







## TP 4 – OpenVPN



On commence par créer le certificat d'autorité :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
pfsense_auth	✓	self-signed	0	CN=cs.sr Valid From: Wed, 11 Jan 2023 07:20:08 +0000 Valid Until: Sat, 08 Jan 2033 07:20:08 +0000		  




On s'en sert ensuite pour signer un nouveau certificat de serveur :

OpenVPN-remote-access Server Certificate CA: No Server: Yes	pfsense_auth	CN=pfsense.cs.sr Valid From: Wed, 11 Jan 2023 07:25:10 +0000 Valid Until: Sat, 08 Jan 2033 07:25:10 +0000	  
--	--------------	---	---

On crée ensuite l'utilisateur Alice, avec un certificat signé par le certificat d'autorité :

<input type="checkbox"/>	 alice	✓	 
--------------------------	---	---	---

On crée ensuite la configuration OpenVPN sur le serveur :

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.189.0/24	Mode: Peer to Peer ( SSL/TLS ) Data Ciphers: AES-256-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	openvpn_server	  

Ne pas oublier de configurer en « **remote access user** » :





Mode Configuration	
<u>Server mode</u>	Remote Access ( User Auth )
<u>Backend for authentication</u>	Local Database
<u>Device mode</u>	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Pour installer le paquet **openvpn-client-export**, j'ai dû reconfigurer les adresses DNS dans la configuration pfSense pour qu'elles fonctionnent sur la connexion de l'université.

Configuration réseau :

WAN	192.168.5.130
LAN	192.168.126.10
IPv4 tunnel net	192.168.189.0/24

On n'oublie pas d'autoriser le port OpenVPN dans le parefeu :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none	   
--------------------------	-------------------------------------	-------	----------	---	---	---	----------------	---	------	---

On considère le réseau interne OpenVPN comme sûr parce qu'il n'y a que des administrateurs qui vont s'y connecter : on laisse donc passer tout le trafic :





Floating

WAN

LAN

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	none			   

On télécharge le fichier de configuration client, on le lance avec les identifiants d'Alice et on se retrouve connecté avec l'adresse 192.168.189.2 (gateway = 192.168.189.1).

Maintenant, lorsqu'on tente de communiquer avec l'hôte LXLE (192.168.126.11), tout le trafic transite par OpenVPN (capture Wireshark)

27	5.441869	192.168.5.1	192.168.5.130	OpenVPN	126	MessageType: P_DATA_V2
28	5.442631	192.168.5.130	192.168.5.1	OpenVPN	126	MessageType: P_DATA_V2
33	6.443974	192.168.5.1	192.168.5.130	OpenVPN	126	MessageType: P_DATA_V2
34	6.446043	192.168.5.130	192.168.5.1	OpenVPN	126	MessageType: P_DATA_V2
39	7.459797	192.168.5.1	192.168.5.130	OpenVPN	126	MessageType: P_DATA_V2
40	7.461687	192.168.5.130	192.168.5.1	OpenVPN	126	MessageType: P_DATA_V2
45	8.468253	192.168.5.1	192.168.5.130	OpenVPN	126	MessageType: P_DATA_V2
46	8.470529	192.168.5.130	192.168.5.1	OpenVPN	126	MessageType: P_DATA_V2
118	18.958427	192.168.5.130	192.168.5.1	OpenVPN	82	MessageType: P_DATA_V2