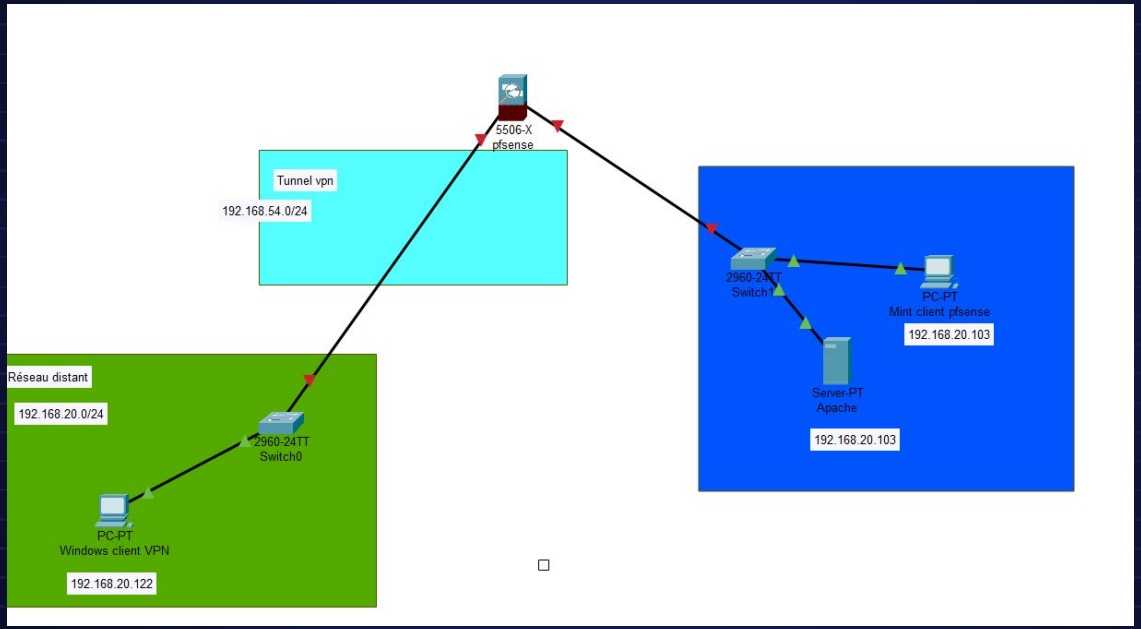
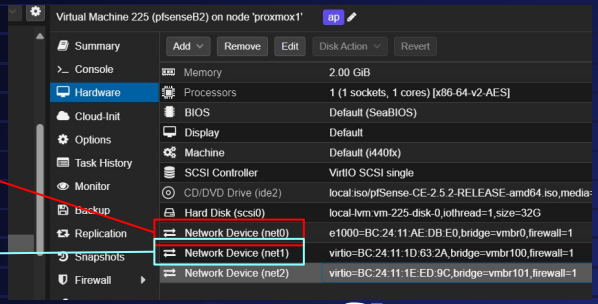
VPN SOUS PFSENSE

TOPOLOGIE


5506-X
pfsense
Tunnel vpn
192.168.54.0/24
2960-24TT
Switch1
PC-PT
Mint client pfsense
192.168.20.103
Server-PT
Apache
192.168.20.103
Réseau distant
192.168.20.0/24
2960-24TT
Switch0
PC-PT
Windows client VPN
192.168.20.122

Mise en place de l'environnement

Premièrement je met en place sur mon proxmox un pfsense avec dans notre contexte, ajouter une carte réseau pour le LAN et garder celle de base pour le wan. (ici la 3ème est pour la DMZ mais c'est optionnel)



Configuration du pfsense

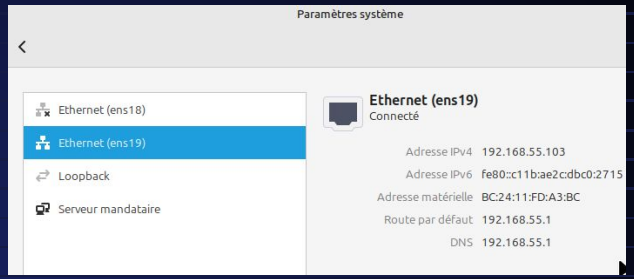
Ensuite quand on lance le pfsense, on assigne les interfaces en appuyant 2

et on attribue une ip aux interfaces wan et lan

```
Starting cron... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 087a611f1adfd52c8b41

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)       -> em0        -> v4/DHCP4: 192.168.20.62/24
LAN (lan)       -> vtnet0     -> v4: 192.168.55.1/24
DMZ (opt1)      -> vtnet1     -> v4: 192.168.65.1/24

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
```

