## 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.

# <u>Aanmaken van DMZ-netwerk</u>

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**'.

ew Organization VDC etwork	General		
1 Scope	Name =	DMZ	
2 Network Type	Gateway CIDR =	10 200 10 1/24	
3 Edge Connection	Description		
4 Genural			
	1.		
	Shared ()	©	
		CANGE	PREVIOUS. 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'.

	C Promitienplate				
Power on					
Operating System					
OS family +	Linex				_
Operating System *	Design GRU/Unui 10 (64-bit)				
Boot image	0606-110,0-07054-perce				
Compute					
Virtual CPUs	(2)				
Cores per socket	0				
Number of sockets	4				
Memory	·				
Storage 200					
ae:	2000 (1990)	1095	224		
	Storage - Sterigerd	Not Addition			
Use oustom storage	0				
Hetworking kas					
Networking i.en		Western Adapter 1 gal	IS Frace	ID Acidemia Pitro	aty fB(C)

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: <u>https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.0.0-amd64-netinst.iso.</u>

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



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

elect a language		
Choose the language ( default language for t	o be used for the installation process. The selected language will also re installed system.	o be the
Language:		
cninese (simplinea)	- 平义(间)种/	
Chinese (Traditional)	- 中文(繁體)	
Croatian	- Hrvatski	
Czech	- Čeština	
Danish	- Dansk	
Dutch	- Nederlands	
Dzongkha	- Knj	
English	- English	
Esperanto	- Esperanto	
Estonian	- Eesti	
Finnish	- Suomi	
French	- Français	
Galician	- Galego	
Georgian	- ქართული	
German	- Deutsch	

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'.

elect your location		
The selected location will be used to set your time zone locale. Normally this should be the country where you l	e and also for example to help select the sys ive.	tem
This is a shortlist of locations based on the language <b>y</b>	ou selected. Choose "other" if your location i	s not
Istea. Country, territory or area:		
Ireland		6
Israel		
New Zealand		
Nigeria		
Philippines		
Seychelles		
Singapore		
South Africa		
United Kingdom		-
United States		
Zambia		
Zimbabwe		

Odeb	ian
Select your location	
The selected location will be used to set your time zone locale. Normally this should be the country where you liv Select the continent or region to which your location belo Continent or region:	and also for example to help select the system re. longs.
Africa Antarctica Asia Atlantic Ocean Caribbean Central America	
Europe Indian Ocean North America Oceania South America other	
Screenshot	Go Back Continue

select your location	
The selected location will be used to set your tin locale. Normally this should be the country wher	ne zone and also for example to help select the system re you live.
Listed are locations for: Europe. Use the <go ba<br="">your location is not listed. Country territory or error</go>	ick> option to select a different continent or region if
country, territory of area:	
Latvia	
Liechtenstein	
Lithuania	
Luxembourg	
Macedonia, Republic of	
Malta	
Moldova	
Monaco	
Montenegro	
Netherlands	
Norway	
Poland	
Portugal	

4. We selecteren 'United States' als locales, gevolgd door 'Continue'.

Configure locales			
There is no locale de select your preferen is listed in the secor	fined for the combination of la ce from the locales available fo d column.	nguage and country you have sele In the selected language. The loca	cted. You can now le that will be used
Country to base defau	It locale settings on:		
canaua	- en_ca.orr-8		
Hong Kong	- en_HK.UTF-8		
India	- en_IN		
Ireland	- en_IE.UTF-8		
Israel	- en_IL		
New Zealand	- en_NZ.UTF-8		
Nigeria	- en_NG	<b>k</b>	
Philippines	- en_PH.UTF-8		
Seychelles	- en_SC.UTF-8		
Singapore	- en_SG.UTF-8		
South Africa	- en_ZA.UTF-8		
United Kingdom	- en_GB.UTF-8		
United States	- en_US.UTF-8		
Zambia	- en_ZM		
Zimbabwe	- en ZW.UTE-8		

