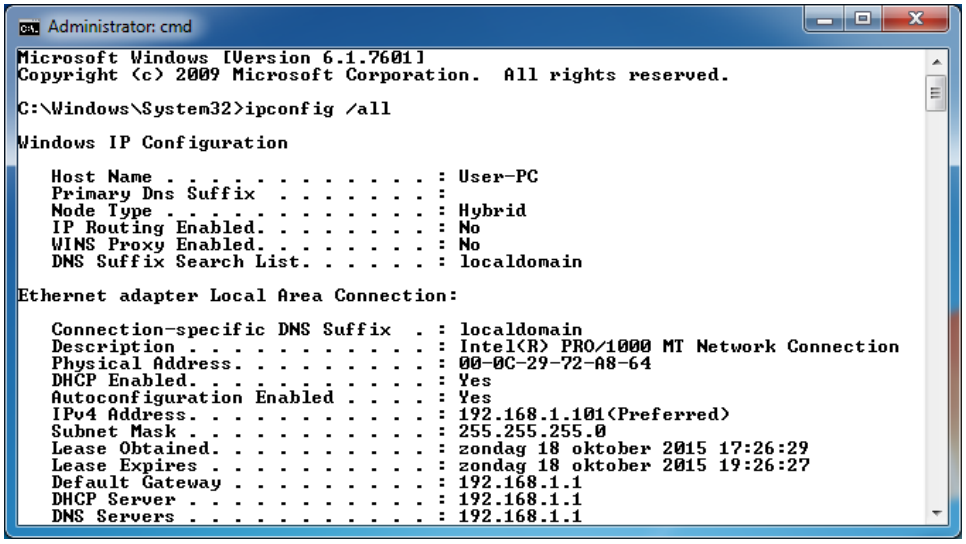
Configuratie van VPN met OpenVPN

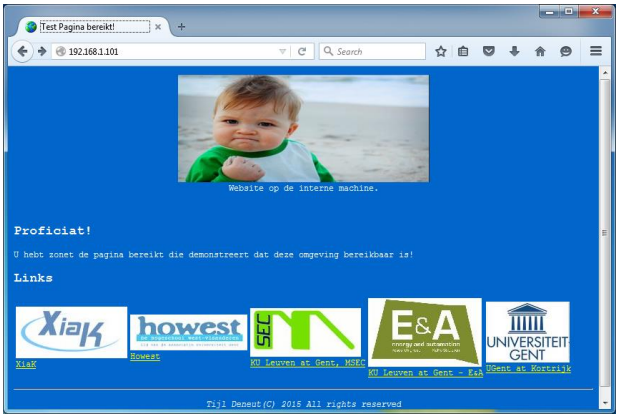
Met pfSense als Firewall/Router

Voorbereiding (Windows 7 op lokale netwerk)

- Bekijk eerst of de machine correcte netwerkgegevens heeft verkregen van de pfSense router:
  - Open cmd en typ *ipconfig /all*



- Indien deze gegevens niet overeenkomen zoals verwacht, moeten de (virtuele) netwerkaansluitingen gecontroleerd worden en een nieuw IP adres aangevraagd:
  - In Windows 7 cmd: *ipconfig /release & ipconfig /renew*
- Indien alles in orde is, probeer dan even of de **lokale webserver** naar behoren werkt:
  - Open een browser (bijv. Firefox) en surf naar het IP adres van de Windows 7 machine
    http://192.168.1.101
    -> Ook http://127.0.0.1 zou moeten werken

