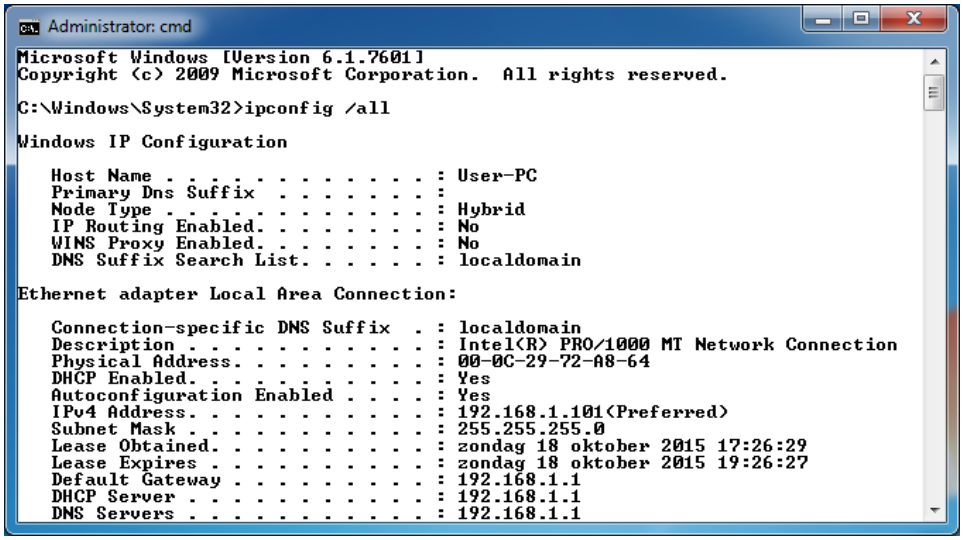
Configuratie van VPN met L2TP/IPsec

Met pfSense als Firewall/Router

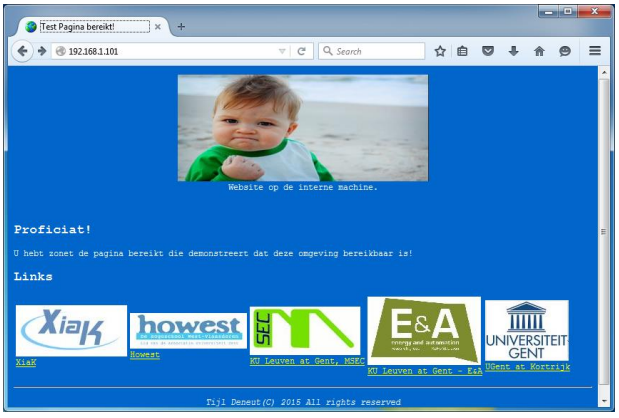
Voorbereiding (Windows 7 op lokale netwerk)

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



Figuur 1: Let erop dat de DHCP Server, Default Gateway en DNS Servers allemaal verwijzen naar het IP adres van de router

