#### PRÉSENTÉ PAR DRUELLE NICOLAS



#### TOPOLOGIE



# **MISE EN PLACE** PFSENSE



#### **INSTALLATION PFSENSE**

	Add V Remove Edit [	Disk Action V Revert
	Memory	2.00 GiB
۲	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]
	BIOS	Default (SeaBIOS)
Ţ	Display	Default
¢,	Machine	Default (i440fx)
8	SCSI Controller	VirtIO SCSI single
0	CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media=cdrom,size=636498K
a	Hard Disk (scsi0)	local-lvm:vm-204-disk-0,iothread=1,size=10G
₽	Network Device (net0)	virtio=BC:24:11:54:4A:21,bridge=vmbr0,firewall=1
1	Network Device (net1)	virtio=BC:24:11:71:D3:9C,bridge=vmbr0,firewall=1
1	Network Device (net2)	virtio=BC:24:11:5D:DA:6D,bridge=vmbr0,firewall=1

#### Dans un premier temps je vais installer PFSENSE sur le Proxmox en ajoutant 2 interfaces réseau supplémentaire



#### **INSTALLATION PFSENSE**

Install	Install pfSense
Rescue Shell	Launch a shell for rescue operations
Recover config.xml	Recover config.xml from a previous install



ZFS Con	figuration
Configure Options:	Proceed with Installation
>>> Install	stripe: 0 disks
T Pool Type/Disks:	*
- Rescan Devices	*
- Disk Info	pfSense
N Pool Name	YES
4 Force 4K Sectors?	NO
E Encrypt Disks?	GPT (BIOS)
P Partition Scheme	2g
S Swap Size	NO
M Mirror Swap?	NO
W Encrypt Swap?	NO
<mark>⟨S</mark> elect≻	<cancel></cancel>



# Une fois les interfaces ajouter je démarre la VM et procède à l'installation

# **INSTALLATION PFSENSE**

stripe	Stripe - No Redundancy Minnon - n-Way Minnoning
raid10	RAID $1+0 - n \times 2-Wau$ Mirrors
raidz1	RAID-Z1 - Single Redundant RA
<b>r</b> aidz2	RAID-Z2 - Double Redundant RA
raidz3	RAID-Z3 - Triple Redundant RA
L	
	<pre>&lt; DK &gt; <cancel></cancel></pre>









### **CONFIGURATION PFSENSE**

Starting CRON... done.

Starting package OpenVPN Client Export Utility...done. pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023 Bootup complete

FreeBSD/amd64 (pfSenseVPN.druelleVPN.com) (ttyv0)

KVM Guest - Netgate Device ID: 62707d4d487eb27d1f37

\*\*\* Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSenseVPN \*\*\*

WAN (wan) -> vtnet0 -> v4/DHCP4: 192.168.20.94/24 LAN (lan) -> vtnet1 -> v4: 192.168.202.100/24

> Une fois l'installation faite je mets en place les ip sur les interfaces WAN et LAN



# **MISE EN PLACE OPENVPN**



#### MISE EN PLACE OPENVPN MISE EN PLACE CERTIFICAT D'AUTORITÉ

System /	Certificate /	Authorities
Authorities	Certificates	Revocation

Create / Edit CA			
Descriptive name	VPNDRUELLE The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /,  ", '		
Method	Create an Internal Certificate Authority		
Trust Store	re Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.		
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.		

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPNDRUELLE	~	self-signed	0	CN=VPNDRUELLE 🚯		<b>∥₩₽</b> Ċ面
				Valid From: Wed, 20 Nov 2024 08:09:37 +0000 Valid Until: Sat, 18 Nov 2034 08:09:37 +0000		

Pour la mise en place du VPN je vais dans un premier temps crée un certificat d'autorité qui va permettre d'authentifiés le serveur ainsi que le client.

Pour cela je me rends dans "System > Certificate > Authorities" Je vais ensuite renseigner les informations suivante : Descriptive name : VPNDRUELLE Method : Create an internal certificate

Une fois cela fait on peut voir que le certificat c'est ajouté

#### **MISE EN PLACE OPENVPN MISE EN PLACE CERTIFICAT SERVEUR**

CAs Certificates	Certificate Revocation		
Add/Sign a New Cer	tificate		
Method	Create an internal Certificate		
Descriptive name	VPNDRUELLE		
Internal Certificate			
Certificate authority	VPNDRUELLE		
Key type	RSA		
	2048     The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.		
Digest Algorithm	t Algorithm sha256 The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid		
Lifetime (days) 3650 The length of time the signed certificate will be valid, in days.			

