TP 28 : VPN entre un client distant et un serveur OpenVPN

Objectifs

Le DSI de GSB souhaite mettre à disposition de ses agents itinérants extérieurs plusieurs applications installées sur les serveurs GSB et utilisables à distance grâce à une connexion sécurisée VPN SSL/TLS de type nomade, c'est à dire ~~**entre un client distant et un serveur VPN**~~.

Très important :

OpenVPN permet de monter un VPN de manière simple et efficace.
OpenVPN peut être installé sur un serveur Linux indépendant (éventuellement placé dans une DMZ).
Il peut aussi être installé sur le routeur-parefeu PfSense puisqu'il est disponible nativement sur Pfsense.

Nous installerons donc le serveur VPN sur le Pfsense.
Les clients VPN seront installés sur des machines Windows ; ils recevront une adresse sur le réseau par défaut 192.168.100.0/24 et auront accès au réseau 192.168.3.0/24.

Le client et le serveur pourraient s'authentifier simplement avec un système de clés partagées.
Mais il est plus judicieux d'utiliser des certificats (SSL/TLS) gérés par une PKI (Public Key Infrastructure) pour une meilleure sécurité.

Le client et le serveur OpenVPN seront donc 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.
Ces certificats seront utilisés uniquement en interne dans la société GSB. Nous allons donc installer une Autorité de Certification interne chez GSB.
On peut installer cette AC sur un serveur Windows qui possède un rôle d'Infrastructure à Clés Publiques (PKI).
Mais Pfsense dispose nativement d'une Infrastructure à Clés Publiques (PKI).
Dans notre cas, nous créerons donc une autorité de certification appelée "**AC_GSB_PKI**" (AC pour *Autorité de Certification* et PKI pour *Public Key Infrastructure*) sur le pfSense faisant office de serveur. Puis nous créerons deux certificats : un certificat client (qui sera utilisé par le Client pour s'authentifier auprès du serveur) et un certificat serveur (qui sera présenté par le Serveur au client qui pourra ainsi authentifier ce serveur). Ces deux certificats seront signés par l'autorité de certification interne GSB que nous aurons créée précédemment.

Attention : lorsqu'un client se connecte au serveur VPN, celui-ci lui présente son certificat contenant la signature par l'AC interne GSB qui a été chiffrée avec la clé privée de cette AC.
Pour valider la signature de ce certificat, le client doit disposer de la clé publique de cette AC.

Or le client ne peut pas posséder cette clé publique dans son magasin de certificats d'autorités de certification puisque l'AC que nous utilisons ici est une AC interne GSB.
Il sera donc nécessaire d'envoyer au client la clé publique de l'AC interne GSB, en même temps que les fichiers de configuration permettant de configurer le logiciel client VPN (cf Annexe 5).

Travail à faire

A - Configuration de l'AC interne GSB et configuration du serveur VPN

Préparer et effectuer l'installation du VPN nomade en tenant compte des contraintes suivantes :

- Le serveur VPN sera OpenVPN ; il sera configuré sur le ROUTEUR-PAREFEU PfSense qui intègre d'origine OpenVPN. Il gérera l'autorité de certification interne GSB et permettra de créer les certificats du serveur OpenVPN et de ses clients OpenVPN.
- On conservera le port 1194 utilisé par défaut dans un serveur OpenVPN pour la transmission sécurisée.
- Dans le VPN, le serveur VPN recevra l'adresse virtuelle 192.168.100.1/24

B - Configuration du client VPN nomade

Préparer et effectuer l'installation du VPN nomade en tenant compte des contraintes suivantes :

- Chaque machine Windows souhaitant se connecter au serveur OpenVPN utilisera le client VPN *OpenVPN GUI for Windows* et disposera d'un certificat client ;
- Un utilisateur de nom ***User_VPN*** et de mot de passe ***faure*** sera créé localement sur le serveur OpenVPN ; tout utilisateur pourra utiliser ce compte local pour s'authentifier lors de la connexion VPN.
- On testera la connexion VPN depuis un poste test de la salle R211.
- Dans le VPN, un client recevra une adresse virtuelle à partir de 192.168.100.2/24.

C -Configuration des applications pour être utilisables à distance, tests et vérification du tunnel (analyse de trames avec Wireshark)

- Les applications utilisables à distance seront installées sur le serveur hôte de session de bureau à distance SERVEUR1 et exécutées grâce à la fonction *Connexion Bureau à distance* des clients distants Windows ; on utilisera *Cisco Packet Tracer* comme application-test distante.
- On utilisera Wireshark pour vérifier que le tunnel est bien mis en place.

Eléments techniques

Téléchargement du client OpenVPN GUI for Windows :
http://openvpn.net/index.php/open-source/downloads.html

- Tutoriel pour la création d'une autorité de certification sur le routeur-parefeu PfSense, et la création du certificat de serveur : Annexe 1
- Tutoriel pour la création d'un utilisateur et de son certificat sur le routeur-parefeu PfSense : Annexe 2
- Tutoriel pour l'exportation de la configuration du client depuis PfSense : Annexe 3
- Tutoriel pour la configuration du serveur OpenVPN sur le routeur-parefeu PfSense : Annexe 4
- Tutoriel pour l'installation du client OpenVPN sur un poste client : Annexe 5
- Tutoriel pour la vérification du tunnel : Annexe 6
- Identifiants et mots de passe à utiliser :

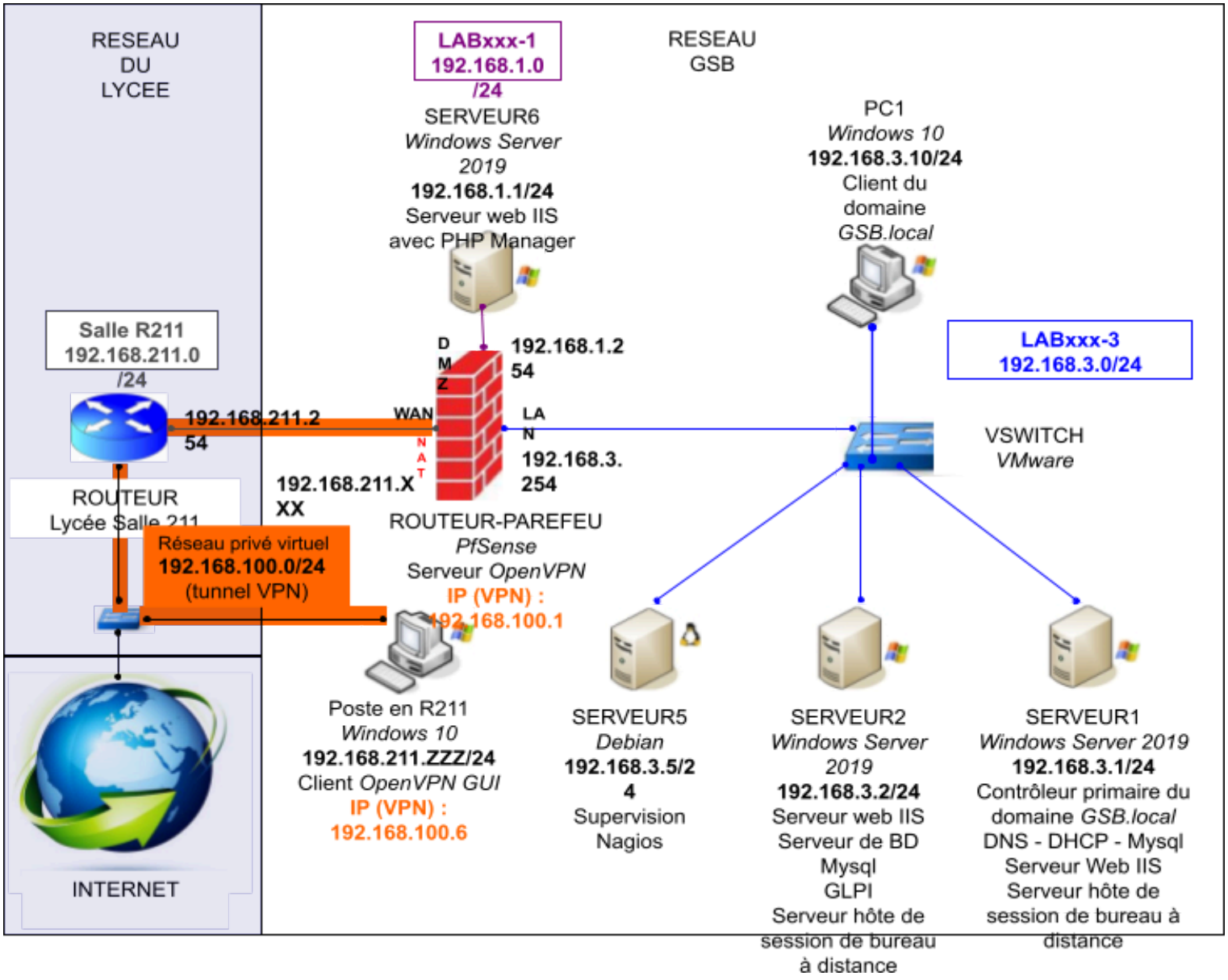
Serveur Windows 2019 :	*Administrateur/Windows2019*
SGBD Msql :	*root/root*
Routeur-parefeu PfSense :	*admin/pfsense*
Serveur Debian :	*root/root* et *debian/debian*
Windows 10 (administrateur local) :	*sio/sio*

