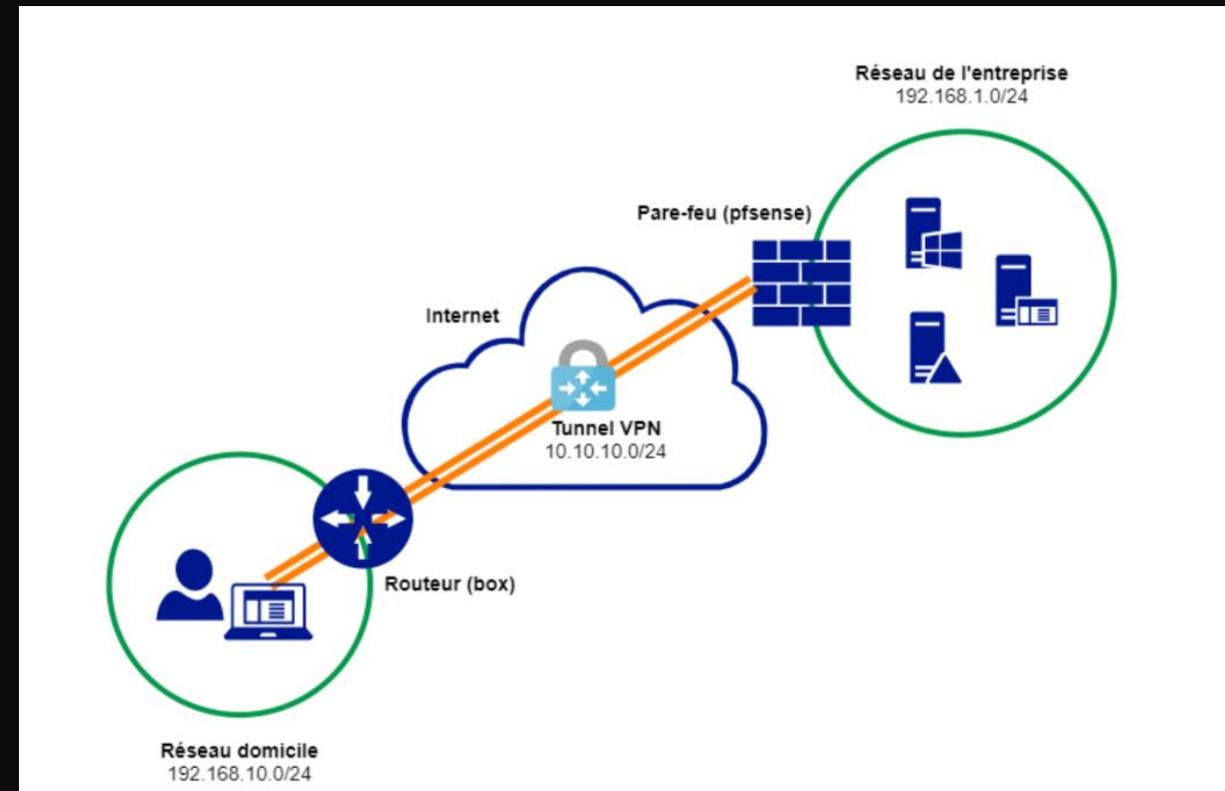


TP VPN



Mise en contexte

Je vais devoir mettre en place un VPN depuis le réseau de l'entreprise à l'aide de Pfsense afin de pouvoir permettre aux utilisateurs de se connecter au réseau depuis chez eux via OpenVPN, nous avons l'infrastructure suivante :



Mise en place du pfsense.

Tout d'abord il faudra mettre en place la machine pfsense, avec deux cartes réseaux, une pour le WAN (vmbro0), et une pour le LAN (vmbro8).

Ensuite pour ce qui est de l'installation de pfsense, elle a été réalisée dans un tp precedent. ([Cliquer ici pour le consulter](#)).

Il faudra mettre la même carte réseau que pour le LAN sur la machine cliente afin de pouvoir le paramétrer.

