Handleiding Client-VPN opzetten i.c.m. Cloud Director

Blog van William van Tienen, Cloud engineer bij Interconnect.

27-9-2021

Soms is het noodzakelijk om een persoon (tijdelijk) toegang te geven tot een netwerk vanaf een voor het bedrijfsnetwerk vreemde locatie. Een goed voorbeeld hiervan is een thuiswerkplek, wat nu steeds vaker voorkomt. Een veel gebruikte mogelijkheid om hierin te voorzien, is het toegang verlenen door middel van een Client-VPN, ook wel Remote Acces VPN, Dialup-VPN of SSL VPN genoemd. In deze blog wordt uitgelegd hoe je dit op een goedkope (open source) en veilige manier kan doen.

Met een Client-VPN kun je 1 apparaat of 1 gebruiker toegang geven tot jouw interne netwerk. Er zijn firewalls en internet-gateways van verschillende leveranciers die deze dienst kunnen bieden. Echter in deze blog laat ik zien, hoe je zelf voor deze functionaliteit kunt zorgen in je eigen netwerkomgeving. Ik maak hierbij gebruik van open source componenten, zoals een VM met Debian Linux en het gratis OpenVPN. Deze OpenVPN installeer ik achter een NSX Edge gateway op onze Cloud Director infrastructuur. Ik maak deze dienst dan bereikbaar vanaf het internet, door middel van een NAT-translatie op de bijbehorende NSX Edge gateway.

Als laatste stap laat ik zien hoe je de OpenVPN-client op een Windows machine installeert en configureert. Hiermee wordt een beveiligde verbinding opgezet vanuit bijvoorbeeld een thuiswerkplek naar de omgeving, die draait op onze Cloud Director infrastructuur.

Aanmaken van DMZ-netwerk

Aangezien we bepaalde diensten beschikbaar gaan maken op het internet, willen we dit op een zo veilig mogelijke manier met zo min mogelijk risico's gaan doen. Een aanbeveling is om gebruik te maken van een DMZ-netwerk. Dit is een apart netwerk waarin je verkeer vanaf het internet terecht laat komen en in deze "zone" wordt bepaald welk verkeer naar andere delen van je netwerk mag. Door gebruik te maken van dit aparte netwerk, kunnen we later bepalen welk verkeer we wel of niet toestaan tussen de OpenVPN-Server en de andere interne netwerken. Dit komt de veiligheid zeker ten goede.

Om een DMZ-netwerk aan te maken in Cloud Director, volg je onderstaande stappen.

1. We loggen in op Cloud Director.
2. We selecteren het virtual datacenter waarvoor we VPN-toegang beschikbaar wil maken.
3. Hierna kiezen we voor '**Networking**', '**Networks**, '**New'**.
4. We kiezen voor '**Current Organization Virtual Data Center**' gevolgd door '**Next**'.
5. Hierna kiezen we voor '**Routed**' gevolgd door '**Next**'.

6. We selecteren nu de Edge waarmee we het netwerk willen verbinden en kiezen vervolgens voor '**Next**'.

   Nu geven we het netwerk een passende naam (DMZ) en geven we bij Gateway CIDR het IP-adres op, die we als gateway zullen gaan gebruiken voor onze VM en het bijbehorende subnet (10.200.10.1/24). Hierna kiezen we voor '**Next**'.

7. We kiezen achtereenvolgens voor '**Next**', '**Next**' en '**Finish**'.

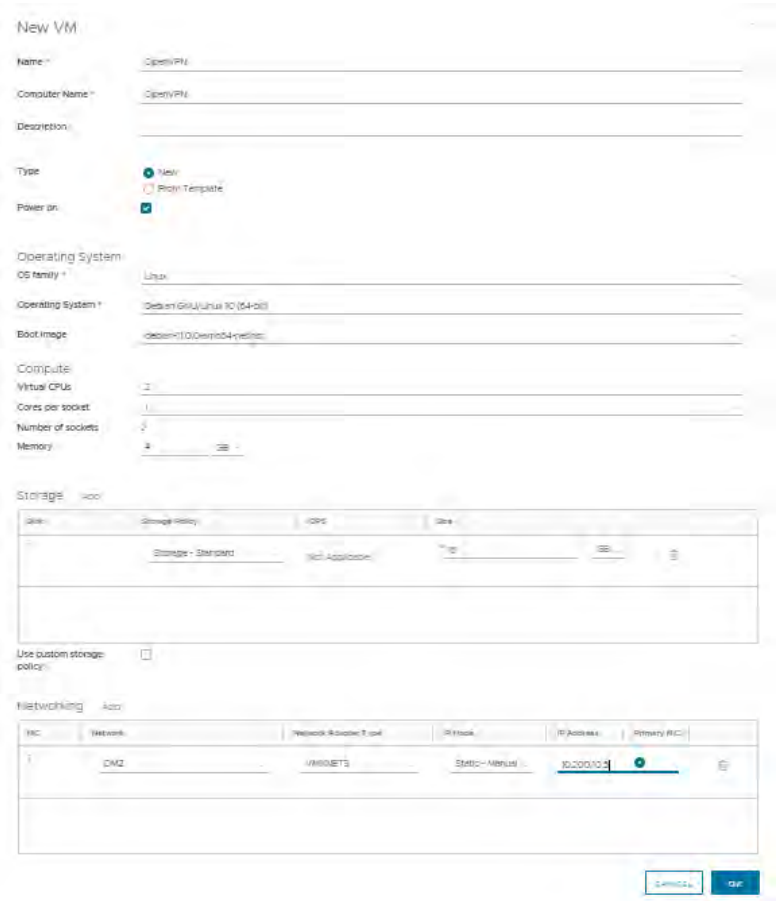
Basisinstallatie Debian 11

1. We loggen in op Cloud Director.

2. We selecteren het virtual datacenter, waarvoor we VPN-toegang beschikbaar willen maken.

3. We maken nu een nieuwe VM aan:
   - Geef de VM een naam.
   - OS Family: Linux
   - Operating System: Debian GNU/Linux 10 (64-bit)
   - Boot image: debian-11.0.0-amd64-netinst
   - Minimaal 2vCPU's
   - Minimaal 4GB RAM
   - Minimaal 16GB opslag
   - Networking: We selecteren het zojuist aangemaakte netwerk, IP-mode: 'Static manual', IP-address: een IP in het subnet behorende bij het eerder aangemaakte netwerk.

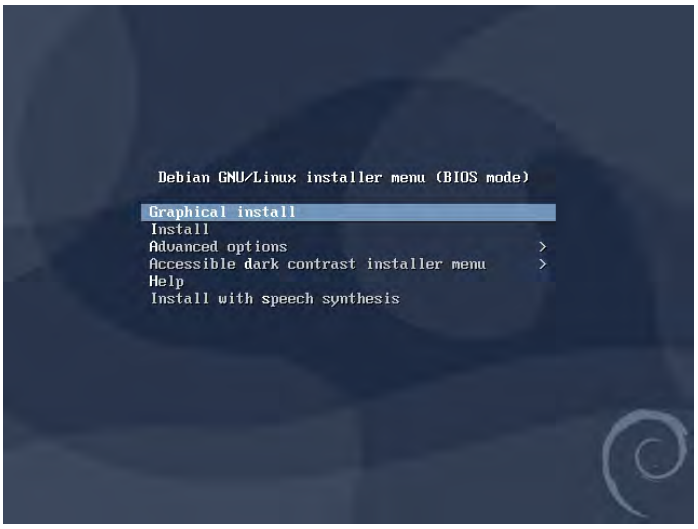
   Hierna kiezen we voor '**Next**'.



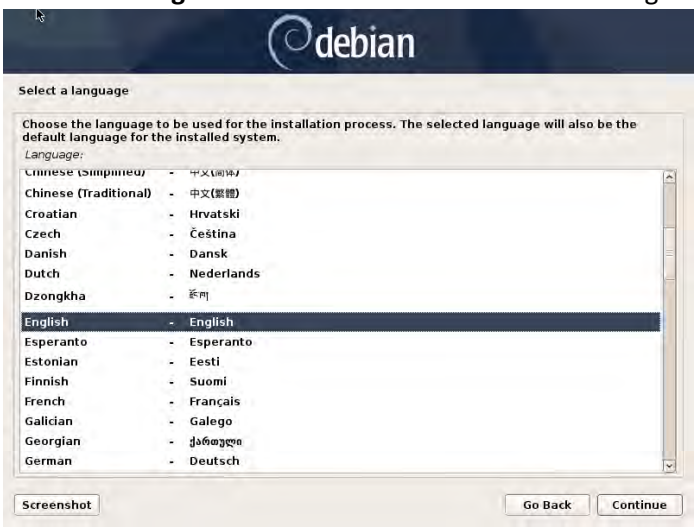
De VM zal nu worden gestart.

