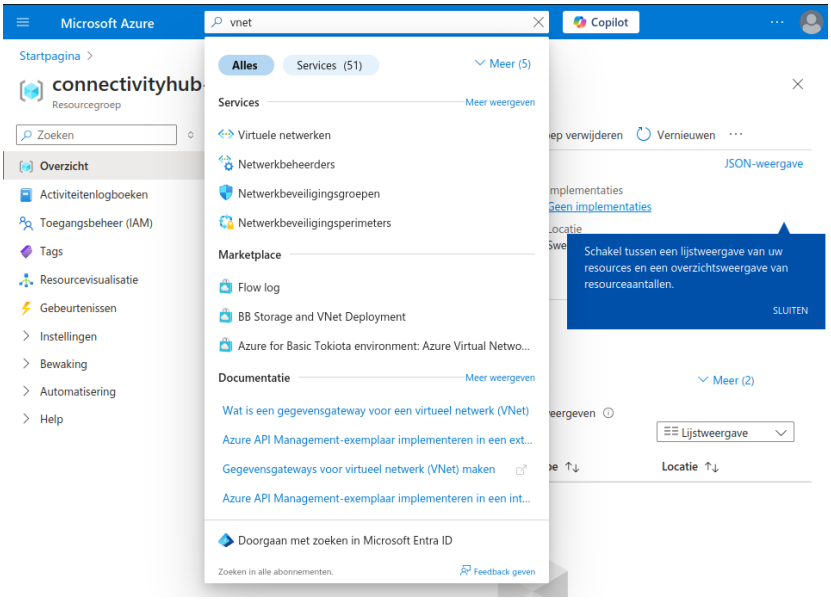
Azure VPN Gateway LAB-Guide

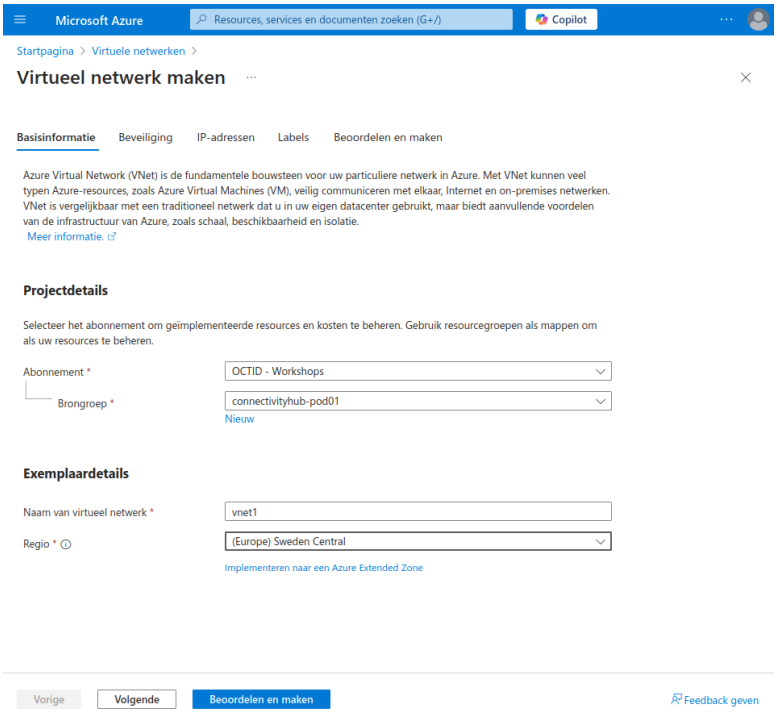
In dit lab ga je de volgende onderdelen maken in Azure:

- VNET
- Subnet
- Virtual Network Gateway
- Local Network Gateway
- Windows server om de connectivity te valideren