Remarques importantes

Tous les certificats créés dans ce TP auront les caractéristiques suivantes :

- leur clé publique aura une taille de 2048 bits (soit 256 octets)
- ils utiliseront l'algorithme de hashage SHA à 256 bits (SHA256)
- ils utiliseront l'algorithme de chiffrement AES-CBC à 256 bits (AES-256-CBC)

Schéma du réseau

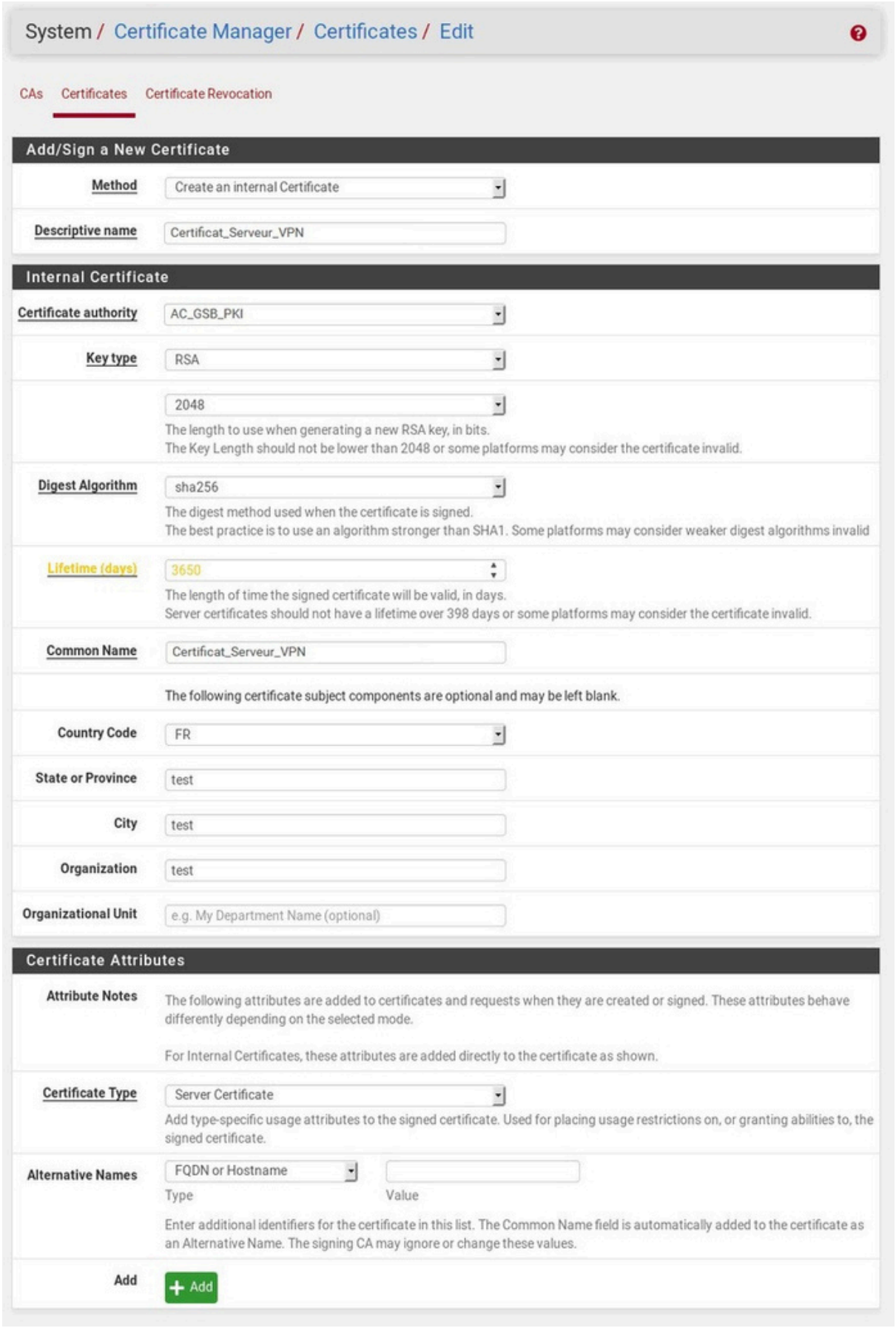


Annexe 1 : Création d'une Autorité de Certification *AC_GSB_PKI* interne à GSB sur le routeur-parefeu PfSense avec son certificat ; création du certificat du serveur OpenVPN

a. Depuisle poste SERVEUR1 par exemple, se connecter à l'interface LAN du routeur-parefeu Pfsense pour le configurer, avec le navigateur Mozilla Firefox.

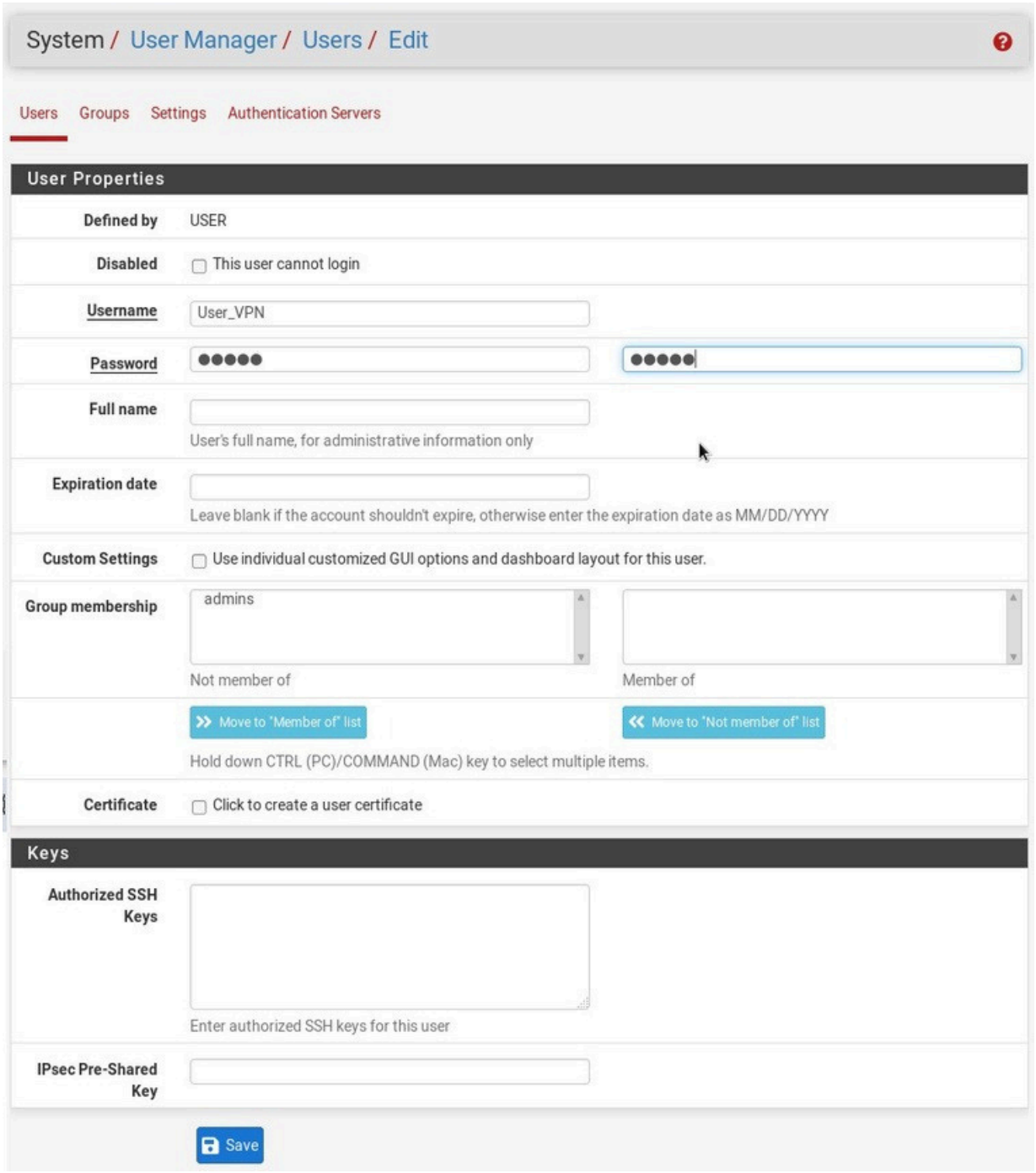
b. Sélectionner la commande PfSense *System Cert Manager*, puis dans l'onglet *CAs*, créer une nouvelle autorité de certification et son certificat d'autorité de certification, en cliquant sur *Add*, de nom *AC_GSB_PKI*, avec une clé *RSA* de *2048* bits, l'algorithme de hashage *sha256*, et en choisissant la méthode *Create an internal Certificate Authority* (**attention : veiller à toujours mettre le même nom pour les champs *Descriptive Name* et *Common Name***) :

c. Toujours dans la commande *System Cert Manager*, mais dans l'onglet *Certificates*, créer un nouveau certificat de nom *Certificat_Serveur_VPN*, le certificat SSL du serveur Pfsense OpenVPN (dont la clé publique permettra de chiffrer le trafic entre client et serveur VPN), de nom *Certificat_Serveur_VPN*, de type ***Server Certificate***, et en choisissant la méthode *Create an internal Certificate* ; sélectionner l'autorité de certification créée précédemment *AC_GSB_PKI* qui va signer ce certificat (**attention : veiller à toujours mettre le même nom pour les champs *Descriptive Name* et *Common Name***) :