Het boot-image is standaard beschikbaar in onze shared catalog op Cloud Director. Mocht je Debian niet vanuit onze Cloud Director portal installeren, dan is deze ook gratis te downloaden via de volgende url: https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.0.0-amd64-netinst.iso.

1. We kiezen ervoor om een **Graphical install** te doen.

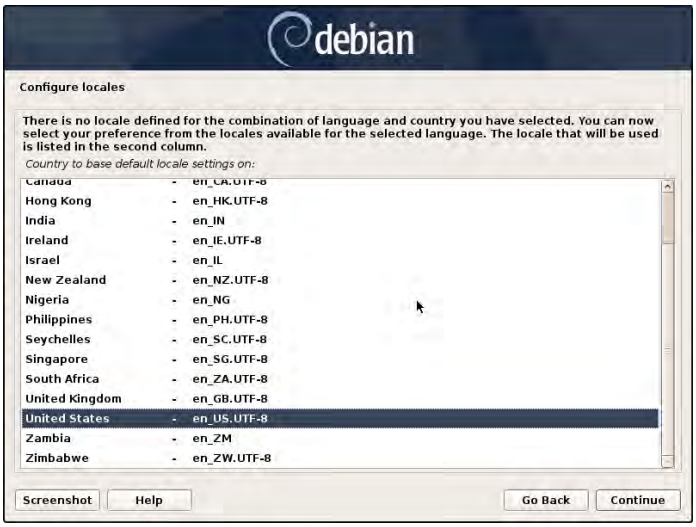


2. We kiezen '**English**' als standaardtaal en kiezen vervolgens '**Continue**'.

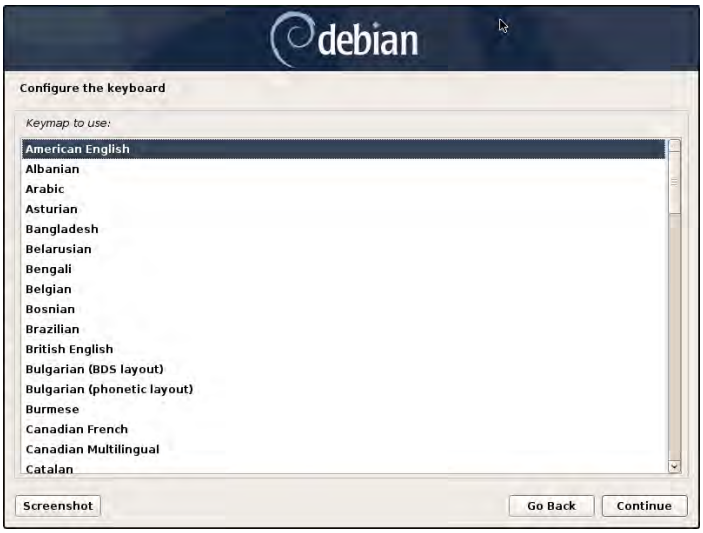


3. Wanneer we een locatie op moeten geven kiezen we voor '**other**' gevolgd door '**Continue**'. Hierna kiezen we achtereenvolgens voor '**Europe**', '**Continue**', '**Netherlands**' en weer '**Continue**'.

4. We selecteren ‘**United States**’ als locales, gevolgd door ‘**Continue**’.



5. We kiezen voor '**American English**' als keymap en kiezen hierna voor '**Continue**' De installatie wordt nu gestart. Dit zal enkele minuten duren.



6. Nu gaan we de netwerkconfiguratie in orde maken. We kiezen '**Continue**' om te starten met deze configuratie.

7. Het is aan te raden om de OpenVPN-server een vast IP-adres te geven. We kiezen hier dus voor de optie '**Configure network manually**', gevolgd door '**Continue**'.

8. We geven een IP-adres op volgens de CIDR-notatie. Hierna kiezen we voor '**Continue**'.

9. We controleren of de Gateway juist is ingevuld. Dit zou hetzelfde IP-adres moeten zijn, die we bij het aanmaken van het DMZ-netwerk hebben opgegeven. Wanneer dit niet het geval is, controleer je de instelling in het voorgaande scherm of pas je het gateway-adres zelf aan. Hierna kiezen we voor '**Continue**'.

10. We geven nu 1 of meerdere DNS-servers op. Aangezien we zelf geen interne DNS-servers beschikbaar hebben in onze omgeving, maken we hier gebruik van de publieke DNS-servers van Google: 8.8.8.8 en 8.8.4.4. Hierna kiezen we voor '**Continue**'.

11. We voeren een herkenbare hostname in en kiezen '**Continue**'.

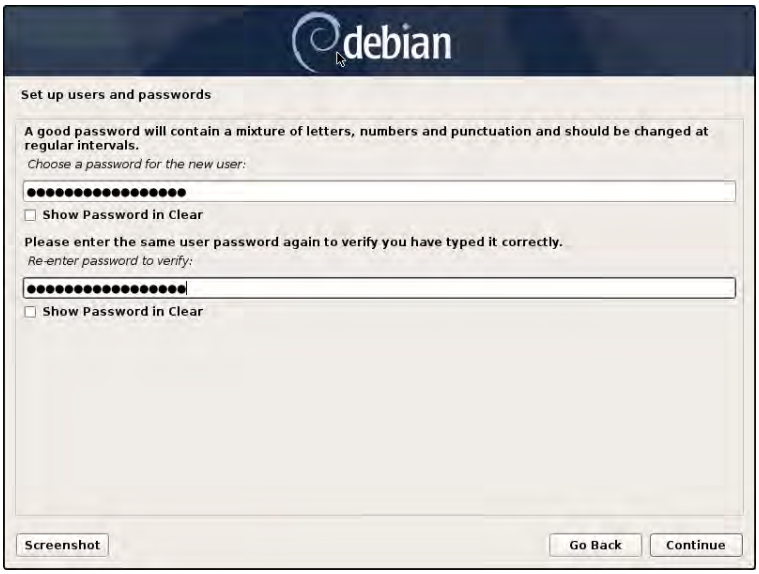
12. Optioneel kunnen we een domeinnaam opgeven. Hierna kiezen we voor '**Next**'.

13. Nu geven we een wachtwoord op voor de root-user en kiezen '**Continue**'.
    Bewaar dit wachtwoord goed!

14. Aanvullend dienen we nog een extra account aan te maken. We geven hiervoor de volledige naam voor dit account op en kiezen voor '**Continue**'.

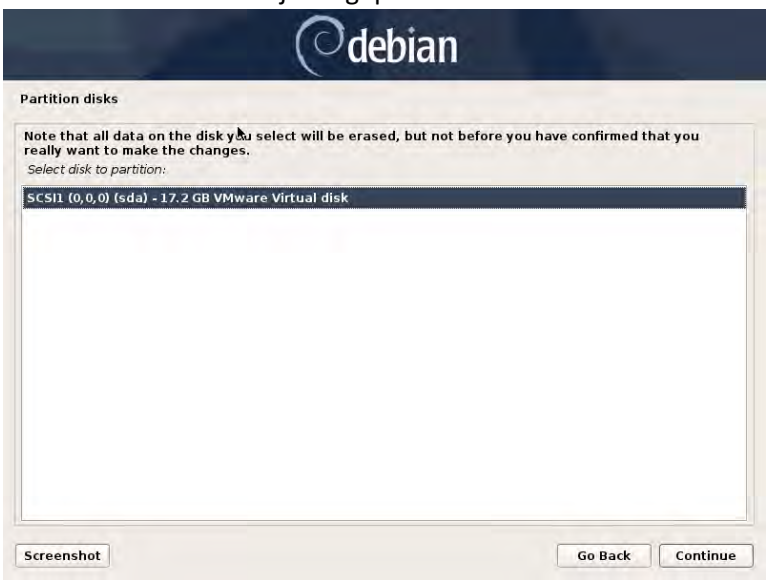
15. Aanvullende geven we ook de gewenste accountnaam op voor dit account en kiezen voor '**Continue**'.