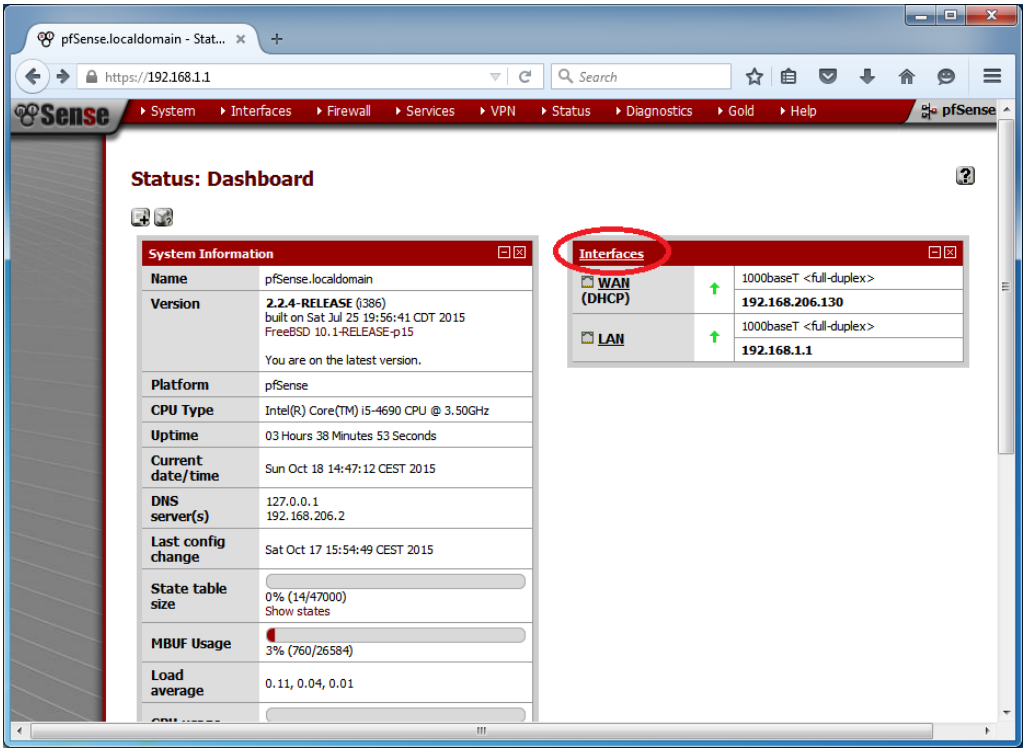


Configuratie pfSense (vanaf de Windows 7 machine op lokale netwerk)

➔ We wensen van buitenaf een VPN te leggen naar het interne netwerk zodat elk toestel op dit netwerk bereikbaar is. Als voorbeeld nemen we de website op de Windows 7 machine.

➔ Het doel is om ***door middel van OpenVPN client software*** een zo veilig mogelijke VPN verbinding te kunnen opzetten.

- Open een browser (bijv. Firefox) en surf naar het IP adres van de router om deze te kunnen configureren.
  - http://192.168.1.1, klik op “I Understand the Risks”, “Add Exception…” en “Confirm Security Exception”.
  - Log in met de standaard gegevens Username: *admin* en Password: *pfsense*
- Aangekomen op de hoofdpagina het Dashboard kan worden geklikt op de link “Interfaces” om een overzicht te verkrijgen van alle IP-gegevens op elke netwerk interface.
  -> Het WAN IP zal later nodig zijn om de VPN te gebruiken.

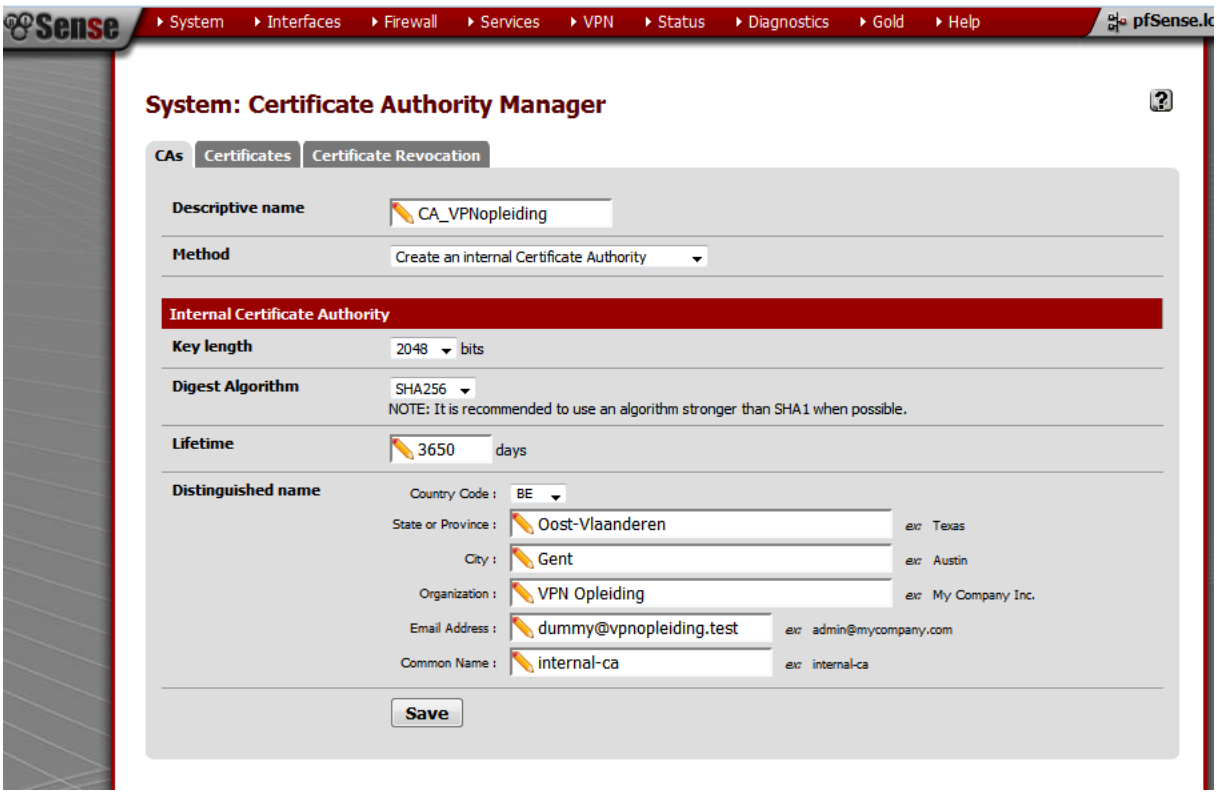


X509 Certificaten

- Voor de *authenticatie* van de clients die de OpenVPN tunnel zullen gebruiken moeten *certificaten* gecreëerd worden. Deze certificaten moeten ondertekend zijn door een *Certificate Autority (CA).* Certificaten kunnen aangekocht of zelf opgesteld worden (self-signed). Pfsense heeft de mogelijkheid om zelf CA's en certificaten op te stellen.

