        leftsendcert = always
        leftsubnet = 192.168.100.0/24
        right = %any
        rightid = %any
        rightauth = eap-radius
        rightsourceip = 192.168.3.0/24
        rightdns = 8.8.8.8,8.8.4.4
        rightsendcert = never
        eap_identity = %any
        ike = aes128-sha1-modp1024!
        esp = aes128-sha1!
```

-Edit /etc/ipsec.secrets

: RSA "server-key.pem"

```
  GNU nano 5.4                                /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

: RSA "server-key.pem"
```

-Edit /etc/strongswan.conf

-In the plugins module define the eap-radius module and the radius server itself

```
  GNU nano 5.4                                /etc/strongswan.conf
# strongswan.conf - strongSwan configuration file
#
# Refer to the strongswan.conf(5) manpage for details
#
# Configuration changes should be made in the included files

charon {
        load_modular = yes
        plugins {
                include strongswan.d/charon/*.conf
                eap-radius {
                        servers {
                                server-a {
                                        address = 10.10.10.2
                                        secret = supersecret
                                }
                        }
                }
        }
}

include strongswan.d/*.conf
```

-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

```
root@debvpn:~# sysctl -p
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
root@debvpn:~#
```

-Restart the strongswan and freeradius

systemctl restart freeradius

systemctl restart strongswan-starter

-To check active connections

ipsec status

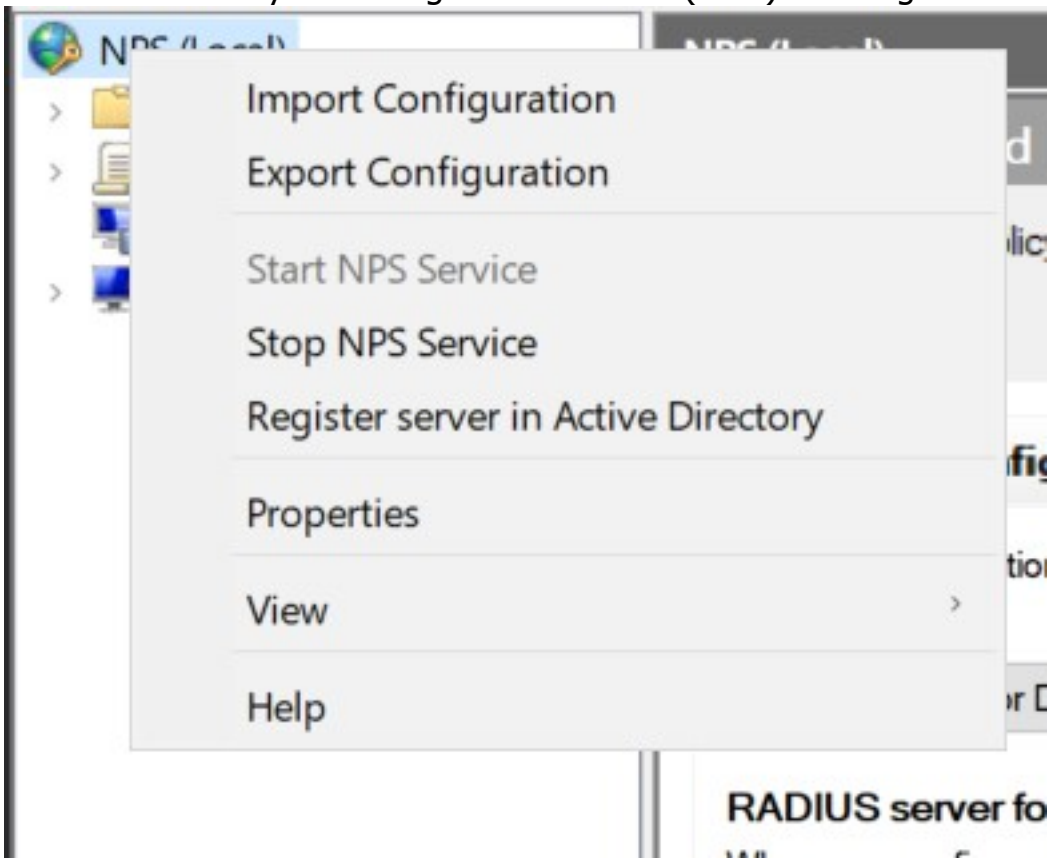
```
root@debvpn:~# ipsec status
Security Associations (2 up, 0 connecting):
   ikev2-vpn[2]: ESTABLISHED 2 minutes ago, 10.10.10.1[10.10.10.1]...10.10.10.100[bob]
   ikev2-vpn{2}:  INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c045f69d_i c991dcb4_o
   ikev2-vpn{2}:   192.168.100.0/24 === 192.168.3.2/32
   ikev2-vpn[1]: ESTABLISHED 3 minutes ago, 10.10.10.1[10.10.10.1]...10.10.10.10[10.10.10.10]
   ikev2-vpn{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: ce708cc6_i 32184764_o