- 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



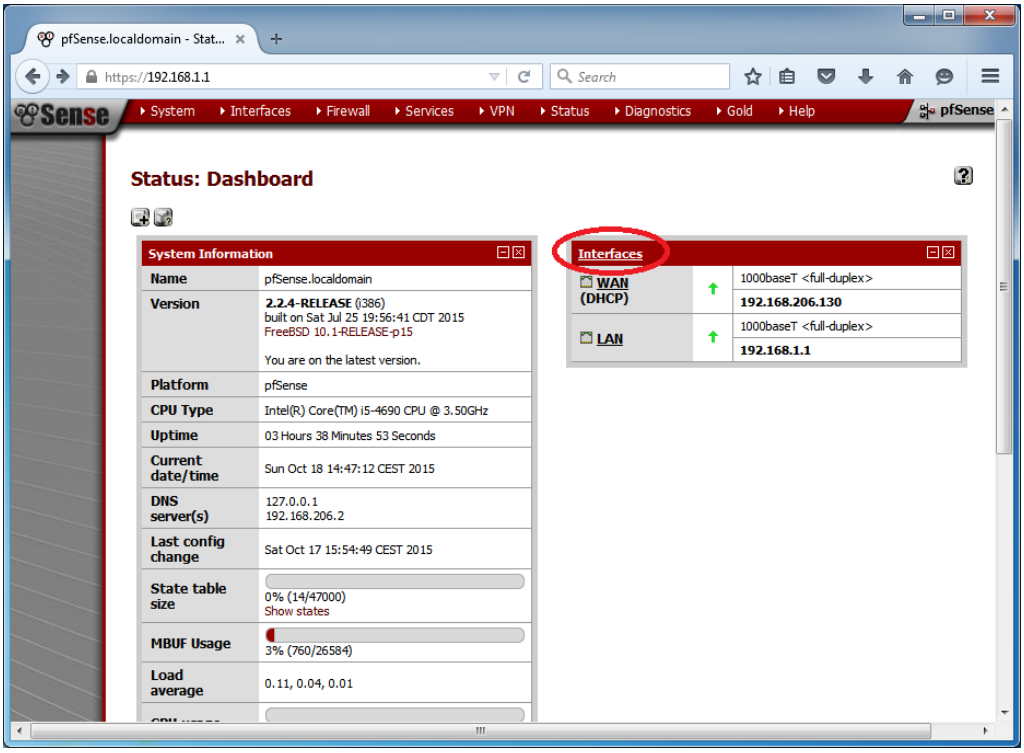
Figuur 2: Website op de interne Windows 7

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 ***ZONDER EXTRA SOFTWARE*** een zo veilig mogelijke VPN verbinding te kunnen opzetten vanuit Windows

- 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.



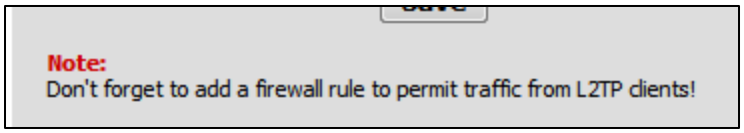
Figuur 3: Klik op "Interfaces" voor een overzicht

L2TP Tunneling Protocol opzetten

➔ 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 192.168.20.0 /24 als netwerk voor de tunnel. Het **laatste IP** wordt in dit voorbeeld gekozen als adres voor de ***gateway*** van de tunnel (dus het IP van de router). Echter: voor de VPN clients dient een deel hiervan gekozen te worden; hier wordt gekozen voor het **192.168.20.0 /25** subnet.

- Ga bovenaan via *VPN* naar *L2TP* en selecteer daar ***Enable L2TP server***
- Laat alles standaard staan:
  - Server Address: vul ***192.168.20.254*** in
  - Remote Address Range: ***192.168.20.0*** met
  - Subnet Mask: ***25***
  - Number of L2TP users: een getal onder 128 zoals bijv. ***10***
- De andere opties zijn in dit voorbeeld niet nodig, er wordt hier gekozen voor *lokale gebruikers*
- Klik eerst ***Save***

- Bovenaan klikken op het tabblad ***Users*** en een nieuwe gebruiker toevoegen door op de corresponderende knop te klikken: 
- Kies een gebruikersnaam (*Username*) en een bijhorend wachtwoord (*Password*)
  - Bijv. **pieter** met wachtwoord **123**
- Het IP mag leeggelaten worden



Figuur 4: Let op de aanwijzing om later de Firewall niet te vergeten

IPsec beveiliging configureren

➔ IPsec laat toe om de authenticatie en communicatie te beveiligen door een combinatie van encryptie*fases*.
Eerst wordt de algemene configuratie vervolledigd op het tabblad *Mobile clients*, vervolgens de twee fases op het tabblad *Tunnels*.