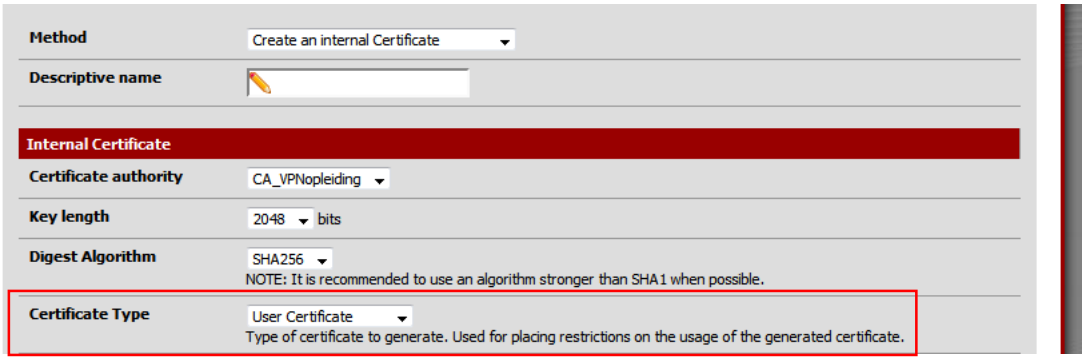
Creatie Certificate Authority

- Onder System -> Cert Manager kan een eigen CA aangemaakt worden via 
- Kies voor ***Create an internal Certificate Authority*** en vul alle velden in. Belangrijk zijn de Key length, Lifetime en Digest algoritme (welke encryptie er gebruikt wordt).

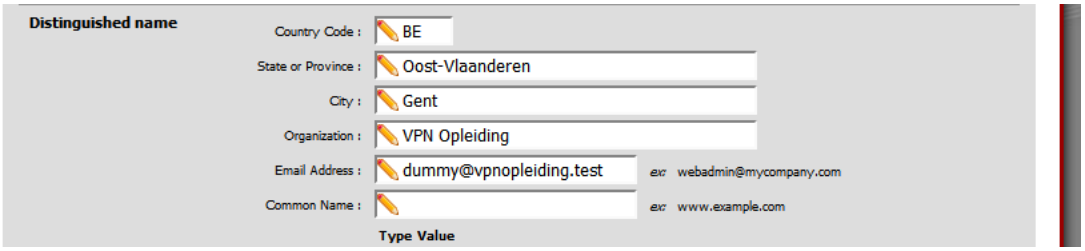


Creatie Certificates

- De nodige certificaten kunnen gecreëerd worden via het tabblad Certificates op  te klikken
- Kies voor ***Create an Internal Certificate*** en selecteer de CA die de certificaten moet ondertekenen
- Er is minstens ***1 server certificaat en 1 user certificaat*** nodig (1 user certificaat per concurrent client)



- Kies een logische common name, bvb: Cert_Naam
- De andere velden mogen ingevuld worden met om het even welke info
- Save telkens de certificaten alvorens een nieuw aan te maken



OpenVPN server configureren

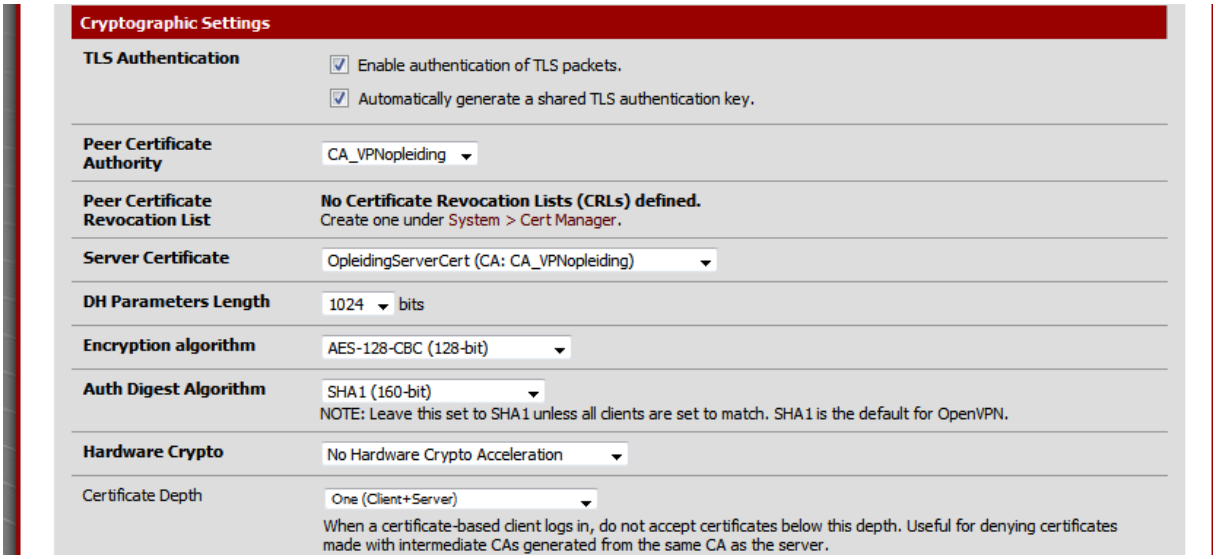
- Ga bovenaan via *VPN* naar *OpenVPN* en voeg een nieuwe **server** toe door op de corresponderende knop te klikken: 