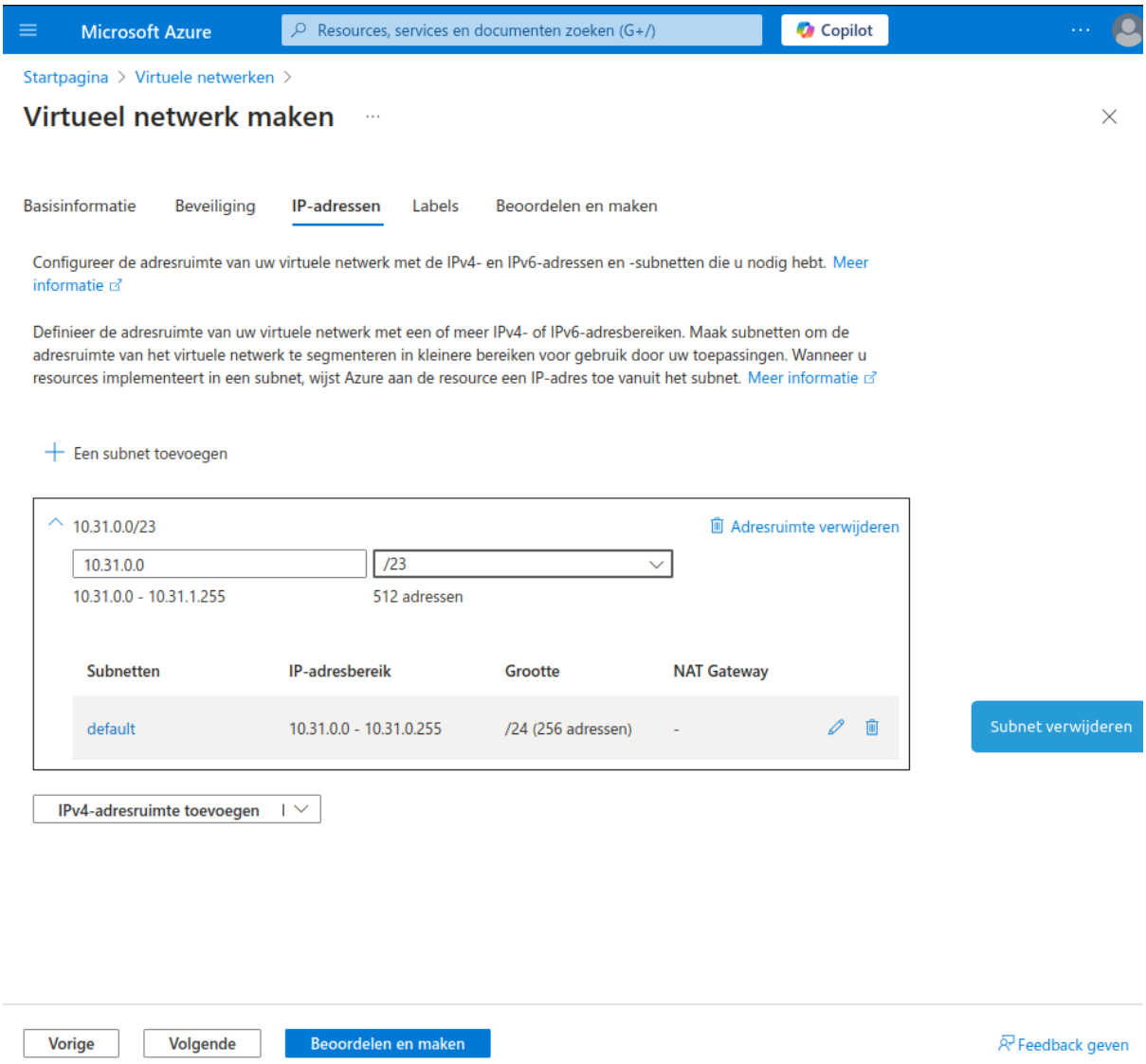
VNET & Subnet



Klik op ’Virtuele netwerken’ en maak het object ‘vnet1’ aan in locatie ‘Sweden Central’



Klik op ‘Volgende’