   ikev2-vpn{1}:   192.168.100.0/24 === 192.168.3.1/32
root@debvpn:~# _
```

-Configuring the Windows Server (ONLY WORKS IN WINDOWS SERVER 2022 for some weird reason)-

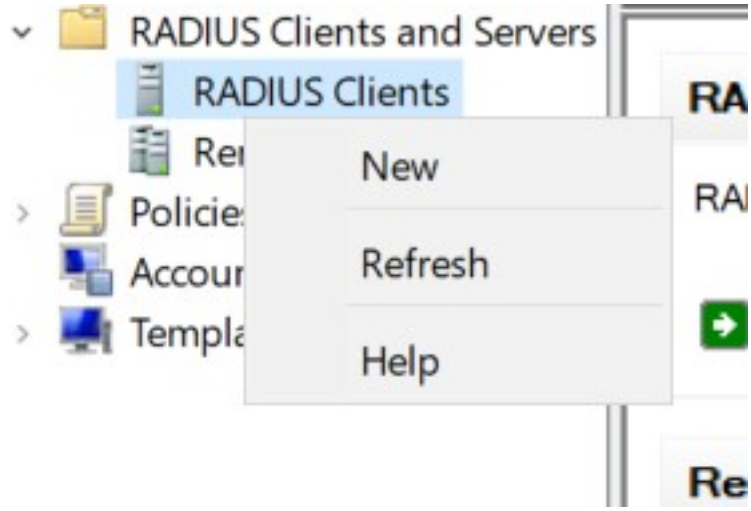
-Install AD DS and Network Policy and Access Service

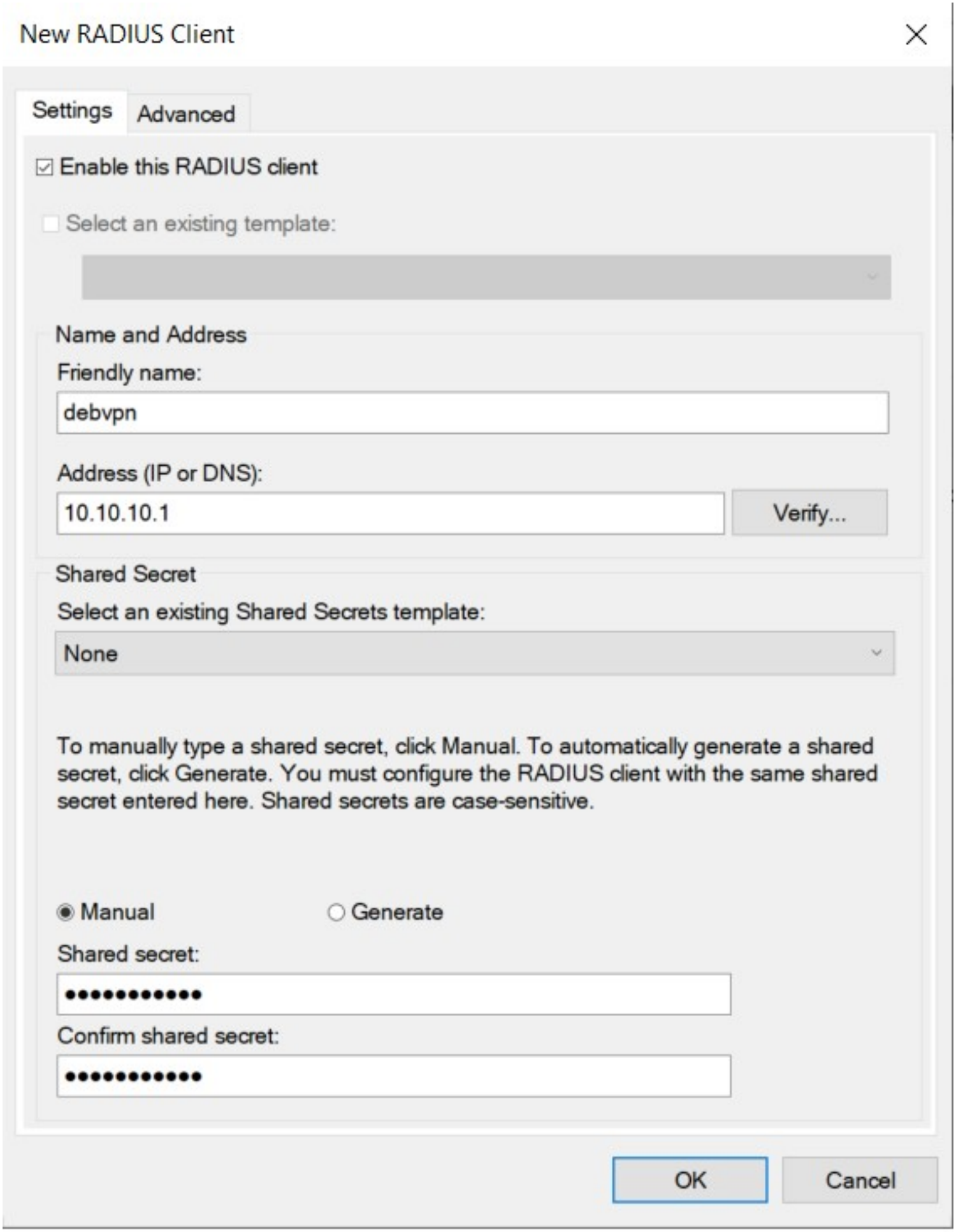
-Setup AD DS with wsc2022.kr domain name

-In Network Policy Server right click on NPS (local) and Register server in Active Directory

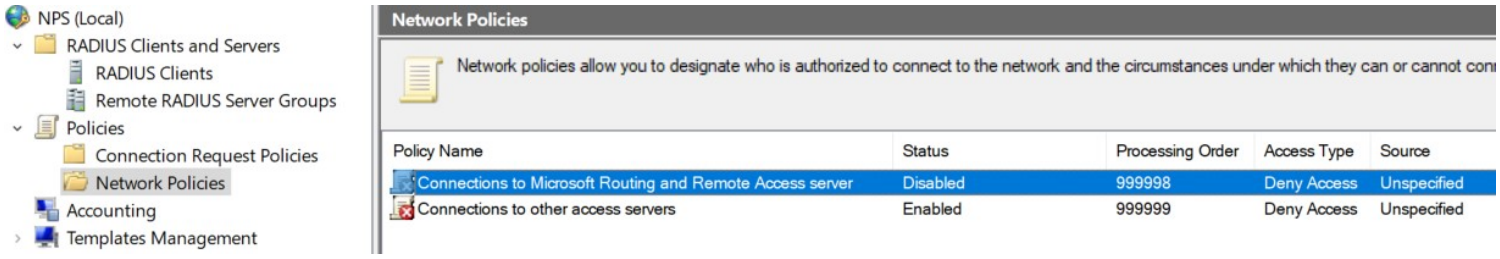


-Right click on RADIUS clients and add the VPN server

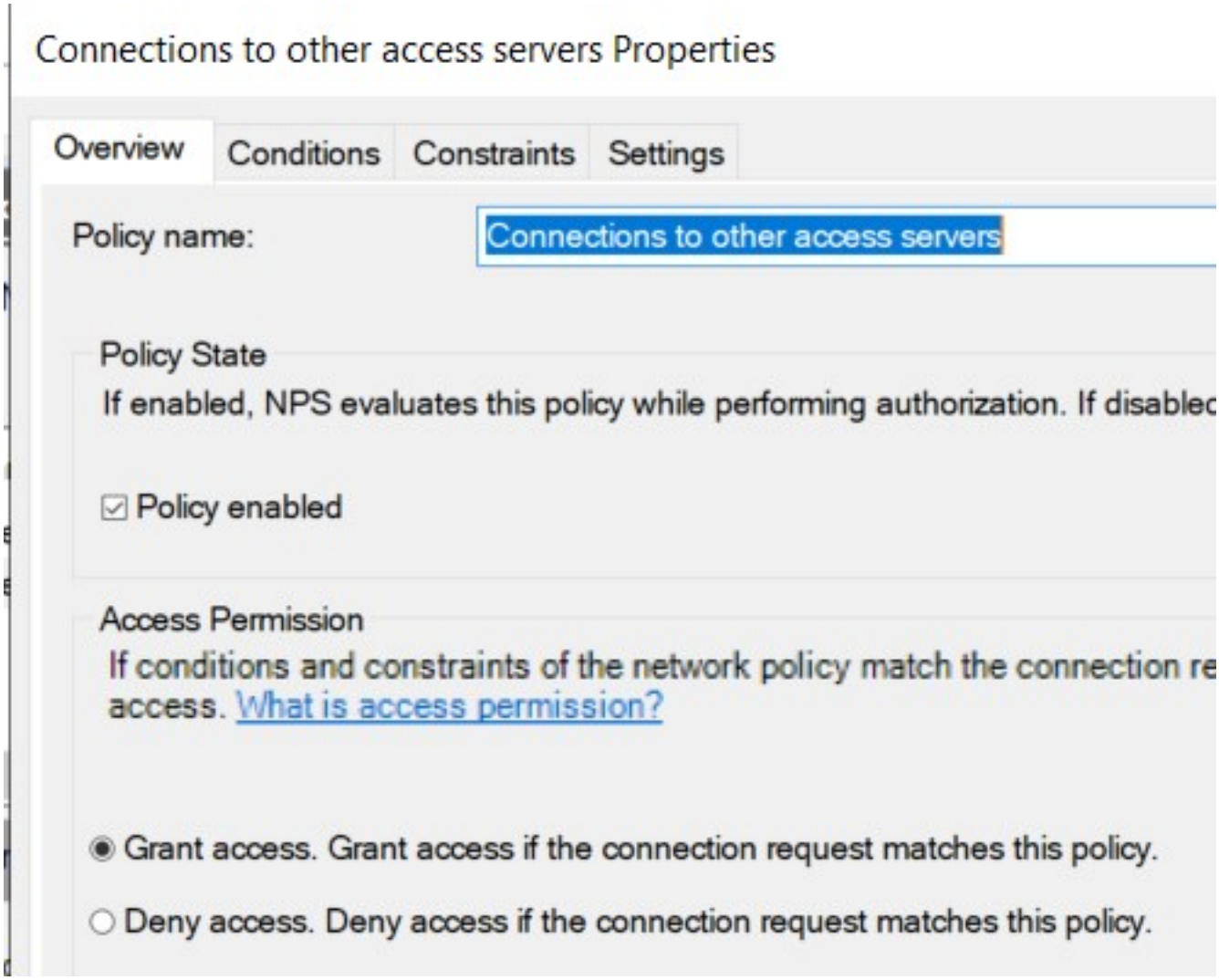

RADIUS Clients and Servers
RADIUS Clients
Rei
Policie
Accour
Templa
New
Refresh
Help
RA
RA
Re



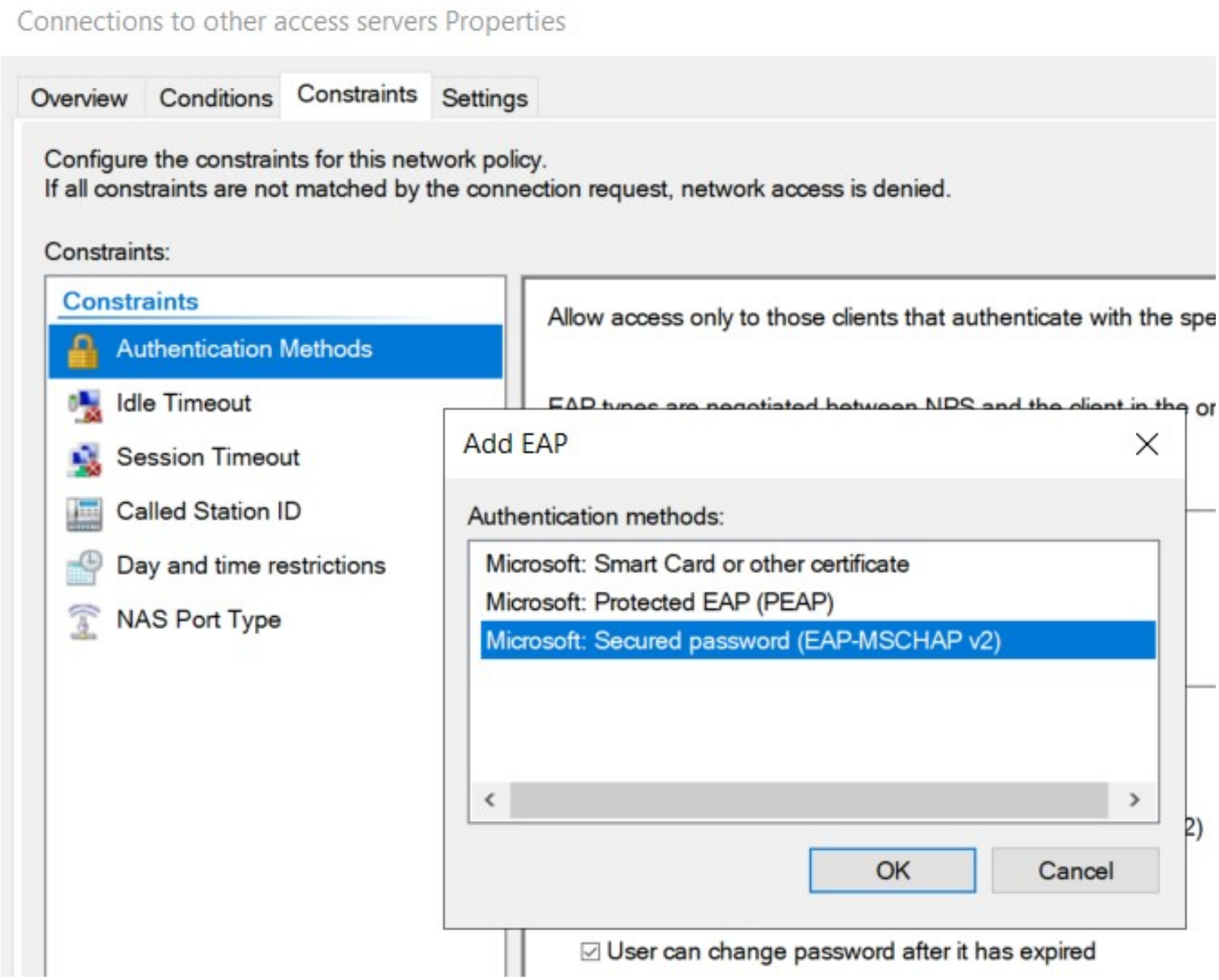
-In Network Policies disable Connections to Microsoft Routing and Remote Access server: Right click -> Disable



-Right click on Connections to other access servers -> Properties -> Overview -> Select Grant Access



-Go to Constraints -> Add EAP Type -> EAP-MSCHAP v2



-Create the new users in AD Users and Computers

-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>"
```