Memory	2.00 GiB
Processors	2 (2 sockets, 1 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media=cdrom,size=636498K
Hard Disk (scsi0)	local-lvm:vm-108-disk-0,iotread=1,size=20G
Network Device (net0)	virtio=BC:24:11:9D:5A:20,bridge=vmbro0,firewall=1
Network Device (net1)	virtio=BC:24:11:2B:00:30,bridge=vmbro8,firewall=1

Memory	4.00 GiB
Processors	4 (1 sockets, 4 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/linuxmint-22-mate-64bit.iso,media=cdrom,size=2832M
Hard Disk (scsi0)	local-lvm:vm-113-disk-0,iotread=1,size=100G
Network Device (net0)	virtio=BC:24:11:EF:27:B6,bridge=vmbro8,firewall=1

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VM Guest - Netgate Device ID: 742f7e85f36e01e8befb
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.90/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24

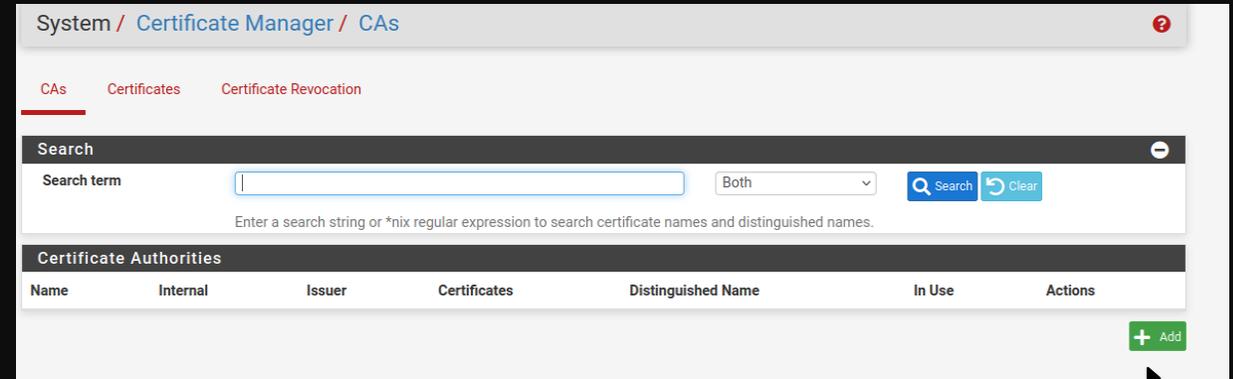
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

Créer une autorité de certification

Pour créer l'autorité de certification qui est nécessaire pour configurer le VPN SSL, il faudra se rendre dans system, et cert manager. Ensuite il faudra cliquer sur Add pour rentrer dans la page de configuration.

Dans Descriptive name, il faudra indiquer le nom du certificat, ici CA-UGO.

Dans Common name, il y'a le nom qui sera intégré dans les certificats qui seront générés, pour ma part j'ai mis ugo. La modification des autres informations n'est pas obligatoire. Ensuite nous pouvons valider la configuration.



System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

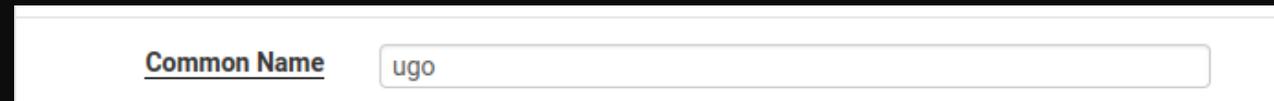
Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
						<input type="button" value="+ Add"/>

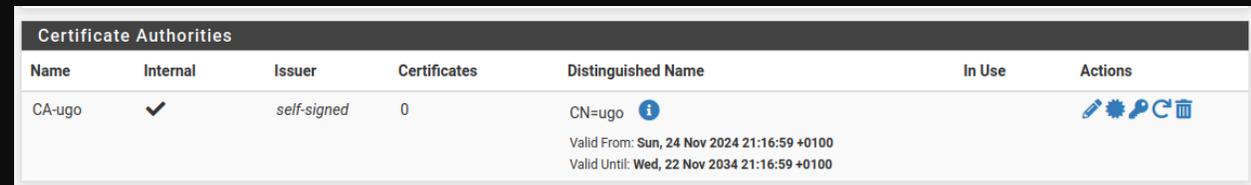


Create / Edit CA

Descriptive name



Common Name



Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-ugo	✓	self-signed	0	CN=ugo <input type="button" value="i"/> Valid From: Sun, 24 Nov 2024 21:16:59 +0100 Valid Until: Wed, 22 Nov 2034 21:16:59 +0100		<input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/>

Création d'un utilisateur

Ensuite nous allons créer un utilisateur sur pfsense dans system, user manager puis add.