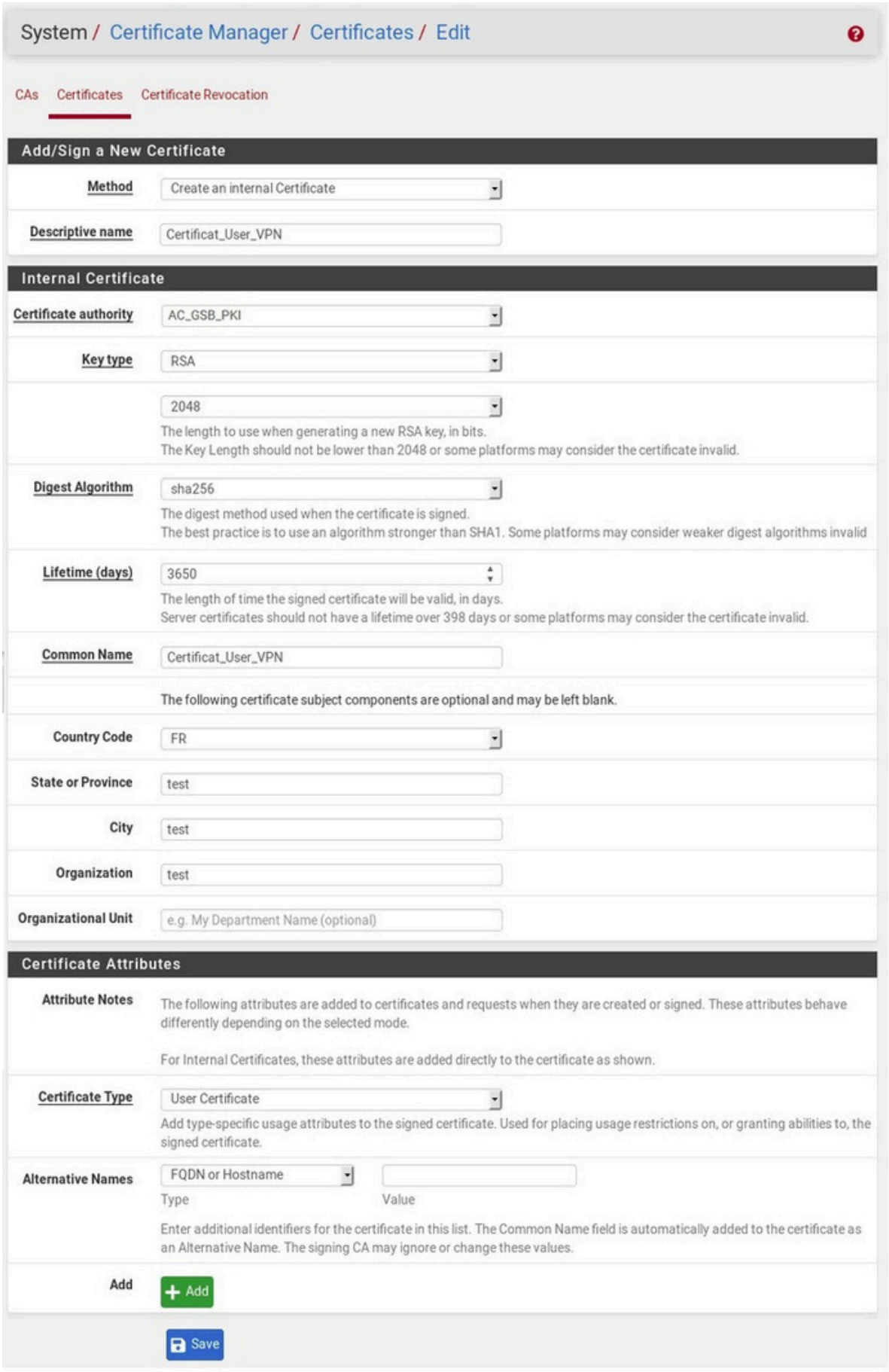


Annexe 2 : Création d'un utilisateur et de son certificat sur le routeur-parefeu PfSense

a. Sélectionnerla commande PfSense *SystemUser Manager* (*Gestionnaire d'usagers*),puisdansl'onglet*Users*, créer un nouvel utilisateur, de nom *User_VPN*, et de mot de passe *faure* :

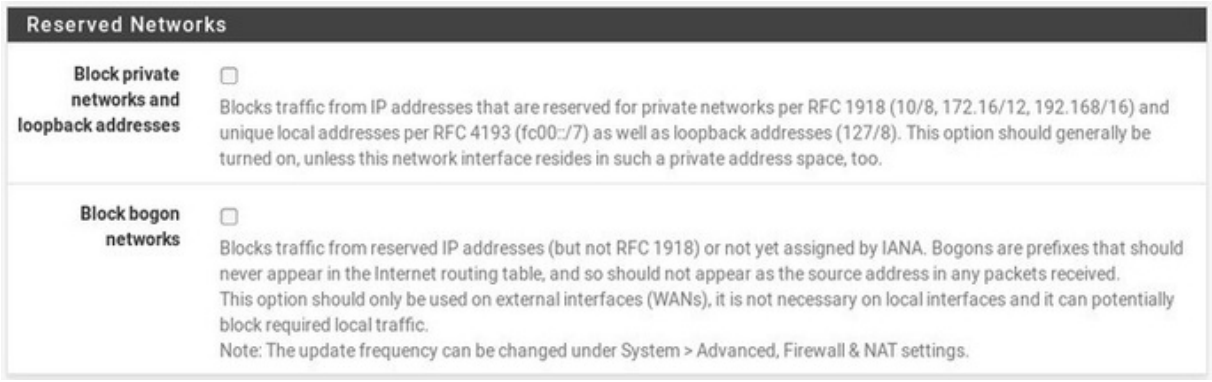


b. Après avoir enregistré l'utilisateur, cliquer sur l'outil en face de cet utilisateur pour le modifier, puis cliquer sur *Add* dans la section *User Certificates* pour associer un nouveau certificat à cet utilisateur ; choisir la méthode *Create an internal Certificate,* le nom *Certificat_User_VPN*, et le **type *User Certificate*** ; l'autorité de certification certifiant ce certificat utilisateur doit être celle créée précédemment : *AC_GSB_PKI*) (**attention : veiller à toujours mettre le même nom pour les champs *Descriptive Name* et *Common Name***) :



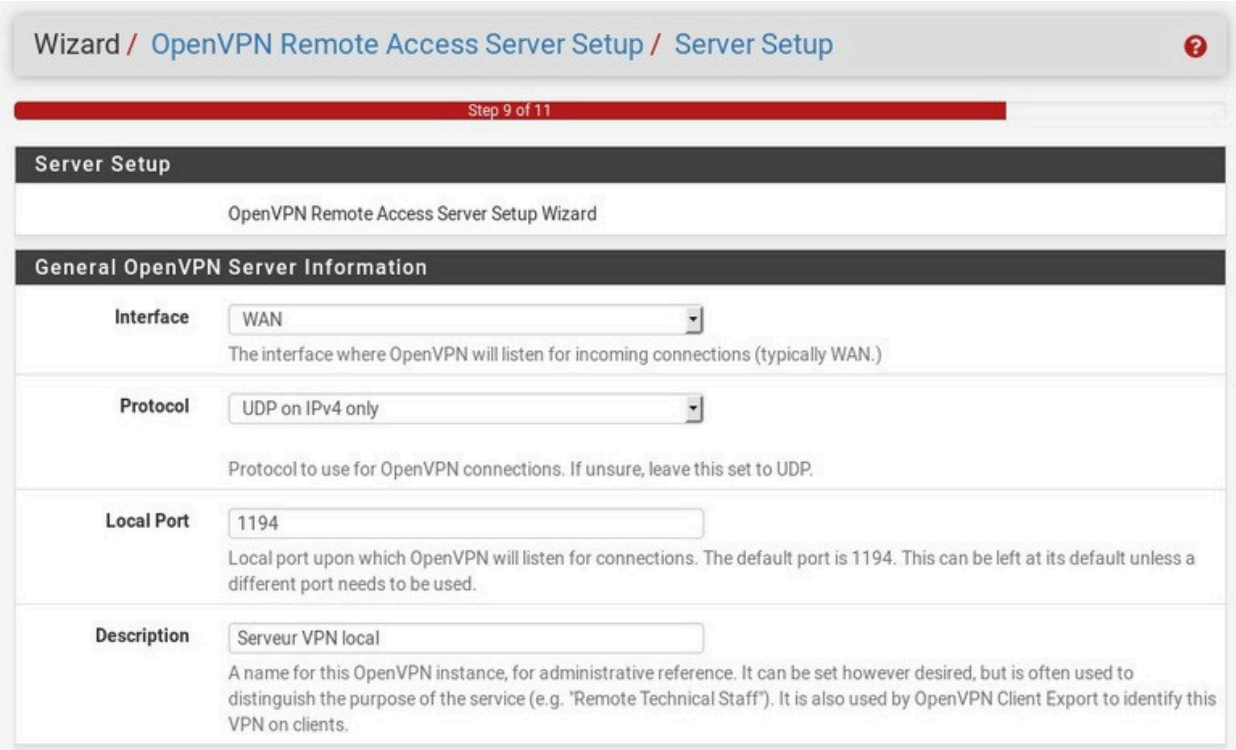
Annexe 3 : Configuration du serveur OpenVPN sur le routeur-parefeu PfSense