<SCREENSHOT HERE>

-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
<SCREENSHOT HERE>

-To connect to the VPN

systemctl start strongswan-starter

-To disconnect

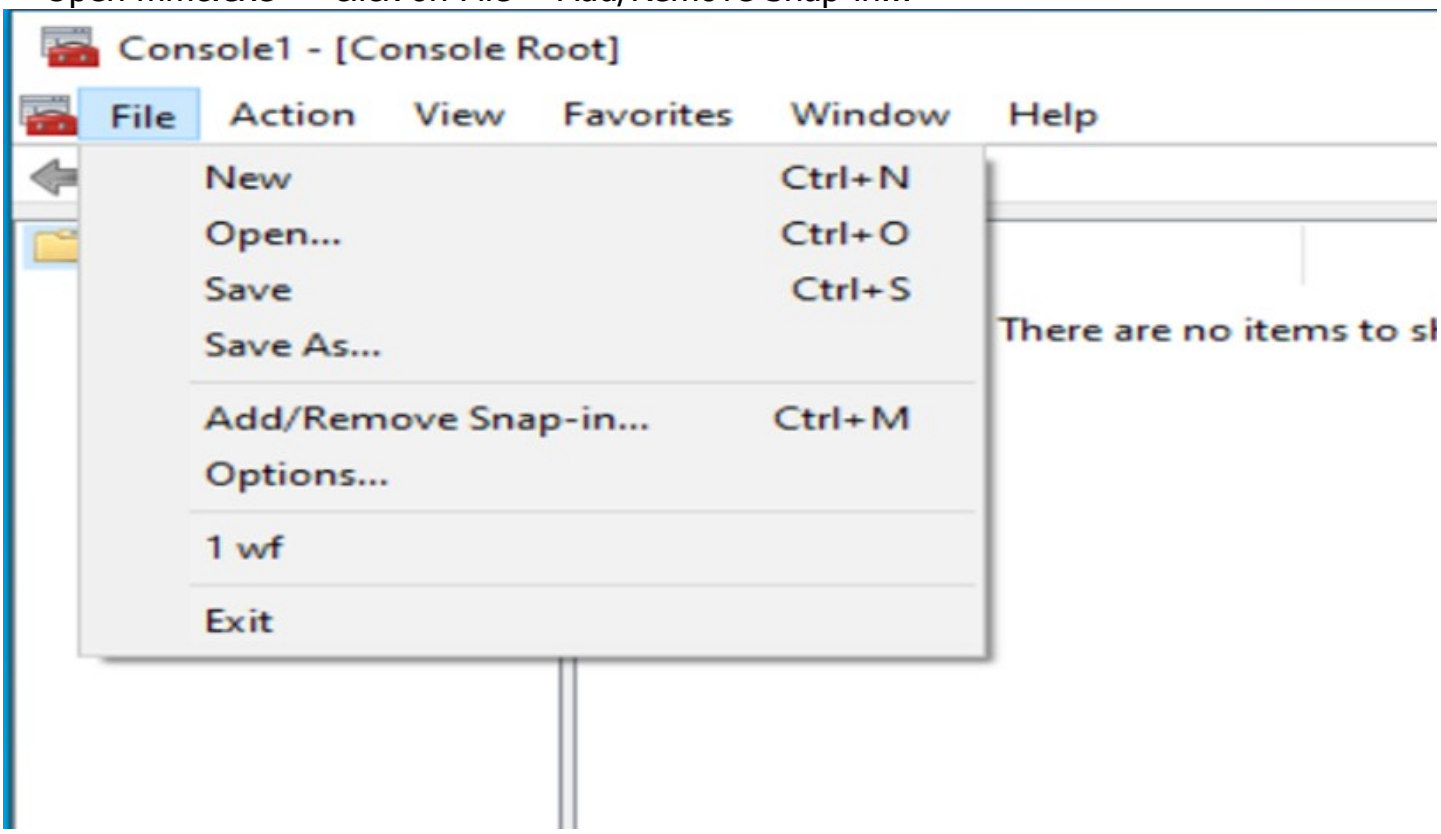
systemctl stop strongswan-starter

-Configuring the Windows client-

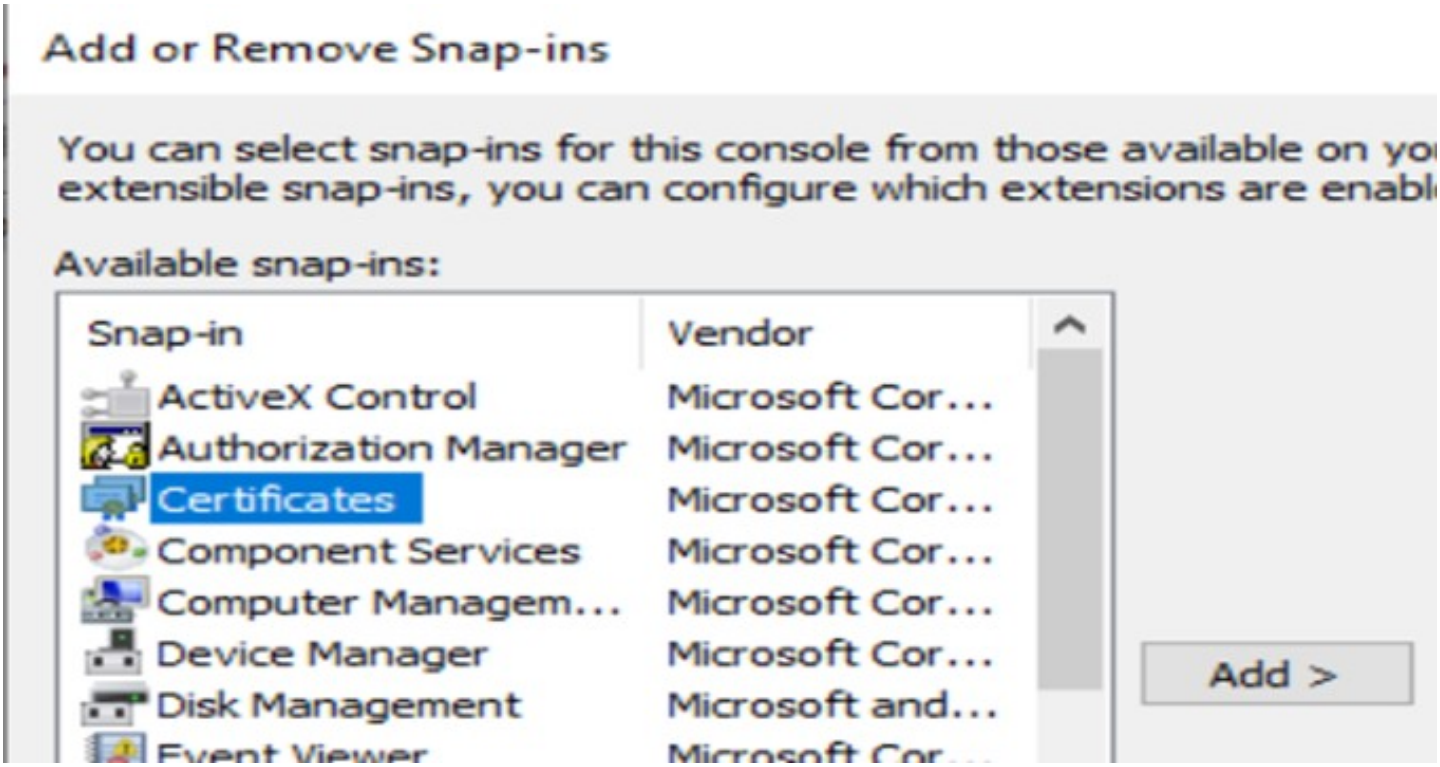
-Copy the CA certificate from the server