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

Od	lebian 👘	
Configure the keyboard		
Keymap to use:		
American English		
Albanian		
Arabic		
Asturian		
Bangladesh		
Belarusian		
Bengali		
Belgian		
Bosnian		
Brazilian		
British English		
Bulgarian (BDS layout)		
Bulgarian (phonetic layout)		
Burmese		
Canadian French		
Canadian Multilingual		
Catalan		
Screenshot	Go	Back Continue

	Odebian	
Load installer component	from CD	
-	Loading additional components	
Retrieving libfuse2-u	leb	

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

Configure the network Network autoconfiguration failed Your network is probably not using the DHCP protocol. Alternatively, the DHCP ser or some network hardware is not working properly.	ver may be slov
Network autoconfiguration failed Your network is probably not using the DHCP protocol. Alternatively, the DHCP ser or some network hardware is not working properly.	ver may be slov

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**'.

onfigure the network	
From here you can choose server takes a long time to DHCP hostname to be sent with a hostname that you Network configuration metho	to retry DHCP network autoconfiguration (which may succeed if your DHCP o respond) or to configure the network manually. Some DHCP servers require a c by the client, so you can also choose to retry DHCP network autoconfiguratio provide. d:
Retry network autoconfig	uration
Retry network autoconfig	uration with a DHCP hostname
Do not configure the netw	ork at this time

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

configure the network		
The IP address is unique to your computer and may be: * four numbers separated by periods (IPv4); blocks of hexadecimal characters separated by colons (IPv6). fou can also optionally append a CIDR netmask (such as */24*). f you don't know what to use here, consult your network administra	itor.	

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**'.

l₹	0	debian			
Configure the network			-	-	
The gateway is an IP add also known as the defau sent through this router blank. If you don't know Gateway:	dress (four numbers sep ult router. All traffic that . In rare circumstances, , the proper answer to th	arated by periods) goes outside your you may have no ro his question, consu	that indicates the LAN (for instance outer; in that case It your network a	e gatewa , to the Ir e, you car dministra	y router, nternet) is n leave this ator.
10.200.10.1					
Screenshot			Go	Back	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**'.

Configure the network	
The name servers are used to look up host names host names) of up to 3 name servers, separated b the list will be the first to be queried. If you don't Name server addresses:	on the network. Please enter the IP addresses (not y spaces. Do not use commas. The first name server want to use any name server, just leave this field bla
8.8.8 8.8.4.4	

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

onfigure the network				
lease enter the hostn he hostname is a sing iostname should be, c ou can make somethii Vactnamo:	ame for this system. Jle word that identifies onsult your network ao ng up here.	; your system to the r dministrator. If you ar	ietwork. If you don't know e setting up your own ho	w what your ome network,
ostname: IpenVPN				

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

The domain name is the part o something that ends in .com, . something up, but make sure y Domain name:	f your Internet addres net, .edu, or .org. If y you use the same dom	s to the right of you ou are setting up a ain name on all you	r host name. It is oft home network, you ca computers.	en an make

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

ou need to set a password for 'root' vith root access can have disastrous not easy to guess. It should not be a associated with you.	, the system administrative account. A malicious or unqualified uses s results, so you should take care to choose a root password that is word found in dictionaries, or a word that could be easily
A good password will contain a mixtu 'egular intervals.	rre of letters, numbers and punctuation and should be changed at
he root user should not have an em lisabled and the system's initial use command.	pty password. If you leave this empty, the root account will be r account will be given the power to become root using the "sudo"
Note that you will not be able to see Root password:	the password as you type it.
Show Password in Clear	
lease enter the same root password	d again to verify that you have typed it correctly.
Please enter the same root password Re-enter password to verify:	d again to verify that you have typed it correctly.
Please enter the same root password Re-enter password to verify:	d again to verify that you have typed it correctly.

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**'.