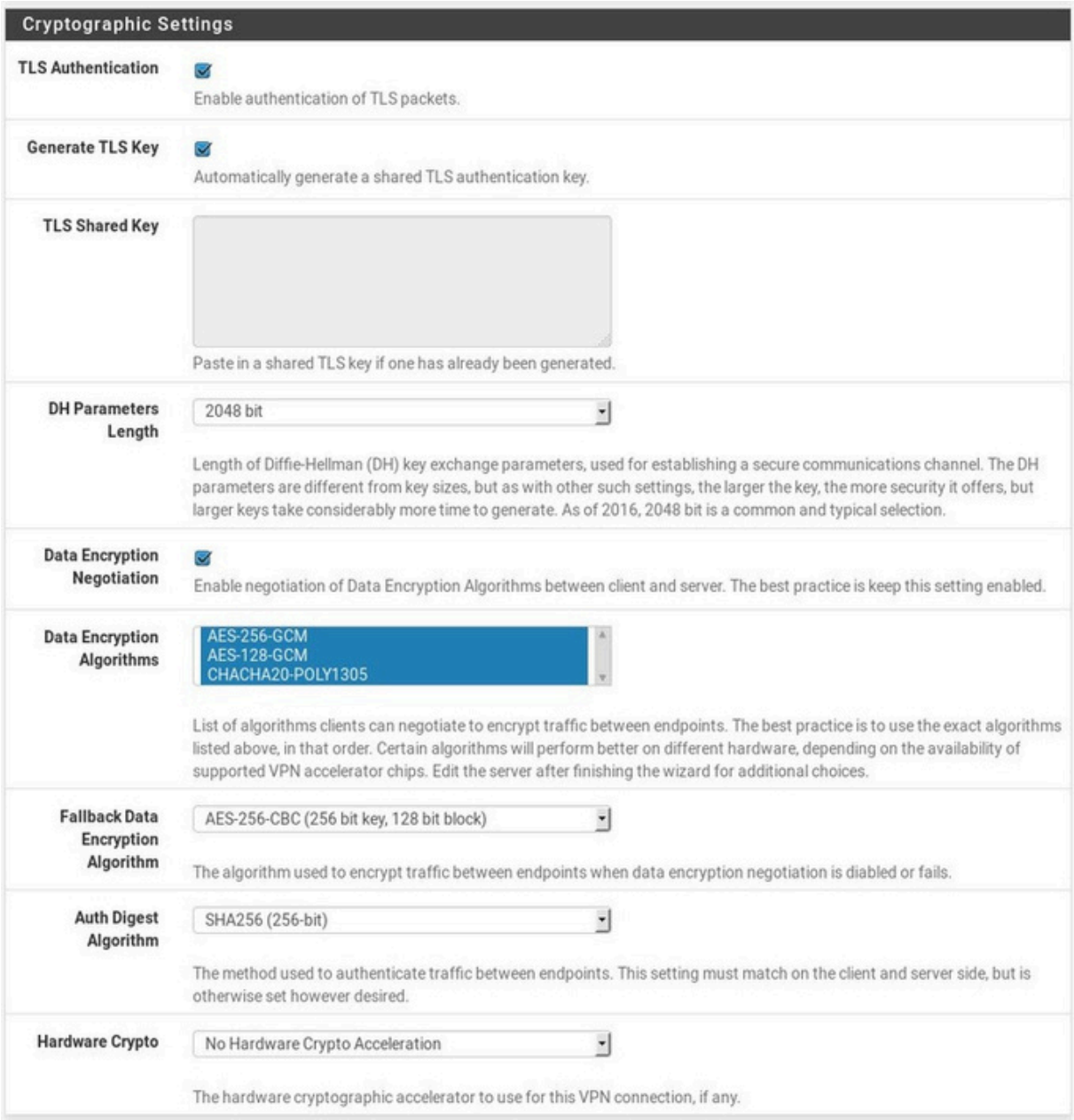
⚠ Rappel préalable : le serveur OpenVPN sera accessible de l'extérieur via son interface WAN ; on devra pouvoir accéder à ce serveur à partir d'un poste de la salle R211 (qui a donc une adresse privée).
Il faut donc bien penser à rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en vérifiant que la case *Block private networks* **de l'interface WAN** est **décochée** :

