

# KUBER NETES

## Inhoud

1	Voorbereiding	2
2	Maak een netwerk aan	3
3	Installeer een pfSense firewall	4
4	Configureer de firewall	6
4.1	Configureer toegang tot de firewall	6
4.2	Wijzig het standaard pfSense wachtwoord	7
4.3	NAT regel om het Kubernetes cluster bereikbaar te maken	7
5	Maak een Kubernetes cluster aan	9
6	Toegang tot het Kubernetes cluster	11

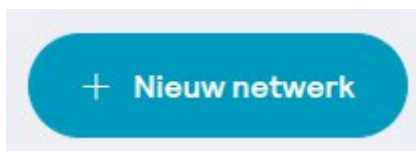
## 1 Voorbereiding

Noteer het ip-adres vanwaar je gaat verbinden met de firewall. Je kunt dit vinden via:

<https://ip.previder.nl/>

## 2 Maak een netwerk aan

Ga in de Previder Portal in het menu naar “IaaS” -> “Netwerken” en klik op “Nieuw Netwerk”.



Vul een naam in het veld “Naam van het netwerk” en kies het type netwerk “Isolated VLAN” of “Segment”. De naam van het netwerk in deze handleiding is: “Kubernetes Demo”

### Configureer het netwerk

**Naam van het netwerk**

**Klant referentie**

**Toevoegen aan groep**

**Tags**

+

**Gedeeld met**

Dit netwerk is niet gedeeld met andere klanten

**Type van het netwerk**

**Isolated VLAN**

Een gratis te gebruiken netwerk die binnen de gehele Previder IaaS omgeving gebruikt kan worden om virtuele servers met elkaar te verbinden.

**Cloud VLAN**

Een netwerk met een vast maandelijks bedrag die kan worden gebruikt om te linken naar andere diensten van Previder, zoals Managed Firewall, SaaS of Colocation.

**VLAN Trunk**

Een netwerk zonder extra kosten. Dit netwerk bevat 1 of meerdere Cloud VLAN's welke als tagged VLAN aan de virtuele server netwerkiterface gekoppeld worden. Dit netwerk bevat geen untagged VLAN.

**Segment**

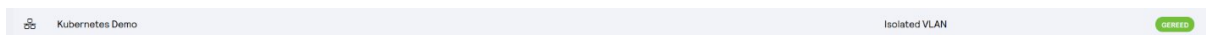
Nieuwe versie van isolated VLAN.

**Gedeelde netwerken**

Het is mogelijk om een netwerk te delen met boven en/of onderliggende klanten. Deze klanten kunnen het netwerk dan gebruiken, maar geen wijzigingen doorvoeren aan dit netwerk.

Annuleren

Wacht tot het netwerk de status “GEREED” heeft.



it starts here.

### 3 Installeer een pfSense firewall


Ga in het menu naar “IaaS” -> “Virtuele servers” en klik op “Nieuwe virtuele server”.



In stap 1 kies je voor de categorie “Linux” en in de dropdown selecteer “pfSense”.

1. Kies een besturingssysteem

☒ Linux



pfSense

In stap 2 kies je een type. “Express” is doorgaans voldoende voor dit type firewall.

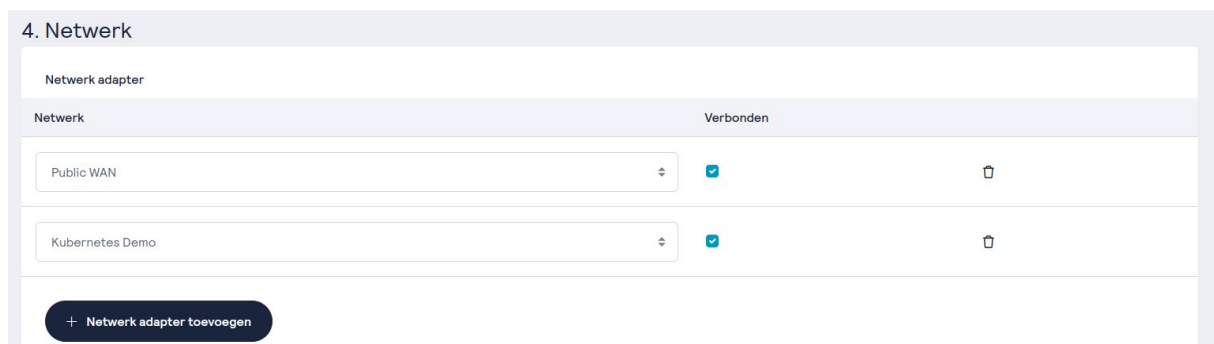
☒ Express

- Web- en applicatiehosting
- Selectie voor 1 datacenter
- Limiet tot 5000 IOPS

Geen voorkeur

In stap 3 laat je de standaard instellingen staan.