Set up users and passwords				
A user account will be created for you to use inst	ead of the root	account for r	non-administrativ	e activities
Please enter the real name of this user. This info emails sent by this user as well as any program v name is a reasonable choice. Full name for the new user:	rmation will be u vhich displays o	sed for inst ruses the u	ance as default c ser's real name.	origin for Your full
Interconnect				

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

nable choice. The username should ination of numbers and more lower-

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

et up users and passwords			
A good password will contain a mixture of letters, numbers regular intervals.	and punctuation	n and should be d	hanged at
Choose a password for the new user:			
••••••			
Show Password in Clear			
Please enter the same user password again to verify you Re-enter password to verify:	ave typed it corr	ectly.	
**********			
🗌 Show Password in Clear			
🗌 Show Password in Clear			
🗆 Show Password in Clear			
🗆 Show Password in Clear			
🗆 Show Password in Clear			
□ Show Password in Clear			
Show Password in Clear			
Show Password in Clear			

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

(Ode	bian
artition disks	
The installer can guide you through partitioning a dis orefer, you can do it manually. With guided partitionir sustomise the results.	k (using different standard schemes) or, if you Ig you will still have a chance later to review and
f you choose guided partitioning for an entire disk, y Partitioning method:	ou will next be asked which disk should be used.
Guided - use entire disk	
Guided - use entire disk and set up LVM	
Guided - use entire disk and set up encrypted LVM	
Manual	
Screenshot	Go Back Continu

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

artition disks				
ote that all data on the eally want to make the c Select disk to partition:	disk yðu select will b hanges.	e erased, but not b	efore you have confirme	d that you
CSI1 (0,0,0) (sda) - 17.2 (	GB VMware Virtual di	sk		

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

artition disks		
Selected for partitioning:		
SCSI1 (0,0,0) (sda) - VMware Virtual disk: 17.2 (	B	
The disk can be partitioned using one of sever one. Partitioning scheme:	ıl different schemes. If yo	ou are unsure, choose the first
All files in one partition (recommended for nev	users)	
Separate /home partition Separate /home, /var, and /tmp partitions		
	*	

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

his is an ile systei	overvie m, mou	w of your cu nt point, etc	irrently config .), a free spa	ured ce to	partitions create pai	and mount points. Select a partition to modify its settings rtitions, or a device to initialize its partition table.
Guide	d parti	tioning				
Config	ure so	ftware RAI	D			
Config	ure th	e Logical V	olume Mana	iger		
Config	ure er	crypted vo	lumes			
Config	ure iS	CSI volume	S			
SCSI1	(0, 0, 0)	(sda) - 17.	2 GB VMwar	e Virt	ual disk	
>	#1	primary	16.2 GB	f	ext4	1
>	#5	logical	1.0 GB	f	swap	swap
Undo	change	es to nartit	lons			
Undu	partiti	ioning and	write chang	ies to	disk	
Finish		And the second second				
Finish						
Jndo	change partiti	es to partit	ions write chang	jes to	o disk	

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

artition disks	
f you continue, the changes listed l further changes manually.	pelow will be written to the disks. Otherwise, you will be able to make
The partition tables of the following SCSI1 (0,0,0) (sda)	devices are changed:
The following partitions are going to partition #1 of SCSI1 (0,0,0) (sda) a partition #5 of SCSI1 (0,0,0) (sda) a	o be formatted: is ext4 is swap
Write the changes to disks?	
) No	
9 Yes	

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

onfigure the package ma	nager
our installation CD or DV	D has been scanned; its label is:
ebian GNU/Linux 10.10.0	_Buster Official amd64 NETINST 20210619-16:11
You now have the option hese should be from the DVDs available, this step	to scan additional CDs or DVDs for use by the package manager (apt). Normall same set as the installation CD/DVD. If you do not have any additional CDs or can just be skipped.
f you wish to scan anoth	er CD or DVD, please insert it now.
Scan another CD or DVD?	
No	
). Yes	

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

onfigure the package manager	
The goal is to find a mirror of the Debian a nearby countries, or even your own, may r	rchive that is close to you on the network be aware that ot be the best choice.
Debian archive mirror country:	
Korea, Republic of	
Kyrgyzstan	
Latvia	
Lithuania	
Luxembourg	
Macedonia, Republic of	
Moldova	
Netherlands	
New Caledonia	
New Zealand	
Norway	
Philippines	
Poland	
Portugal	
Demonio	