General information

- Kies voor ***Remote access (SSL/TLS)***. Op die manier wordt er gekozen om gebruik te maken van certificaten om de remote clients te authenticeren.
- De andere velden mogen standaard blijven

Cryptographic Settings

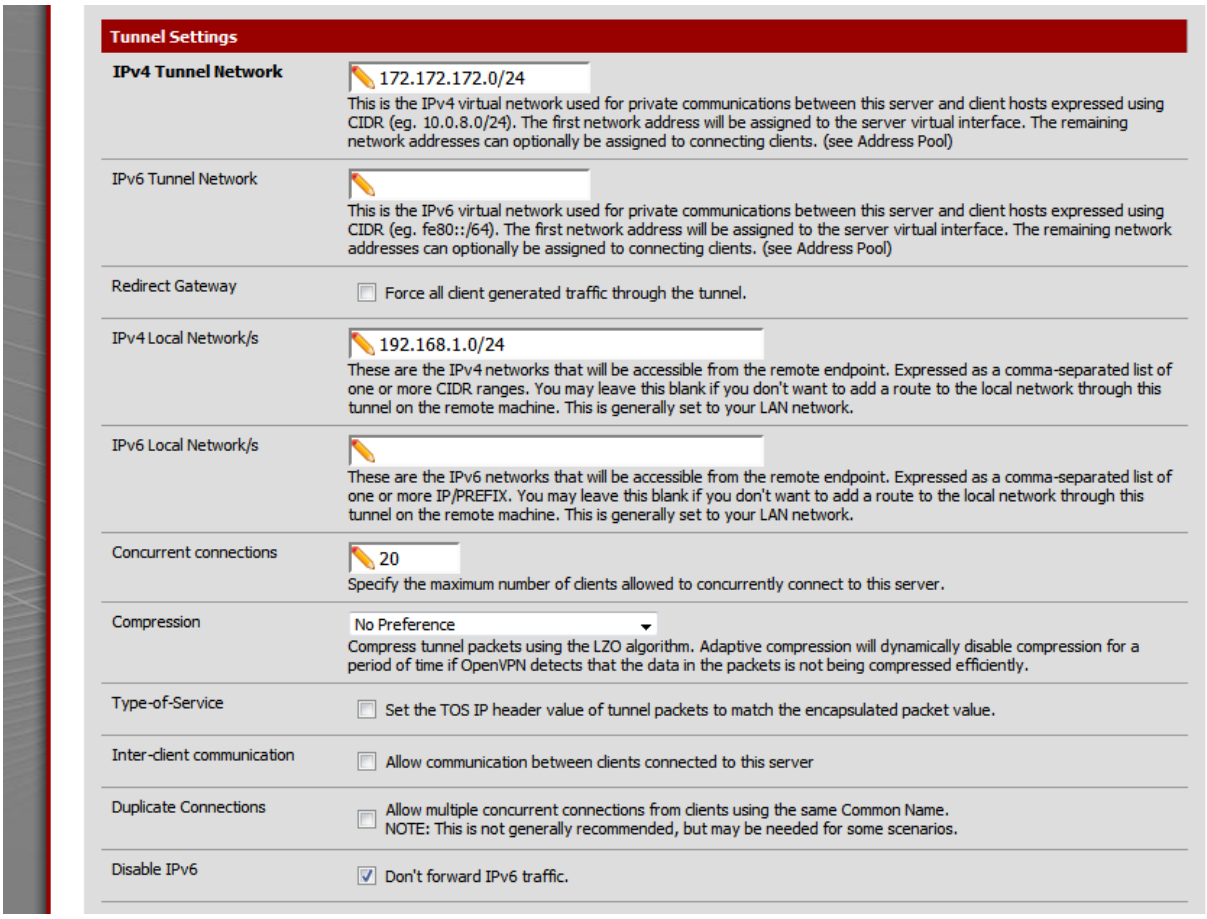
- Kies de gewenste CA die de OpenVPN server zal gebruiken voor het **valideren van de client certificaten** en stel het certificaat in die de server zelf moet gebruiken
- Andere settings mogen blijven staan, maar moeten wel overeenkomen met de mogelijkheden van de clients



Tunnel setting

- Een tunnel houdt in dat een **apart netwerk gecreëerd wordt** tussen twee punten, er moet dus een nieuw netwerk verzonnen worden.
  Hier wordt gekozen voor **172.172.172.0 /24** als netwerk voor de tunnel. Het eerste IP wordt gereserveerd als adres voor de ***OpenVPN Server*** binnen de tunnel (dus voor de pfsense router zelf). OpenVPN clients kunnen optioneel een ander IP adres binnen dit subnet toegewezen krijgen. *Dit netwerk moet een uniek* zijn, het mag nog nergens anders in het bestaande netwerk of in de routing tabellen bestaan.