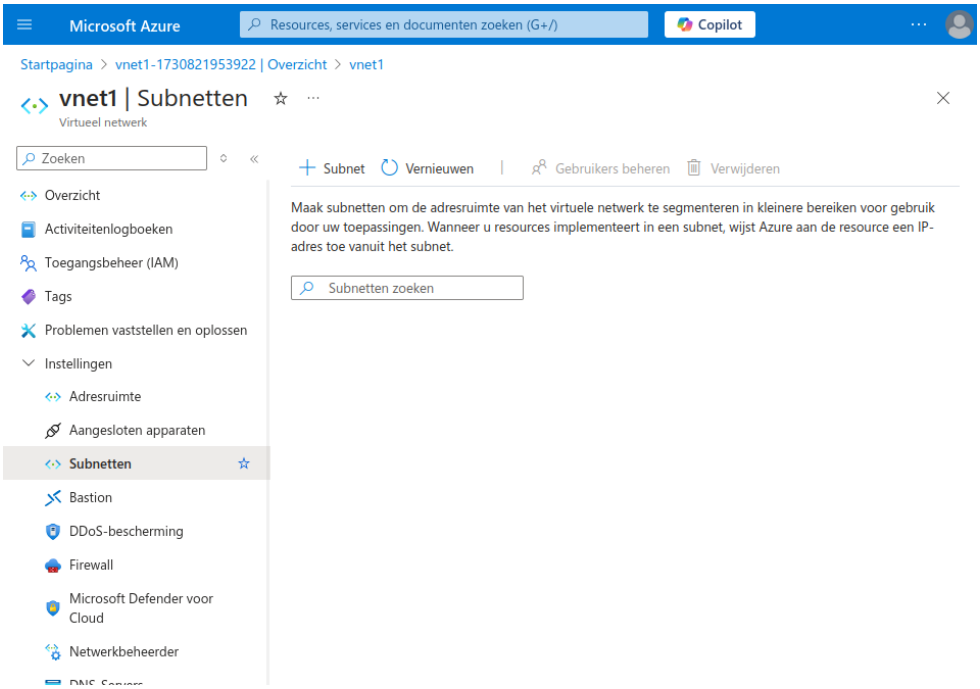


Kies hier de adresruimte die past bij je pod; 10.xx.0.0/23

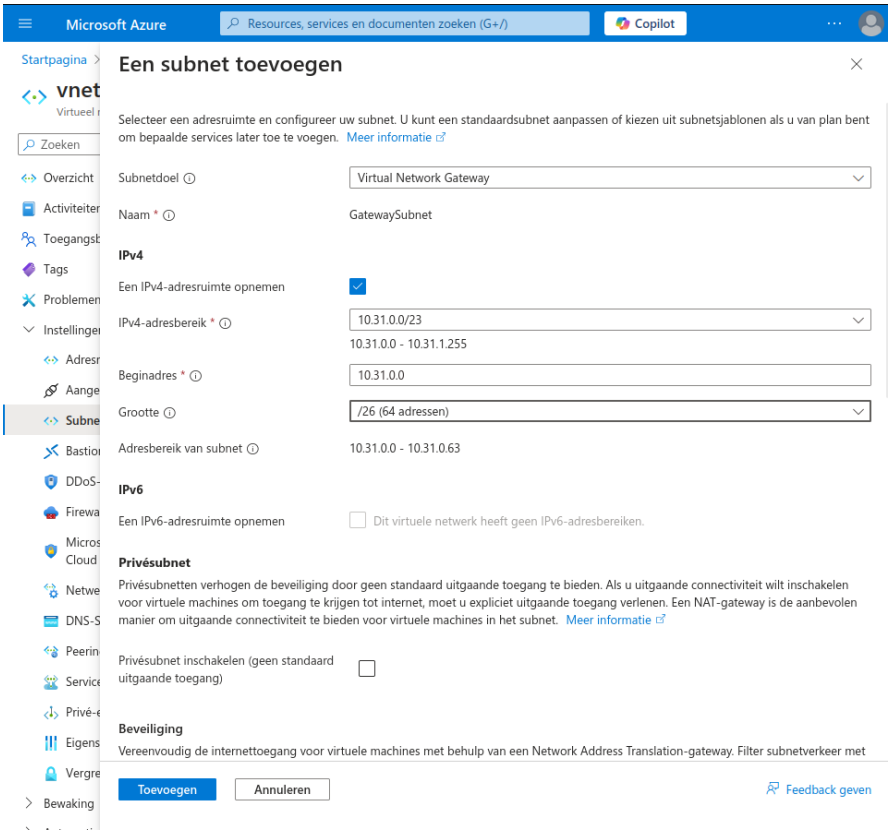
xx = 30 + Pod nummer (pod01 = 31; pod10 = 40)

Verwijder het voorgestelde subnet ‘default’ die maken we zo zelf aan.

