

Use Case: OpenVPN

statische en dynamische ip adressen

Korte inleiding

VPN: Virtual Private Network

Bv.: 10.11.0.0/16

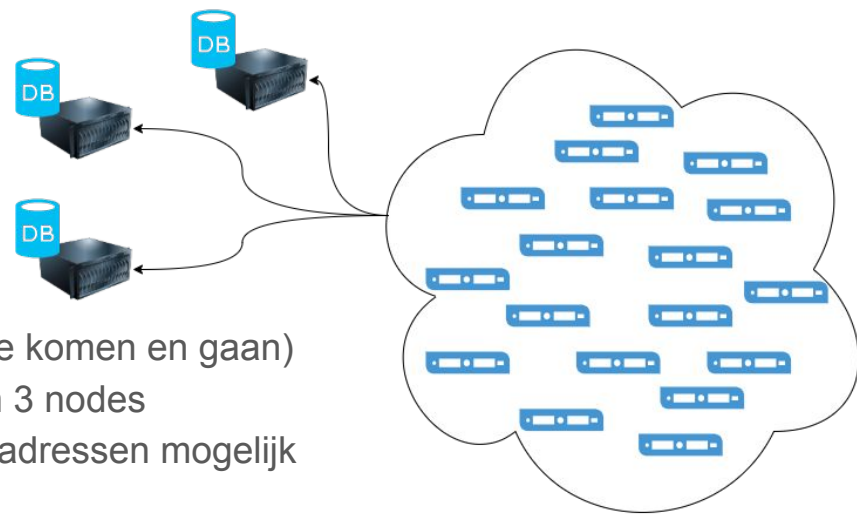
Apart interface (bv. tun0)

Veel configuratie mogelijkheden, vooral met routing.

Meest voorkomende situaties:

- **Alleen** VPN verkeer door de VPN tunnel - bv. bij een klant-server
- Juist **alles** via je VPN - bv. voor thuis: je komt dan altijd vanaf een vast IP: het publiek IP van je VPN-server
(push "redirect-gateway def1 bypass-dhcp")

Use case



- Veel clients met wisselende IP adressen (dockers die komen en gaan)
- Deze moeten connecten met een mongo-cluster van 3 nodes
- Geen authenticatie op mongo dus geen publieke IP-adressen mogelijk

Het idee: zet de clients en de 3 mongo's in een VPN.

Maar:

- De clients komen en gaan en kun je geen vast VPN-adres geven
- De drie mongos zitten in een cluster en hebben wel een vast IP-adres nodig

Nodig: een VPN-netwerk met 3 nodes met een vast IP. En alle andere nodes met een dynamische IP.

Dat gaan we configgen!

OpenVPN config

- De 3 mongos hebben eigen certificaten nodig: anders geen onderscheid
- Maak op de server een Client Config Dir: /etc/openvpn/ccd
- Dan doe je:

```
echo "ifconfig-push 10.11.0.2 255.255.0.0" > /etc/openvpn/ccd/ mongo1  
○ de naam "mongo1" moet overeenkomen met de client certificate CN ("Common Name" in de .crt)
```

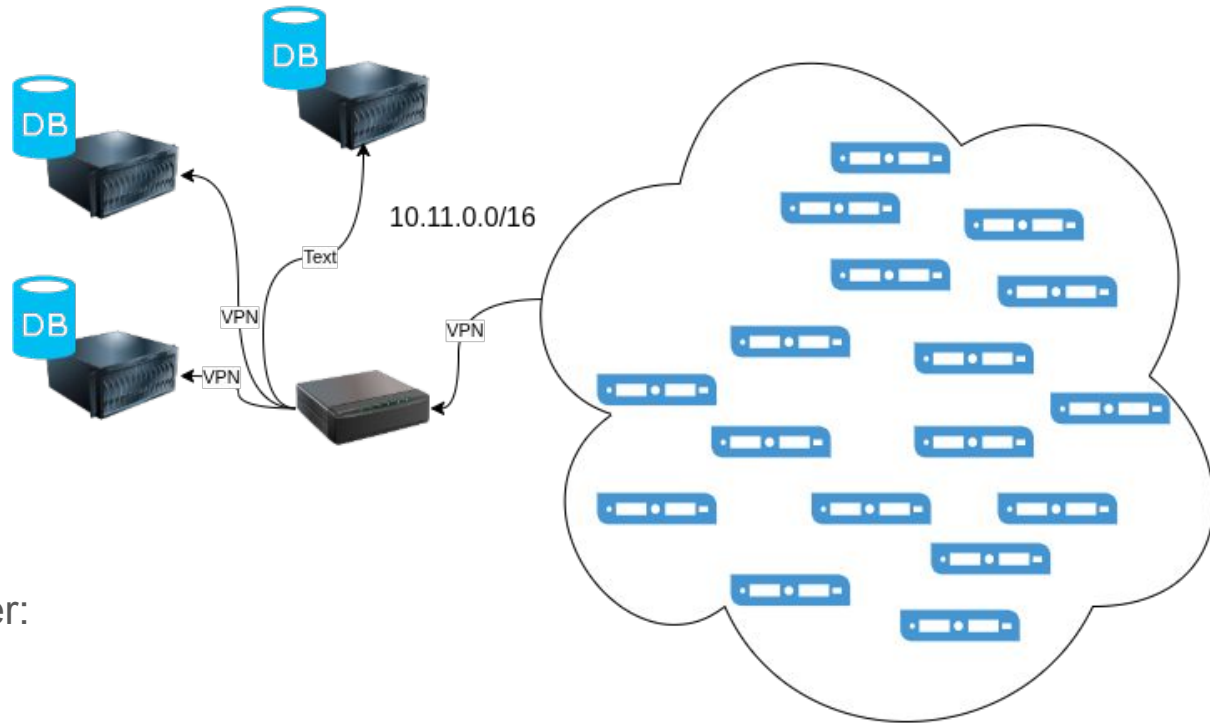
Op deze manier krijgt de client mongo1 een vast ip-adres (..).

Dan op de server in /etc/openvpn/server/cluster.conf zet je:

- dev tun (default)
- topology subnet (default)
- client-config-dir /etc/openvpn/ccd
- server 10.11.0.0 255.255.0.0 **nopool**
- ifconfig-pool 10.11.0.5 10.11.255.254 255.255.0.0
- **duplicate-cn** (deprecated...). Beter:
 - elke client eigen certificaat
 - nog steeds dezelfde certs maar met user authenticatie ("auth-user-pass").

```
systemctl enable --now openvpn-server@cluster.service
```

```
(systemctl stop|disable|mask openvpn.service)
```



Op de openvpn server:

sysctl:

```
net.ipv4.ip_forward = 1
```

In /etc/ufw/before.rules:

```
-A ufw-before-forward -i tun0 -o tun0 -j ACCEPT
```

Biertje?