- Er moet ook nog gedefinieerd worden welk **lokaal netwerk** bereikbaar moet zijn door de tunnel. Indien dit blanco blijft kan er door de tunnel enkel gecommuniceerd worden met de router en niet met zijn onderliggend netwerk.
- Alle IPv6 instellingen mogen overgelaten worden want IPv6 wordt uitgeschakeld via de laatste parameter
- Redirect Gateway niet aanvinken om ervoor te zorgen dat **enkel verkeer voor het lokale netwerk** via de tunnel gaat. Aanvinken zorgt ervoor dat alle verkeer van de clients via de tunnel gaat (zie LL2P IPsec)
- Het maximum aantal gelijktijdige client connecties invullen
- Andere instellingen mogen blijven

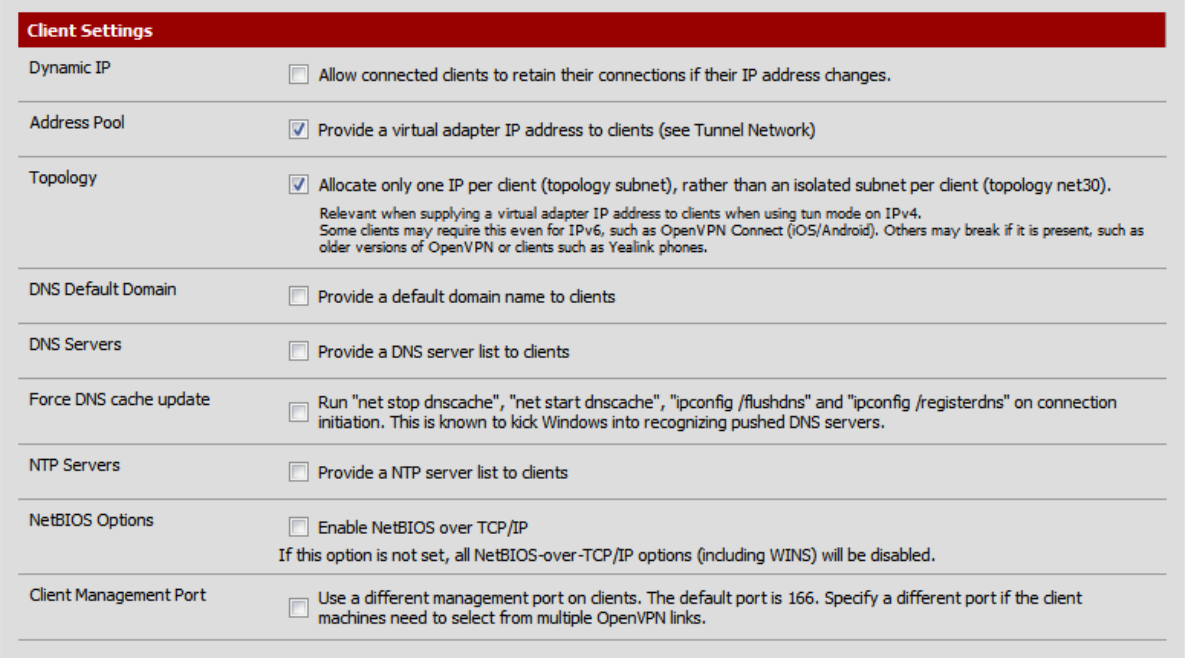


Client settings

- **Dynamic IP** laat toe dat de VPN connectie behouden blijft (automatisch opnieuw opgesteld wordt), indien het publiek IP adres van de client verandert. Dit kan nuttig zijn voor mobile clients die overschakelen naar 3G/4G indien hun wifi signaal wegvalt.
- **Address Pool** aanvinken om ervoor te zorgen dat de clients een IP adres voor binnen de tunnel toegewezen krijgen van de OpenVPN server. De adres range wordt bepaald uit de Tunnel Network instelling
- Sommige (oudere) clients vereisen een **geïsoleerd subnet** binnen een tunnel, ze verwachten hierbij een /30 netwerk waarbij de server het 1ste en de client het 2de IP krijgt. Clients zitten dan telkens in een aparte tunnel en kunnen elkaar onderling niet zien. Bij de **subnet**