Mise en place d'une debian

Dans un premier temps, je vais simplement cloner ma VM modèle, et je vais lui modifier sa carte réseau pour la pointer sur vmbr100 qui permettra d'être sur le LAN du réseau

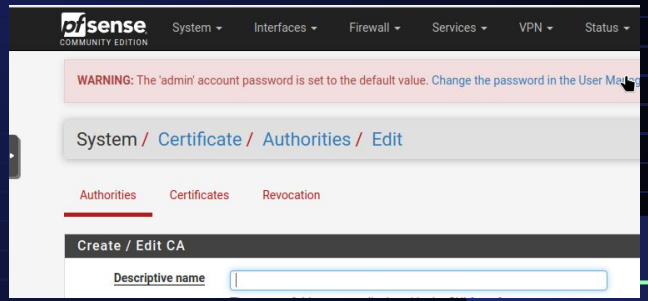


Configuration du VPN

Une fois toutes les étapes précédentes réalisées, je dispose à présent d'un PFsense vierge . Il ne nous reste plus qu'à configurer le VPN, appliquer des règles firewalll, et tester.

Autorité de certification.

Le client et le serveur VPN sont authentifiés à l'aide de certificats. Pour cela, ces certificats doivent être émis par une autorité de certification reconnue comme sûre aussi bien par le serveur que par le client. Dans notre cas, c'est avec notre PFsense que nous créerons une autorité de certification, pour ce faire, je vais dans System>Certificate > Authorities.



Je vais par la suite, remplir les informations suivantes :

Descriptive name: MorellePFSenseVPN

Method : Create a internal CA

Common-name: Morelle

Créer un certificat serveur.

Ensuite, pour créer un certificat de type serveur, je me rends dans System>Certificates>Certificates.

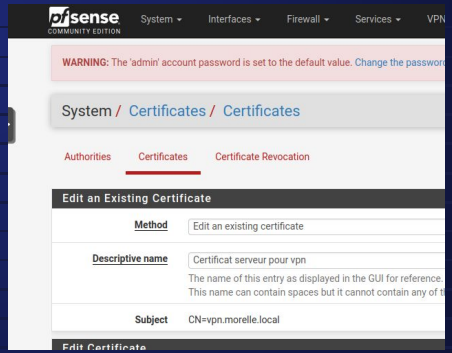
Dans cette page, je renseigne les informations suivantes :

Descriptivename: Certificat Serveur pour VPN

Common Name : vpn.morelle.local

Certificat Type : Server Certificate

Alternative Names: vpn.morelle.local



Créer un user et son certificat.

Dans cette étape, je vais créer un utilisateur ainsi que son certificat, celui-ci nous permettra de nous connecter au VPN. Pour créer un utilisateur, je me rends dans System> UserManager.

Ici, nous allons créer notre user, je précise les informations nécessaires, à savoir:

Username: lorenzo.vpn Password: sio$2024

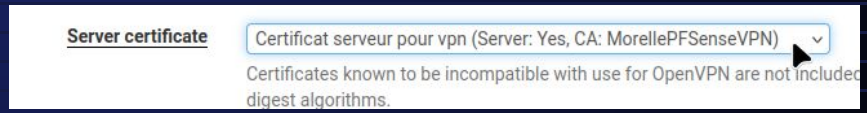
Fullname: lorenzomorelle Et je veille bien à cocher ”Click to create à user certificate”

et pour Descriptive name je met Certificat-VPN

Config OpenVPN Serveur.

Place à la configuration d’OPEN VPN, je me rends dans l’onglet VPN > OPENVPN > Server Voici les informations renseignées :

Dans général Information :Description : VPNMORELLE
Dans mode configuration Server mode : Remote Access (SSL/TLS + User Auth)
Backend for auth. : Local Database
Device mode : tun – Layer 3 Tunnel Mode
Dans endpoint Configuration :Protocol: UDP on IPv4 only
Interface: WAN
Local port : 1194
Dans Cryptographic Settings : Server certificate: Certificat Serveur pour VPN (celui créer précédemment)
Ensuite on laisse par défaut pour cette partie



Config OpenVPN Serveur.

La configuration maintenant à moitié faites, il ne nous reste plus qu'à faire la configuration liée au tunnel VPN.

Dans tunel Settings Je renseigne dans IPv4 Tunnel Network, l'adresse réseau que nous assignons au tunnel vpn je met : 192.168.54.0/24

Dans IPv4 Local Network, j'entre la / les adresse réseau que je désire mettre à disposition de mes clients VPN ici 192.168.55.0/24

Puis, dans Concurrent Connections, j'entre la valeur 10, cette variable correspond au nombre d'user simultanés

Dans client settings on va opter pour la topology net30 (attention, avec cette option 1user = 4 ip)

Dans Advanced Client settings on coche DNS Default Domain, et on met comme nom ici **vpn.morelle.local** de DNS.