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

Configure the package manager	
Please select a Debian archive mirror. You should know which mirror has the best Internet connect	d use a mirror in your country or region if you do not tion to you.
Usually, deb.debian.org is a good choice. Debian archive mirror:	
ftp.debian.org	
ftp.nl.debian.org	
debian.snt.utwente.nl	
mirror.nl.leaseweb.net	
deb.debian.org	
debian-archive.trafficmanager.net	
mirror.i3d.net	
debian.mirror.cambrium.nl	
ftp.debian.xs4all.net	
ftp.nluug.nl	
mirror.dataone.nl	
mirror.nforce.com	
mirror.duocast.net	
mirror.novg.net	

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

onfigure the package ma	nager			
f you need to use a HTTP Otherwise, leave this blan	proxy to access the outs k.	ide world, enter th	e proxy information here	÷
The proxy information sho HTTP proxy information (blan	uld be given in the stand k for none):	lard form of "http://	[[user][:pass]@]host[:po	rt]/".

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

Configuring popularity-contes	t
The system may anonymously packages on this system. Thi first distribution CD.	supply the distribution developers with statistics about the most used information influences decisions such as which packages should go on th
If you choose to participate, 1 to the distribution developer:	he automatic submission script will run once every week, sending statistic s. The collected statistics can be viewed on https://popcon.debian.org/.
This choice can be later modil Participate in the package usage	ied by running "dpkg-reconfigure popularity-contest". • survey?
• No	
) Yes	

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

hoose software to install one of more of the ronowing predenited conections of software.  Debian desktop environment  GNOME  Kfce  Kfce  CMDE Plasma  Cinnamon  MATE  LXOE  LXOE  LXQE  web server  SSH server  SSH server  SSH server	t the moment, only the core of the syst	em is installed. To tune the system to your needs, you can
Debian desktop environment  GNOME  Kfce  Kfce  KDE Plasma  Cinnamon  MATE  LXDE  LXQE  web server print server SSH server SSH server SSH server	Choose software to install:	owing predenned conections of software.
GNOME           Xfce           KDE Plasma           Cinnamon           MATE           LXDE           LXQt           web server           print server           SSH server	Debian desktop environment	
Xfce         KDE Plasma         Cinnamon         KATE         LXDE         LXQt         web server         print server         SSH server	GNOME	
KDE Plasma         Cinnamon         MATE         LXDE         LXDE         LXQt         web server         print server         Z SSH server	🗌 Xfce	
Cinnamon         MATE         LXDE         LXQt         web server         print server         Z SSH server	🗌 KDE Plasma	
MATE         LXDE         LXQt         web server         print server         Z SSH server	🗌 Cinnamon	
LXDE       LXQt       web server       print server       SSH server	MATE	
LXQt     web server     print server     SSH server	LXDE	
web server print server SSH server	LXQt	
grint server SSH server	web server	
SSH server	print server	
	SSH server	

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

nstall the GRUB boot lo	ader on a hard disk	¢			
t seems that this new i to install the GRUB boo	installation is the c t loader to the mas	only operating sys ter boot record of	tem on this comput your first hard driv	er. If so, it sho e.	uld be safe
Warning: If the installer nodifying the master b an be manually configu	r failed to detect ar oot record will mak ured later to boot i	nother operating s e that operating s t.	system that is press system temporarily	ent on your co unbootable, ti	mputer, 10ugh GRUE
Install the GRUB boot load	ler to the master boo	t record?			
No					
Yes					

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

on a hard disk		
r installed system bootable, b this is to install GRUB on the RUB elsewhere on the drive, ion:	y installing the GRUB boot loader of master boot record of your first has or to another drive, or even to a flo	on a bootable ard drive. If oppy.
b) a t	y installed system bootable, t o this is to install GRUB on the GRUB elsewhere on the drive, <i>ition</i> :	y installed system bootable, by installing the GRUB boot loader to this is to install GRUB on the master boot record of your first h GRUB elsewhere on the drive, or to another drive, or even to a flo tion:

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

ß	Odebian		
Finish the installation			
Installation complete Installation is complete installation media, so	e, so it is time to boot into your new s that you boot into the new system ra	system. Make sure to rem ther than restarting the i	ove the nstallation.
Screenshot		Go Back	Continue

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.



