•

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*

an Administrator: cmd	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	
C:\Windows\System32>ipconfig /all	=
Windows IP Configuration	
Host Name : User-PC Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled : No WINS Proxy Enabled : No DNS Suffix Search List : localdomain Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix : localdomain Description : : Intel(R) PRO/1000 MT Network Connection Physical Address : 00-0C-29-72-A8-64 DHCP Enabled : : Yes Autoconfiguration Enabled : Yes Subnet Mask : : 192.168.1.101(Preferred) Subnet Mask : : zondag 18 oktober 2015 17:26:29 Lease Obtained : zondag 18 oktober 2015 19:26:27 Default Gateway : : 192.168.1.1 DHCP Servers : : : 192.168.1.1 DHCS Servers : : : : : : : : : : : : : : : : : : :	Ŧ

- 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.
 - <u>http://192.168.1.1</u>, 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.

PfSense.local	domain - Stat 🗙	+									x
🗲 🔶 🔒 https:	//192.168.1.1		⊽ C	Q Search		☆	é (9 +	⋒	ø	≡
Sense	 System Interview 	erfaces Firewall Services	► VPN	 Status Diagnostic 	s ≯G	iold	▶ Help			밝e pfS	ense 🔺
S	Status: Dash	board								6	9
	System Informat	non		Interfaces		1000	aseT < ful	-dupley>			
	Version	2 2 4-RELEASE (1386)		DHCP)	+	192.1	168.206.1	30		Ξ	
	Cabion	built on Sat Jul 25 19:56:41 CDT 2015		_		1000	oaseT <ful< th=""><th>-duplex></th><th></th><th></th><th></th></ful<>	-duplex>			
		You are an the latest version				192.	168.1.1				
	Platform	nfSense									1
	CPU Type	Intel(R) Core(TM) i5-4690 CPU @ 3.50G	Hz								
	Uptime	03 Hours 38 Minutes 53 Seconds									
	Current date/time	Sun Oct 18 14:47:12 CEST 2015									
	DNS server(s)	127.0.0.1 192.168.206.2									
	Last config change	Sat Oct 17 15:54:49 CEST 2015									
	State table size	0% (14/47000) Show states									
	MBUF Usage	3% (760/26584)									
	Load average	0.11, 0.04, 0.01									
	0011	(_	T
											•

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 (selfsigned). 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 III
- 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).

Sense	▶ System	► Interfaces	► Firewall	 Services 	► VPN	▶ Status	▶ Diagnost	ics 🔹 🕨 Gold	▶ Help	片 pfSense.l
	System: CAs Certif	Certificat	t e Autho r icate Revocat	rity Man	ager					3
	Descriptiv	re name	<mark>∕\</mark> CA_V	/PNopleiding						
	Method		Create an	n internal Certif	icate Author	ity 👻				
	Internal C	ertificate Autho	ority							
	Key lengt	n	2048 👻	bits						
	Digest Alg	orithm	SHA256 NOTE: It is	▼ s recommended	l to use an a	lgorithm strong	er than SHA1	when possible		
	Lifetime		8650	days						
	Distinguisl	hed name	Country State or Pro Organi Email Ar Common Save	Code : BE ovince : 0 O City : 6 G ization : VI ddress : 0 di Name : in	▼ ost-Vlaano ent PN Opleidi ummy@vp iternal-ca	leren ng nopleiding.te	est exr exr	admin@mycom; internal-ca	ex: Texas ex: Austin ex: My Compa pany.com	any Inc.

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)

Method	Create an internal Certificate 🗸
Descriptive name	
Internal Certificate	
Certificate authority	CA_VPNopleiding 👻
Key length	2048 🗸 bits
Digest Algorithm	SHA256 ▼ NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Certificate Type	User Certificate

- 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

Distinguished name	Country Code :	N BE	
	State or Province :	📏 Oost-Vlaanderen	
	City :	📏 Gent	
	Organization :	📏 VPN Opleiding	
	Email Address :	N dummy@vpnopleiding.test	ex webadmin@mycompany.com
	Common Name :	<u>N</u>	ex www.example.com
		Type Value	

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

cryptographic seconds	
TLS Authentication	Enable authentication of TLS packets.
	\bigtriangledown Automatically generate a shared TLS authentication key.
Peer Certificate Authority	CA_VPNopleiding -
Peer Certificate Revocation List	No Certificate Revocation Lists (CRLs) defined. Create one under System > Cert Manager.
Server Certificate	OpleidingServerCert (CA: CA_VPNopleiding)
DH Parameters Length	1024 🗸 bits
Encryption algorithm	AES-128-CBC (128-bit) -
Auth Digest Algorithm	SHA1 (160-bit) NOTE: Leave this set to SHA1 unless all dients are set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	No Hardware Crypto Acceleration 👻
Certificate Depth	One (Client+Server)
	When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates

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

IFV4 Tunnet Network	172.172.172.0/24
	This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
IPv6 Tunnel Network	
	, This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining networ addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway	Force all dient generated traffic through the tunnel.
IPv4 Local Network/s	192.168.1.0/24
	, These are the IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list o one or more CIDR ranges. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
IPv6 Local Network/s	
	These are the IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Concurrent connections	20
	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	No Preference 🗸
Compression	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Compression Type-of-Service	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Compression Type-of-Service Inter-client communication	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently. Set the TOS IP header value of tunnel packets to match the encapsulated packet value. Allow communication between clients connected to this server
Compression Type-of-Service Inter-client communication Duplicate Connections	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently. Set the TOS IP header value of tunnel packets to match the encapsulated packet value. Allow communication between dients connected to this server Allow multiple concurrent connections from dients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

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 1^{ste} en de client het 2^{de} 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.

Client Settings	
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
Address Pool	✓ Provide a virtual adapter IP address to clients (see Tunnel Network)
Topology	I Allocate only one IP per client (topology subnet), rather than an isolated subnet per client (topology net30).
	Relevant when supplying a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this even for IPv6, such as OpenVPN Connect (iOS/Android). Others may break if it is present, such as older versions of OpenVPN or clients such as Yealink phones.
DNS Default Domain	Provide a default domain name to dients
DNS Servers	Provide a DNS server list to clients
Force DNS cache update	Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Servers	Provide a NTP server list to dients
NetBIOS Options	Enable NetBIOS over TCP/IP
	If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Client Management Port	Use a different management port on clients. The default port is 166. Specify a different port if the client machines need to select from multiple OpenVPN links.

OpenVPN server klaar

• Save de configuratie en de OpenVPN server wordt toegevoegd

System	 Interfaces 	▶ Firewall	Services	► VPN	 Status 	Diagnostics	▶ Gold	▶ Help	; pfSense	
VD									808	
penVPN: Server										
erver Cli	ent Client Sp	ecific Overrid	les Wizards							
Disabled	Protocol / Port	Tunnel Net	work		Descri	ption				
NO	UDP / 1194	172.172.172	.0/24		Standa	ard OpenVPN conne	ectie voor de	e demo	a a	
									3	
Additional O	penVPN server	s can be add	ed here.							

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**
 - \circ 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

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

Floa	ting	W	AN LAI	N OpenVPN								
		TD	Ducks	C	Daut	Destination	Daut	Calana	0	Cabadula	Description	9 7
		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
	8		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	2 2 E
	۵		IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			
												2 Ce

- 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 E.
 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*

Floating WAN LAN OpenVPN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	œ
۵		IPv4*	*	*	*	*	*	none		Allow all traffic through tunnel	
											3 Ce

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

			Package into	
OpenVPN Client Export Utility	Security	RELEASE 1.2.20 platform: 2.2	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum	B
- · ·				

- 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

OpenVPN: Client Export Utility

Server Client Client Specif	ic Overrides Wizards Client Export Shared Key Export				
Remote Access Server	Standaard OpenVPN connectie voor de demo UDP:1194 👻				
Host Name Resolution	Interface IP Address				
Verify Server CN	Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible				
	Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.				
	Only use tls-remote if you must use an older dient that you cannot control. The option has been deprecated by OpenVPN and will be removed in the next major version.				
	With tis-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain dients cannot parse the server CN. Some dients have problems parsing the CN with quotes. Use only as needed.				
Use Random Local Port	Use a random local source port (port) for traffic from the dient. Without this set, two dients may not run concurrently.				
	NOTE: Not supported on older clients. Automatically disabled for Yealink and Snom configurations.				

- 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.
- Kies hier voor de **32 bit windows installer (x86-win6)**

Client Install Packages				
User	Certificate Name	Export		
Certificate (SSL/TLS, no Auth)	OpleidingClientCert	Standard Configurations: Archive File Only Inline Configurations: Android OpenVPN Connect (iOS/Android) Others Windows Installers (2.3.8-1x01): x86-xp x64-xp x86-win6 x64-win6 Mac OS X: Viscosity Bundle Yealink SIP Handsets: T28 T386 (1) T386 (2) - SNOM SIP Handset		

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 <u>http://192.168.1.101</u> (IP van de Windows7 machine)
- Probeer ook eens <u>https://192.168.1.1</u> 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 1800 ff ab 39 29 e2TAP-Windows Adapter U9 1508 fc 93 58 14 06Bluetooth Device (Personal Area Network) 1100 0c 29 09 f5 88Intel(R) PRO/1000 MT Network Connection 1Software Loopback Interface 1 1200 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter 1300 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2 1700 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3 1900 00 00 00 00 00 00 e0 Microsoft Gto4 Adapter								
IPv4 Route Table								
Active Routes:								
Network Destinatio	n 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				
170.170.170.000	255-255-255-255	0- 11-h	170.170.170.0	276				
192.168.1.0	255.255.255.0	172.172.172.1	172.172.172.2	20				
444.0.0.0	240.0.0.0	Vn-link	147.0.0.1	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				
			=======================================					
None None								

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