Il faudra renseigner son username, ici vpn.ugo et créer un mot de passe.

Ensuite il faudra cocher la case "click to create a user certificate" pour pouvoir paramétrer la création du certificat utilisateur, il faudra rentrer un descriptive name et vérifier que l'autorité de certificat correspond à celle créée précédemment.

Ensuite nous pouvons valider et l'utilisateur et son certificat est créé.

Dans le manager de certificat, nous pouvons constater que le certificat de type utilisateur a été créé.

The screenshot shows the 'Properties' form for creating a user. It includes the following fields and options:

- Defined by:** USER
- Disabled:** This user cannot login
- Username:** vpn.ugo
- Password:** Two masked password input fields.

The screenshot shows the 'Create Certificate for User' form with the following fields:

- Descriptive name:** Certificat-VPN-Ugo
- Certificate authority:** CA-UGO

The screenshot shows a list of users. The user 'vpn.ugo' is listed with a checkmark in the status column, indicating successful creation.

The screenshot shows the details of a certificate in the manager. The certificate is named 'User Cert' and is associated with the CA 'CA-UGO'. The details are as follows:

- Certificate:** Certificat-VPN-Ugo
- Type:** User Certificate
- CA:** No
- Server:** No
- Authority:** CA-UGO
- Common Name (CN):** CN=vpn.ugo
- Valid From:** Wed, 20 Nov 2024 09:50:45 +0100
- Valid Until:** Sat, 18 Nov 2034 09:50:45 +0100

Installation du paquet OpenVPN

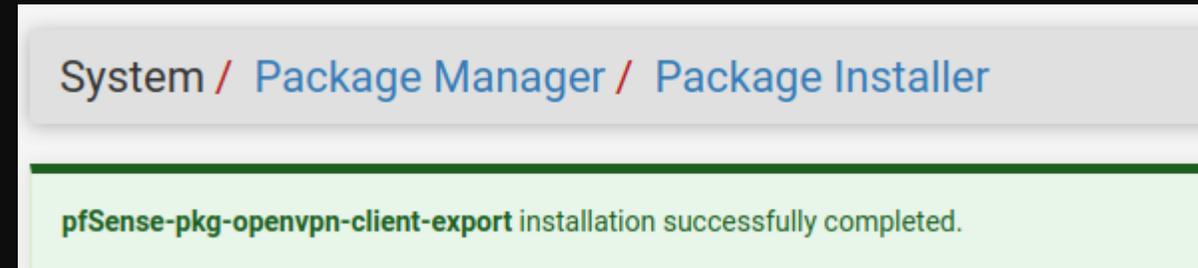
Afin de paramétrer le VPN, il faudra installer le paquet OPENvpn Servers.

Il faudra se rendre dans system, puis package manager puis package installer et rechercher openvpn et installer.

Ensuite, pour pouvoir le paramétrer, il faudra se rendre dans VPN, puis OpenVPN, puis servers et add.

Pour ce qui est de la configuration, on choisira le mode serveur remote access ssl/tls + user auth, le protocole sera UDP sur l'interface WAN et le port sera 1194.

Pour ce qui est de l'encryption, utiliser AES-256-CBC sera plus sécurisé.



Mode Configuration

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication Local Database

Device mode 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.)

Endpoint Configuration

Protocol UDP on IPv4 only

Interface WAN

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 1194

The port used by OpenVPN to receive client connections.

Data Encryption Algorithms

AES-256-CBC (256 bit key, 128 bit block)
AES-256-CFB (256 bit key, 128 bit block)
AES-256-CFB1 (256 bit key, 128 bit block)
AES-256-CFB8 (256 bit key, 128 bit block)
AES-256-GCM (256 bit key, 128 bit block)
AES-256-OFB (256 bit key, 128 bit block)
CAMELLIA-128-CBC (128 bit key, 128 bit block)
CAMELLIA-128-CFB (128 bit key, 128 bit block)
CAMELLIA-128-CFB1 (128 bit key, 128 bit block)
CAMELLIA-128-CFB8 (128 bit key, 128 bit block)

Available Data Encryption Algorithms

AES-256-CBC

Allowed Data Encryption Algorithms. Click an algorithm name to remove.