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.

** KlantX-Edge	SERVICES REDEPLO	DY SYNC SYSLOG					
General	Gateway	T Subnet	T Default Gateway	T Primary IP	7	External Network	
Configuration Gateway Interfaces IP Allocations Rate Limits	212 83 222 153	212 83 222 192/29	@ Enabled	212.83.222.154		v13820 - 212 83 222 153/29	

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.

	_		
General			
Configuration	Gateway	т	Subnet
comguration	212 02 222 152		212 02 222 152/20
Gateway Interfaces	212.03.222.133		212.03.222.132/29
IP Allocations			
Pate Limits			

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

Edge Gateway - KlantX-Edge									
Firewall	DHCP	NAT	Routing	Load Balancer	VPN	Certificates	Grouping Objects	Statistics	Edge Settings

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



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:	ТСР
Original Port:	22
ICMP Type:	[Leeg]
Translated IP/Range:	Het (interne) IP-adres van de OpenVPN Server
Translated Port:	22

pplied On:	v13820 - 212.83.2	22.153/29	11
Driginal IP/Range	212.83.222.154		
	SELECT		
rotocol	TCP		
Priginal Port	22	*	
СМР Туре			
ranslated IP/Range	10.200.10.5		4
ranslated Port	22		
ource IP Address			
ource Port			

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:	ТСР
Original Port:	443
ICMP Type:	[Leeg]
Translated IP/Range:	Het (interne) IP-adres van de OpenVPN Server
Translated Port:	443

Add DNAT Rule								
Applied On:		vi3820 - 212.83.222.153/29	1	1				
Original IP/Range		212.83.222.154						
		SELECT	- 1					
Protocol		ТСР						
Original Port		443						
ІСМР Туре								
Translated IP/Range		10.200.10.5						
Translated Port		443						
Source IP Address		1						
Source Port								
		DISCARD	KEEP	£				
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'. ▲ 'w Ver anwerd stepse.

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

Severationary Discord chenuwy

# 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'.

	~	Edge Gateways
🖽 Compute	~	
vApps		SERVICES REDEPLOY SYNC SYSLOG
Virtual Machines		Name 🛧 🕆 Status
Affinity Rules		💽 KlantX-Edge ⊘ Normal
Networking	~	
Networks		
Edges		

- We kiezen 'Firewall', normaal gesproken is dit venster al geopend. Firewall
- 5. We kiezen voor '+' om een nieuwe firewall-regel toe te voegen.
- 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 b	We geven hier een beschrijving van het doel van deze regel.					
Туре:	Kan niet aangepast v	Kan niet aangepast worden; User.					
Source:	External	External					
Destination:	Het externe IP-adres	Het externe IP-adres gekoppeld aan onze OpenVPN-server					
Service:	Protocol:	ТСР					
	Source Port:	Any					
	<b>Destination Port:</b>	22					
	Action:	Accept					

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

- 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.				
Туре:	Kan niet aangepast worden; User.				
Source:	External				
Destination:	Het externe IP-adres gekoppeld aan onze OpenVPN-server				
Service:	Protocol:	ТСР			
	Source Port:	Any			
	Destination Port:	443			
Action:	Accept				

No.	Name	Туре	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.
Туре:	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	Туре	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'.

A You have unserved shanges.

Severithempes Decord chenuwy

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 IPadres, 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 libpcsclitel libpkcsll-helperl libusb-1.0-0
  opensc opensc-pkcsll pcscd
Suggested packages:
 pcmciautils resolvconf openvpn-systemd-resolved
The following NEW packages will be installed:
  easy-rsa libccid liblzo2-2 libpcsclitel libpkcsll-helperl libusb-1.0-0
  opensc opensc-pkcsll 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/easyrsa/releases/download/v3.0.8/EasyRSA-3.0.8.tgz