16. We geven ook een wachtwoord op voor dit account en kiezen voor '**Continue**'.

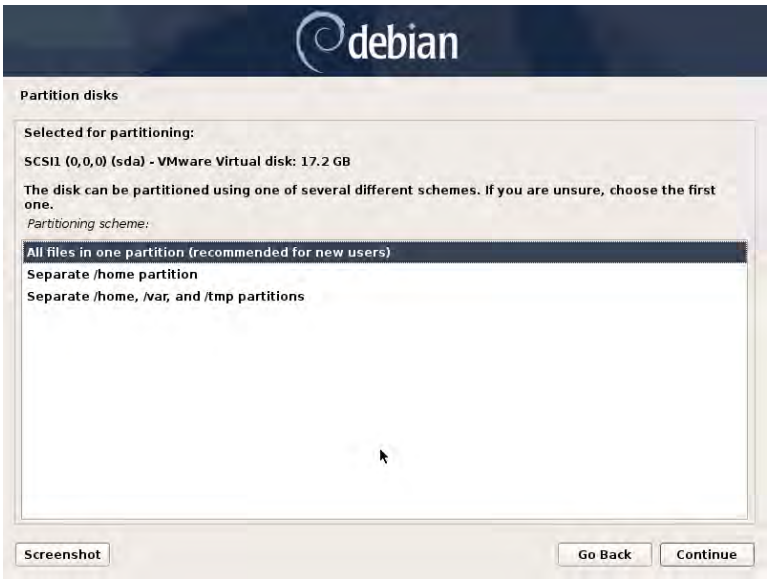


17. We kiezen voor '**Guided' – use entire disk**' als partitioning method en kiezen vervolgens voor '**Continue**'.

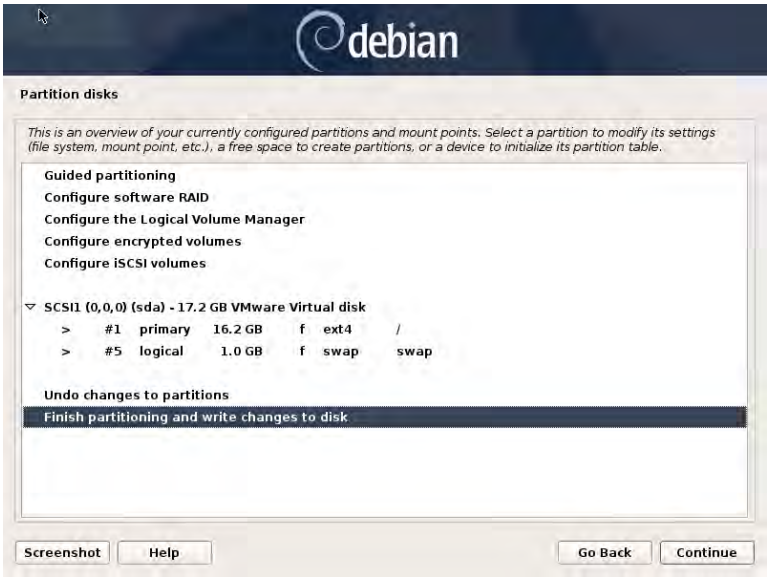
18. We selecteren een schijf die gepartitioneerd moet worden en kiezen voor '**Continue**'.



19. We kiezen voor '**All files in one partition (recommend for new users)**' en kiezen hierna voor '**Continue**'.



20. We kiezen '**Finish partitioning and write changes to disk**' gevolgd door '**Continue**'.



21. We kiezen '**Yes**' om de gemaakte wijzigingen naar disk te schrijven en kiezen vervolgens voor '**Continue**'.

22. We kiezen voor '**No**', zodat er geen aanvullende Cd's of Dvd's gescand gaan worden en kiezen daarna voor '**Continue**'.

23. We selecteren '**Netherlands**' op als voorkeurslocatie voor de download van packages en kiezen daarna voor '**Continue**'.

24. We selecteren 1 van de Debian archive mirrors en kiezen voor '**Continue**'.

25. Aangezien er geen gebruik gemaakt wordt van een HTTP-proxy kiezen we hier voor '**Continue**'.

26. We kiezen ‘No’ om geen deel te nemen aan de package usage enquête.

27. We selecteren hier alleen ‘**SSH-server**’ en ‘**standard system utilities**’ en kiezen daarna ‘**Continue**’.

28. We kiezen voor '**Yes**' om de GRUB-boot loader te installeren en kiezen daarna voor '**Continue**'.

29. We selecteren **'/dev/sda**' als locatie voor het installeren van de boot loader en kiezen daarna voor '**Continue**'.

30. Hierna is de basisinstallatie van Debian afgerond. We kiezen voor '**Continue**' om het systeem opnieuw op te laten starten.

31. We loggen nu in op de console met het root-account.
    We gaan aanvullende packages installeren en draaien hiervoor het commando:
    `apt-get install open-vm-tools iptables-persistent -y`

    We kiezen 2x voor '**Yes**' om de bestaande tables voor IPv4 en IPv6 te behouden wanneer hierom wordt gevraagd.

32. Nu gaan we ervoor zorgen dat het root-account ook gebruik kan maken van SSH om verbinding te maken. Standaard staat dit namelijk uitgeschakeld.

    We openen hiervoor het bestand /etc/sshd/sshd_config. Met het commando:
    `nano /etc/sshd/sshd_config`

We passen nu de regel:

```
#PermitRootLogin prohibit-password
```

aan naar:

```
PermitRootLogin yes
```

en slaan deze wijziging op met [**Ctrl**] + **X**, '**y**', gevolgd door [**Enter**].

Aansluitend herstarten we de SSH-service met het commando:

```
service ssh restart
```

33. Aangezien onze VM als een soort van router gaat dienen voor het VPN-verkeer moeten we dit toestaan binnen Debian.

    Open hiervoor het bestand /etc/sysctl.conf met het commando:

    ```
    nano /etc/sysctl.conf
    ```

    We halen nu het '#' weg voor de regel met net.ipv4.ip_forward = 1

    ```
    # Uncomment the next line to enable packet forwarding for IPv4
    net.ipv4.ip_forward=1
    ```

    En slaan de wijzigingen op met [**Ctrl**] + **x**, '**y**' gevolgd door [**Enter**].

    De nieuwe configuratie passen we toe met commando:

    ```
    sysctl -p
    ```

34. Nu gaan we ervoor zorgen dat VPN-verkeer door deze VM ge-NAT kan gaan worden en dat dit ook gehandhaafd blijft na een herstart.

    Dit doen we met onderstaande 2 commando's:

    ```
    iptables -t nat -A POSTROUTING -o ens192 -j MASQUERADE
    iptables-save > /etc/iptables/rules.v4
    ```

Configuratie van NSX Edge firewall

Het gebruik van SSH zal het configureren van onze OpenVPN-server vereenvoudigen. Bij de installatie van Debian hebben we bij stap 27 al aangegeven dat SSH geïnstalleerd moet worden.

Je kunt dit controleren door in te loggen op de console en het commando '**service sshd status**' in te typen. Het is belangrijk dat de service 'Active (running)' als status heeft.

```
root@OpenVPN:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-30 16:46:08 CEST; 3 days ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 428 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 434 (sshd)
    Tasks: 1 (limit: 4701)
   Memory: 4.7M
   CGroup: /system.slice/ssh.service
           └─434 /usr/sbin/sshd -D
```

Om onze OpenVPN-server bereikbaar te maken van buitenaf, moeten we enkele wijzigingen doorvoeren op de NSX Edge firewall. Deze is standaard beschikbaar bij een virtueel datacenter bij Interconnect op basis van Cloud Director.

Aanmaken Destination-NAT rules

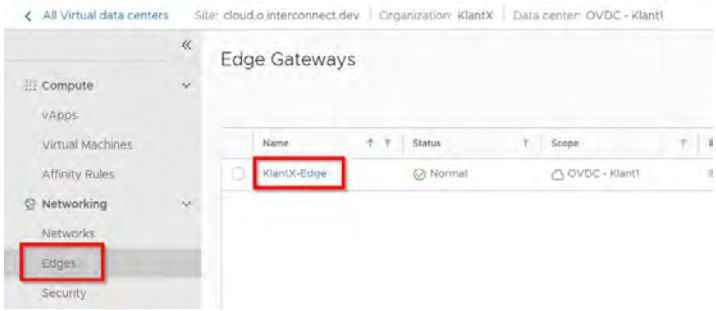
1. We loggen in op Cloud Director.