Klik de resource open en ga naar de subnetten:

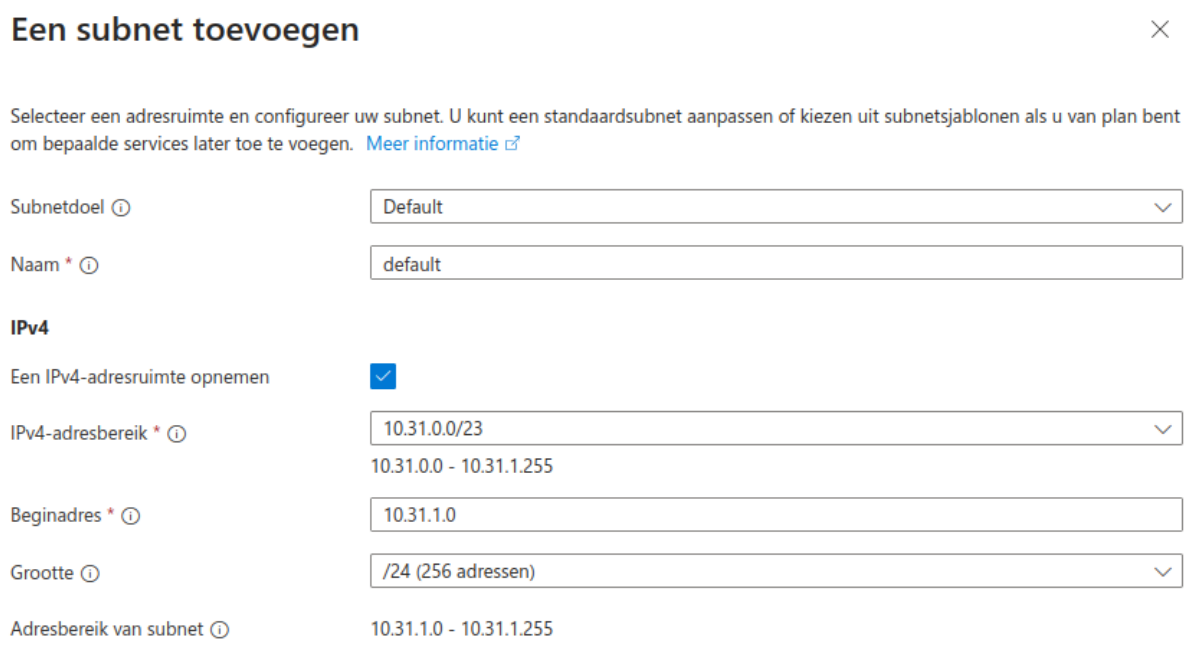


Maak hier een nieuw subnet aan van het type ’Virtual Network Gateway’



Dit is een /26 netwerk. Hierin komt de VPN gateway straks te draaien.

Vervolgens maken we nog een extra subnet aan voor de resources in Azure die we via de VPN gateway willen ontsluiten naar ons on-prem netwerk:

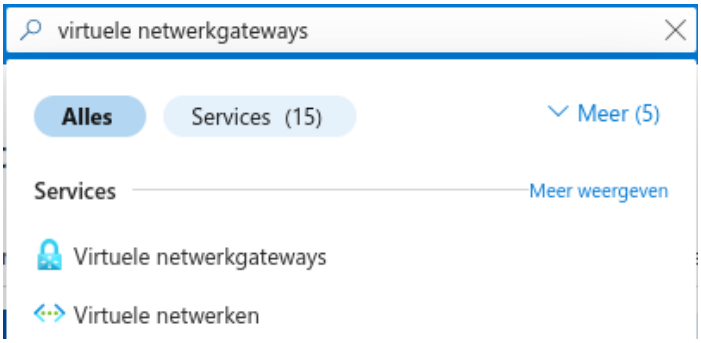


Hier kunnen we de defaults accepteren.