- 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
- We navigeren nu naar de nieuwe EasyRSA-map: cd /etc/openvpn/easy-rsa
- 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\_COUNTRYLand waar organisatie is gevestigdEASYRSA\_REQ\_PROVINCEProvincie waar organisatie is gevestigdEASYRSA\_REQ\_CITYPlaats waar organisatie is gevestigd

EASYRSA REQ ORG Naam organisatie EASYRSA REQ EMAIL e-mailadres voor contact EASYRSA\_REQ\_OU Naam afdeling set var EASYRSA REQ COUNTRY "NT." Set\_varEASYRSA\_REQ\_PROVINCE"NL"set\_varEASYRSA\_REQ\_PROVINCE"Noord-Brabant"set\_varEASYRSA\_REQ\_CITY"'s-Hertogenbosch"set\_varEASYRSA\_REQ\_ORG"Interconnect DEV"set\_varEASYRSA\_REQ\_EMAIL"service@interconnect.nl"set\_varEASYRSA\_REQ\_OU"Interconnect DEV CA" "\$PWD" set var EASYRSA "\$EASYRSA/pki" set var 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\_varEASYRSA\_CRL\_DAYS3650set\_varEASYRSA\_NS\_SUPPORT"no"set\_varEASYRSA\_EXT\_DIR"\$EASYRSA/x509-types"set\_varEASYRSA\_SSL\_CONF"\$EASYRSA/openssl-easyrsa.cnf"set\_varEASYRSA\_KEY\_SIZE4096 set\_var EASYRSA CRL DAYS 4096 set var EASYRSA KEY SIZE set var EASYRSA DIGEST "sha512"

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.



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.

roo:@OpenYFN:/etc/openypn/easy-ras# ./easyrsa gen-dh
Note: using Easy-BSA configuration from: /etc/openymp/easy-tsa/vars Using SSL: openal OpenSSL: Ini.d 10 Sep 2019 Generating DH parameters, 4086 bit long asfe prime, generator 2 This is going to take a long time
++
++
·
·+
+
+
+
+
++
+
·
++
++++
+
+
+
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·
+
+++
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·
+.
+.
······································
DN parameters of size 4096 created at /etc/openymp/easy-rsa/pki/db.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 VPNclients.

Voorbeeld: server 10.8.0.0 255.255.255.0

```
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
```

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.
- 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.



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/<u>[naam vpnclient]</u>.crt /etc/openvpn/client/
cp pki/private/<u>[naam vpnclient]</u>.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.
- We openen een browser en downloaden de OpenVPN Windows x64 client. De installatiebestanden voor de verschillende operating systems zijn te vinden op: <u>https://openvpn.net/community-downloads</u>

Community Do	wnloads	
OpenVPN 2.5,3 Released 17 June, 202	1	+
The OpenVPN community project team is p release fixes a possible security issue with included in Windows installers.	roud to release OpenVPN 2.5.3. Besid OpenSSL config autoloading on Wind	es a number of small improvements and bug fixes, this ows (CVE-2021-3606). Updated OpenVPN GUI is also
Source tarball (gzip)	GnuPG Signature	openvpn-2.5.3.tar.gz
Source tarball (xz)	GnuPG Signature	openvpn-2.5.3.tar.xz
Source zip	GnuPG Signature	openvpn-2.5.3.zip
Windows 32-bit MSI installer	GnuPG Signature	OpenVPN-2.5.3-I601-x86.msi
Windows 64-bit MSI installer	GnuPG Signature	OpenVPN-2.5.3-I601-amd64.msi
Windows ARM64 MSI installer	GnuPG Signature	OpenVPN-2.5.3-I601-arm64.msi

- 3. We starten met de installatie door te clicken op het gedownloade bestand.
- 4. We kiezen voor 'Install Now'.

Setup OpenVPN 2.5.3-1601		×
Choose setup type.		Q
	Sinstall Now	
	Customize	

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.

Setup OpenVPN 2,5,3-601	×
OpenVPN Installing Completed	Q
	Close

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.