Common Name	vpn.druelle.local			
	The following certificate subject components are optional and may be left blank.			
Country Code	(FR v)			
State or Province	e.g. Texas			
City	e.g. Austin			
Organization	e.g. My Company Inc			
Organizational Unit	e.g. My Department Name (optional)			
Certificate Attributes				
Attribute Notes	Ittribute Notes         The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.           For Internal Certificates, these attributes are added directly to the certificate as shown.			
Certificate Type	Server Certificate			
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the sign				
Alternative Names	FQDN or Hostname			
	Type Value Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.			

Je vais en suis je vais créer le certificat serveur pour cela je me rends dans "System > Certificates > Certificates".

Une fois sur cette page je renseigne les informations: Method: Create an internal Certificate **Descriptivename : VPNDRUELLE** Commun name : vpn.druelle.local **Certificat type : Server Certificate** 

#### MISE EN PLACE OPENVPN MISE EN PLACE CERTIFICAT SERVEUR

CAs Certificates	Certificate Revocation			
Search Search term		Both 🗸	Q Search	Clear
Certificates	Enter a search string	or *nix regular expression to search certificate names and distinguished names.		
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (673d9126e0fab) Server Certificate CA: <b>No</b> Server: <b>Yes</b>	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-673d9126e0fab Valid From: Wed, 20 Nov 2024 07:35:03 +0000 Valid Until: Tue, 23 Dec 2025 07:35:03 +0000		Add/Sign

2

# On peut ici voir que le certificat à été créer

#### MISE EN PLACE OPENVPN CRÉATION UTILISATEUR

Pour la création de l'u	Itil
>	U

Dans ce menu je créer un nouvel utilisateur en renseignant les informations suivante : Username : DRUELLEVPN Password : azerty Fullname : nicodruelle Je coche ensuite "Click to create a user certificate"

Dans les renseignements du certificat user je vais renseigner l'autorité de certifications précédemment créer

Defined by	USER			
Disabled	This user cannot login			
Username	DRUELLEVPN			
Password				
Full name	nicodruelle User's full name, for administrative information only			
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY			
Custom Settings	Use individual customized GUI options and dashboard layout for this user.			
Group membership	admins	Į.		
	Not member of	Member of		
	>> Move to "Member of" list	K Move to "Not member of" list		
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.			
Certificate	Click to create a user certificate			

Create	0	fiente	6	llee
Create	Certi	ricate	TOP	Use

Certificate authority	VPNDRUELLE	~	
Key type	RSA	~	
	2048	~	
	The length to use when generating a new RSA k The Key Length should not be lower than 2048	ey, in bits. r some platforms may consider the certificate invalid.	
Digest Algorithm	sha256	~	
	The digest method used when the certificate is	signed.	
	The best practice is to use an algorithm stronge	r than SHA1. Some platforms may consider weaker digest algorithms invalid	
	3650		
Lifetime			

Syster	System / User Manager / Users 0									
Users	Groups	Settings	Authentication Servers							
Users	Users									
	Username		Full name	Status	Groups	Actions				
	admin		System Administrator	~	admins	ø				

lisateur je me rends dans "System IserManager"

### **MISE EN PLACE OPENVPN CONFIGURATION**

Description	VPNDRUELLE	
	A description of this	a VPN for administrative reference.
Disabled	<ul> <li>Disable this service</li> </ul>	ver
	Set this option to di	isable this server without removing it from the list.
Unique VPN ID	Server 1 (ovpns1)	
V	PN / OpenVPN	/ Servers / Edit
Se	rvers Clients	Client Specific Overrides Wizards
Ge	neral Information	
	Disabled	Disable this server
	Ursabied.	Set this option to disable this server without removing it from the list.
	Server mode	Remote Access (SSL/TLS + User Auth )
	Backend for authentication	Local Database
	Protocol	
		our of it reading
	Device mode	tun - Layer 3 Tunnel Mode V
		tun mode carries inva and invo (Usi rayer 3) and is the most common and compatible goode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
	Interface	WAN
		The interface or Virtual IP address where OpenVPN will receive client connections.
	Local port	1194
Cruptographic Se	ttinge	
Cryptographic St	rttings	
TLS Configurat	A TLS key enha	ey nces security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake.
	This layer of HM	AAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or protections. The TLS Key does not have any effect on tunnel data
	unautionized of	Anneusona, me i La regisse and nave any enection cumersara.
	Automatical	ly generate a TLS Key.
Peer Certificate Autho	VPNDRUELLE	▼
Peer Certific	ate No Certificate R	Revocation Lists defined. One may be created here: System > Cert. Manager
Revocation	list	
OCSP Che	ck 🗌 Check client	certificates with OCSP
Server certific	Ate VPNDRUELLE	(Server: Yes, CA: VPNDRUELLE)
DH Parameter Len	2048 bit	
	Dime-Hellman (	Unj parameter set used for key exchange.
ECDH Cu	Use Default	~