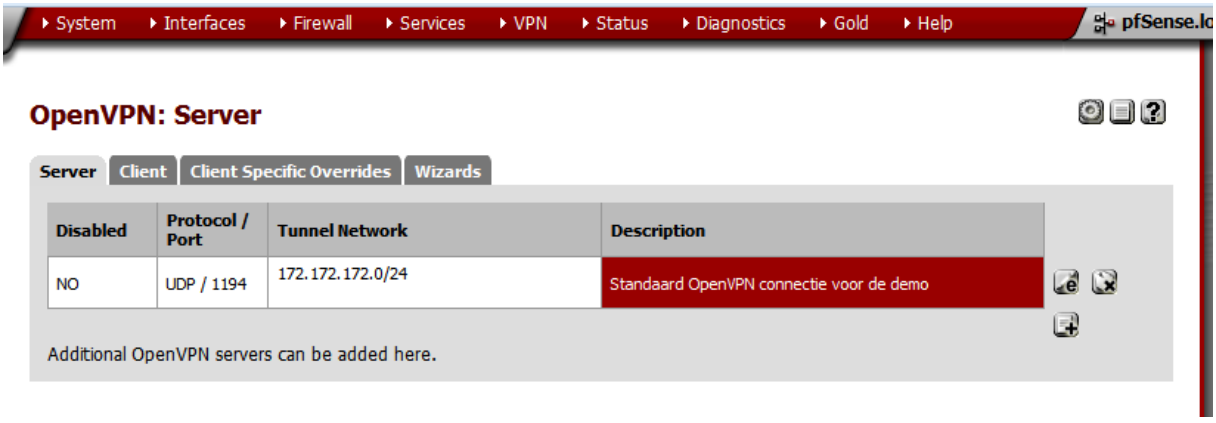
topologie wordt 1 netwerk opgebouwd binnen de tunnel en krijgen de clients een IP in dit subnet waardoor ze elkaar wel kunnen zien.

- De overige instelling mogen standaard blijven, deze dienen om DNS en andere gegevens te pushen naar de client.



OpenVPN server klaar

- Save de configuratie en de OpenVPN server wordt toegevoegd

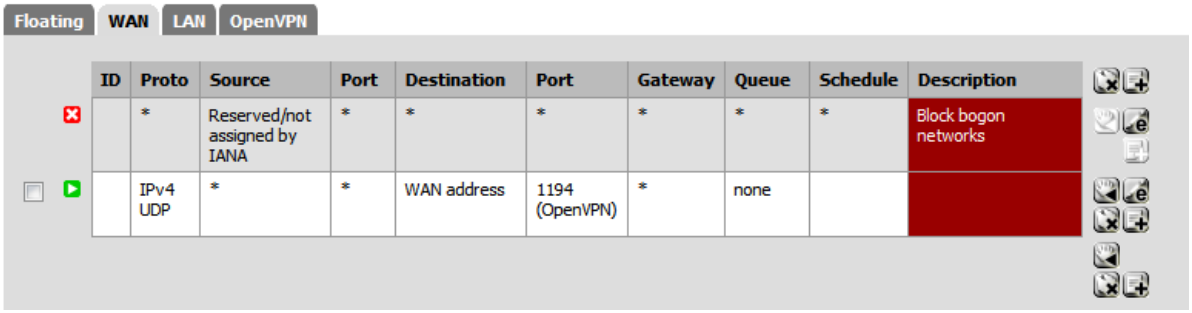


Configuratie van de Firewall

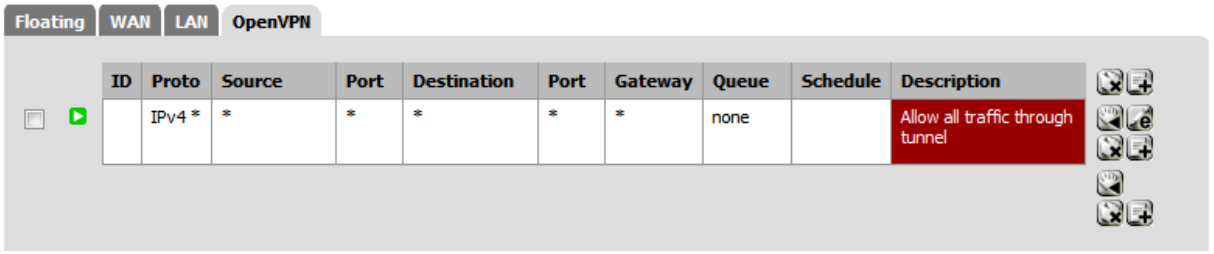
De pfSense Firewall moet ingesteld worden voor een aantal interfaces waaronder, WAN, LAN en OpenVPN. De laatste is de virtuele interface die dus enkel bestaat bij een OpenVPN verbinding. Floating regels zijn regels die niet rechtstreeks op een specifieke interface van toepassing zijn.