In stap 4 druk je op de knop “Netwerk adapter toevoegen” en selecteer het netwerk dat je in de vorige stap hebt aangemaakt.



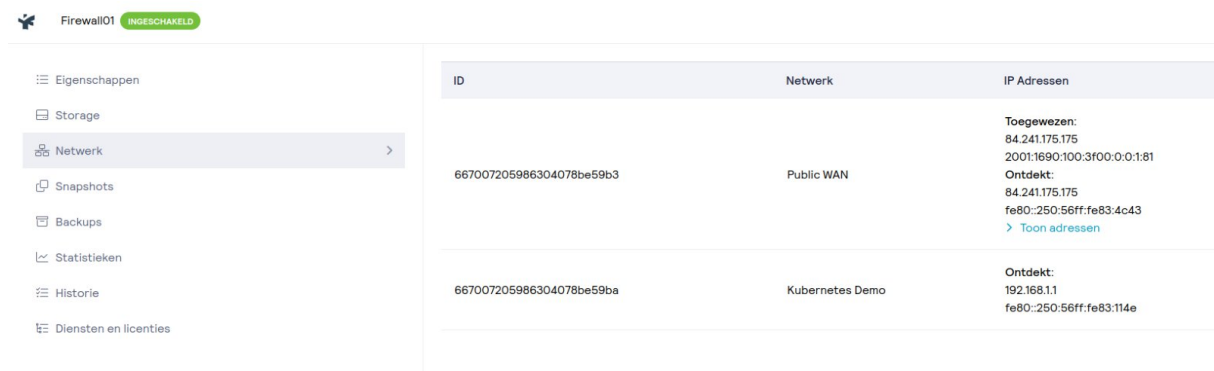
In stap 5 laat je de standaard instellingen staan.


In stap 6 vul je de naam in die deze firewall moet krijgen.

Druk op de knop “Aanmaken” om de firewall aan te maken.



Noteer het toegewezen ip-adres dat de firewall heeft gekregen in het “Public WAN” netwerk. Deze heb je straks nodig om te verbinden met de firewall.



Open de console door te klikken op het volgende pictogram (  ), wacht tot de firewall is opgestart en het pfSense menu op de voorgrond staat.

## 4 Configureer de firewall

### 4.1 Configureer toegang tot de firewall

Druk op 8 om een shell te openen. We gaan de firewall software tijdelijk uitschakelen om toegang te krijgen tot de web interface.

Voer onderstaande commando uit om de firewall uit te schakelen:

“pfctl -d”

```
WAN (wan)      -> vmx0      -> v4: 84.241.175.175/24
LAN (lan)      -> vmx1      -> v4: 192.168.1.1/24

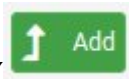
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.7.2-RELEASE][root@Firewall101.home.arpa]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@Firewall101.home.arpa]/root: █
```

Open nu een gangbare browser (Chrome, Firefox of Edge) en navigeer naar het Public WAN adres van de firewall (bijvoorbeeld: <https://84.241.175.175/>).

Log in met gebruikersnaam admin. Het wachtwoord vind je onder de eigenschappen van je virtuele server bij de tekst: Initiële login gegevens

Open in het menu “Firewall” -> “Rules” en druk op het “add” pictogram (  ) om een regel aan te maken die je toegang geeft tot de firewall.

Wijzig onder “Source” de dropdown “Any” naar “Address or Alias” en voer bij “Source address” het ip-adres in dat je hebt genoteerd bij de voorbereiding.

Wijzig onder “Destination” het veld “From” naar “HTTPS (443)”

it starts here.