-Import the root cert

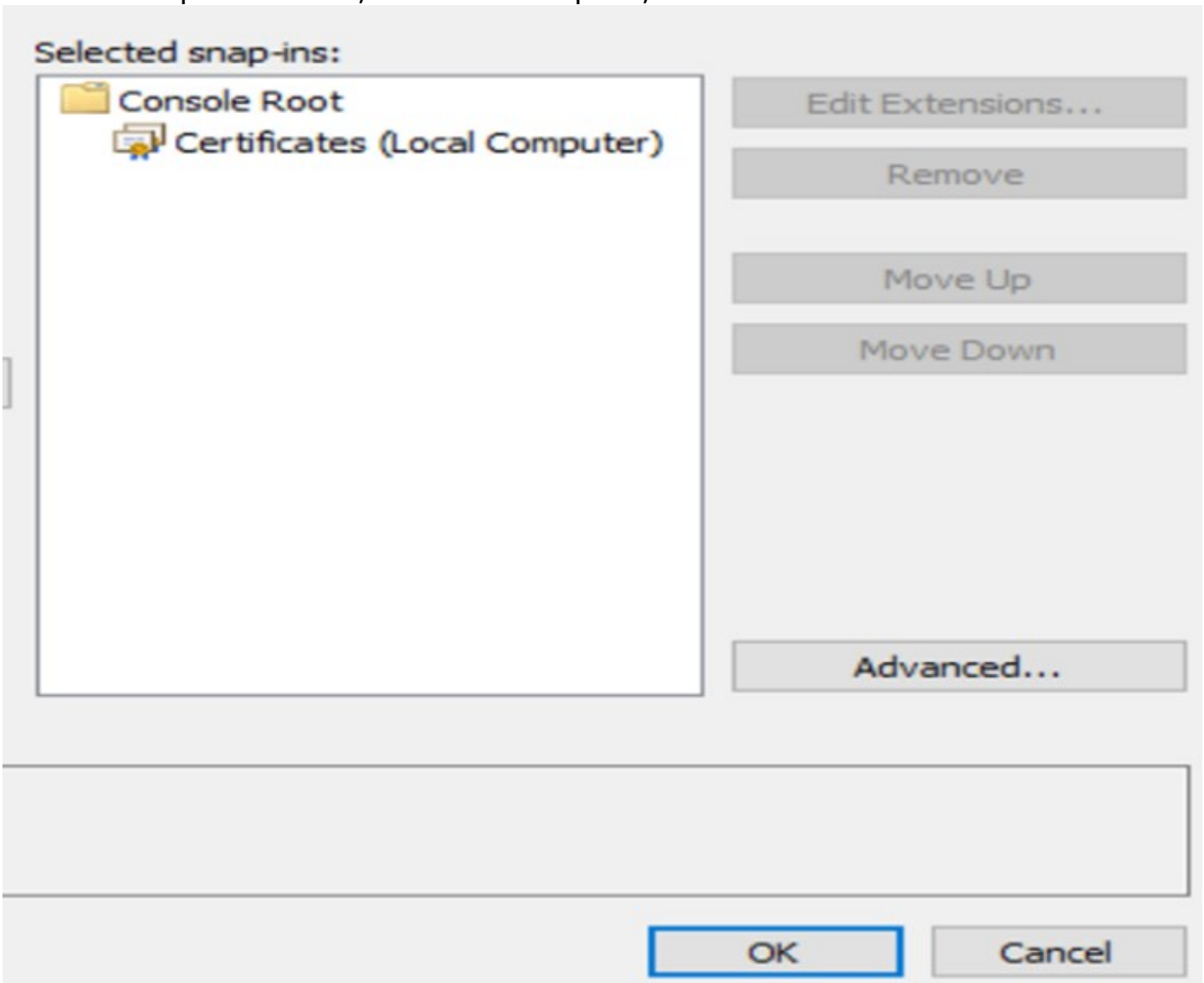
-Open mmc.exe -> click on File > Add/Remove Snap-in...