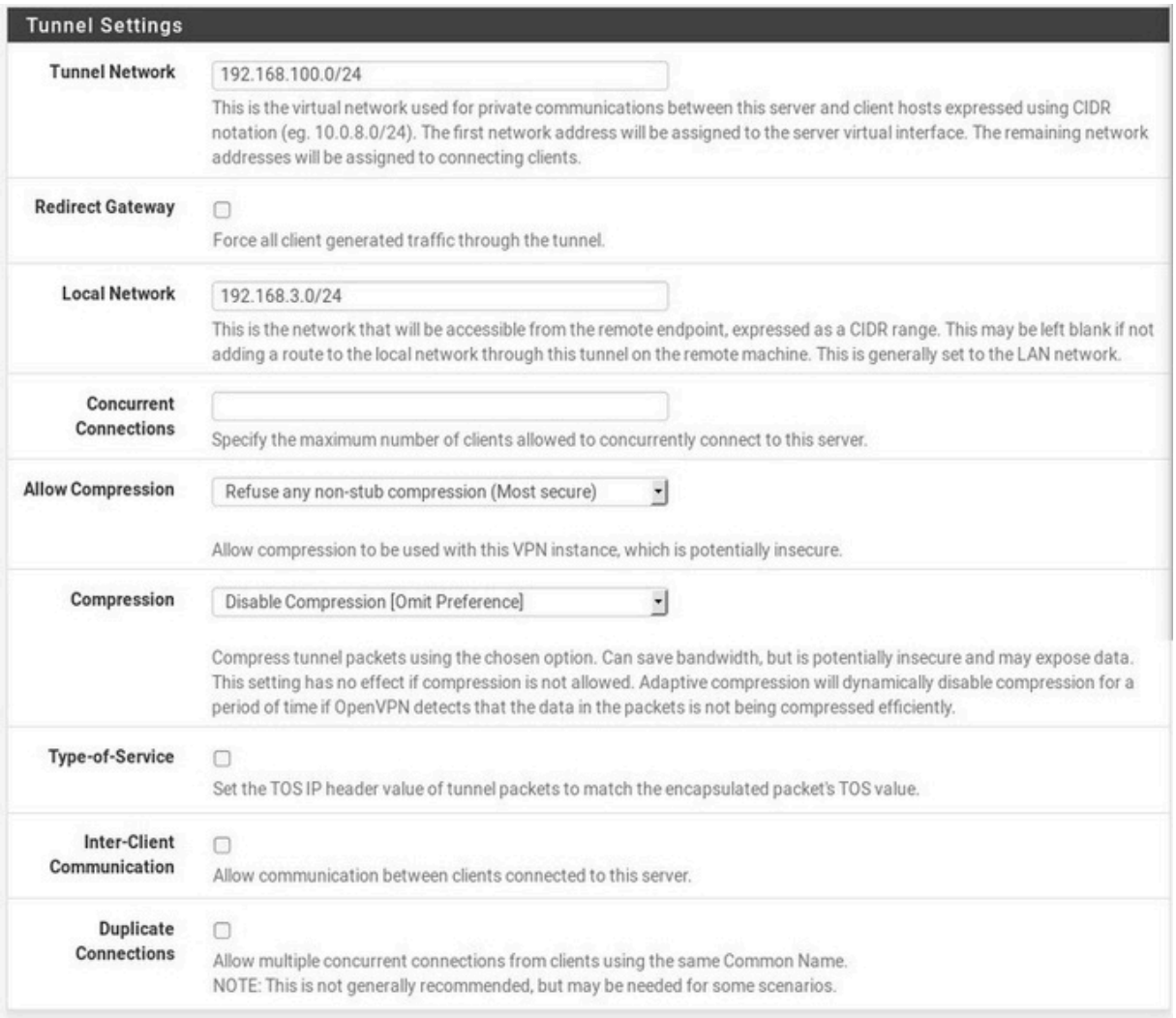


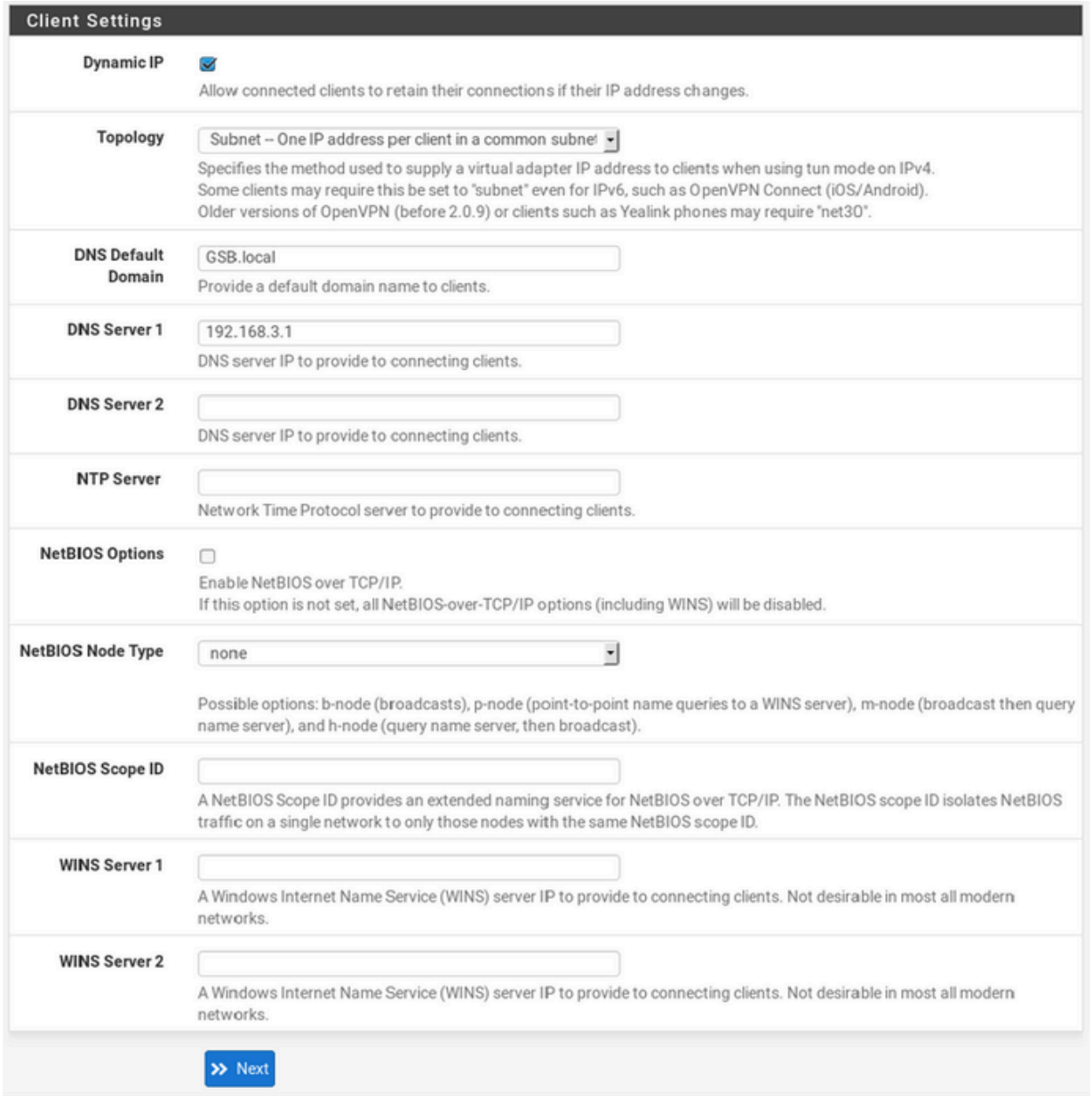
a. Configurer la connexion VPN, avec la commande *VPN OpenVPN*, dans l'onglet *Wizards* (*Assistants*) :

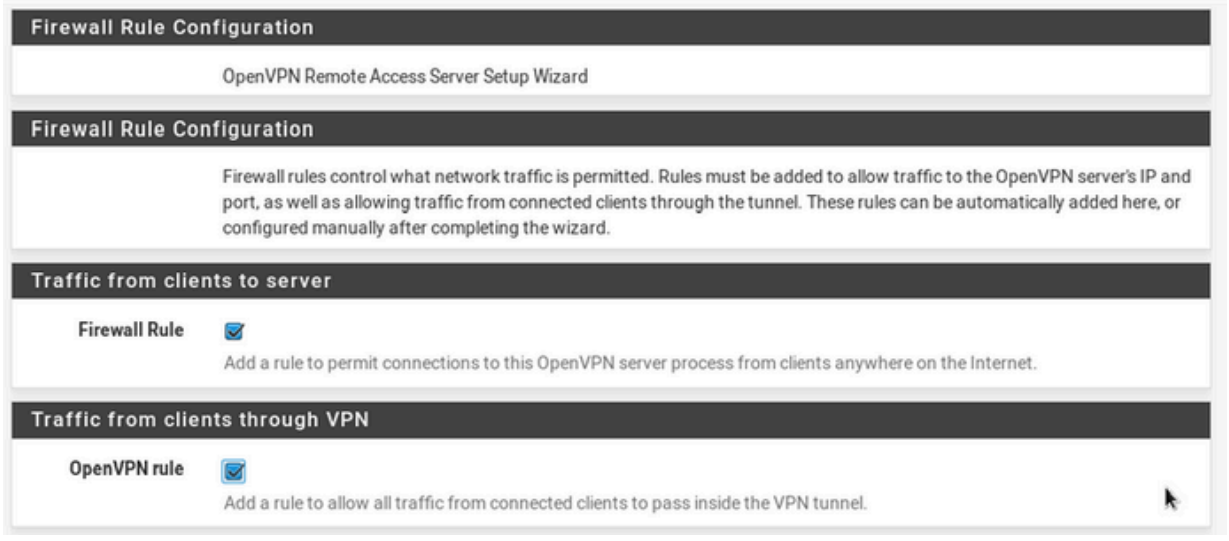
Type of Server (type de serveur d'authentification) :	*Local User Access*
Certificate Authority :	AC_GSB_PKI
Certificate (certificat du serveur OpenVPN) :	*Certificat_Serveur_VPN*
Description :	*Serveur VPN local*
Local Port :	*1194*




Cryptographic Settings
TLS Authentication
Enable authentication of TLS packets.
Generate TLS Key
Automatically generate a shared TLS authentication key.
TLS Shared Key
Paste in a shared TLS key if one has already been generated.
DH Parameters Length
2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation
Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.
Auth Digest Algorithm
SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto
No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.

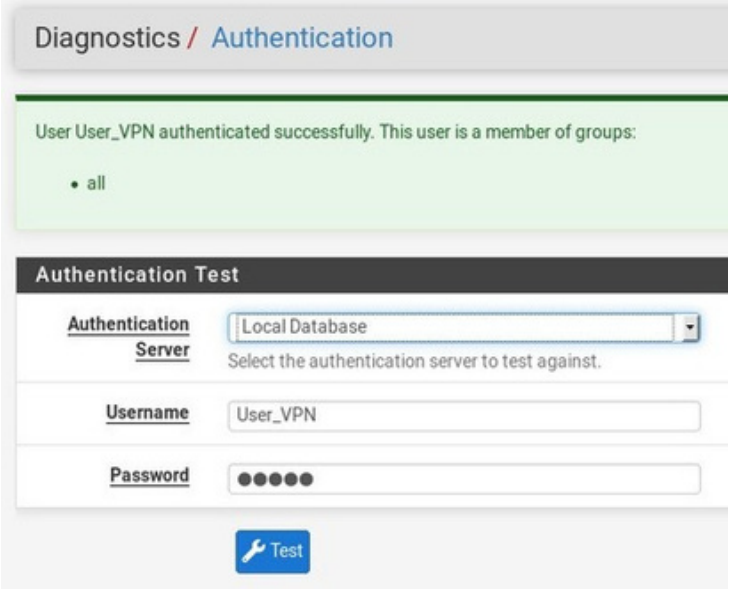

Tunnel Settings
Tunnel Network
192.168.100.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway
Force all client generated traffic through the tunnel.
Local Network
192.168.3.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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.
Concurrent Connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance, which is potentially insecure.
Compression
Disable Compression [Omit Preference]
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. 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.
Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication
Allow communication between clients connected to this server.
Duplicate Connections
Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.


Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet -- One IP address per client in a common subnet
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".
DNS Default Domain
GSB.local
Provide a default domain name to clients.
DNS Server 1
192.168.3.1
DNS server IP to provide to connecting clients.
DNS Server 2
DNS server IP to provide to connecting clients.
NTP Server
Network Time Protocol server to provide to connecting clients.
NetBIOS Options
Enable NetBIOS over TCP/IP.
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type
none
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Next


Firewall Rule Configuration
OpenVPN Remote Access Server Setup Wizard
Firewall Rule Configuration
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.
Traffic from clients to server
Firewall Rule
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.
Traffic from clients through VPN
OpenVPN rule
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

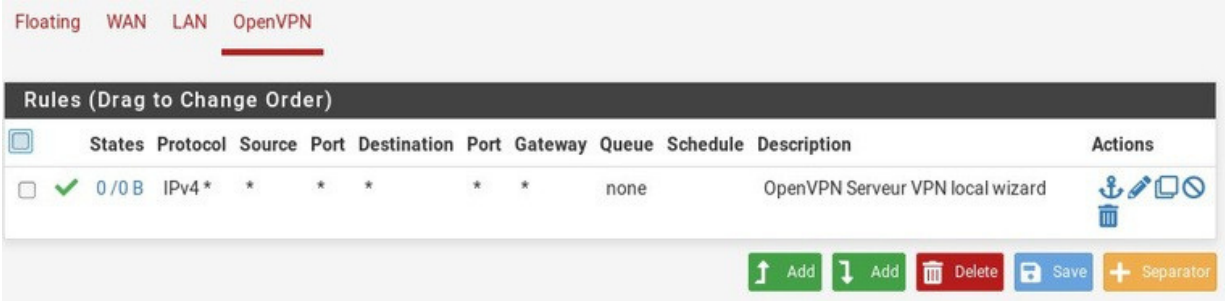
Le fait d'avoir coché les cases *Firewall Rule* et *OpenVPN rule* a automatiquement ajouté des règles de filtrage.

b. Vérifier avec la commande *Firewall Rules* que ces règles ont bien été créées.
c. Vérifier avec la commande *Diagnostics Authentication*, que l'utilisateur *User_VPN* est authentifié par le serveur OpenVPN :

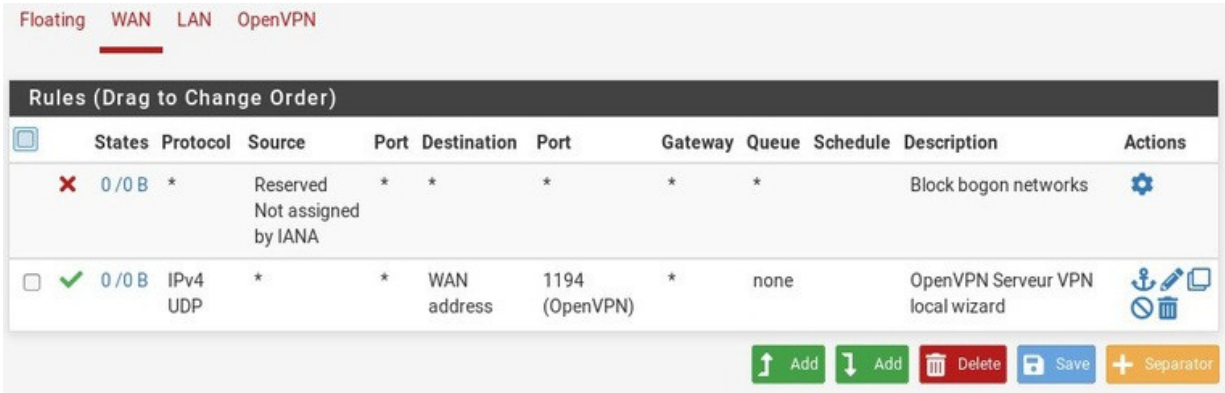


Les règles de filtrage qui ont été créées par l'assistant sont les suivantes :

- sur l'interface **OpenVPN** (créée pour la connexion VPN) :



-sur l'interface **WAN** :



Attention !

Dans certaines versions de Pfsense, il y a un bug qui ne permet pas d'utiliser plusieurs connexions VPN simultanément. Si une autre connexion VPN a déjà été configurée, il faut la désactiver.

Vérifier si besoin avec la commande *VPN* *OpenVPN* *Servers*, que seule la connexion VPN que l'on veut utiliser (ici celle utilisant le serveur local Pfsense sur le port 1194) est active.

Remarque :

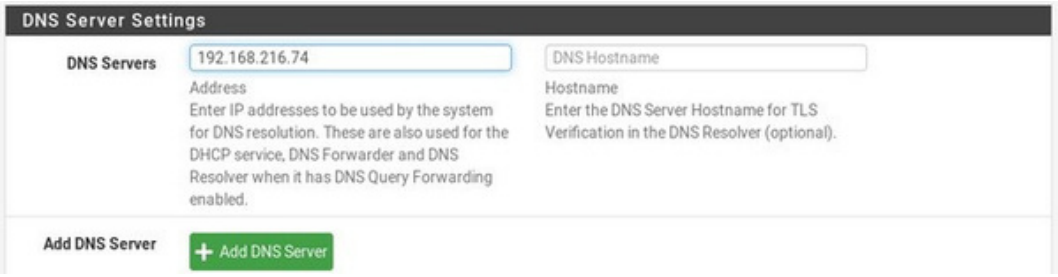
Dans les paramètres cryptographiques, vous avez vu qu'une clé TLS supplémentaire est générée pour renforcer la sécurité d'une connexion OpenVPN en exigeant que les deux parties disposent d'une clé commune avant qu'un pair puisse effectuer un handshake TLS.
Cette clé symétrique n'est utilisée que pour signer les paquets du canal de contrôle avec une signature HMAC pour l'authentification lors de l'établissement du tunnel.
Elle n'a aucun effet sur les données du tunnel.

Annexe 4 : Exportation de la configuration du client depuis PfSense

Nous allons configurer le PfSense pour qu'il accède à Internet, de façon à pouvoir installer un nouveau package qui nous permettra d'exporter vers les ordinateurs clients le fichier de configuration et le certificat-client.

a. Sélectionner la commande *System General Setup*, afin de configurer l'adresse du DNS :

DNS Server : *192.168.216.74*
Cliquer sur *Save* pour enregistrer la configuration. **Redémarrer** ensuite le Pfsense.

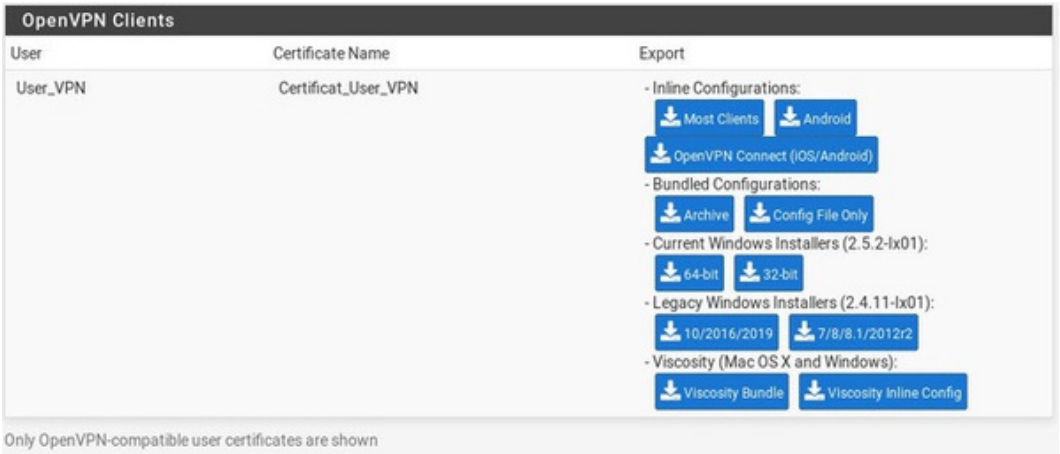


Le package *OpenVPN Client Export Utility* permet d'exporter facilement la configuration qui devra êtreinstallée sur l'ordinateur client, ainsi que la clé publique de l'AC interne GSB nécessaire pour que le client puisse déchiffrer la signature du certificat du serveur VPN. Nous allons donc déjà installer ce package sur le PfSense serveur :

b. Installer le package *OpenVPN Client Export Utility* :

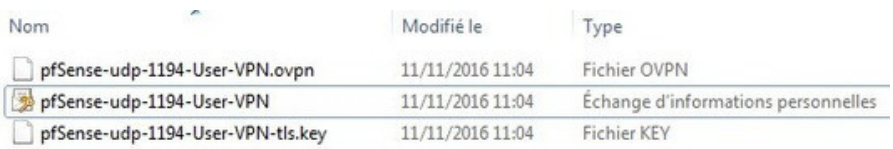
Sélectionner la commande *System Packages*, puis cliquer sur l'onglet *Available Packages*.
Sur la ligne *OpenVPN Client Export Utility*, cliquer sur le signe **+** pour ajouter le package.
Après l'installation, cliquer sur l'onglet *Installed Packages* pour vérifier que le module a bien été installé.

c. Sélectionner la commande *VPN OpenVPN*, dans l'onglet *Client Export*, pour l'utilisateur *User_ VPN* afin de vérifier la présence de l'archive (contenant les trois fichiers de configuration), ou mieux encore, de l'exécutable *Windows Installer*, qui est à exporter sur les machines clientes :



d. Cliquer sur le lien *64-bits* dans la rubrique *Current Windows Installer* pour exporter un fichier exécutable qui installera automatiquement les fichiers de configuration, ou sur le lien *Archive* pour exporter les trois fichiers de configuration eux-mêmes ; il faut les enregistrer dans un endroit accessible aux postes clients (sur le serveur 192.168.216.74 par exemple, ou sur une clé USB).
Remarque : Le fichier *.ovpn*

e. contient la configuration à installer sur chaque poste client OpenVPN.