- Eerst moet toegelaten worden dat de OpenVPN clients op **UDP poort 1194** toegang krijgen tot de OpenVPN server op de **WAN interface**
  - Selecteer het tabblad *WAN* en klik op de plus knop
  - Protocol: wijzig het protocol naar UDP
  - Source mag standaard blijven (*any*)
  - Destination mag standaard blijven (*any*) of mag veranderd worden naar het WAN adres van de router

- Destination port range wordt ***tweemaal 1194*** (oftewel *OpenVPN* uit de lijst)
- Klik onderaan op ***Save*** en vervolgens op ***Apply changes***

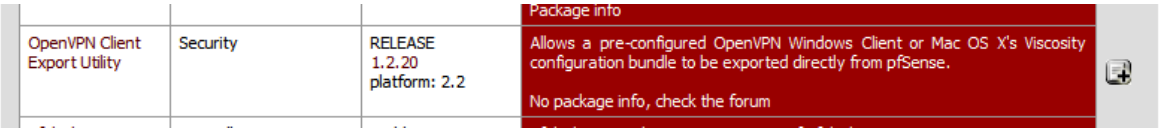


- Daarna configureren we de regels voor het verkeer in de tunnel, in dit voorbeeld wordt dit helemaal open gezet, zodat elk type verkeer naar binnen toegelaten wordt (bijv. een ping naar de router op zijn interne interface)
  - Selecteer het tabblad *OpenVPN* en klik op de plus knop  .
    Het enige dat hier gewijzigd dient te worden is het protocol:
  - *Protocol*: ***Any*** (dus én TCP én UDP én ICMP etc…)
  - Klik onderaan op ***Save*** en vervolgens op ***Apply changes***

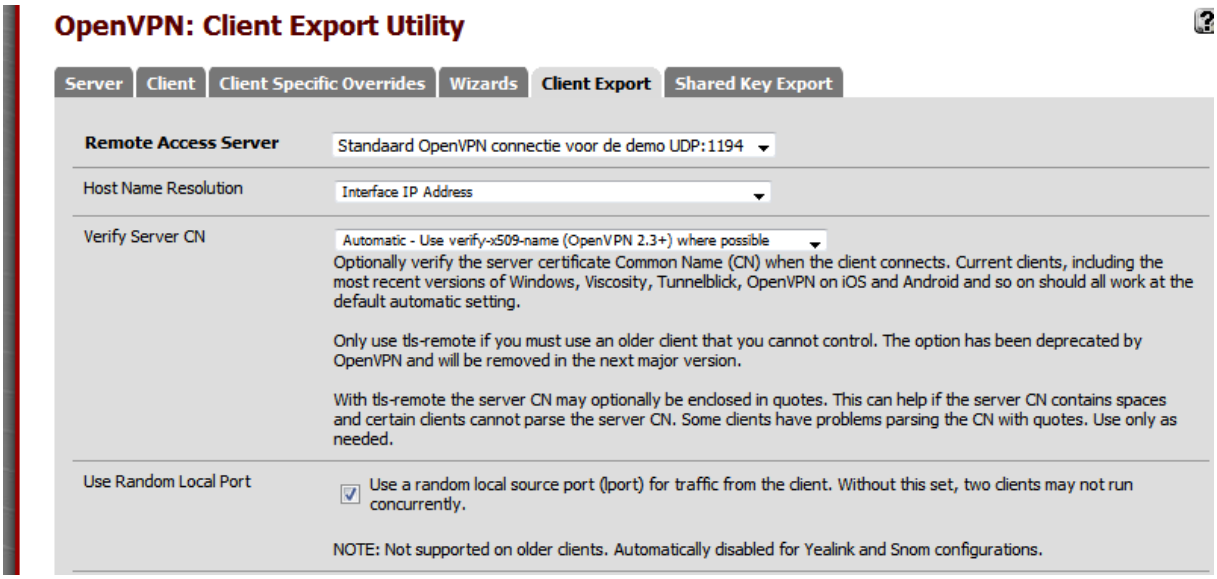


Client Certificaten exporteren

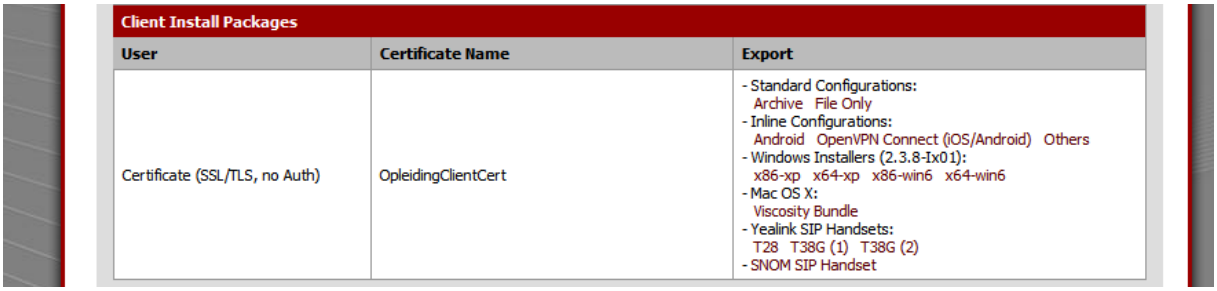
- De certificaten die in pfsense gecreëerd zijn kunnen eenvoudig geëxporteerd worden om te gebruiken in de OpenVPN clients. De mogelijkheid bestaat zelfs om naast de **certificaten** ook **volledige configuratiefiles en installers** voor **bekende clients** te exporteren. Op die manier moet de OpenVPN client niet meer geconfigureerd worden.
- Onder System -> packages -> available packages kan de **export functie geïnstalleerd** worden door deze toe te voegen via de knop 