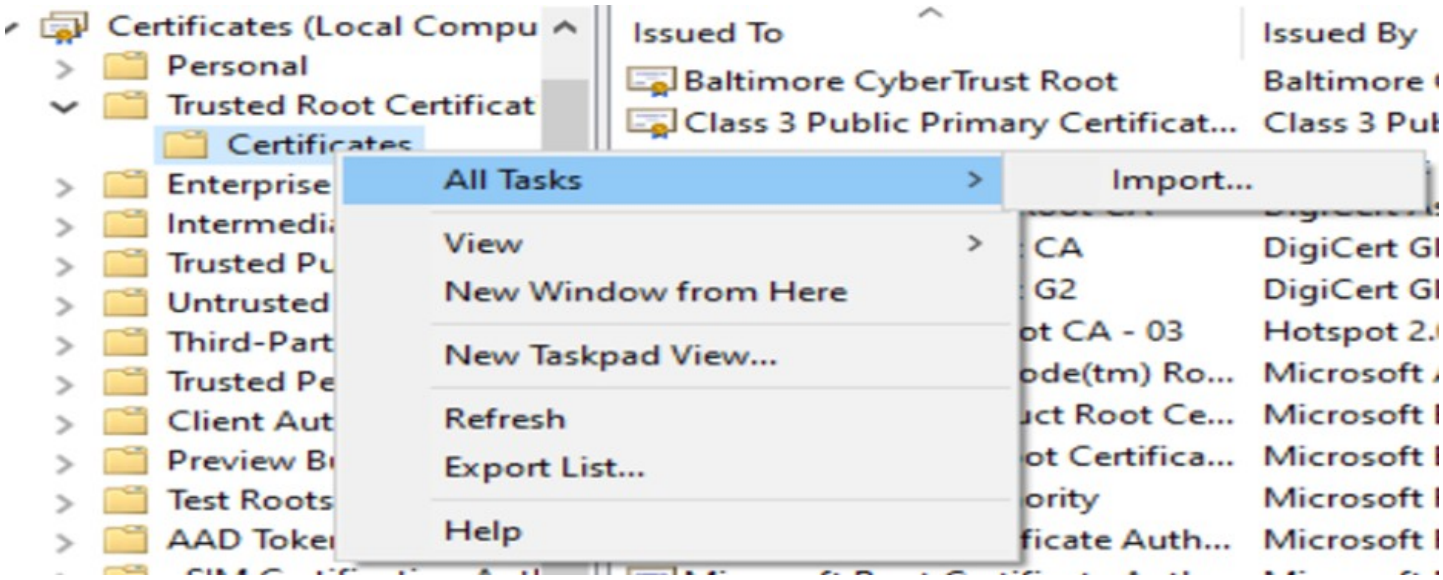
-Add the Certificates snap-in



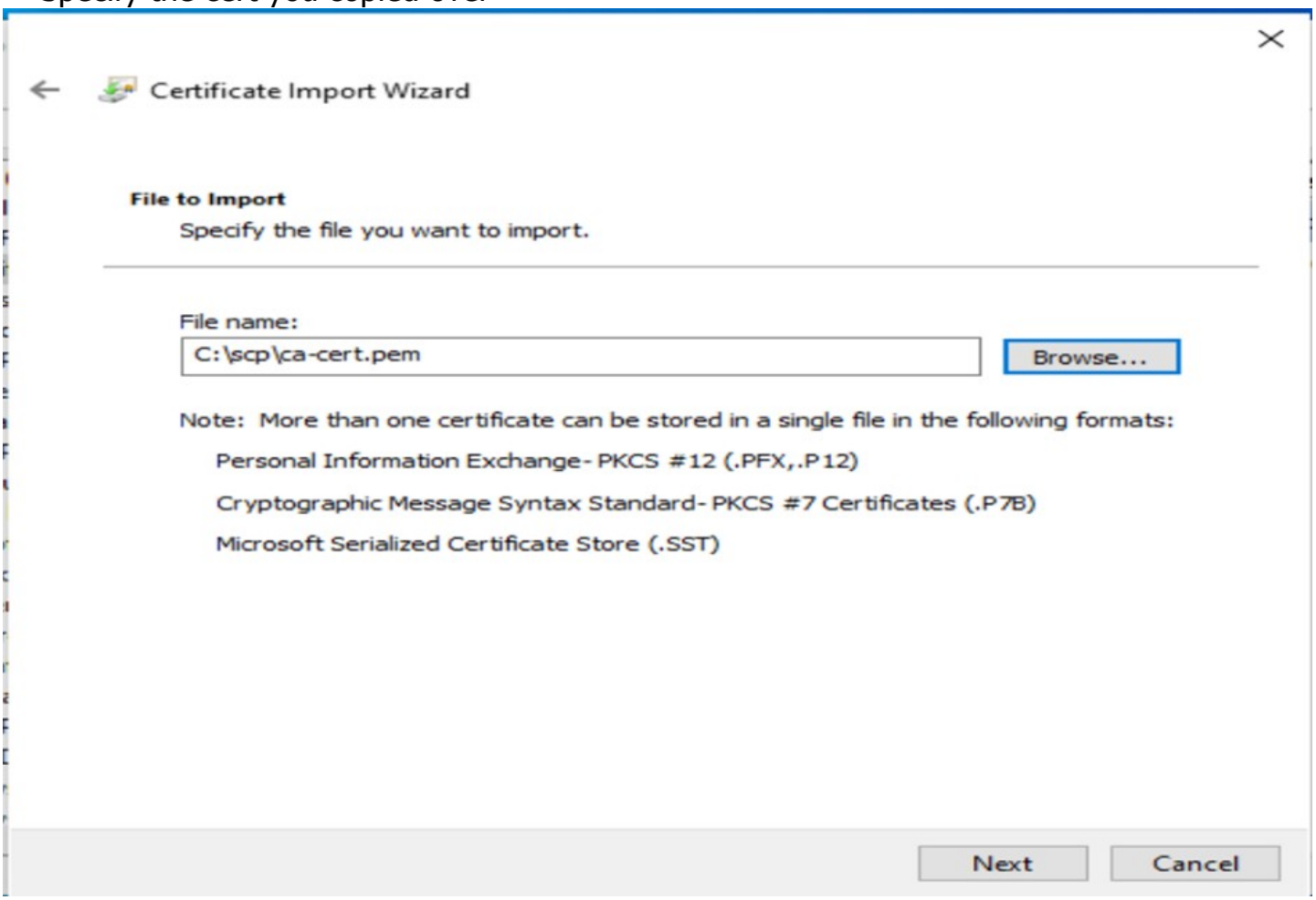
-Select Computer Account, then Local Computer, then OK