Annexe 5 : Installation du client OpenVPN sur un poste client

a. Sur le poste client, télécharger le client OpenVPN depuis le site suivant (onglet *Community*, *Windows Installer 64 bits*) :

http://openvpn.net/index.php/open-source/downloads.html

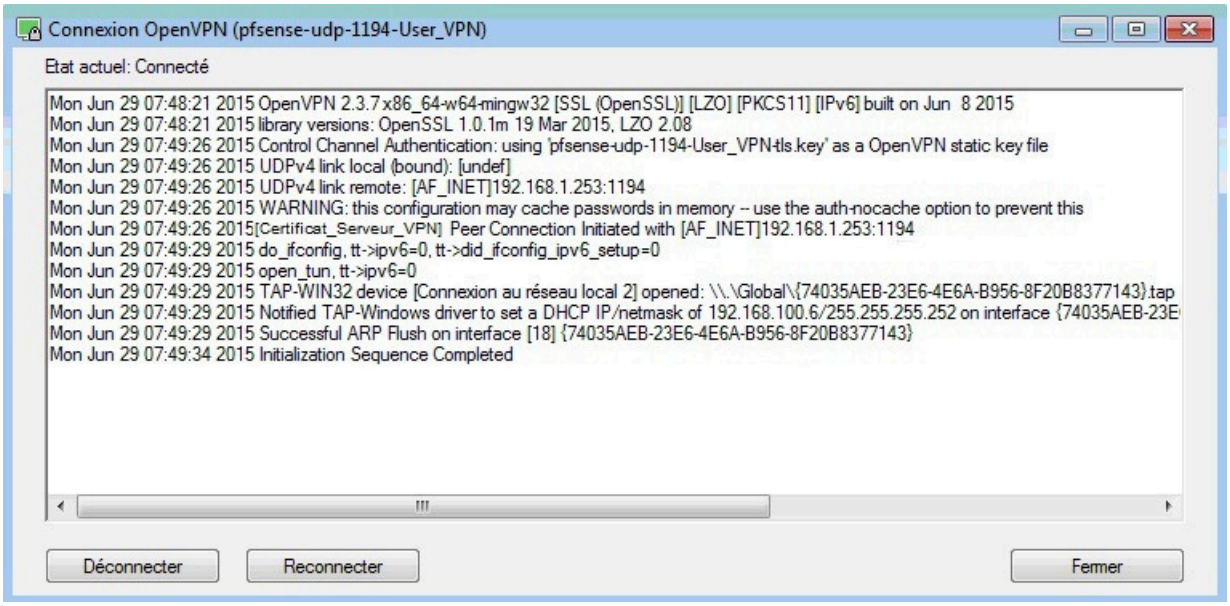
b. Installer ce logiciel client sur le poste (installer aussi le logiciel *TAP-Windows Provider V9 Cartes réseau*).

c. Recopier le fichier d'installation exécutable dans le dossier C:\Programmes\OpenVPN\Config (si la copie directe ne fonctionne pas, on pourra copier le fichier d'abord dans le dossier Documents du PC local, puis du dossier Documents vers C:\Programmes\OpenVPN\Config) puis exécuter ce fichier qui installera automatiquement les 3 fichiers de configuration dans le dossier.

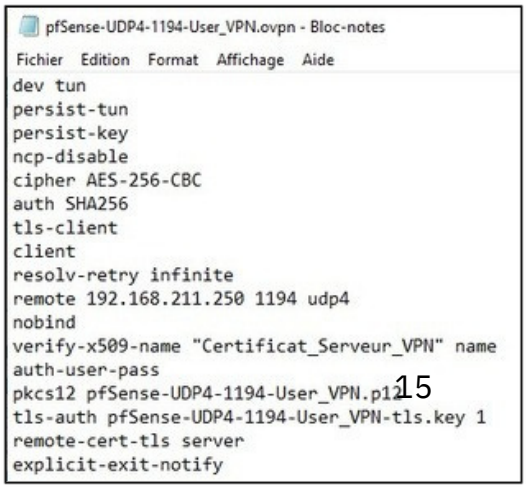
d. Cliquer-doit sur l'icône de l'application OpenVPN GUI et sélectionner la commande *Régler les problèmes de compatibilité*, puis le bouton *Essayer les paramètres recommandés* ; lancer ainsi l'application.
L'application OpenVPN GUI devra ensuite toujours être lancée en mode administrateur.

e.

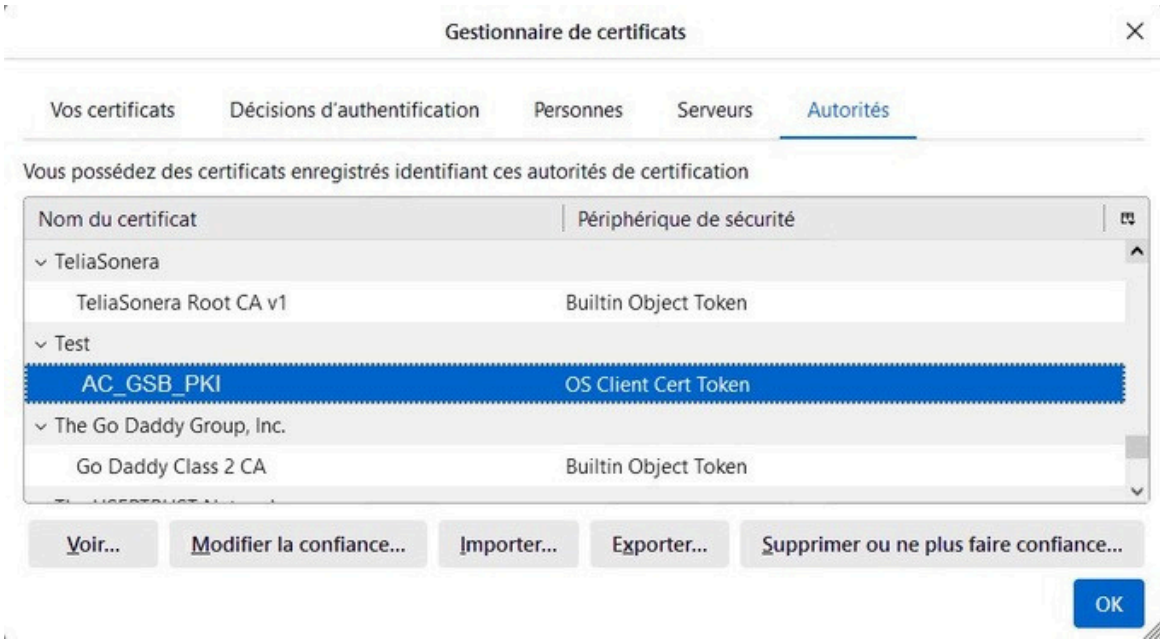
f. Se connecter avec l'utilisateur *User_VPN* et le mot de passe *faure* :



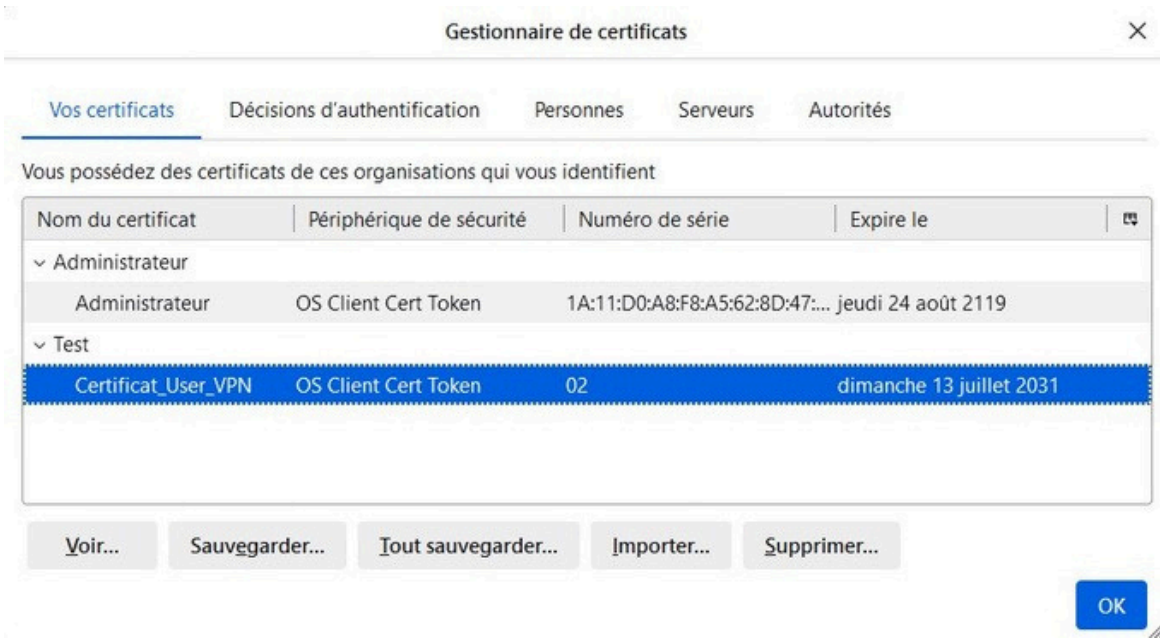
Pour info, le fichier de configuration du client OpenVPN,
de nom *pfSense-udp-1194-User_VPN.ovpn*
doit avoir le contenu suivant :



