OPENVPN ACCESS SERVER

Maak in één avond jouw eigen VPN-verbinding

We zitten allemaal wel eens buiten ons eigen (bedrijfs) netwerk, maar op sommige momenten zou het heel prettig zijn om tóch even in het eigen (bedrijfs) netwerk te komen. Dan is het handig om in korte tijd een VPN-verbinding op te zetten en vanaf het (bedrijfs) netwerk dat te doen wat je wilde doen. **Arjan ten Hoopen**

Een VPN-verbinding opzetten, dat kan best nog wel eens wat voeten in de aarde hebben. Een VPN Client is niet moeilijk, maar een Access Server is weer hele andere koek. Ik heb me hierin een beetje verdiept en eigenlijk valt het best wel mee. Door gebruik te maken van OpenVPN en Lets Encrypt is het snel in de lucht te krijgen. Kruip achter je toetsenbord en fröbel in een avondje een OpenVPN Access Server (OpenVPN AS) in elkaar. Het enige dat je nodig hebt, is wat lef en kennis om in DNS een A-record te maken en kunde hoe je een (onbeveiligde) website opzet (ik gebruik zelf Apache, maar elke andere kan in principe ook).

Bij OpenVPN kun je de software downloaden voor diverse distributies. Ik werk met OpenSUSE maar de aangeboden OpenVPN AS is er alleen voor 13.1. Dat is wel héél lang geleden en gelukkig is er ook een bèta programma. Daar vind je een OpenVPN AS versie voor Leap 42.3. Het is bèta, maar ik heb vertrouwen in de mannen en vrouwen van OpenVPN.

Nog een kleine opmerking over de licentie behorende bij OpenVPN. Je krijgt een gratis licentie voor twee devices (clients). Mocht je meer devices willen gebruiken, dan zit hier een kostenplaatje aan vast. Voor nu komen we met twee devices een heel eind.

Eerst nog even wat grondwerk. We gaan straks gebruik maken van Lets Encrypt. Hiermee kan je op een hele makkelijke manier certificaten verkrijgen. Echter, Lets Encrypt is geoptimaliseerd om min of meer standaard (http) websites om te butsen naar een beveiligde (https) website. Wij hoeven niet persé de http-website veilig te maken, want we willen straks alleen de certificaten.

Om dit allemaal voor elkaar te krijgen, maken we in DNS een A-Record aan voor een website. In dit artikel gebruiken we als voorbeeld openvpn.mijnwebsite.nl. Het IP adres dat hierbij hoort, is het IP adres van de server waarop je de OpenVPN AS gaat installeren. Doe dit eerst voordat je verder gaat.

Download OpenVPN Access Server software van de OpenVPN website en installeer het via de packagemanager. Let op: openvpn-as niet openvpn!! OpenVPN – AS wordt geïnstalleerd in /usr/local/openvpn_as. Ga naar de bin directory en voer ovpn-init uit. Dit is de configuratie. Een leuk vraag en antwoord spelletje, maar gelukkig zijn we tevreden met alle default antwoorden met uitzondering van de vraag:

Please specify the TCP port number for the OpenVPN Daemon

Deze vraag verdient aandacht. De default is 443, maar als je ook een webserver hebt lopen met één of meer beveiligde sites (https), dan luistert de webserver ook naar deze poort. In dat geval kan je poort 443 niet gebruiken, maar moet je een andere nemen. Ik heb een webserver lopen met beveiligde sites en heb daarom gekozen voor poort 444 (en open gezet in de firewall).

Heb je geen webserver lopen (of andere programma's/deamons die luisteren naar poort 443) dan kan je met een gerust hart poort 443 kiezen. Deze, 443, moet je dus (wel) open zetten in de firewall. OpenVPN AS gebruikt ook poort 943, zet deze ook open in je firewall.

Tijdens de configuratie is een user (openvpn) aangemaakt. Deze moet nog een password

LISTING 1

```
#
# letsencrypt
#
Alias /.well-known     "/<echte-dir-op-disk>/.well-known"
#
<Directory "/<echte-dir-op-disk>/.well-known">
  Options +FollowSymLinks +Indexes
  AllowOverride None
  Require all granted
</Directory>
```

LISTING 2

```
letsencrypt-auto certonly --webroot -w /<dir-op-disk-van-de-website-minus htdocs> -d openvpn.mijnwebsite.nl
--email mijzelf@mijnwebsite.nl
```

LISTING 3

```
47 4 1,7,14,21 * * /<volle-pad>/letsencrypt-auto renew
```

hebben. Via deze user kan je niet op de linux server inloggen als gebruiker. Het is alleen een user-id voor de gebruiker van OpenVPN – AS. Maak het password voor deze user (/usr/bin/passwd) en onthoud haar goed.

We gaan nu een website bouwen voor **http://openvpn.mijnwebsite.nl**. Deze site wordt gerund door (bijvoorbeeld) Apache en bestaat alleen maar om voor ons het leven makkelijker te maken. Nog nooit eerder gedaan? El Goog is je vriend.