Dan gaan we verder met het aanmaken van de Virtuele Netwerkgateway

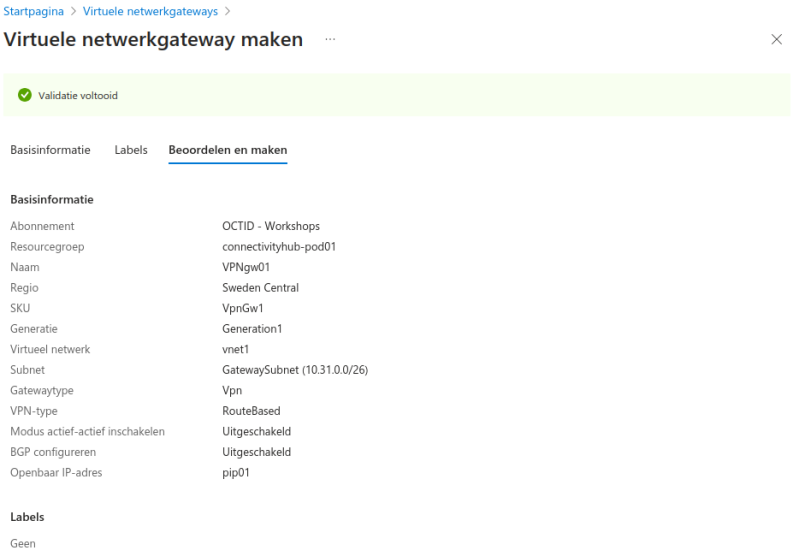
Virtuele netwerkgateway

We gaan in de portal naar het onderdeel VPN gateways en klikken op ‘Maken’



Hier kiezen we de volgende opties en dan maken we deze aan.

- Naam: VPNgw1
- Regio: Sweden Central
- GatewayType: VPN
- SKU: VpnGw1
- Generatie: Generation1
- Virtueel Netwerk: vnet1
- Subnet (automatisch geselecteerd): GatewaySubnet
- Openbaar IP-adres: Nieuwe maken
- Openbare IP-adresnaam: pip01
- Modus actief-actief inschakelen: Uitgeschakeld
- BGP configureren: Uitgeschakeld
- Toegang tot Key Vault inschakelen: Uitgeschakeld