- Ga bovenaan via VPN naar IPsec en selecteer eerst het tabblad *Mobile clients*, selecteer daar ***Enable IPsec Mobile Client Support***
- User Authentication: klik op ***Local Database*** (er is geen verbinding met RADIUS of andere bronnen)
- Klik onderaan op ***Save***
- Er verschijnt bovenaan een melding om de eerste fase te configureren, klik op ***Create Phase1***

Phase 1 (Mobile Client)

- Laat het meeste standaard, er wordt hier dus gebruik gemaakt van IKEv1 over IPv4 op de WAN interface via Mutual PSK (Pre Shared Key)
- *Negotation mode:* hier wordt voor het veiligere ***Main*** gekozen
- Als algoritmes worden de standaard instellingen gelaten op AES-256 bits als *Encryption algorithm* en SHA1 als *Hash algorithm*.
- Voor de Windows VPN client is een Diffie Hellman sleutel sterkte van 2048 bit vereist:
DH key group: ***14 (2048 Bit)***
- Klik onderaan op ***Save***

Phase 2 (Mobile Client)

- Klik eerst op het plus teken  naast *Show 0 Phase-2 entries* en klik vervolgens op  om een tweede fase toe te voegen.
- *Mode:* Selecteer hier zeker ***Transport***
Tunnel mode wordt voornamelijk gebruikt om een tunnel te creëren tussen twee routers terwijl Transport mode dan weer geschikt is voor verkeer tussen een VPN cliënt en een router.
- Verder kan hier alles standaard worden gelaten.
- Klik onderaan op ***Save***

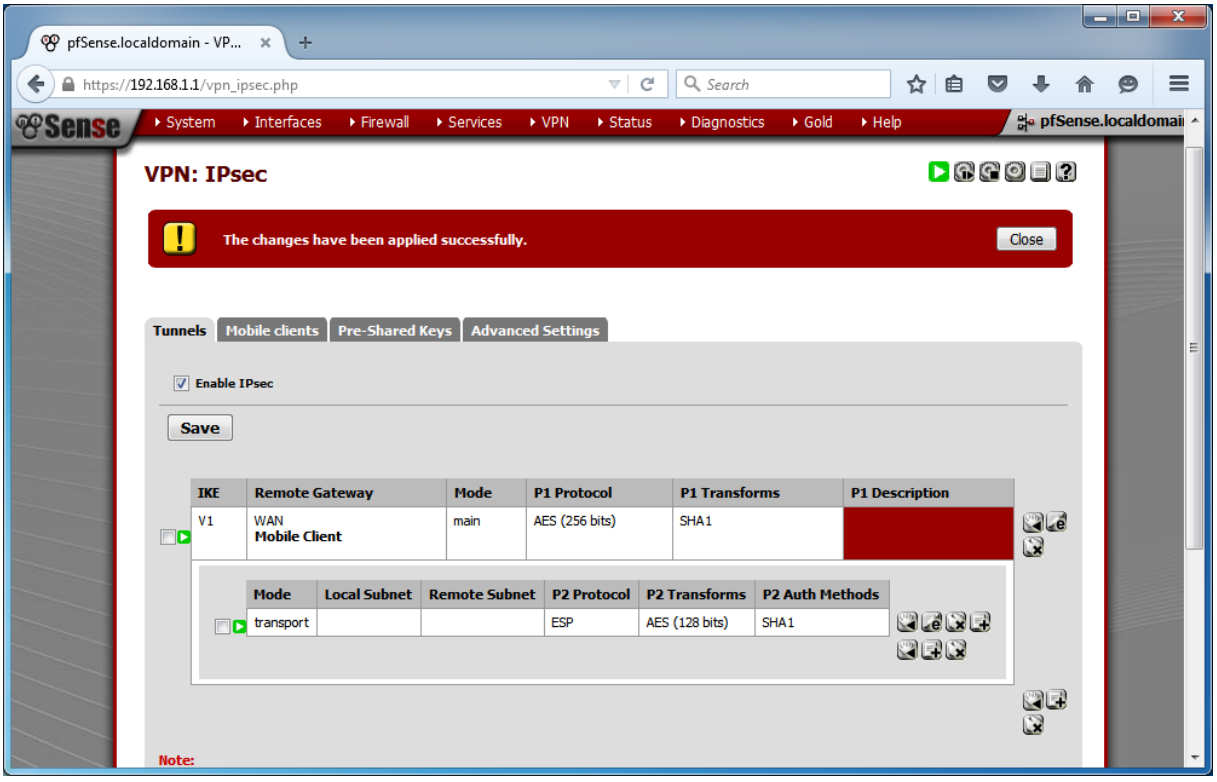
Pre-Shared Key

IPsec heeft een Pre-Shared Key nodig, in dit geval in de vorm van een wachtwoord:

- Klik bovenaan op het tabblad *Pre-Shared Keys* en vervolgens op het plus-symbool  om een wachtwoord toe te voegen.
- *Identifier*: Hier wordt letterlijk ***allusers*** getypt om deze PSK voor iedereen te laten tellen.
- *Pre-Shared Key*: Kies hier een wachtwoord, bijv. ***wachtwoord123***.
- Klik onderaan op ***Save*** en vervolgens bovenaan op ***Apply changes***.

IPSEC ENABLEN

- Controleer op het tabblad *Tunnels* of ***Enable IPsec*** aangevinkt is.
- Vink dit aan en klik op ***Save***



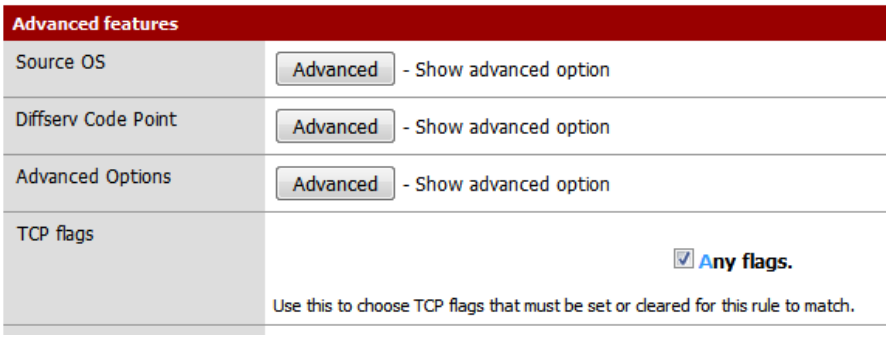
Figuur 5: IPsec geconfigureerd

Configuratie van de Firewall

De pfSense Firewall moet ingesteld worden voor een aantal interfaces waaronder, WAN, LAN, L2TP én IPsec. De laatste twee zijn virtuele interfaces die dus enkel bestaan bij een VPN verbinding. Floating regels zijn regels die niet rechtstreeks op een specifieke interface van toepassing zijn.

- Eerst moet toegelaten worden dat de L2TP VPN Clients op poort 500 UDP (ISAKMP) toegang krijgen tot de VPN IKEv1 service:
  - Ga naar de Firewall rules via *Firewall* > *Rules*
  - Selecteer het tabblad *L2TP VPN* en klik op de plus knop . Laat alles standaard (dus pass op de L2TP VPN interface op IPv4.
  - Protocol: wijzig het protocol naar ***UDP***
  - Source mag standaard blijven (*any*)
  - Destination mag standaard blijven (*any*)
  - Destination port range wordt ***tweemaal 500*** (oftewel *ISAKMP* uit de lijst)
  - Klik onderaan op ***Save*** en vervolgens op ***Apply changes***
- Daarna configureren we de IPsec regels, 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 *IPsec* 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***
- Hoewel VPN plus verkeer binnen de tunnel nu mogelijk is, zullen opgebouwde TCP sessies nog steeds geblokkeerd worden. Alsook verkeer dat via de VPN tunnel naar buiten gaat zal door de firewall tegengehouden worden. Dit moet opgelost worden via een Floating regel:

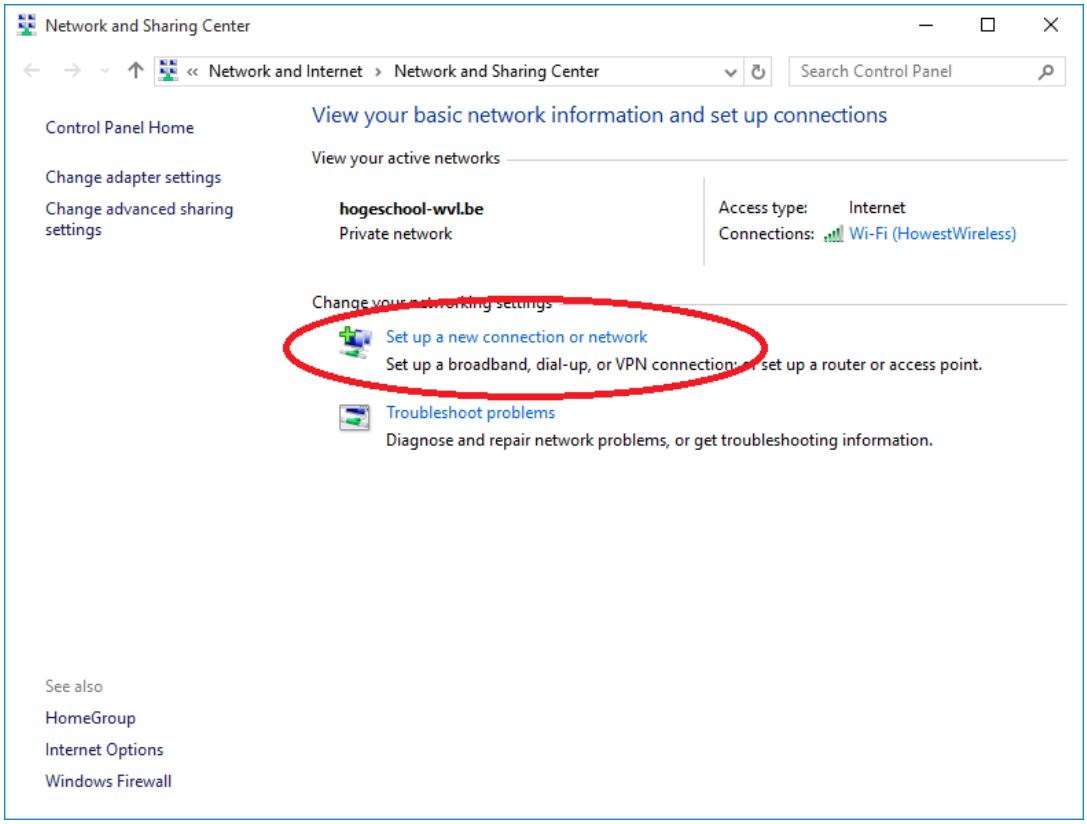
- Selecteer het tabblad *Floating* en klik op de plus knop  .
  Ook hier wordt slechts één ding gewijzigd: de TCP Flags:
- Onderaan, bij de geavanceerde instellingen, naast **TCP flags**: klik op **Advanced** en vink **Any flags** aan
- Klik onderaan op **Save** en vervolgens op **Apply changes**



Figuur 6: Geavanceerde instellingen van de firewall

VPN instellen op Windows

Het instellen van een VPN verbinding onder Windows (7, 8 of 10) gaat vrij simpel en start bij het *Network and Sharing Center*:



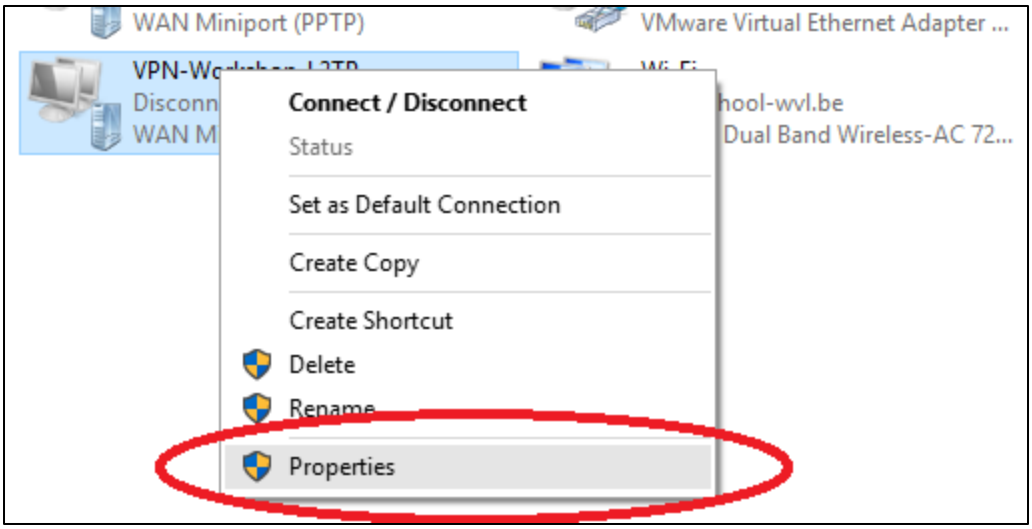
Figuur 7: Network and Sharing Center, startpunt voor een VPN configuratie

- Klik hier op ***Setup a new connection or network*** en kies vervolgens ***Connect to a workplace***
- Na een druk op ***Next*** kan een nieuwe connectie gecreëerd worden, gebruik daarvoor de aanwezige Internet verbinding (***Use my Internet connection (VPN)***)
- Internet address: Typ het **externe IP adres** van de pfSense Router, hier 192.168.206.130

- Destination name: Dit is een gebruiksvriendelijke naam, zoals VPN-Workshop-L2TP
- Bij Windows 7 (niet 8 en 10) kan hier via de knop ***Next*** meteen een gebruikersnaam en passwoord ingevuld worden. In ons geval zou dit dus ***pieter/123*** zijn.
- Klik tot slot op ***Create*** of ***Create***, indien een verbindingspoging plaatsvind (Windows 7) kan op ***Skip*** worden geklikt

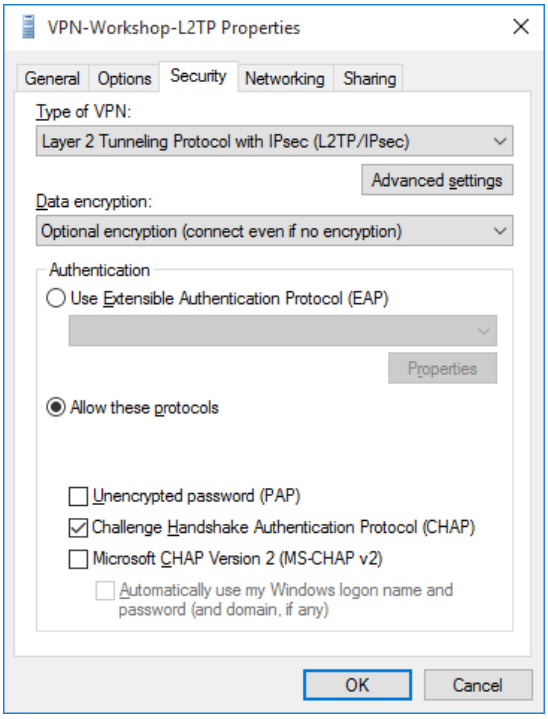
➔ Terug in het *Network and Sharing Center* krijgen we een overzicht van alle adapters via ***Change adapter settings*** (bovenste optie aan de linkerkant van het scherm)

- Zoek de verbinding die net is aangemaakt, klik op met de **rechtermuistoets** en selecteer ***Properties***



Figuur 8: Properties van de VPN verbinding

- Ga naar het tabblad ***Security*** en selecteer bovenaan als ***Type of VPN*** het type ***Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)***
  - Klik vervolgens op de knop ***Advanced settings*** en selecteer "Use preshared key for authentication", typ de Shared Secret (PSK) in (***wachtwoord123***), sluit af met ***OK***
- Tot slot; selecteer "***Allow these protocols***" en vink **énkel** ***Challenge Handshake Authentication Protocol (CHAP)*** **aan**