We gaan een certificaat aanvragen bij Lets Encrypt (meer achtergrond hierover heb je kunnen lezen in je favoriete magazine). Je hebt dadelijk een website **http://openvpn.mijnwebsite.n**l (die geserviced wordt door Apache). Bouw deze nu. De inhoud van deze website is volledig onbelangrijk. Wat wel belangrijk is, is dat er een directory is genaamd .well-known. Deze gebruikt Lets Encrypt voor het opzetten van de certificaten. Ik hou de eigenlijke website graag apart van side-effects, dus ik heb voor .well-known een alias gemaakt (zie **Listing 1**).

Herstart Apache om alle instellingen actief te maken en ga vervolgens met de browser naar **http://openvpn.mijnwebsite.nl** om te controleren of je website werkt.

We hebben nu een http website die Lets Encrypt als basis kan nemen om er https van te maken (maar het is ons te doen om de certificaten). We gaan een certificaat aanvragen (meer achtergrond hierover heb je kunnen lezen in je favoriete magazine), te zien in **Listing 2**.

Nadat je dit succesvol hebt afgerond, heb je de certificaten gekregen in de directory /etc/letsencrypt/live/openvpn.mijnwebsite.nl. De certificaten hebben een beperkte levensduur (3 maanden) dus zorg er ook voor dat je op gezette tijdstippen (in de cron) letsencrypt-auto uitvoert om het certificaat te vernieuwen (zie **Listing 3**).

Bovenstaande cron entry renewed elke week, dit is met name handig als je meerdere certificaten gebruikt van Lets Encrypt.

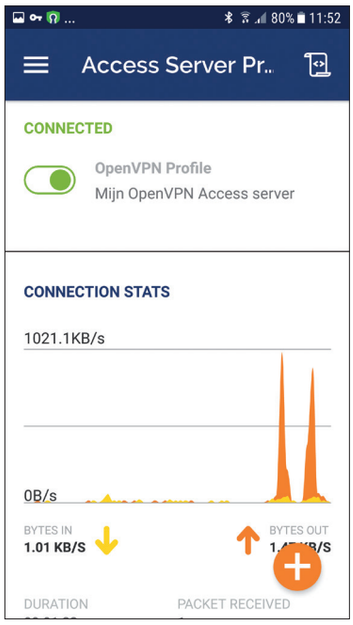
De certificaten die OpenVPN AS gebruikt, staan in /usr/local/openvpn_as/etc/web-ssl/. In de documentatie staat hoe je via de Admin UI of via de backend certificaten plaatst. Maar dit vereist ouderwets handwerk en daar willen we natuurlijk van af. Een andere vrolijke knutselaar heeft hier ook mee zitten worstelen. Zijn script houden we aan; alleen omgezet naar systemd tijden (zie **Listing 4**).

Deze commando's moet je nog samenvatten in een scriptje en (in de cron) uitvoeren op gezette tijden (levensduur van certificaat is 3 maanden). Speciale aandacht voor de "> /dev/null". Als je die weglaat, dan komt je private key op je scherm (of in de mail als je het door cron laat uitvoeren). Dit wil je niet. Dus zorg dat er "> /dev/null" staat.

We benaderen nu Admin WebUI via **https://openvpn.mijnwebsite.nl:943/admin** (de normale User WebUI is te benaderen via **https://openvpn.mijnwebsite.nl:943**). Het is tijd voor de laatste puntjes op de i. Log op het Admin UI in als openvpn met het password dat je goed onthouden hebt. Ga via Configuration naar de Network Settings. Zet hier de Hostname naar openvpn.mijnwebsite.nl. Kies Save Settings, kies Update Running Server.

Ga nu via Configuration naar Web Server en controleer of hier openvpn.mijnwebsite.nl staat en of de certificaten hierbij horen. De server is nu klaar voor gebruik. Dan nog een VPN-verbinding opzetten. Bijvoorbeeld vanaf een Android telefoon. Installeer op de telefoon OpenVPN Connect (uit de Play Store). Start deze op en selecteer de optie om met een Access Server te verbinden.

Vul de gevraagde gegevens in en check de checkbox voor Import autologin profile. Kies vervolgens Add, zet haar vervolgens aan en geef je wachtwoord. You are in business! Veel plezier van je VPN-verbinding.



LINKS

https://openvpn.net/index.php/access-server/download-openvpn-as-sw.html
https://docs.openvpn.net/openvpn-access-server-beta-program/
http://www.linuxmag.nl/2-algemeen/949-let-s-encrypt-simpel-een-gratis-certificaat
https://sideras.net/2016/02/24/lets-encrypt-https-certificates-for-openvpn-as-access-server/

LISTING 4

```
/usr/bin/systemctl stop openvpnas
/usr/local/openvpn_as/scripts/confdba -mk cs.ca_bundle -v "`cat /etc/letsencrypt/live/openvpn.mijnwebsite.nl/
fullchain.pem`"
/usr/local/openvpn_as/scripts/confdba -mk cs.priv_key -v "`cat /etc/letsencrypt/live/openvpn.mijnwebsite.nl/priv-
key.pem`" > /dev/null
/usr/local/openvpn_as/scripts/confdba -mk cs.cert -v "`cat /etc/letsencrypt/live/openvpn.mijnwebsite.nl/cert.
pem`"
/usr/bin/systemctl start openvpnas
```