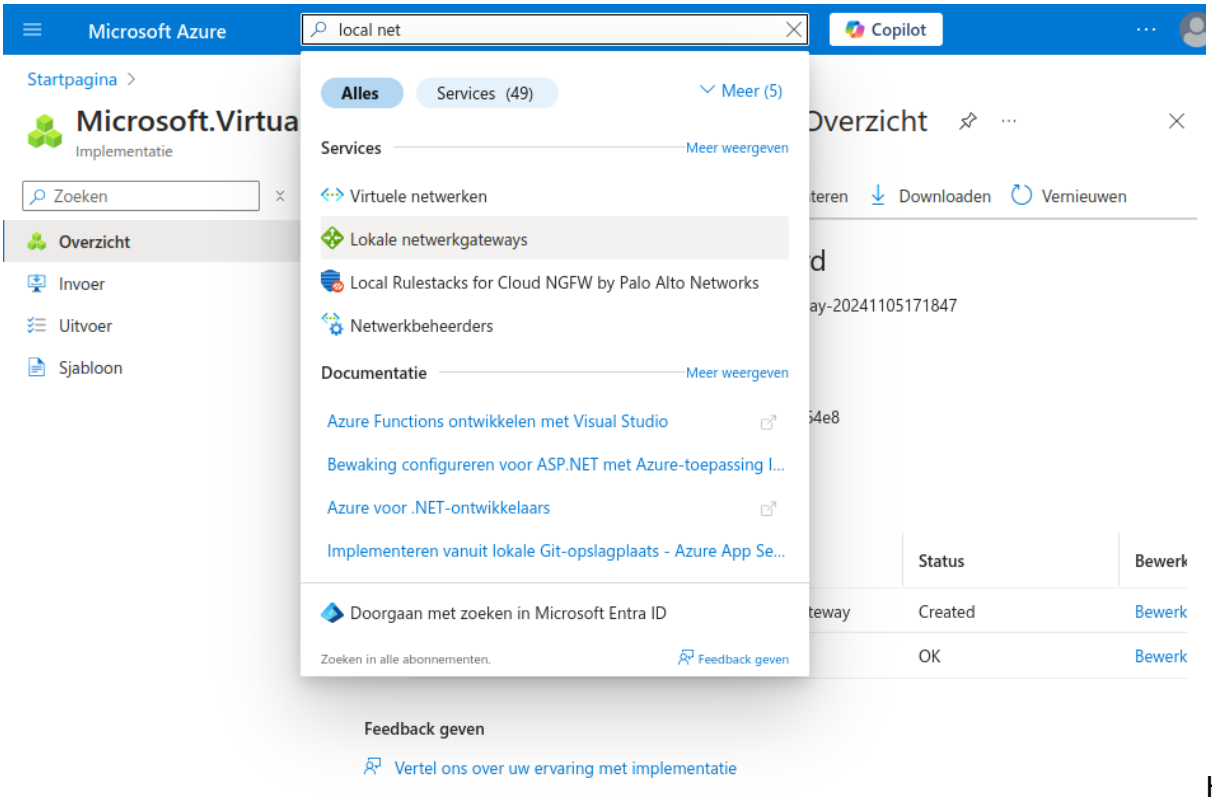


Het maken van deze VPN Gateway kan een ~10-50 minuten duren.

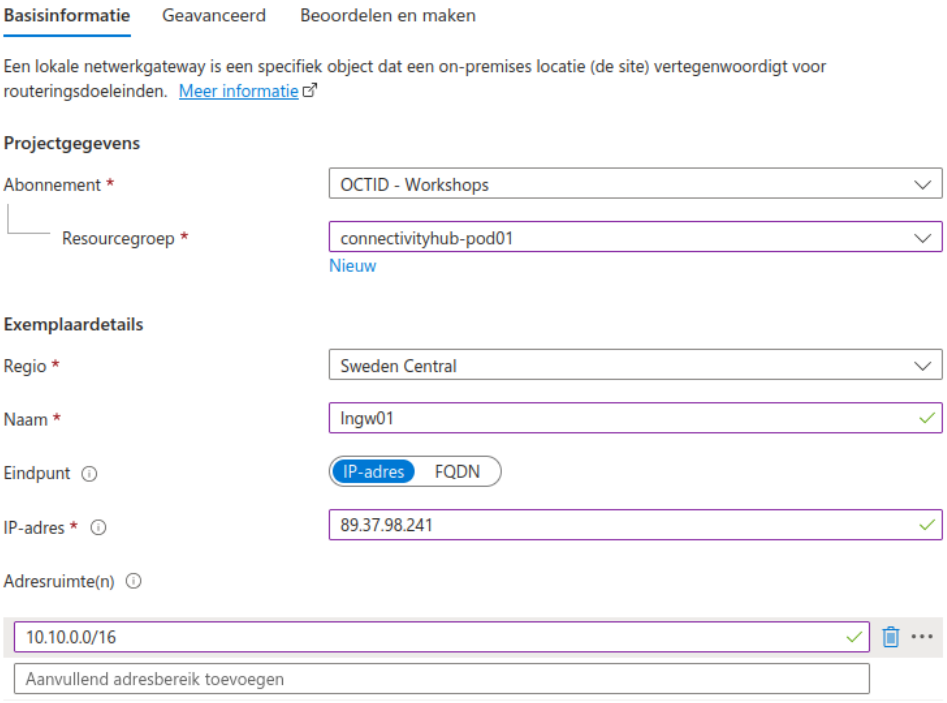
Ondertussen kunnen we de andere resources maken.