2. We selecteren het virtual datacenter waarvoor we VPN-toegang beschikbaar wil maken.

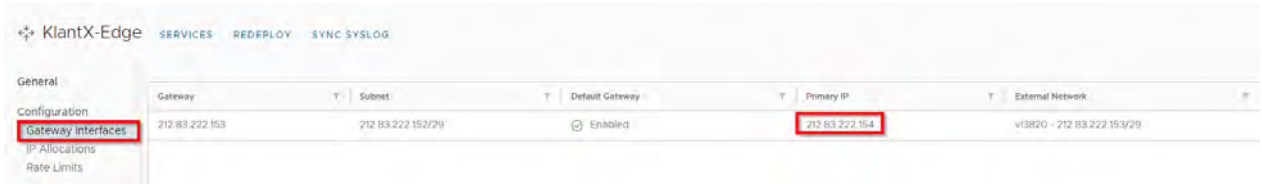
3. Om onze OpenVPN-server met een private IP-adres benaderbaar te maken vanaf het internet, moeten we een zogenaamde Destination-NAT translatie configureren. Hiermee koppelen we een public IP-adres aan een private IP-adres.

   We gaan eerst kijken over welke publieke IP-adressen onze NSX Edge beschikt en welke we kunnen gebruiken voor onze Destination-NAT configuratie.

   We kiezen hiervoor '**Networking**', '**Edges**' en dubbelklikken op de naam van de gateway.



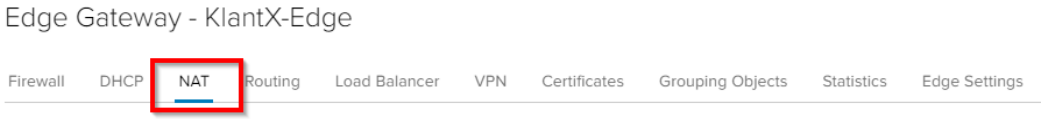
4. We kiezen nu voor '**Gateway interfaces**' om te kunnen zien welke IP-range er geconfigureerd is op de Edge gateway. In ieder geval het primary IP is altijd beschikbaar om Destination-NAT op toe te passen. Dit is het adres wat we gaan gebruiken in dit voorbeeld. Noteer dit IP-adres.



In veel gevallen, zijn er nog andere IP-adressen te gebruiken, maar dit valt buiten de scope van dit artikel.

5. We kiezen nu voor '**Services**' om de Edge gateway te gaan configureren.

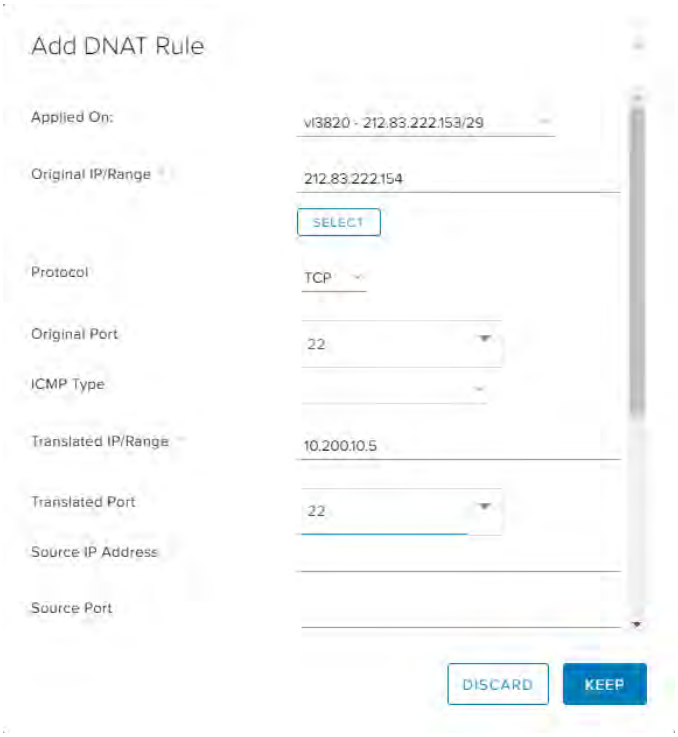
6. We kiezen '**NAT**' in het menu aan de bovenzijde.



7. We kiezen '**+ DNAT rule**' om een nieuwe Destination-NAT regel aan te maken.

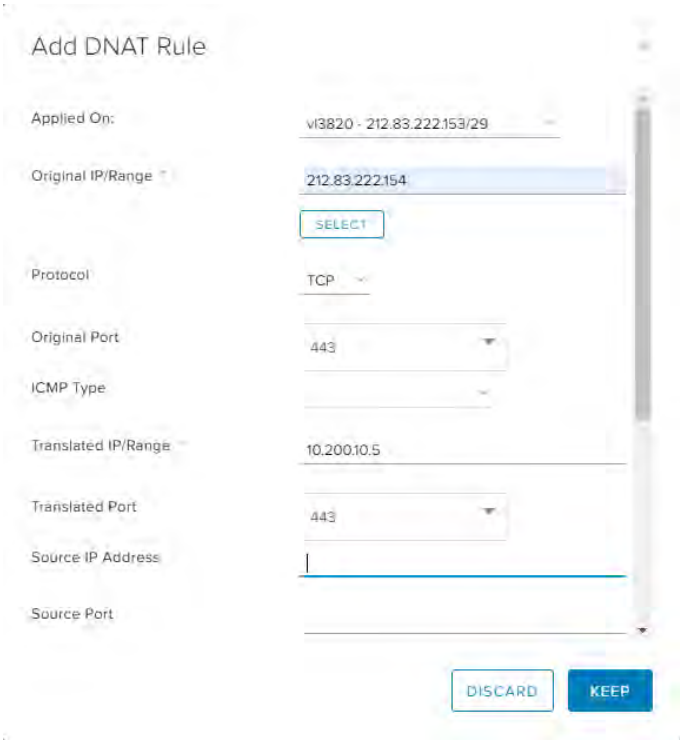
8. We maken nu een regel aan om onze OpenVPN server bereikbaar te maken voor SSH (poort 22). Vul het formulier in. Aansluitend kiezen we voor '**Keep**' om dit op te slaan

Applied On:	Dit staat al vaak juist ingevuld, laat dit dus staan.
Original IP/Range:	Hier vullen we het IP-adres uit stap 4 in.
Protocol:	TCP
Original Port:	22
ICMP Type:	[Leeg]
Translated IP/Range:	Het (interne) IP-adres van de OpenVPN Server
Translated Port:	22



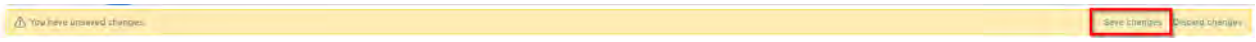
9. We maken ook eenzelfde soort regel aan, zodat het VPN-verkeer naar de OpenVPN server wordt gestuurd. We maken hiervoor een nieuwe DNAT-regel aan en vullen deze volgens onderstaand voorbeeld in. Hierna kiezen we voor '**Keep**' om dit op te slaan.

Applied On:	Dit staat al vaak juist ingevuld, laat dit dus staan.
Original IP/Range:	Hier vullen we het IP-adres uit stap 4 in.
Protocol:	TCP
Original Port:	443
ICMP Type:	[Leeg]
Translated IP/Range:	Het (interne) IP-adres van de OpenVPN Server
Translated Port:	443



204811	User-defined	DNAT	vl3820 - 212.83.222.153/2	212.83.222.154	22	10.200.10.5	22	tcp	✓ ✗
204812	User-defined	DNAT	vl3820 - 212.83.222.153/2	212.83.222.154	443	10.200.10.5	443	tcp	✓ ✗

10 BELANGRIJK! Om de NAT-wijzigingen op te slaan in de actieve configuratie van de NSX Edge gateway kiezen we voor '**Save Changes**'.



De NAT-regels zijn nu aangemaakt. In de volgende stap gaan we firewall-regels aanmaken, zodat het verkeer voor deze rules ook wordt toegestaan.

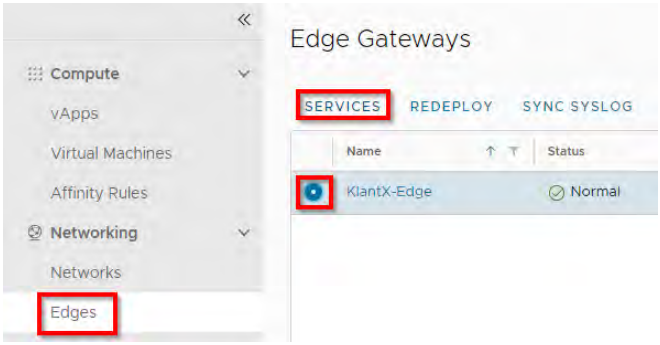
Aanmaken van firewall-rules

Met behulp van de firewall-regels kunnen we verkeer toestaan of juist blokkeren. We gaan nu een 2-tal firewall-regels aanmaken voor het verkeer naar onze OpenVPN-server.