**Source**

Source ☐ Invert match Address or Alias x.x.x.x /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

Destination ☐ Invert match Any Destination Address /

**Destination Port Range** HTTPS (443) From Custom To HTTPS (443) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Druk onderaan de pagina op “Save” en druk op “Apply Changes” om de wijziging door te voeren:

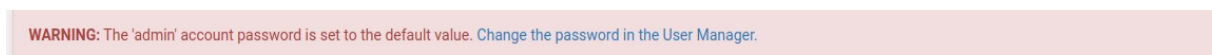


Ga nu weer naar de console van de firewall om met onderstaande commando de firewall weer te activeren:

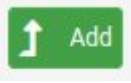
“pfctl -e”

## 4.2 Wijzig het standaard pfSense wachtwoord

Vergeet niet om het standaard wachtwoord te wijzigen:



## 4.3 NAT regel om het Kubernetes cluster bereikbaar te maken

Ga in het menu naar “Firewall” -> “NAT” en druk op het “Add” pictogram (  ) om een regel aan te maken.

Wijzig in het scherm de volgende velden:

Protocol: TCP

Destination port range:

From port: 6443

To port: 6443

Redirect target IP address: 192.168.1.220



it starts here.

Redirect target port: 6443

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Display Advanced

Destination

Invert match.

WAN address

Type

Address/mask

/

Destination port range

Other

From port

6443

Custom

Other

To port

6443

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

Type

192.168.1.220

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope",  
i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

Redirect target port

Other

Port

6443

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

Druk op Save, en Apply changes:

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

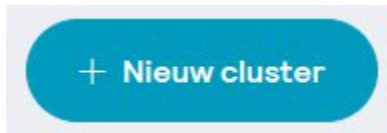
✓

Apply Changes

## 5 Maak een Kubernetes cluster aan

Ga naar Previder portal en kies in het menu voor “Kubernetes” -> “Clusters”.

Druk op “Nieuw cluster”.



Kies in stap 1 (Type) een type voor je cluster. In deze handleiding kiezen we voor “Express”.

Voer in stap 4 een cluster naam in. In deze handleiding geven we de naam: “Kubernetes Demo”.

Verifieer bij stap 5 dat onder “Installeer een CNI” de optie “Cilium” is geselecteerd.

Vink onder “Netwerk” aan dat in het netwerk DHCP en DNS aanwezig is en selecteer het netwerk dat we eerder hebben aangemaakt: “Kubernetes Demo”.

Voeg onder VIP het adres “192.168.1.220” toe en druk op “+”.

Voeg onder “Endpoints” het Public WAN ip-adres toe en druk op “+”.

5. Eenmalige instellingen

<b>Installeer een CNI in het cluster</b> Wanneer je een CNI kiest zal deze automatisch worden geïnstalleerd in je cluster. Selecteer Geen als je een eigen CNI wilt installeren.	<b>Netwerk</b> Dit netwerk zal worden gekoppeld aan alle nodes. Netwerken zijn te vinden onder IaaS.
<div>Cilium</div>	<div><input checked="" type="checkbox"/> Ik heb een netwerk aangemaakt waarin DHCP (of een IP pool) is geconfigureerd en waarin DNS beschikbaar is.</div> <div>Kubernetes Demo</div>
<b>VIP</b> Je cluster zal beschikbaar zijn op dit VIP in het gekozen netwerk. Voorbeeld: 192.168.1.10	<b>Endpoints</b> Deze hostnames zullen worden toegevoegd aan het cluster certificaat en kan worden gebruikt om verbinding te maken met het cluster. Voorbeeld: cluster01.customer.dev
<div>Item toevoegen</div> <div>192.168.1.220</div>	<div>Item toevoegen</div> <div>84.241.175.175</div>

Druk op de knop “Aanmaken” om het Kubernetes cluster aan te maken.

Wacht tot het Kubernetes cluster de status “GEREED” heeft. Dit kan enkele minuten duren.

Overzicht van je Kubernetes clusters		
Q Zoeken...		
Naam ↕	Versie ↕	Status ↕
Kubernetes Demo	1.30.2	GEREED

it starts here.

## 6 Toegang tot het Kubernetes cluster

Selecteer het Kubernetes cluster uit de lijst en navigeer naar het tabblad “Endpoints”.

Download de Kubeconfig door achter het Public WAN ip-adres op de knop “Download” te klikken.

Je kunt nu onderstaande commando gebruiken om je cluster te beheren:

```
~ $ kubectl --kubeconfig Kubernetes\ Demo-kubeconfig get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
xxxx00-kubernetesdemo-000448-n2wfg-4md54	Ready	<none>	59m	v1.30.2
xxxx00-kubernetesdemo-000448-xvqxk	Ready	control-plane	47m	v1.30.2