Figuur 9: VPN instellingen voor L2TP/IPsec

Uittesten

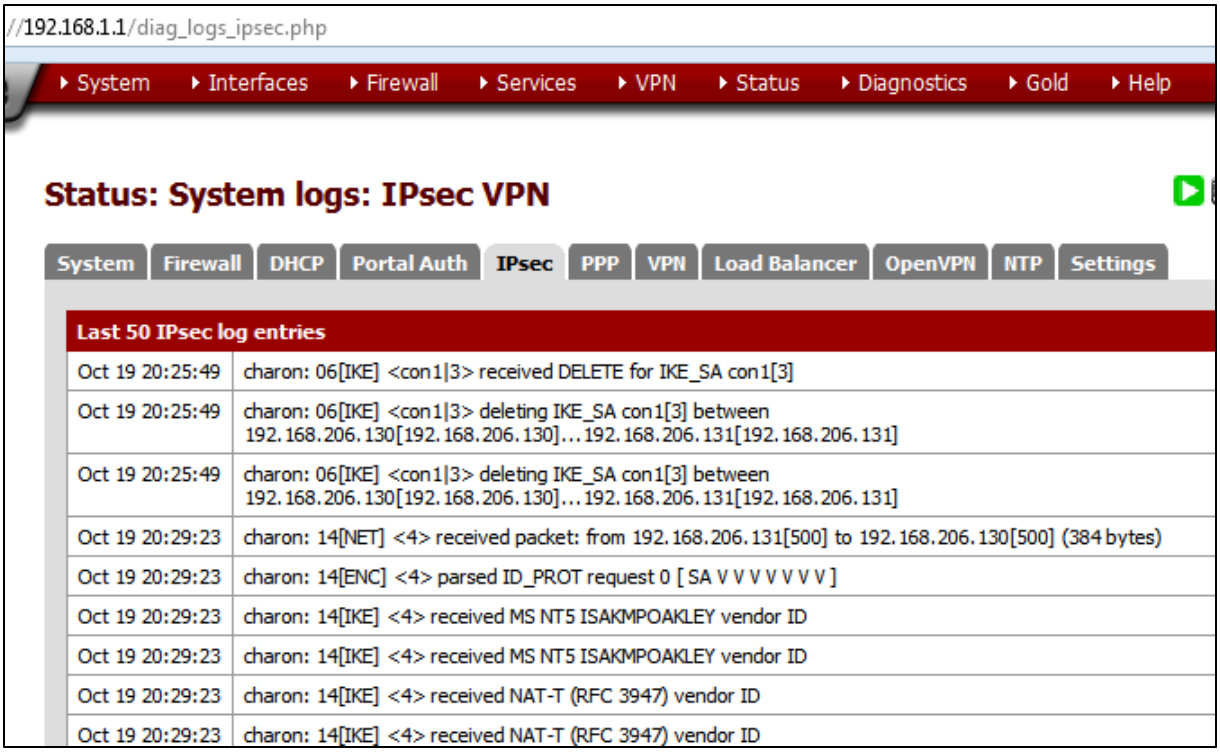
➔ Opmerking: indien gebruik wordt gemaakt van een niet-virtuele Windows machine die de host is van de pfSense en Windows 7 virtuele machines, zal internet toegang niet langer werken.
Dit komt door de aanwezigheid van een vicieuze cirkel: internet verkeer van de host wordt door de tunnel gestuurd, pfSense 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 (192.168.206.0/24) te plaatsen.
Indien dit klonen gebeurd via een kopieer-actie in Windows, zal het MAC adres tweemaal voorkomen, gelieve dus voor het starten van de machine in de instellingen van de netwerkkaart op "Generate" te klikken, te vinden onder de "Advanced" knop.

- Start tenslotte de VPN verbinding, indien een gebruikersnaam wordt gevraagd, geef dan deze in van bij de L2TP configuratie (***pieter*/*123***).
- 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*)

- Terug in de pfSense interface kan genavigeerd worden naar *Status > System Logs > tabblad IPsec*. Daar is o.a. het IP adres van de VPN client terug te vinden.



Figuur 10: IPsec Systeem Logs