Paramètres du serveur VPN

Ensuite, il faudra renseigner le autorité de certificate, et le certificate du serveur.

Pour l'IPv4 du tunnel Network, comme vu précédemment, le réseau sera 10.10.10.0/24 et le réseau local sera 192.168.1.0/24.

Il est recommandé d'active le mode IP dynamique afin de permettre aux clients mobiles géographiquement de pouvoir se connecter.

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances 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 HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority CA-ugo

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate Certificat-OpenVPN (Server: Yes, CA: CA-ugo)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

Tunnel Settings

IPv4 Tunnel Network 10.10.10.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts 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. The remaining usable addresses will be assigned to connecting clients.
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 not compatible with several options, including Exit Notify, and Inactive.

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 hosts expressed using CIDR notation (e.g. fe80::/64). The -1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

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) 192.168.1.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network 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 set to the LAN network.

Client Settings

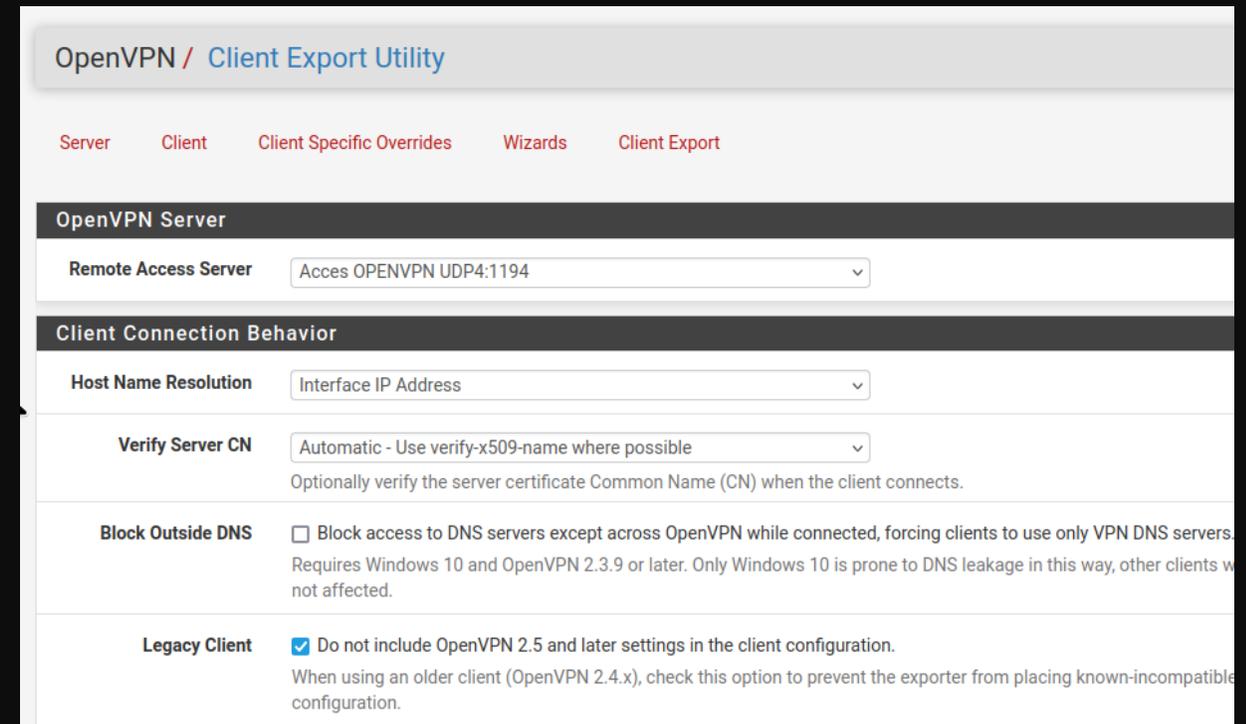
Dynamic IP Allow connected clients to retain their connections if their IP address changes.

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 clients such as Yealink phones may require "net30".