Local Network Gateway

In dit deel geven we het public IP op van onze on-prem IPSEC oplossing. Tevens wordt hier het subnet opgegeven welke achter de on-prem gateway bereikbaar is.



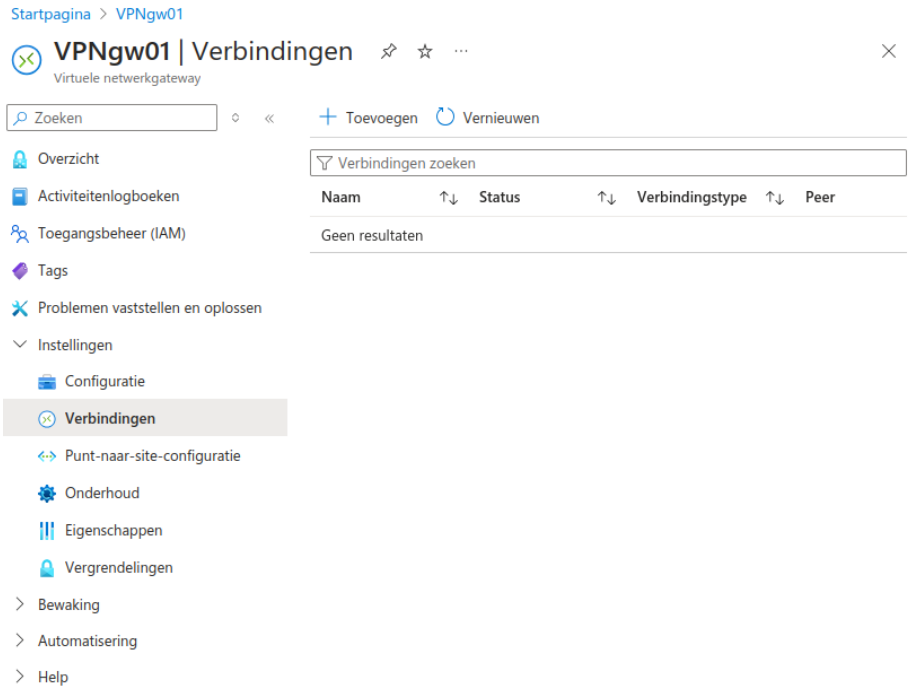
Hier maken we een nieuw object met de volgende eigenschappen:



Het IP adres is hier 89.37.98.[240 + pod nummer]