Puis dans **Advanced Configuration**, je vais saisir l'option customisé "auth-nocache" qui va apporter une couche de protection en plus, pour empêcher la mise en cache de logins.

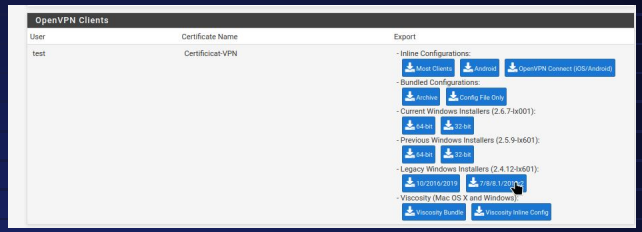
Exporter le certificat.

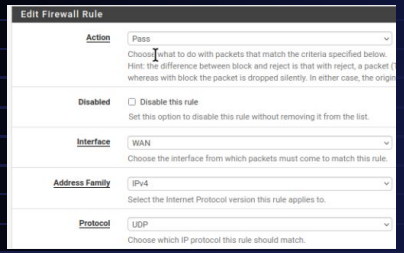
Pour exporter la configuration, on va aller dans System > Packet manager. Je vais chercher OpenVPN Client export dans available package, et je vais le télécharger. On devrait le retrouver dans l'onglet "installed packages".

Par la suite, je me rends sur "OPENVPN", puis dans "client export". Ici, on prend connaissance des configurations mises par défaut, dans mon cas je ne change rien sauf dans Advanced > "additionnal configuration options" où je vais écrire "auth-nocache".

Exporter le certificat.

Puis je fais “Save as Default”. Ensuite, en bas de cette page, on distingue une section “OPENVPN Clients”. Ici, je vais cliquer sur “Archive” dans Bundled Config. Et j’irais prendre plus tard l’installateur pour Windows10 pour mon client) .

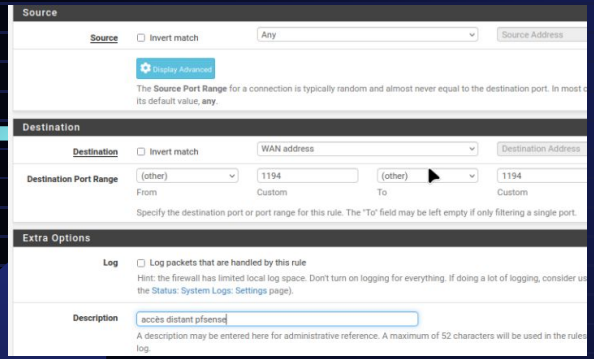




Règles Firewall openVPN

Voici la règle mise en place dans l’interface WAN. Allez dans firewall>rules>WAN et mettez comme sur les screen

Action : Pass **Interface** : WAN **Address Family** : Ipv4 **Protocol** : UDP



Source : any

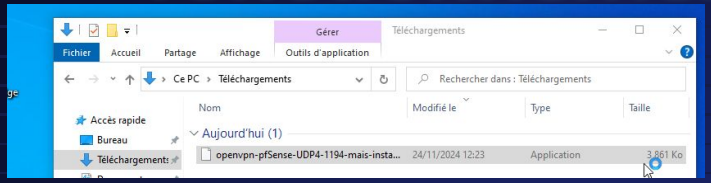
Destination : WAN Address

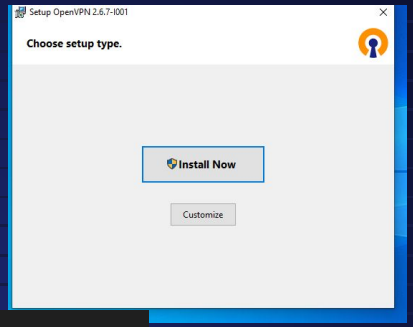
Port Range : (notre port de vpn, par défaut : 1194)

Description: Accès distant pfsense

Vérifications du fonctionnement du VPN.

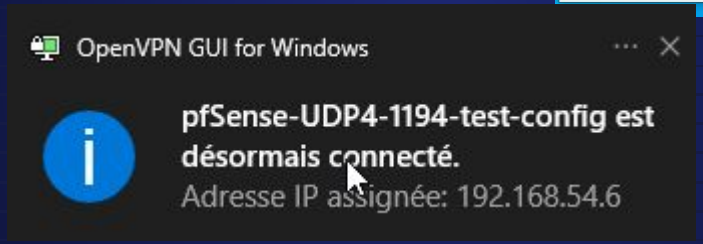
On clique sur le .exe





et on fais install now

on fait clique droit se connecter dans la barre des tache sur l'icône de notre logiciel et on met le user et le mdp



Tests avec HTTP

On peut donc se connecter et ça vérifie donc que le vpn fonctionne