Exporter la configuration

Pour exporter la configuration VPN, il faudra se rendre dans OpenVPN, puis Client export utility et server, mettre dans le host name resolution "interface IP address et" cocher legacy client pour les clients utilisant une vieille version d'openvpn.

Ensuite il faudra télécharger la version archive de la configuration.



OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server: Acces OPENVPN UDP4:1194

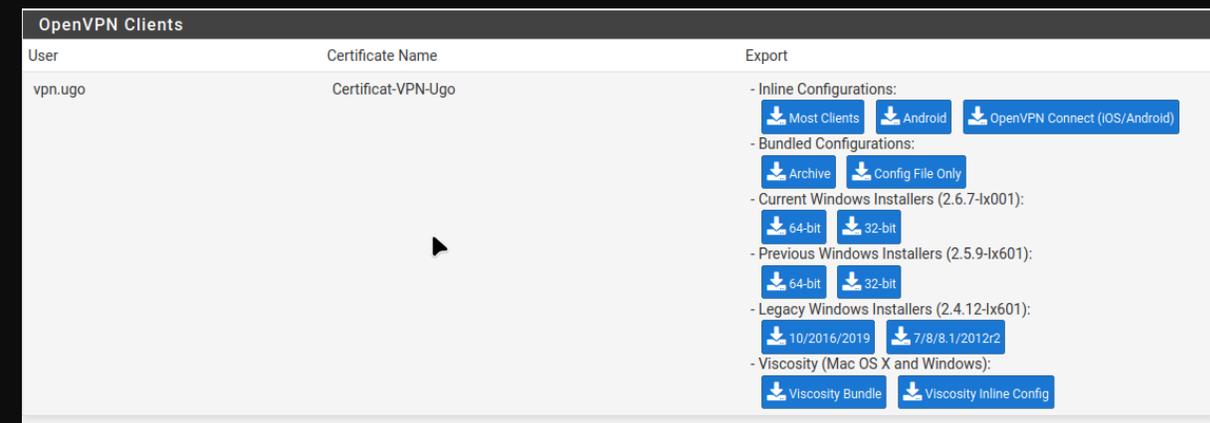
Client Connection Behavior

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS: Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will not be affected.

Legacy Client: Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible configuration.



OpenVPN Clients

User	Certificate Name	Export
vpn.ugo	Certificat-VPN-Ugo	<ul style="list-style-type: none">- Inline Configurations:<ul style="list-style-type: none">Most ClientsAndroidOpenVPN Connect (iOS/Android)- Bundled Configurations:<ul style="list-style-type: none">ArchiveConfig File Only- Current Windows Installers (2.6.7-1x001):<ul style="list-style-type: none">64-bit32-bit- Previous Windows Installers (2.5.9-1x601):<ul style="list-style-type: none">64-bit32-bit- Legacy Windows Installers (2.4.12-1x601):<ul style="list-style-type: none">10/2016/20197/8/8.1/2012r2- Viscosity (Mac OS X and Windows):<ul style="list-style-type: none">Viscosity BundleViscosity Inline Config

Ajout de règles du pare-feu

Ensuite, il faudra se rendre dans les règles du WAN, et ajouter une règle autorisant le protocole UDP pour le port 1194.

Et il faudra également rajouter une règle sur le pare-feu pour OpenVPN qui autorise les requêtes à destination du port 3389 pour le réseau 192.168.1.0

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol UDP
Choose which IP protocol this rule should match.

Destination

Destination Invert match WAN address Destination Address /

Destination Port Range OpenVPN (1194) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

0/0 B IPv4 UDP * * WAN address 1194 (OpenVPN) * none

Firewall / Rules / OpenVPN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN **OpenVPN**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	IPv4	TCP	*	192.168.1.0	3389 (MS RDP)	*	none			

Destination

Destination Invert match Address or Alias 192.168.1.0 /

Destination Port Range MS RDP (3389) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Connexion avec le client

Ensuite il faudra télécharger le client OpenVPN sur la machine et télécharger le fichier de configuration exporté précédemment. Il faudra exporter ce fichier dans le dossier C:/programfiles/OpenVPN/config sur Windows.

Ensuite il faudra ouvrir OpenVPN et saisir le nom d'utilisateur et le mot de passe créé sur pfsense précédemment.