1. We loggen in op Cloud Director.

2. We selecteren het virtual datacenter waarvoor we VPN-toegang beschikbaar wil maken.

3. We kiezen nu '**Networking**', '**Edges**' selecteren de NSX Edge gateway en kiezen '**Services**'.



4. We kiezen '**Firewall**', normaal gesproken is dit venster al geopend.

5. We kiezen voor '**+**' om een nieuwe firewall-regel toe te voegen.

6. Er verschijnt nu een nieuwe 'lege' firewall-regel, die we aan kunnen passen.
We gaan deze firewall-regel dusdanig configureren dat er alleen SSH-verkeer toegestaan wordt vanaf het Internet naar onze OpenVPN-server. En alleen vanaf ons eigen IP-adres. Dit is belangrijk, omdat je niet wil dat potentiële aanvallers toegang krijgen tot SSH van de OpenVPN-server.

   We vullen daarvoor deze firewall-regel zo in:

Name:	We geven hier een beschrijving van het doel van deze regel.	
Type:	Kan niet aangepast worden; User.	
Source:	External	
Destination:	Het externe IP-adres gekoppeld aan onze OpenVPN-server	
Service:	Protocol:	TCP
	Source Port:	Any
	Destination Port:	22
	Action:	Accept

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1 ✔	SSH Toegang voor beheer OpenVPN-server	User	external	212.83.222.154	tcp:22:any	Accept	☐

7. We kiezen opnieuw voor '**+**' om nog een nieuwe firewall-regel toe te voegen.

8. We gaan nu een regel aanmaken die alleen VPN-verkeer toestaat voor iedereen vanaf het internet naar de OpenVPN-server. Hiervoor gebruiken we poort 443 aangezien deze poort ook

gebruikt wordt voor web-browsing. In de meeste (publieke) netwerken staat deze al open en is daardoor gemakkelijk te gebruiken.

We vullen de firewall-regel zo in:

Name:	Geef hier een beschrijving van het doel van deze regel.	
Type:	Kan niet aangepast worden; User.	
Source:	External	
Destination:	Het externe IP-adres gekoppeld aan onze OpenVPN-server	
Service:	Protocol:	TCP
	Source Port:	Any
	Destination Port:	443
Action:	Accept	

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	VPN-Toegang tot OpenVPN-server	User	Any	212.83.222.154	tcp:443:any	Accept	

9. We kiezen opnieuw '**+**' om nog een nieuwe firewall-regel toe te voegen.

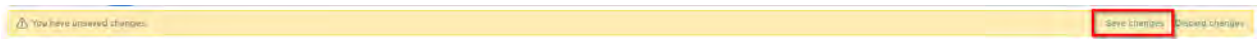
10. Als laatste gaan we een firewall-regel aanmaken die verkeer toestaat vanaf de OpenVPN-server naar andere IP-adressen of subnets binnen het interne netwerk via de VPN-verbinding.

    We maken hiervoor een firewall-regel aan zoals onderstaande:

Name:	We geven hier een beschrijving van het doel van deze regel.
Type:	Kan niet aangepast worden; User.
Source:	IP-adres van OpenVPN-server
Destination:	IP-adressen/Subnetten die toegankelijk moeten zijn vanaf de VPN
Service:	Alleen poorten toestaan die toegankelijk zouden moeten zijn. Source-port is vrijwel altijd 'any'.
Action:	Accept

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	Netwerk-toegang vanaf OpenVPN-server	User	10.200.0.15	10.200.1.0/24 10.200.0.0/24	tcp:3389:any	Accept	

11. Om alle gemaakte wijzigingen door te voeren kiezen we '**Save changes**'.



Installatie en configuratie van OpenVPN

Nu we de configuratie op de NSX Edge gateway in orde hebben gemaakt, zouden we via SSH onze OpenVPN-server moeten kunnen beheren. Hiervoor gebruiken we Putty als client op een Windows machine.

1. We starten Putty of een soortgelijke SSH-client en maken verbinding naar het externe IP-adres, die we hebben geconfigureerd op de NSX Edge gateway.

2. We loggen in met het root-account.

3. We gaan nu OpenVPN installeren door het commando '**apt-get install openvpn -y**' te gebruiken.

   De installatie van OpenVPN zal nu worden gestart.

```
interconnect@OpenVPN:~$ sudo apt-get install openvpn -y
[sudo] password for interconnect:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  easy-rsa libccid liblzo2-2 libpcsclite1 libpkcs11-helper1 libusb-1.0-0
  opensc opensc-pkcs11 pcscd
Suggested packages:
  pcmciautils resolvconf openvpn-systemd-resolved
The following NEW packages will be installed:
  easy-rsa libccid liblzo2-2 libpcsclite1 libpkcs11-helper1 libusb-1.0-0
  opensc opensc-pkcs11 openvpn pcscd
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,306 kB of archives.
After this operation, 6,508 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 easy-rsa all 3.0.6-1 [37.9
kB]
```

4. Ook EasyRSA hebben we nodig. Deze kunnen we met onderstaand commando downloaden op onze VM. Op dit moment is versie 3.0.8 de meest recente versie van easy-rsa.

   wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.8/EasyRSA-3.0.8.tgz

5. We pakken het bestand uit met commando:
   tar -xvzf EasyRSA-3.0.8.tgz

6. En na het uitpakken, kopiëren we deze bestanden naar een andere map.
   cp -r EasyRSA-3.0.8 /etc/openvpn/easy-rsa

7. We navigeren nu naar de nieuwe EasyRSA-map:
   cd /etc/openvpn/easy-rsa

8. We maken een configuratiebestand aan voor de creatie van enkele certificaten, die vereist zijn voor de versleuteling.
   nano vars

   Vul de onderstaande variabelen in en kopieer het geheel naar de editor.

EASYRSA_REQ_COUNTRY	Land waar organisatie is gevestigd
EASYRSA_REQ_PROVINCE	Provincie waar organisatie is gevestigd
EASYRSA_REQ_CITY	Plaats waar organisatie is gevestigd

EASYRSA_REQ_ORG	Naam organisatie
EASYRSA_REQ_EMAIL	e-mailadres voor contact
EASYRSA_REQ_OU	Naam afdeling

=== vars-file ==========

```
set_var EASYRSA_REQ_COUNTRY     "NL"
set_var EASYRSA_REQ_PROVINCE    "Noord-Brabant"
set_var EASYRSA_REQ_CITY        "'s-Hertogenbosch"
set_var EASYRSA_REQ_ORG         "Interconnect DEV"
set_var EASYRSA_REQ_EMAIL       "service@interconnect.nl"
set_var EASYRSA_REQ_OU          "Interconnect DEV CA"
set_var EASYRSA                 "$PWD"
set_var EASYRSA_PKI             "$EASYRSA/pki"
set_var EASYRSA_DN              "cn_only"
set_var EASYRSA_ALGO            rsa
set_var EASYRSA_CA_EXPIRE       3650
set_var EASYRSA_CERT_EXPIRE     3650
set_var EASYRSA_CRL_DAYS        3650
set_var EASYRSA_NS_SUPPORT      "no"
set_var EASYRSA_EXT_DIR         "$EASYRSA/x509-types"
set_var EASYRSA_SSL_CONF        "$EASYRSA/openssl-easyrsa.cnf"
set_var EASYRSA_KEY_SIZE         4096
set_var EASYRSA_DIGEST          "sha512"
```

=== vars-file ==========

We drukken op **[Ctrl] + X** en kies '**Y**' gevolgd door [**Enter**] om het bestand op te slaan.