•	U	1 10	0	
📙 🚽 🔜 🖬 Jan	Jansen-VPN			- 🗆 🗙
File Home	Share View			~ 0
< - × ↑	Interconnect > OpenVPN > config	> JanJansen-VPN	5 ~	🔎 Search JanJan
	Name	Date modified	Туре	Size
P Quick access	a.crt	06/09/2021 13:56	Security Certificate	2 KB
- Desitop	JanJansen-VPN.crt	07/09/2021 13:39	Security Certificate	8 KB
Downloads	JanJansen-VPN.key	07/09/2021 13:31	KEY File	4 KB

- 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.

```
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
```

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

File Home	Jansen-VPN Share View					×
← → ↑ □	> Interconnect	> OpenVPN > config > J	anJansen-VPN	~	S	, Search JanJan
	Name	^	Date modified	Туре		Size
<ul> <li>Quick access</li> <li>Desktop</li> </ul>	🖌 🗔 ca.	crt	06/09/2021 13:56	Security Cert	ificate	2 KB
🕹 Downloads	🖈 🕞 Jan	Jansen.ovpn Jansen-VPN.crt	07/09/2021 16:48 07/09/2021 13:39	OpenVPN Co Security Cert	ificate	1 KB 8 KB
E Documents	🖈 🗋 Jan	Jansen-VPN.key	07/09/2021 13:31	KEY File		4 KB

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.

Current State: Connecting	
Wed Sep 08 11:10:09 2021 OPTIONS IMPORT. p Wed Sep 08 11:10:09 2021 OPTIONS IMPORT. a Wed Sep 08 11:10:09 2021 OPTIONS IMPORT. d Wed Sep 08 11:10:09 2021 Outgoing Data Channe Wed Sep 08 11:10:09 2021 Incoming Data Channe Wed Sep 08 11:10:09 2021 interactive service mag Wed Sep 08 11:10:09 2021 Incoming Data Channe Wed Sep 08 11:10:09 2021 ROUTE_GATEWAr1 Wed Sep 08 11:10:09 2021 ROUTE_GATEWAr1 Wed Sep 08 11:10:09 2021 APU-Windows Divery I Wed Sep 08 11:10:09 2021 APU-Windows Divery I Wed Sep 08 11:10:09 2021 APU-Windows Divery I Wed Sep 08 11:10:09 2021 APU-Windows Divery I	evid set
Wed Sep 08 11:10:09:2021 Nothiet TAP-Windows 10 Wed Sep 08 11:10:09:2021 Nothiet TAP-Windows Wed Sep 08 11:10:09:2021 Successful ARP Rush Wed Sep 08 11:10:09:2021 MANAGEMENT: STZ Wed Sep 08 11:10:09:2021 IPv4 MTU set to 1500	subret mode network./local/netmask = 10.8.0.0/10.8.1 driver to set a DHCP IP/netmask of 10.8.0.2/255.255.2 ninterface [7] (33597CB6-B2A1435C-83E1-3292DE6' TE:1631092209,ASSIGN_IP.,10.8.0.2, ninterface 7 using service
Ved Sep 08 11:10:09 2021 Notified TAP-Vindows Wed Sep 08 11:10:09 2021 Notified TAP-Vindows Wed Sep 08 11:10:09 2021 Natified ARP Rush Wed Sep 08 11:10:09 2021 NAAGE(MENT: ST7 Wed Sep 08 11:10:09 2021 IPv4 MTU set to 1500 <	subnet mode network/local/netmask = 10.8.0.0/10.8.1 iliverto set a DICP (P)-memask of 10.8.0.2/25.255.2 in interface [7] (93597CB6-82A1-435C-83E1-3292DE6' TE-1631092209.ASSIGN_IP, 10.8.0.2, in interface 7 using service
Wed Sep 08 11:10:09 2021 Notfied TAP-Windows Wed Sep 08 11:10:09 2021 Notfied TAP-Windows Wed Sep 08 11:10:09 2021 Notfied ARP Rush Wed Sep 08 11:10:09 2021 ANAGE(MENT-STZ Wed Sep 08 11:10:09 2021 IPv4 MTU set to 1500 <	subnet mode network/local/netmask = 10.8.0.0/10.8.1 liver to set a DICP (P)-netmask of 10.8.0.2/25.55.2 in interface [7] (93597/266-82A1-435C-83E1-3292DE6' TE-1631952202 ASSIGN_UP10.8.0.2, in interface 7 using service

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.