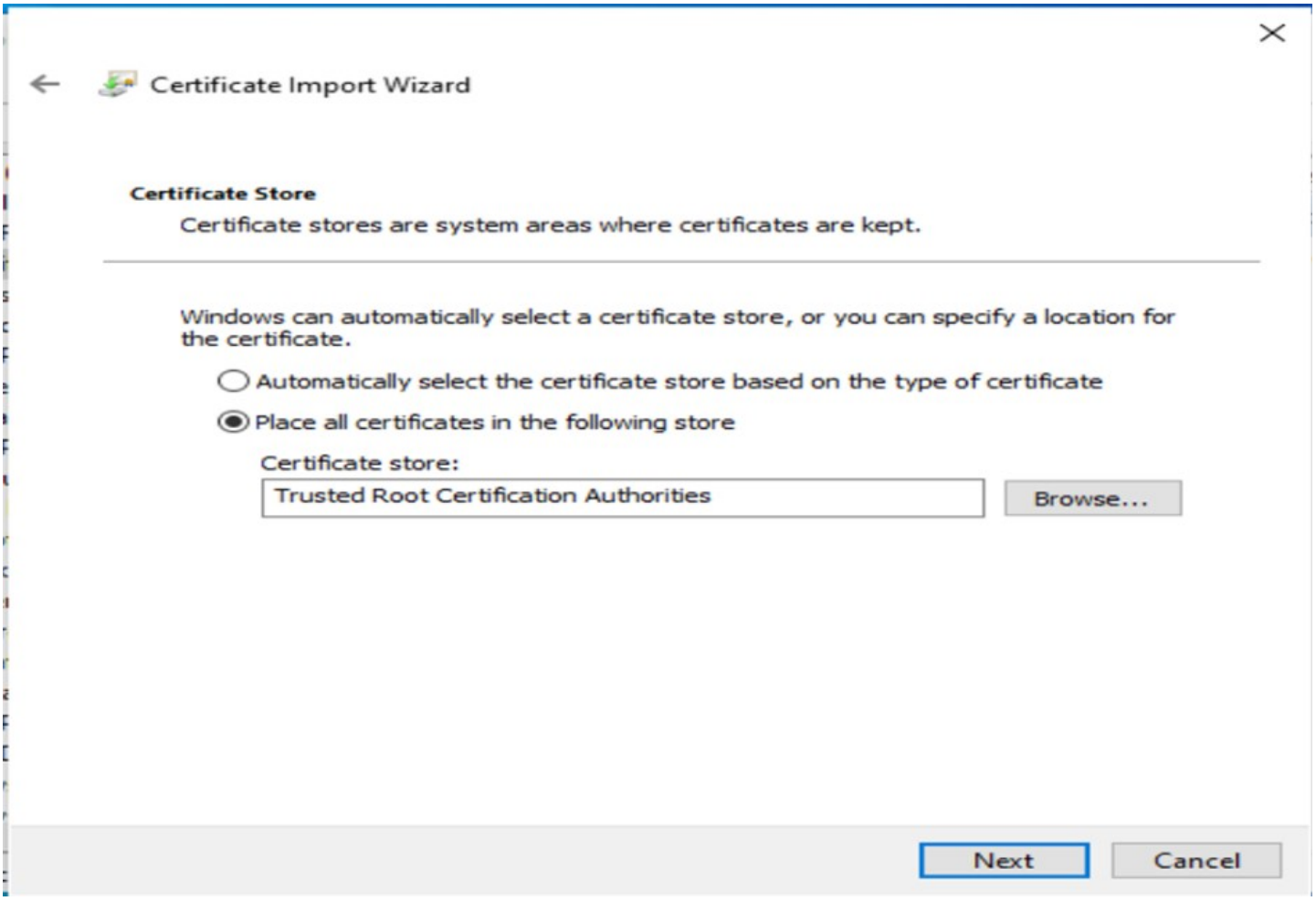
-Open Trusted Root Certification Authorities and right click on Certificates, then click on All tasks > Import