9. We gaan nu het systeem gereed maken voor de uitgifte van certificaten.
   `./easyrsa init-pki`

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/pki
```

10. We gaan nu 2 bestanden aanmaken, die nodig zijn voor onze certificaatserver. Dit zijn de bestanden ca.crt en ca.key.
    `./easyrsa build-ca nopass`

    We krijgen nu de vraag om een 'Common Name' in te vullen.
    De common name wordt gebruikt in de naam van het zogenaamde root-certificaat, die gebruikt zal worden voor deze server. Het is dus van belang om hier een toepasselijke naam op te geven, zoals bijvoorbeeld 'OpenVPN-server' of 'vpnserver'.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa build-ca nopass
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.............+++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:OpenVPN-server

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/pki/ca.crt
```

11. Nu gaan we een certificaat genereren, die we gaan gebruiken als certificaat voor onze OpenVPN-server.
    `./easyrsa gen-req OpenVPN-server nopass`

    Ook hier wordt gevraagd om een ‘Common Name’ op te geven. We kiezen hier [**Enter**] om de bestaande naam ‘OpenVPN-server’ te behouden.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa gen-req OpenVPN-server nopass
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Generating a RSA private key
......+++++
...............................+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-4376.2mpR86/tmp.5oNAFP'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [OpenVPN-server]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/OpenVPN-server.req
key: /etc/openvpn/easy-rsa/pki/private/OpenVPN-server.key
```

12. Nu moeten we het gegenereerde certificaat voor de OpenVPN-server signeren met het eerder gegenereerde certificaat van de certificaatserver.

    Dit doen we met het commando:
    `./easyrsa signa-req server OpenVPN-server`

    We typen ‘**yes**’ om door te gaan.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa sign-req server OpenVPN-server

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Can't open /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf for reading, No such file or directory
139715687531648:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf','r')
139715687531648:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
Can't open /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf for reading, No such file or directory
139705884624000:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf','r')
139705884624000:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 3650 days:

subject=
    commonName                = OpenVPN-server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Can't open /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf for reading, No such file or directory
139830230119552:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf','r')
139830230119552:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-604.wJguye/tmp.FFQ6W1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'OpenVPN-server'
Certificate is to be certified until Sep  4 11:58:20 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/OpenVPN-server.crt
```

13. In deze stap gaan we een zogenaamde “Diffie-Hellman key” genereren, die gebruikt zal worden voor het uitwisselen van verschillende encryptiesleutels.

    We gebruiken hiervoor het commando: **`./easyrsa gen-dh`**

    Het kan zeker een minuut of 10 duren voordat deze sleutel gegenereerd is.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Generating DH parameters, 4096 bit long safe prime, generator 2
This is going to take a long time
```

```
DH parameters of size 4096 created at /etc/openvpn/easy-rsa/pki/dh.pem
```

14. Nu gaan we een deel van de gegenereerde bestanden kopiëren naar een map waar OpenVPN ze kan gebruiken.

```
cp pki/ca.crt /etc/openvpn/server/
cp pki/dh.pem /etc/openvpn/server/
cp pki/private/OpenVPN-server.key /etc/openvpn/server/
cp pki/issued/OpenVPN-server.crt /etc/openvpn/server/
```

15. Nu gaan we de configuratie van OpenVPN zelf aanpassen.

Hiervoor openen we het configuratie-bestand /etc/openvpn/server.conf. Dit doe je met het commando: **`nano /etc/openvpn/server.conf`**

Kopieer nu onderstaande tekst en pas in ieder geval de regels onder 'Pushed routes' aan. Hier geef je aan welke subnetten zich bevinden achter de OpenVPN-server. Je kan hier meerdere subnetten opgeven.
Voorbeeld: `push "route 10.200.0.0 255.255.255.0"`

Optioneel pas je de 'OpenVPN-Server DHCP IP-range' aan wanneer deze conflicteert met andere netwerken. Dit is namelijk de reeks die de OpenVPN-server zelf gebruikt voor zijn tunnel-interface en vanuit deze reeks worden ook de IP-adressen uitgedeeld aan de VPN-clients.
Voorbeeld: `server 10.8.0.0 255.255.255.0`

=== server.conf ==========

```
port 443
proto tcp
dev tun
user nobody
group nogroup
persist-key
persist-tun
keepalive 10 200
topology subnet

# Allow client to connect multiple times
duplicate-cn

# OpenVPN-Server DHCP IP-range
server 10.8.0.0 255.255.255.0

# Pushed routes
push "route 10.200.0.0 255.255.255.0"
push "route 10.200.1.0 255.255.255.0"

# Certificates
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/OpenVPN-server.crt
key /etc/openvpn/server/OpenVPN-server.key
dh /etc/openvpn/server/dh.pem
# crl-verify /etc/openvpn/easy-rsa/pki/crl.pem

# Encryption
cipher AES-256-GCM
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-
SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA2$
auth SHA512
auth-nocache


# daemon
```

```
# Logging
log-append /var/log/openvpn.log
verb 3
```

=== server.conf ==========

We slaan de wijzigingen op met [**Ctrl**] + **X** en kiezen '**y**' gevolgd door [**Enter**].

16. Om de gemaakte wijzigingen in de configuratie door te voeren, gaan we de OpenVPN-service starten. Ook zorgen we ervoor dat deze service automatisch wordt gestart wanneer de VM wordt gestart. Dit doen we met de volgende commando's:

    `systemctl start openvpn@server`
    `systemctl enable openvpn@server`

VPN-Client aanmaken

Het is verstandig om voor elke gebruiker/apparaat een eigen certificaat aan te maken. Op deze manier kun je namelijk later ook weer certificaten van gebruikers en/of apparaten intrekken als deze niet meer nodig zijn. Op deze manier zorg je ervoor dat je Client-VPN veilig blijft.

Op deze manier maak je een VPN-client aan:

1. We start Putty of een andere SSH-client en maak verbinding naar het externe IP-adres, die je hebt geconfigureerd op de NSX Edge gateway.

2. We loggen in met het root-account.

3. En wisselen van map:
   `cd /etc/openvpn/easy-rsa`

4. We gebruik nu het commando om een certificaat voor een Client-VPN te genereren:
   `./easyrsa gen-req [naam vpnclient] nopass`

   Geef de client een herkenbare naam op de plaats van [naam vpnclient].

   Bijvoorbeeld: `./easyrsa gen-req JanJansen-VPN nopass`

   Kies [**Enter**] om de naam van de Client-VPN te bevestigen.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa gen-req JanJansen-VPN nopass

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Generating a RSA private key
.............................................++++
..............++++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-4196.ZTGMrP/tmp.sOgtoB'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [JanJansen-VPN]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/JanJansen-VPN.req
key: /etc/openvpn/easy-rsa/pki/private/JanJansen-VPN.key
```

5. Nu moeten we het certificaat voor deze Client-VPN gaan signeren.
   We gebruik hiervoor het commando:
   `./easyrsa sign-req client [naam vpnclient]`

   Bijvoorbeeld: `./easyrsa sign-req client JanJansen-VPN`

   We typen '**yes**' en kies '**Enter**' om het Client-VPN certificaat te signeren.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa sign-req client JanJansen-VPN

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Can't open /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf for reading, No such file or directory
140243646919808:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf','r')
140243646919808:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
Can't open /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf for reading, No such file or directory
140703989228672:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf','r')
140703989228672:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3650 days:

subject=
    commonName                = JanJansen-VPN


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-4219.DlMGZs/tmp.WgyuXt
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'JanJansen-VPN'
Certificate is to be certified until Sep  5 11:39:48 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/JanJansen-VPN.crt
```

6. Nu dienen we de relevante certificaten in de juiste folder neer te zetten, zodat OpenVPN deze kan gebruiken.

   We passen hiervoor de naam van de Client-VPN certificaten in de onderstaande commando's aan, zodat deze matchen met de eerder opgegeven naam.

   `cp pki/ca.crt /etc/openvpn/client/`

   `cp pki/issued/[naam vpnclient].crt /etc/openvpn/client/`
   `cp pki/private/[naam vpnclient].key /etc/openvpn/client/`

   Bijvoorbeeld:
   `cp pki/ca.crt /etc/openvpn/client/`

```
cp pki/issued/JanJansen-VPN.crt /etc/openvpn/client/
cp pki/private/JanJansen-VPN.key /etc/openvpn/client/
```