Command Prompt	- 0 7	×
Microsoft Windows [Version 10.0.18363.1734] (c) 2019 Microsoft Corporation. All rights reserved.		^
C:\Users\Interconnect>ping 10.200.0.10		
Pinging 10.200.0.10 with 32 bytes of data: Reply from 10.200.0.10: bytes-32 time-2ms TTL-62 Reply from 10.200.0.10: bytes-32 time-1ms TTL-62 Reply from 10.200.0.10: bytes-32 time-1ms TTL-62 Reply from 10.200.0.10: bytes-32 time-1ms TTL-62		
Ping statistics for 10.200.0.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms		
C:\Users\Interconnect>tracert 10.200.0.10		
Tracing route to 10.200.0.10 over a maximum of 30 hops		
1 1 ms 1 ms <1 ms 10.8.0.1 2 1 ms 1 ms <1 ms 10.200.0.1 3 1 ms <1 ms (1 ms 10.200.0.10		
Trace complete.		
C:\Users\Interconnect>		
		Ļ

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: opensal 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.1bTSql
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.

Current State: Connecting					
Wed Sep 06 12:38:15 20 Wed Sep 08 12:38:15 21 Wed Sep 08 12:38:15 21 Wed Sep 08 12:38:15 21	221 TCP_CLIENT link local: (not box 121 TCP_CLIENT link local: (not box 121 TCP_CLIENT link lemote: (AF 1) 221 MANAGEMENT: STATE: 1631 221 MANAGEMENT: STATE: 1631 221 TLS: thild packet from (AF JNE 221 VERIFY OK: depth=1, CN-Oper 221 VERIFY KU OK 221 VeRIFY CHICAL has EXU (str) TLS 221 VERIFY EXU OK 221 VERIFY EXU OK 221 VERIFY OK: depth=0, CN-Oper	and) NET[212.83.222.154.443 097495, WAIT 097495, AUTH 17[212.83.222.154:443, sid= 17[212.83.222.154:443, sid= 17[21].283.222.154:443, sid= 17[21].284.202.202.202.202.202.202.202.202.202.20	e279c6	9e 76e38 s TLS We	о D!
Wed Sep 08 12:38:15 20 Wed Sep 08 12:38:15 20 Wed Sep 08 12:38:15 20 Wed Sep 08 12:38:15 20	021 SIGUSR1[soft,connection:reset] 021 SIGUSR1[soft,connection:reset] 021 MANAGEMENT: >STATE:1631 021 Restart pause, 5 second(s)	received, process restarting 097495, RECONNECTING, c	onnecti	on-reset,	•••
Wed Sep 08 12:38:15 2 Wed Sep 08 12:38:15 2 Wed Sep 08 12:38:15 2 Wed Sep 08 12:38:15 2	221 SIGUSR 1[soft, connection-reset] 221 MANAGEMENT: >STATE-1631 221 Restart pause, 5 second(s)	received, process restarting 097495, RECONNECTING, c	onnecti	on-reset,	
Wed Sep 08 12:38:15 20 Wed Sep 08 12:38:15 20 Wed Sep 08 12:38:15 20	221 SIGUST Isoft connector reset. 221 SIGUST Isoft connector reset 221 MANAGEMENT: >STATE:1631 221 Restart pause, 5 second(s)	received, process restarting 097495,RECONNECTING,c	onnecti	on reset,	
Wed Sep 08 12:38:15 24 Wed Sep 08 12:38:15 24 Wed Sep 08 12:38:15 24 < < Space of the second	22 Contector reset, resulting (p) 22 IGUSR Joint connection-reset 22 MANAGEMENT: STATE: 1631 221 Restart pause, 5 second(s)	received, process restarting 097495,RECONNECTING,c OpenVPN (	onnecti GUI 11.	on reset 3 25 0.0/2.1	5.3

#### 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

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

# <u>Onderhoud</u>

#### 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 email naar <u>sales@interconnect.nl</u>.