- Je vais ensuite configurer le serveur OpenVPN pour cela je me rends dans "VPN > OPENVPN > Server"
- Dans un premier temps je vais renseigner les information suivante : **Description: VPNDRUELLE** 
  - Server mode: Remote Access (SSL/TLS + User Auth) Backend for auth : Local Database Protocol: UDP on IPv4 only Device mode : tun - Layer 3 Tunnel Mode Interface : WAN Local port: 1194
- Server certificate : je renseigne ce lui créer précédemment

#### **MISE EN PLACE OPENVPN CONFIGURATION**

inner oettingo		
IPv4 Tunnel Network	192.168.222.0/24	
	This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client h expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. T usable addresses will be assigned to connecting clients.	iosts The remaining
	A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is no with several options, including Exit Notify, and Inactive.	ot compatible
IPv6 Tunnel Network		
	This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client h expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining will be assigned to connecting clients.	iosts ng addresses
Redirect IPv4 Gateway	Force all client-generated IPv4 traffic through the tunnel.	
Redirect IPv6 Gateway	Force all client-generated IPv6 traffic through the tunnel.	
IPv4 Local network(s)	192.168.202.0/24	
	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or hos type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally LAN network.	t/network set to the
IPv6 Local network(s)		
	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/ aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set t network.	network type to the LAN
oncurrent connections	5	

Client Settings	
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
Topology	net30 – Isolated /30 network per client
	Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Advanced Client Settings						
DNS Default Domain	Provide a default domain name to clients					
DNS Default Domain	vpn.druelle.local					

- Ensuite je renseigne les informations dans IPv4 Tunnel Network l'adresse réseau que nous assignons au tunnel vpn.
- IPv4 Local Network : je renseigne la adresse réseau que je vais assigner au client Concurrent Connextions : je mets 5 ce qui correspond au nombre d'utilisateur en simultanés
  - Dans Advanced Client Setting je met le nom du DNS

#### MISE EN PLACE OPENVPN CONFIGURATION

#### Advanced Configuration

Custom options	auth-nocache
	Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"
Username as Common	Use the authenticated client username instead of the certificate common name (CN).
Name	When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.
UDP Fast I/O	Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
Exit Notify	Reconnect to this server / Retry once
	Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel Network, this value controls how many times this instance will attempt to send the exit notification.
Send/Receive Buffer	Default v
	Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.



Dans Advanced Configuration j'ajoute "authnocache" ce qui ca permettre d'ajouter une protection et empêcher la mise en cache des logins

Une fois cela fait on peut voir que la configuration c'est ajouté

#### **MISE EN PLACE OPENVPN** INSTALLATION PACKAGE EXPORT

System / P	ackage Manager / Available Packages	0
Installed Package	Available Packages	
Search		Θ
Search term	OpenVPN Both V Q Search Clear	
	Enter a search string or *nix regular expression to search package names and descriptions.	
Deekeese		_
Packages		
Name Ver	ion Description	
openvpn- 1.9.	2 Exports pre-configured OpenVPN Client configurations directly from pfSense software.	- Install
client-export	Package Dependencies: Ø openvpn-client-export-2.6.7 Ø openvpn-2.6.8_1 Ø zip-3.0_1 Ø 7-zip-23.01	
Installed P	ackages Available Packages Package Installer	
Package	Installation	
All reposi	tories are up to date.	<b>^</b>
The follow New packag 7- 1i op pf zi	<pre>ing 5 package(s) will be affected (of 0 checked): es to be INSTALLED: zip: 23.01 [pfSense] bsysinfo: 0.0.3_2 [pfSense] envpn-client-export: 2.6.7 [pfSense] Sense-pkg-openvpn-client-export: 1.9.2 [pfSense] p: 3.0_1 [pfSense]</pre>	
Number of	packages to be installed: 5	
The proces 23 MiB to [1/5] Fetc	s will require 31 MiB more space. be downloaded. hing openvpn-client-export-2.6.7.pkg:	ļ

Pour installer le package pour exporter le client VPN je me rends dans "System > Packet manager > Available Packages" Une fois dans celui si je vais chercher "OpenVPN Client export" et le télécharger.

pfSense-pkg-openvpn-client-export installation successfully completed.