```
root@OpenVPN:/etc/openvpn/easy-rsa# cp pki/ca.crt /etc/openvpn/client/
root@OpenVPN:/etc/openvpn/easy-rsa#
root@OpenVPN:/etc/openvpn/easy-rsa# cp pki/issued/JanJansen-VPN.crt /etc/openvpn/client/
root@OpenVPN:/etc/openvpn/easy-rsa# cp pki/private/JanJansen-VPN.key /etc/openvpn/client/
```

De Client-VPN is nu aangemaakt op de OpenVPN-server.

7. We kopiëren nu alle onderstaande bestanden met een SCP-programma, zoals Wisch, naar een map op je eigen systeem:
    - ca.crt
    - JanJansen-VPN.crt
    - JanJansen-VPN.key

    Deze bestanden hebben we later nodig bij het configureren van de Client-VPN.

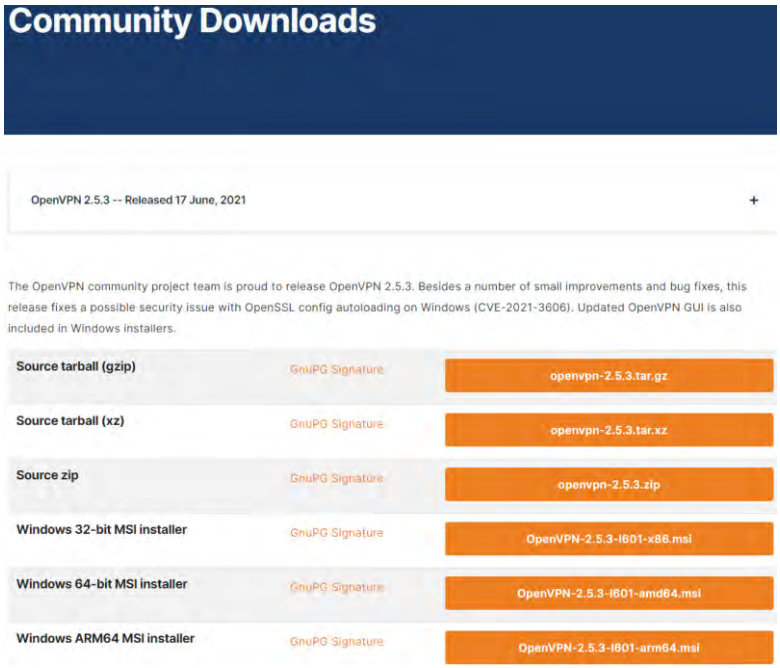
    LET OP! Ben voorzichtig met de opslag en verspreiding van deze bestanden, deze vormen de sleutel voor VPN-toegang vanaf het internet!

    De bestanden zouden op de onderstaande locaties moeten staan:
    - /etc/openvpn/easy-rsa/pki
    - /etc/openvpn/easy-rsa/pki/issued
    - /etc/openvpn/easy-rsa/pki/private

Installatie en configuratie van Windows OpenVPN-client

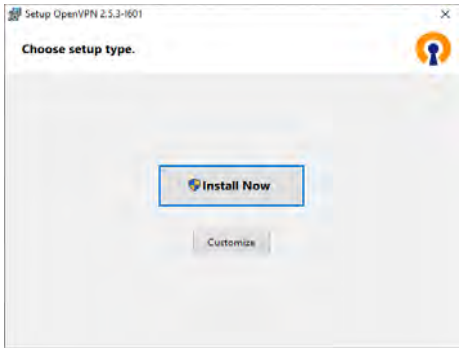
1. We loggen in op een Windows machine die we toegang willen verlenen tot onze Client-VPN. Het is belangrijk dat het account waarmee we inloggen rechten heeft om software te installeren.

2. We openen een browser en downloaden de OpenVPN Windows x64 client.
   De installatiebestanden voor de verschillende operating systems zijn te vinden op:
   https://openvpn.net/community-downloads

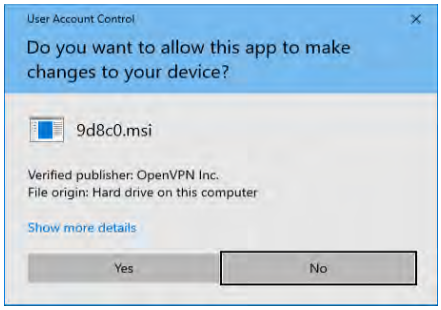


3. We starten met de installatie door te clicken op het gedownloade bestand.

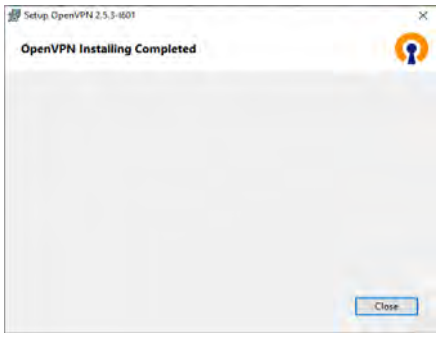
4. We kiezen voor '**Install Now**'.



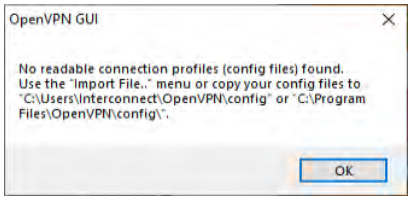
5. Als er een venster verschijnt vanuit User Account Control, kiezen we '**Yes**' om verder te gaan met de installatie.



6. Wanneer de installatie is afgerond, kiezen we '**Close**' om het scherm te sluiten.



7. De OpenVPN-client zal nu automatisch worden gestart. Mogelijk komt er een melding naar voren dat er nog geen configuratie aanwezig is. Deze melding kunnen we negeren. Kies hiervoor '**Ok**'.



8. We gaan nu een configuratie aanmaken voor onze Client-VPN.

   De standaardlocatie voor de OpenVPN-configuratiebestanden is:
   %userprofile%\OpenVPN\config

   Open deze map in verkenner.

   In deze map maken we een nieuwe map aan, waarin we de configuratiebestanden voor de Client-VPN zullen plaatsen.

9. Kopieer in de nieuw aangemaakte map nu de al opgeslagen certificaat- en sleutelbestanden.

10. We gaan nu het bijbehorende configuratiebestand aanmaken. Open hiervoor notepad.

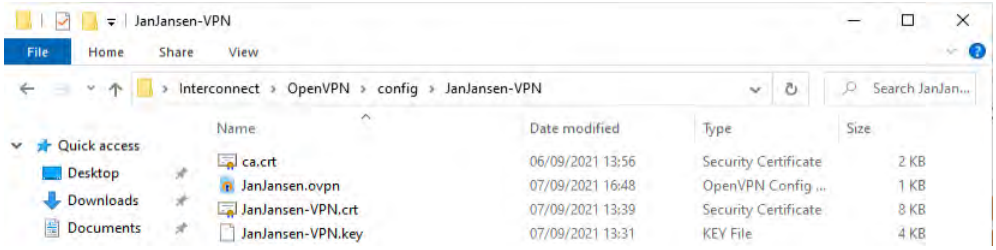
11. We passen de onderstaande waarden voor **remote**, **cert** en **key** aan en kopiëren deze naar notepad.
    In plaats van een IP-adres te vermelden als remote adres, mag hier ook een FQDN gebruikt worden.

    === JanJansen.ovpn ==========