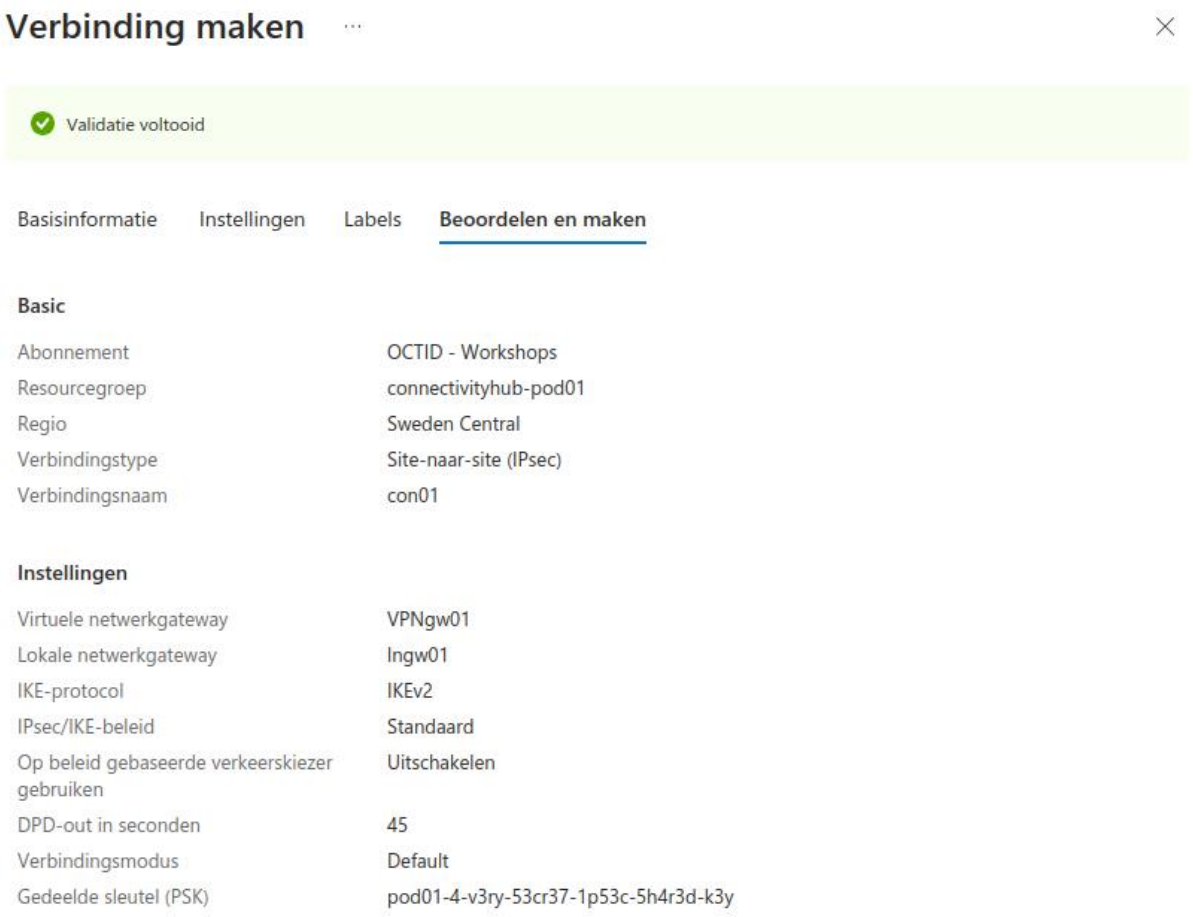
Connection van de VPN Gateway

Hier stellen we de pre-shared-key in voor de site-to-site tunnel. Deze optie komt pas beschikbaar als de VPN gateway is aangemaakt.



Maak een nieuwe verbinding aan met de opties:

- Verbindingstype: site-naar-site (IPsec)
- Naam: con01
- Virtuele netwerkgateway: VPNgw1
- Lokale netwerkgateway: lngw01
- Verificatiemethode: Gedeelde sleutel (PSK)
- Gedeelde sleutel (PSK): podXX-4-v3ry-53cr37-1p53c-5h4r3d-k3y (XX is pod nummer)
- IKE-protocol: IKEv2



Remote resources

Tenslotte willen we dan nog een resource in Azure die we kunnen benaderen vanuit on-prem of vice-versa.

Klik bijvoorbeeld een windows server 2022 aan met een eigen public IP (poort 3389 voor RDP open).

Zorg ervoor dat deze in het bestaande vnet1 komt in het ‘default’ subnet dat we hiervoor hebben gemaakt.

VPN tunnel activeren

Indien de VPN Gateway succesvol is ingericht kan je het public IP hiervan doorgeven aan mij en zal ik de fysieke router instellen zodat de tunnel online kan komen. Het zou daarna mogelijk moeten zijn om de on-prem raspberry pi te kunnen benaderen op:

http://10.10.10.10/

Alles verwijderen

Indien je tot hier bent gekomen kan je alle resources **onder** je resourcegroup verwijderen.

Indien je eerder bent afgehaakt is dit ook belangrijk voor je de volgende stap gaat zetten.

Nadat je alles onder je resource-group hebt gewist gaat de presentatie hier verder.

DevOps

Op http://tiny.cc/n3ptzz kan je de pipeline aftrappen die hoort bij je pod; hiermee worden alle resources door terraform opnieuw aangemaakt.

Zoek in de azure portal het public IP op van de VPN gateway en geef deze door aan mij.

Vervolgens is het weer mogelijk om vanuit de Windows VM via RDP de on-prem resources te benaderen.