### **MISE EN PLACE OPENVPN**



Only OpenVPN-compatible user certificates are show



- Je me rends ensuite dans "OpenVPN > Client export" et y ajoute "auth-nocache" dans "Advanced > additionnal configuration options"
- Enfin je me rends dans "OPENVPN Clients" puis dans "Archives" je vais télécharger la "Bundled Config" ainsi que le client windows 10 afin de pouvoir le mettre en place sur mon client à l'avenir

#### **MISE EN PLACE OPENVPN RÉGLE FIREWALL**

\Xi 📖 🗐 🙆

Action	Pass		~				
	Choose what to do with pa Hint: the difference betwee whereas with block the page	ckets that match the criteria en block and reject is that wi cket is dropped silently. In ei	a specified below. ith reject, a packet (TC ither case, the original	P RST or ICM packet is dis	/IP port unreachable for UDF scarded.	<sup>D</sup> ) is returned to the s	ender,
Disabled	Disable this rule Set this option to disable the set the set of	his rule without removing it	from the list.				
Interface	WAN		~				
	Choose the interface from	which packets must come t	to match this rule.				
Address Family	IPv4		*				
	Select the Internet Protoco	I version this rule applies to	L				
Protocol	UDP		*				
	Choose which IP protocol t	this rule should match.					
irce <u>Source</u>	<ul> <li>Invert match</li> <li>Display Advanced</li> </ul>	any		~	Source Address	1	v
Irce Source	Invert match  Display Advanced  The Source Port Range for its default value, any.	any a connection is typically rand	dom and almost never	✓ equal to the o	Source Address destination port. In most case	/	<b>~</b> emain at
stination	Invert match  Display Advanced  The Source Port Range for its default value, any.	any a connection is typically rand	dom and almost never	▼ equal to the o	Source Address	es this setting must r	v emain at
stination Destination	Invert match  Display Advanced  The Source Port Range for its default value, any.  Invert match	any a connection is typically rand WAN address	dom and almost never	♥ equal to the o	Source Address destination port. In most case Destination Address	es this setting must r	emain at
stination Port Range	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match</li> <li>(other) </li> </ul>	any a connection is typically rand WAN address 1194	dom and almost never	equal to the o	Source Address destination port. In most case Destination Address	es this setting must r	emain at
etination Destination stination Port Range	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match         <ul> <li>(other)</li> <li>From</li> </ul> </li> </ul>	any a connection is typically rand WAN address 1194 Custom	dom and almost never	equal to the o	Source Address destination port. In most case Destination Address 1994 Custom	es this setting must r	emain at
etination Destination stination Port Range	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match         <ul> <li>(other)</li> <li>From</li> <li>Specify the destination port</li> </ul> </li> </ul>	any a connection is typically rand WAN address 1194 Custom t or port range for this rule. Th	dom and almost never (other) To he "To" field may be lef	equal to the o	Source Address destination port. In most case Destination Address 1994 Custom ly filtering a single port.	es this setting must r	emain at
etination Destination atination Port Range ra Options Log	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match         <ul> <li>(other)</li> <li>From</li> <li>Specify the destination port</li> <li>Log packets that are hard</li> </ul> </li> </ul>	any a connection is typically rand WAN address 1194 Custom t or port range for this rule. The ndled by this rule	dom and almost never (other) To he "To" field may be lef	equal to the o	Source Address destination port. In most case Destination Address 1994 Custom ly filtering a single port.	es this setting must r	emain at
etination Destination stination Port Range ra Options Log	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match         <ul> <li>(other)</li> <li>From</li> </ul> </li> <li>Specify the destination port</li> <li>Log packets that are hand Hint: the firewall has limited the Status: System Logs: Second Science Scienc</li></ul>	any a connection is typically rand WAN address 1194 Custom t or port range for this rule. The ndled by this rule d local log space. Don't turn of ettings page).	dom and almost never (other) To he "To" field may be lef	equal to the o	Source Address destination port. In most case Destination Address 1994 Custom ly filtering a single port.	es this setting must r	emain at
etination Control Cont	<ul> <li>Invert match</li> <li>Display Advanced</li> <li>The Source Port Range for its default value, any.</li> <li>Invert match         <ul> <li>(other)</li> <li>From</li> <li>Specify the destination port</li> <li>Log packets that are har Hint: the firewall has limited the Status: System Logs: So</li> <li>Accès VPN</li> </ul> </li> </ul>	a connection is typically rand WAN address 1194 Custom t or port range for this rule. The ndled by this rule d local log space. Don't turn of ettings page).	dom and almost never (other) To he "To" field may be lef	equal to the o	Source Address destination port. In most case Destination Address 1994 Custom ly filtering a single port.	es this setting must r	emain at