```
client
dev tun
proto tcp
remote 212.83.222.154 443
ca ca.crt
cert JanJansen-VPN.crt
key JanJansen-VPN.key
cipher AES-256-GCM
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-
CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-
SHA256
resolv-retry infinite
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
remote-cert-tls server
```

=== JanJansen.ovpn ==========

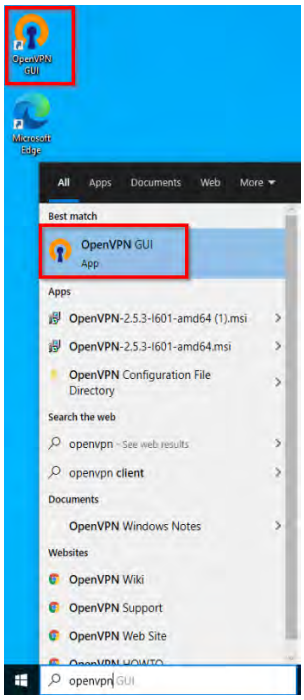
Sla dit bestand op in dezelfde map als de Client-VPN bestanden en geef deze de extensie .ovpn mee.



12. We hebben nu de Client-VPN geconfigureerd.

De Client-VPN gebruiken

1. We starten de OpenVPN-client op de Windows machine. De snelkoppeling bevindt zich standaard op het bureaublad en in het startmenu.

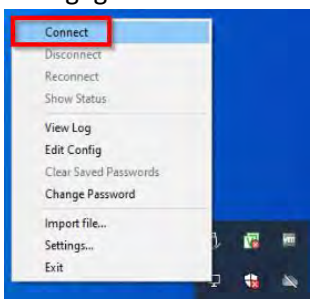


Normaal gesproken wordt de OpenVPN-client al gestart bij het starten van de desktop. Wanneer deze gestart is, vind je het icoontje hiervan langs de klok rechtsonder in het scherm.

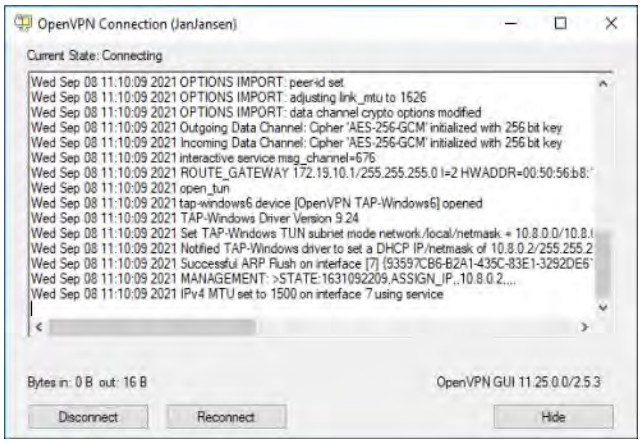
2. We klikken nu met de rechter-muisknop op het icoontje ‘OpenVPN GUI’, rechtsonder in het scherm en kiezen voor ‘**Connect**’.

   Wanneer er geen optie ‘connect’ aanwezig is, wil dit zeggen dat er iets niet goed is gegaan met de configuratie van de Client-VPN op deze machine. Het kan zijn dat er geen .ovpn-bestand aanwezig is of dat deze in de verkeerde map is geplaatst.

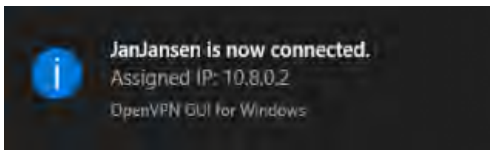
   Wanneer er meerdere client-VPN’s zijn geconfigureerd, zullen deze gegroepeerd worden weergegeven in dit menu. Kies dan eerst de betreffende VPN, gevolgd door ‘connect’.



3. De VPN-verbinding zal nu worden opgezet.

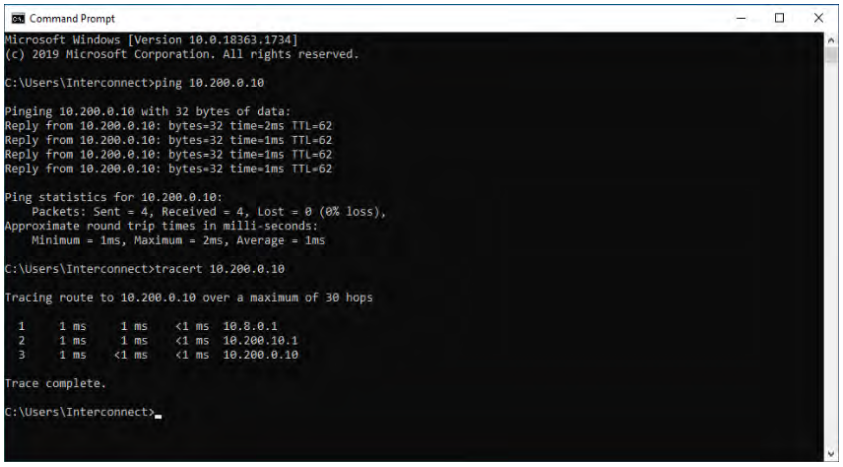


Wanneer de verbinding succesvol is opgezet, wordt hiervan een pop-up bericht getoond.

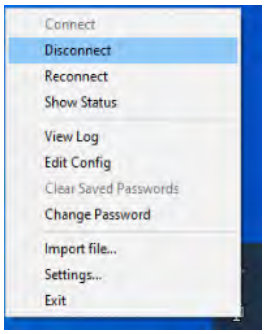


4. We zouden nu verbinding over de Client-VPN moeten kunnen maken naar IP-adressen, die zich bevinden aan de andere zijde van de VPN.

   We kunnen dit eenvoudig testen door te pingen of trace-routen naar een IP-adres aan de andere zijde.



5. Wanneer we de Client-VPN af willen breken, klikken we wederom met de rechter-muisknop op het ‘VPN GUI’-icoontje naast het klokje en kiezen we voor ‘**disconnect’**.



VPN-Client verwijderen

Wanneer we een gebruiker of apparaat om welke reden dan ook geen toegang meer willen geven tot de Client-VPN, dan zullen we hiervoor enkele zaken uit moeten voeren op de OpenVPN server.

OpenVPN maakt gebruik van een zogenaamde Certificate Revocation List (CRL), waarin wordt bijgehouden welke certificaten er ingetrokken zijn.

Afzonderlijke clients verwijderen

1. We starten Putty of een andere SSH-client en maken verbinding naar het externe IP-adres, die we geconfigureerd hebben op de NSX Edge gateway.

2. We loggen in met het root-account.

3. We wisselen nu van map:
   `cd /etc/openvpn/easy-rsa`

4. Nu draaien we voor elke client, die we willen verwijderen het commando:
   `./easyrsa revoke [naam vpnclient]`

   Bijvoorbeeld:
   ./easyrsa revoke JanJansen-VPN

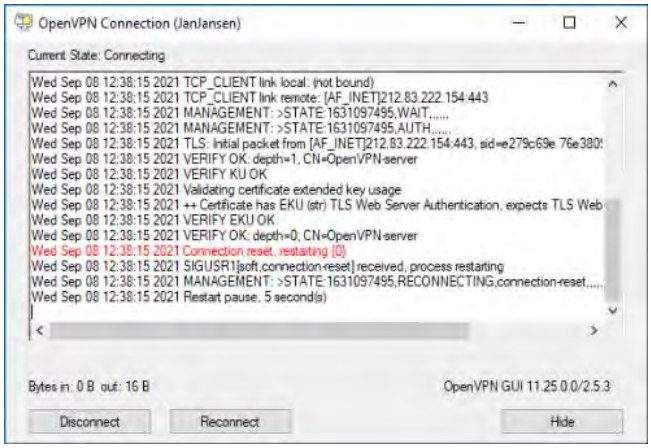
   Hierna typen we '**yes**' om het intrekken van dit certificaat te bevestigen.

```
root@OpenVPN:/etc/openvpn/easy-rsa# ./easyrsa revoke JanJansen-VPN

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019


Please confirm you wish to revoke the certificate with the following subject:

subject=
    commonName                = JanJansen-VPN


Type the word 'yes' to continue, or any other input to abort.
  Continue with revocation: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-15062.SnFUMO/tmp.lbTSq1
Revoking Certificate 4AD22DED8AB7BFAD474F9A387D1D0698.
Data Base Updated

IMPORTANT!!!

Revocation was successful. You must run gen-crl and upload a CRL to your
infrastructure in order to prevent the revoked cert from being accepted.
```

5. Wanneer we alle Client-VPN certificaten op bovenstaande manier verwijderd hebben, moeten we op basis hiervan een crl genereren. Dit doen we met het uitvoeren van het commando: **`./easyrsa gen-crl`**

6. Vervolgens herstarten we de OpenVPN service om de wijziging door te voeren. **`service openvpn restart`**

7. De clients waarvan het certificaat zojuist is ingetrokken zullen geen toegang meer hebben tot de Client-VPN. Ook actieve connecties van deze client worden direct verbroken.



Eenmalig OpenVPN configuratie aanpassen

Nadat de eerste Client-VPN certificaten zijn ingetrokken, dienen we de OpenVPN serverconfiguratie aan te passen, zodat deze in het vervolg kijkt naar welke certificaten ingetrokken zijn.

Voor deze eenmalige aanpassing voeren we het volgende uit.
Let op: doe dit niet voordat er certificaten ingetrokken zijn, want anders werkt de VPN voor geen enkele client meer.

1. We starten Putty of een andere SSH-client en maken verbinding naar het externe IP-adres, die we geconfigureerd hebben op de NSX Edge gateway.

2. We loggen in met het root-account.

3. We openen het configuratiebestand van de OpenVPN server.
   `nano /etc/openvpn/server.conf`

4. We zoeken de volgende regel op:
   ```
   # crl-verify /etc/openvpn/easy-rsa/pki/crl.pem
   ```
   en halen het '#' voor deze regel weg.
   ```
   crl-verify /etc/openvpn/easy-rsa/pki/crl.pem
   ```

   Vervolgens drukken we op de knoppen **[Ctrl] + X** en kiezen '**Y**' gevolgd door [**Enter**] om het bestand op te slaan.

5. We herstarten de OpenVPN service met commando:
   `service openvpn restart`

Onderhoud

Updaten van packages

Het is aan te raden om op de Debian-server alle geïnstalleerde packages up-to-date te houden. Hiervoor wordt geadviseerd 1x per maand het onderstaande commando te draaien als root.

`apt-get update && apt-get upgrade -y`

Meer informatie?

Als je hierover vragen hebt, dan kun je contact met ons opnemen via tel. 073 88 000 00. Of stuur een e-mail naar sales@interconnect.nl.