- Onder VPN -> OpenVPN zullen nu 2 tabbladen toegevoegd zijn. Bij de **client export** kunnen de certificaten of configuraties geëxporteerd worden.
- Kies de betreffende OpenVPN server
- Host Name Resolution: Interface IP
- Verify Server CN: een extra verificatie in de client van de server certificaat naam. Dit is niet mogelijk voor oudere clients
- Use Random local port is noodzakelijk indien het gewenst is om **2 of meerdere clients op 1 toestel** tegelijk te laten connecteren



- Al de bovenstaande instellingen zijn eigenlijk de **configuratie van de client**. Indien gekozen wordt om enkele de certificaten te exporteren (export als archive) doen deze er niet toe. In de configuratie file van de client kunnen deze eigenschappen en andere ook nog achteraf aangepast worden.
- Alle certificaten die met de ingestelde configuratie kunnen geëxporteerd worden, zijn weergegeven onderaan. Door de op de gewenste export te klikken worden de bestanden gedownload naar de PC. Deze moeten dan naar het gewenste toestel gekopieerd worden om daar te gebruiken.
- Kies hier voor de **32 bit windows installer (x86-win6)**



VPN instellen op Windows

- De installer uitvoeren als administrator om de client met correcte configuratie te installeren (virtuele TAP adapter ook installeren).
- De geïnstalleerde OpenVPN client starten als **administrator** om de OpenVPN tunnel op te zetten. Er komt nu een icoontje bij in de taakbalk die de status van de tunnel weergeeft en waarmee de connectie gestart en gestopt kan worden. Indien meerdere configuraties gedefinieerd zijn, moet de gewenste tunnel gekozen worden door rechts te klikken op het icoontje.

Uittesten

➔ Opmerking: indien gebruik wordt gemaakt van een niet-virtuele Windows machine die de host is van de pfSense en Windows 7 virtuele machines, zal internet toegang niet langer werken.

Dit komt door de aanwezigheid van een vicieuze cirkel: internet verkeer van de host wordt door de tunnel gestuurd, pfSense stuurt dit verkeer door naar VMware die het via de NAT router doorstuurt naar de host die het op zijn beurt terug door de tunnel stuurt.

➔ Een logischer scenario is eventueel het opnieuw aanmaken (klonen) van de Windows 7 machine en deze op zijn beurt op het NAT netwerk te plaatsen.

- Na een succesvolle connectie kan een willekeurige browser worden gestart en bij wijze van test gesurft worden naar het IP http://192.168.1.101 (IP van de Windows7 machine)
- Probeer ook eens https://192.168.1.1 uit

- Bekijk even het eigen IP van de VPN client, let op het IP adres en subnetmasker dat is gebruikt om de tunnel op te bouwen.
- Bekijk eventueel ook de route tabel (*route print -4*). Een groot voordeel van OpenVPN ten opzichte van L2TP IPsec VPN is dat **enkel het verkeer bedoeld voor het interne netwerk van de VPN router** (hier pfsense) **door de tunnel gaat**. Ander verkeer zal via het lokale netwerk van de client gaan, en niet door de tunnel. Er zijn extra regels toegevoegd aan de route tabel voor verkeer bedoeld voor het interne netwerk van de VPN router.

```
C:\Users\virtueel_WIN7>route print
===========================================================================
Interface List
 18...00 ff ab 39 29 e2 ......TAP-Windows Adapter V9
 15...d8 fc 93 58 14 06 ......Bluetooth Device (Personal Area Network)
 11...00 0c 29 09 f5 88 ......Intel(R) PRO/1000 MT Network Connection
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 19...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.0.1      172.16.10.1     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
       172.16.0.0        255.255.0.0         On-link      172.16.10.1    266
     172.16.10.1  255.255.255.255         On-link      172.16.10.1    266
   172.16.255.255  255.255.255.255         On-link      172.16.10.1    266
    172.172.172.0    255.255.255.0         On-link     172.172.172.2    276
    172.172.172.2  255.255.255.255         On-link     172.172.172.2    276
[redacted]                                                             276
      192.168.1.0    255.255.255.0    172.172.172.1     172.172.172.2     20
[redacted]                                                             306
        224.0.0.0        240.0.0.0         On-link      172.16.10.1    266
        224.0.0.0        240.0.0.0         On-link     172.172.172.2    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      172.16.10.1    266
  255.255.255.255  255.255.255.255         On-link     172.172.172.2    276
===========================================================================
Persistent Routes:
  None
```

- Terug in de pfSense interface kan genavigeerd worden naar *Status -> OpenVPN.* Daar zijn de **actieve client connecties** terug te vinden.