Firewall / Rules / Edit

Je vais dans un dernier temps mettre en place une règles de Firewall OpenVPN sur l'interface WAN avec les informations suivante : Action : Pass Interface : Wan Address Familly : IPv4 Protocol: UDP

Source : Any **Destination : Wan Address** Port range: le port VPN 1194

### **TEST CLIENT VPN**

Accès rapide Bureau	Nom	,		Dasharahar daar 70	lásharra
Accès rapide Bureau a Téléchargements a	Nom		~ C	Rechercher dans : Té	lécharge
Bureau a			Modifié le	Туре	Taille
Téléchargements	<ul> <li>Aujourd'hui (2) –</li> </ul>				
Documente	7z openvpn-pfSense	PN-UDP4-1194-DRUE	22/11/2024 23:58	Application	3 86
vocuments x	pfSenseVPN-UDP4	4-1194-DRUELLEVPN-c	22/11/2024 22:54	Dossier compressé	
Image					
	Setup Open//PN 2.6 7-1001				
	g setup openvin 2.0.7 1001				
	Choose setup type.			$\mathbf{O}$	
		Customize			
	config			- 0	×
← → × ↑	vertage Africhage	> OpenVPN > config	× õ	Rechercher dans : config	0
	Nom	^	Modifié le	Type Taille	
	s A	DP4-1194-DRUELLEVPN	23/11/2024 00:19	Dossier de fichiers	

#### Sur le client j'installe OpenVPN précédemment télécharger.



Une fois celui-ci installer je me rends dans "C://Utilisateur/Windows/OPENVPN/config" Une fois dans celui-cij'y ajoute la configuration.

### **TEST CLIENT VPN**

Afficher le statut Voir le log	Configuration Quitter		<b>i</b>
Reprendre	Importer	>	it o
Déconnecter	pfSenseVPN-UDP4-1194-DRUELLEVPN-config	>	
Connecter	pfSenseVPN-UDP4-1194-DRUELLEVPN	$\rightarrow$	

Connexion OpenV	PfSenseVPN-UDP4-1194-DRUELLEVPN	× - • ×
Sat Nov 23 00:20:39 Sat Nov 23 00:20:39 Sat Nov 23 00:20:39 Sat Nov 23 00:20:39 Sat Nov 23 00:20:39	Utilisateur: DRUELLEVPN Mot de passe:	ndows [SSL (OpenSSL)] [LZO] [l d64 executable 2.10
<		>
Déconnecter	Reprendre	OpenVPN GUI 11.45.0.0/2.6.7 Fermer

#### Une fois cela fait je lance le VPN et me connecte à celui ci en renseignant l'utilisateur précédemment créer. On peut voir ici que le VPN ce connecte bien





#### **TEST ACCES SERVEUR LAMP**

Apache2 Debian Default Page: It v × +				-	Ð	×
C Non sécurisé   192.168.202.22	ටන්	A∿ ⊡a	☆	£≞		0
Apache2 Debian Default Pag	je					Î
debian						
It works!						
This is the default welcome page used to test the correct operation of the Apa installation on Debian systems. If you can read this page, it means that the A installed at this site is working properly. You should <b>replace this file</b> (located /var/www/html/index.html) before continuing to operate your HTTP server.	ache2 server after Apache HTTP server d at					
If you are a normal user of this web site and don't know what this page is about that the site is currently unavailable due to maintenance. If the problem persistie's administrator.	out, this probably means ists, please contact the					
Configuration Overview						
Debian's Apache2 default configuration is different from the upstream default into several files optimized for interaction with Debian tools. The configuration <b>documented in /usr/share/doc/apache2/README.Debian.gz</b> . Refer to documentation. Documentation for the web server itself can be found by acce apache2-doc package was installed on this server.	: configuration, and split n system is <b>fully</b> ) this for the full essing the <b>manual</b> if the					l
The configuration layout for an Apache2 web server installation on Debian sys	stems is as follows:					
<pre>/etc/apache2/   apache2.conf   ` ports.conf   mods-enabled     *.load   ` *.conf   conf-enabled   ` *.conf   sites-enabled   ` *.conf</pre>	Activer Win	dows				
	Accédez aux p	ramètres p				
<ul> <li>apache2.conf is the main configuration file. It puts the pieces together by</li> </ul>	including all remaining					÷

#### On peut ici voir que je peux accéder à mon serveur