-Specify the cert you copied over

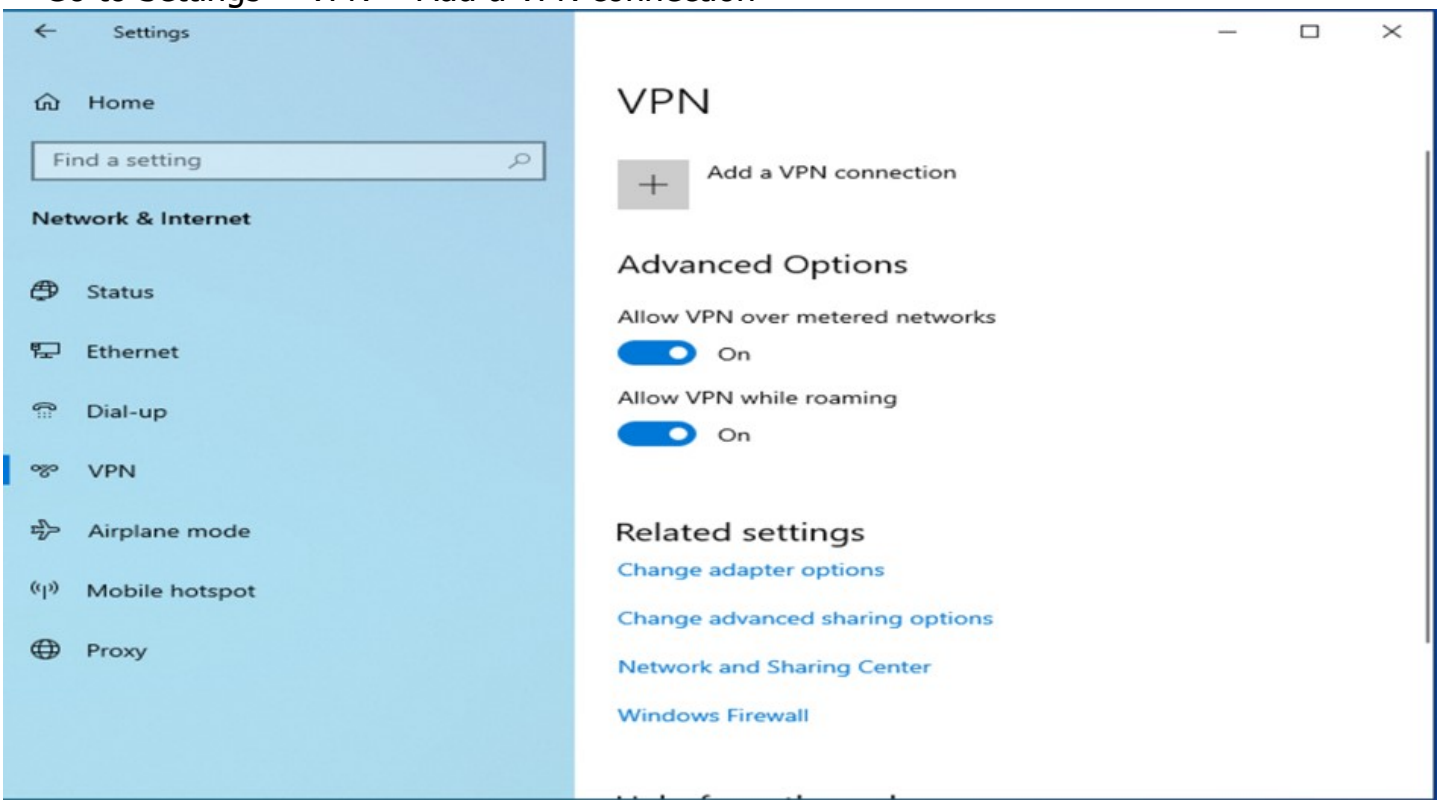


-Make sure it goes to the Trusted Root Certification Authorities

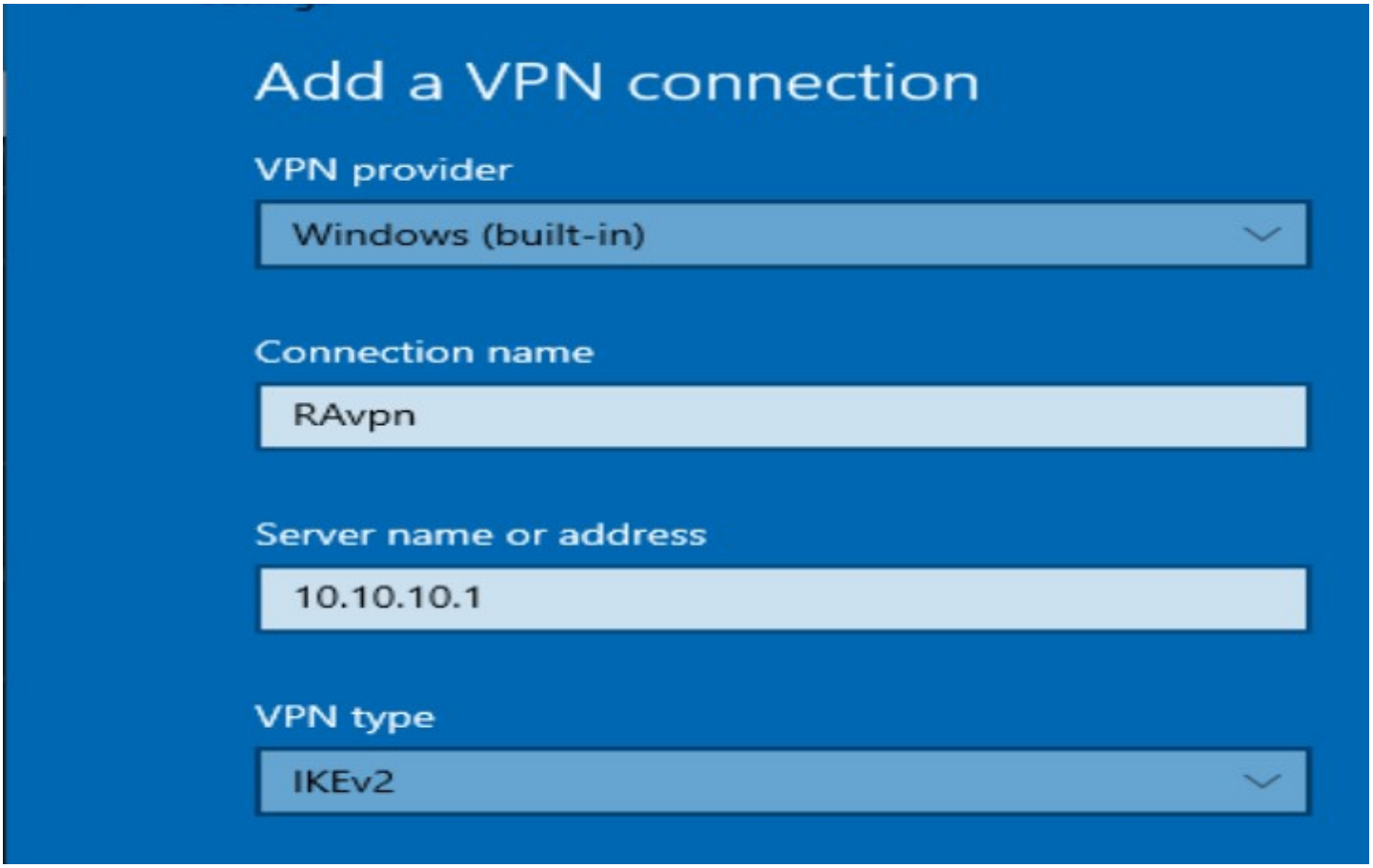


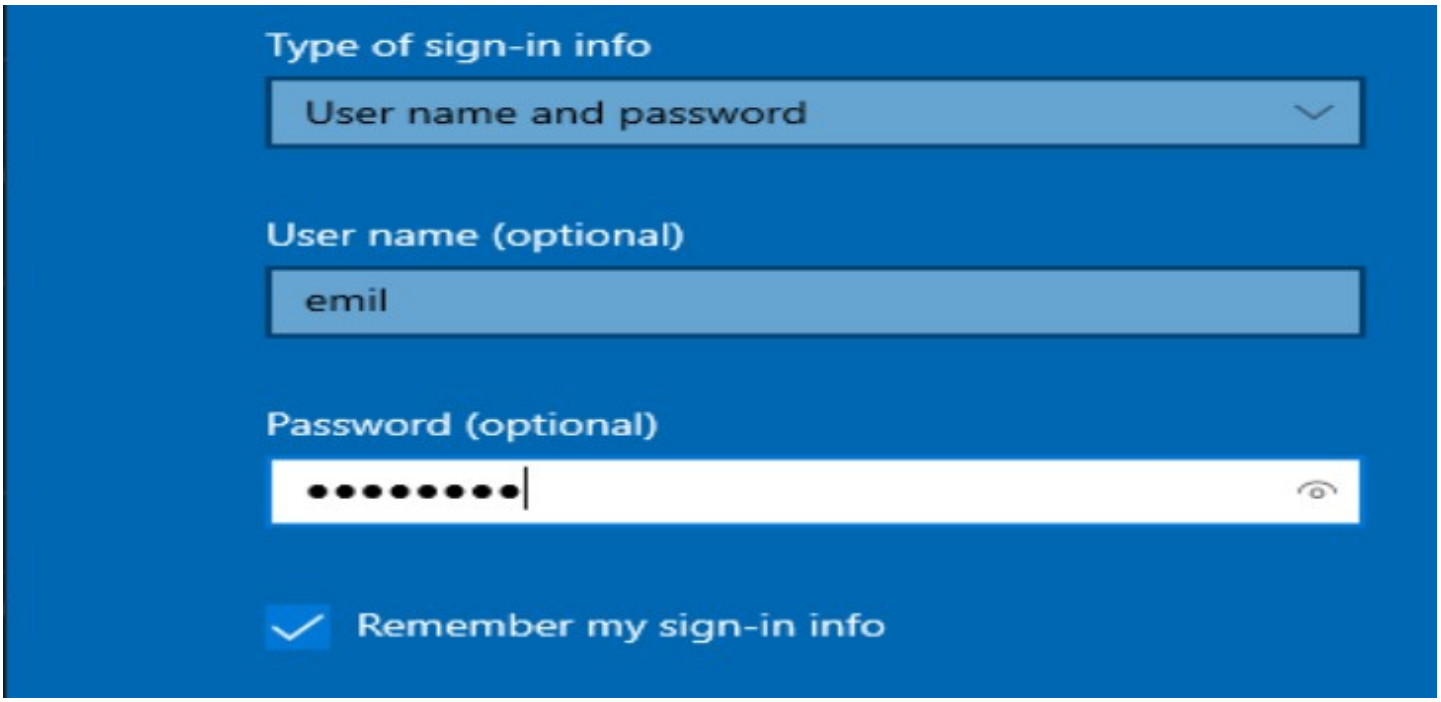
-Add a new VPN connection

-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

```
C:\Users\LocalAdmin>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=1ms TTL=64
Reply from 192.168.100.100: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
bob@debClient:~$ ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=64 time=1.24 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=0.808 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=0.712 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=0.966 ms
^C
--- 192.168.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.712/0.930/1.237/0.198 ms
bob@debClient:~$
```