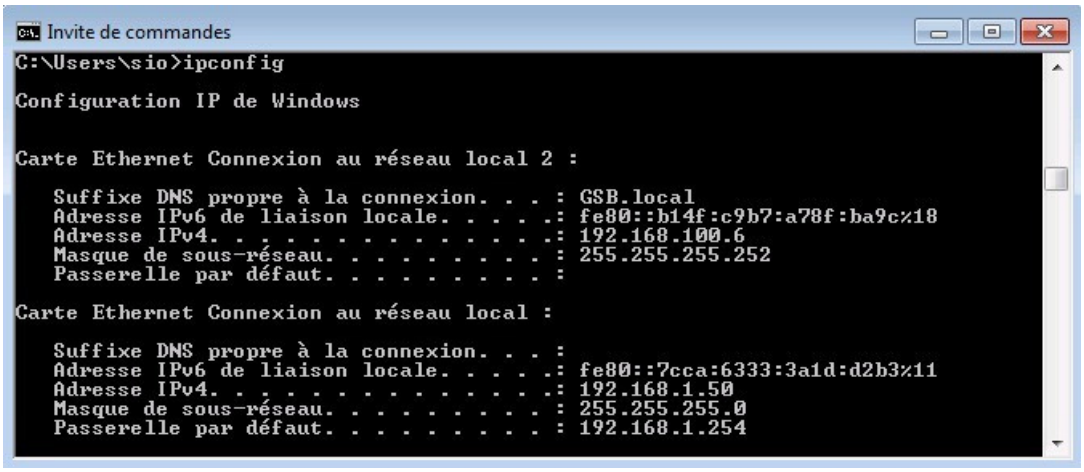
g. Sur le poste client, lancer le navigateur, puis ouvrir le *Gestionnaire de certificats* de ce navigateur ;
- Vérifier dans la magasin de certificats d'*Autorités* de Certification, que le certificat de l'AC interne GSB ***AC_GSB_PKI*** est bien présent (il est à rechercher dans la liste alphabétique dans les T puisque cette organisation a été nommée *Test*) :

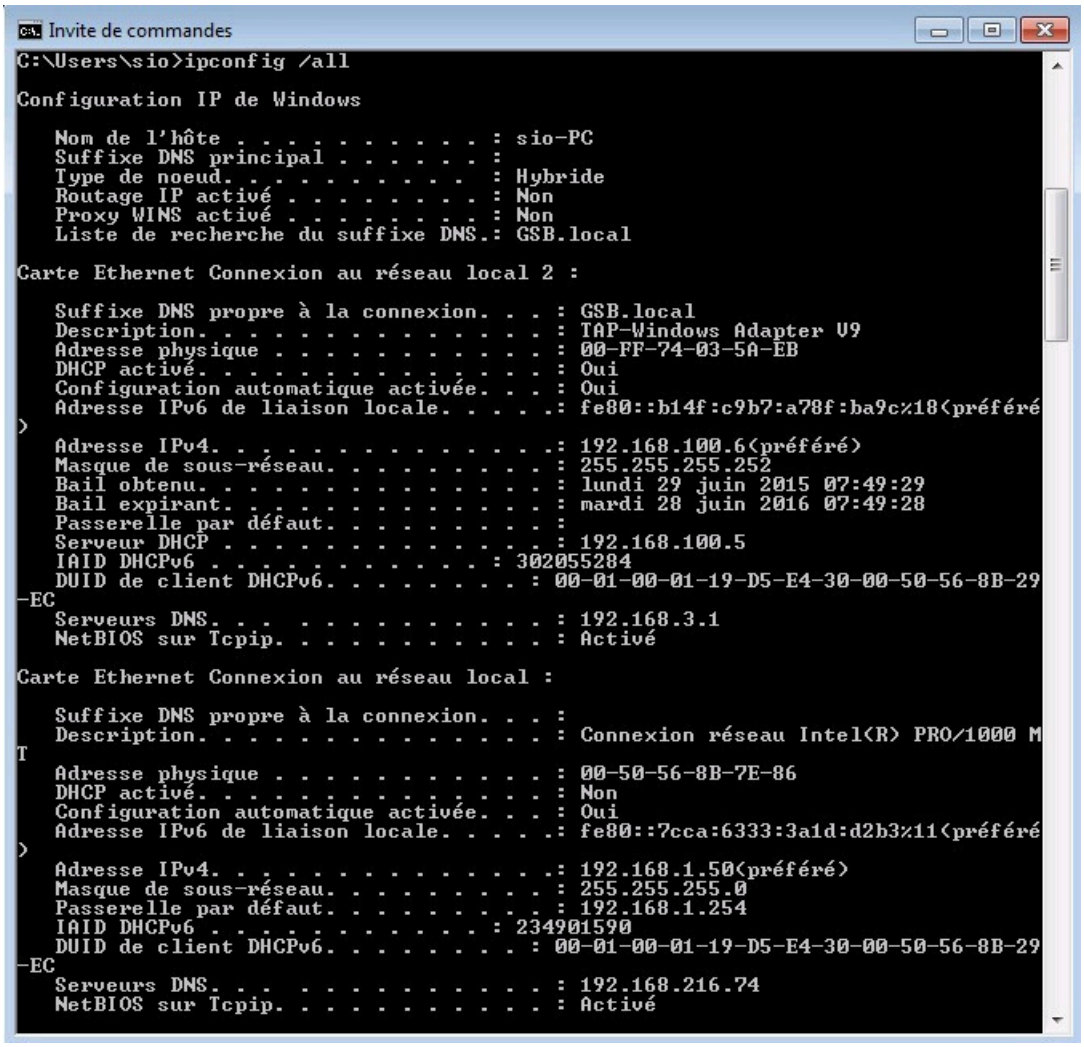


- Vérifier dans la magasin de certificats *Vos certificats*, que le certificat de l'utilisateur ***Certificat_User_VPN*** est bien présent (il est à rechercher dans la liste alphabétique dans les T puisque cette organisation a été nommée *Test*) :



h. Vérifier que le poste client a bien deux connexions en cours :




Invite de commandes
C:\Users\sio>ipconfig /all
Configuration IP de Windows
Nom de l'hôte . . . . . : sio-PC
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: GSB.local
Carte Ethernet Connexion au réseau local 2 :
Suffixe DNS propre à la connexion. . . : GSB.local
Description. . . . . : TAP-Windows Adapter V9
Adresse physique . . . . . : 00-FF-74-03-5A-EB
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . .: fe80::b14f:c9b7:a78f:ba9c%18(préféré
)
Adresse IPv4. . . . . .: 192.168.100.6(préféré)
Masque de sous-réseau. . . . . : 255.255.255.252
Bail obtenu. . . . . : lundi 29 juin 2015 07:49:29
Bail expirant. . . . . : mardi 28 juin 2016 07:49:28
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 192.168.100.5
IAID DHCPv6 . . . . . : 302055284
DUID de client DHCPv6. . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
Serveurs DNS. . . . . : 192.168.3.1
NetBIOS sur Tcpip. . . . . : Activé
Carte Ethernet Connexion au réseau local :
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Connexion réseau Intel(R) PRO/1000 M
T
Adresse physique . . . . . : 00-50-56-8B-7E-86
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . .: fe80::7cca:6333:3a1d:d2b3%11(préféré
)
Adresse IPv4. . . . . .: 192.168.1.50(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.254
IAID DHCPv6 . . . . . : 234901590
DUID de client DHCPv6. . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
Serveurs DNS. . . . . : 192.168.216.74
NetBIOS sur Tcpip. . . . . : Activé

i. Vérifier sur le serveur OpenVPN avec la commande *Status OpenVPN*, les connexions des clients en cours :

Status: OpenVPN

Serveur VPN local UDP:1194 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
User_VPN	192.168.1.50:56769	192.168.100.6	Sat Nov 19 09:13:01 2016	7 KB	11 KB

Running

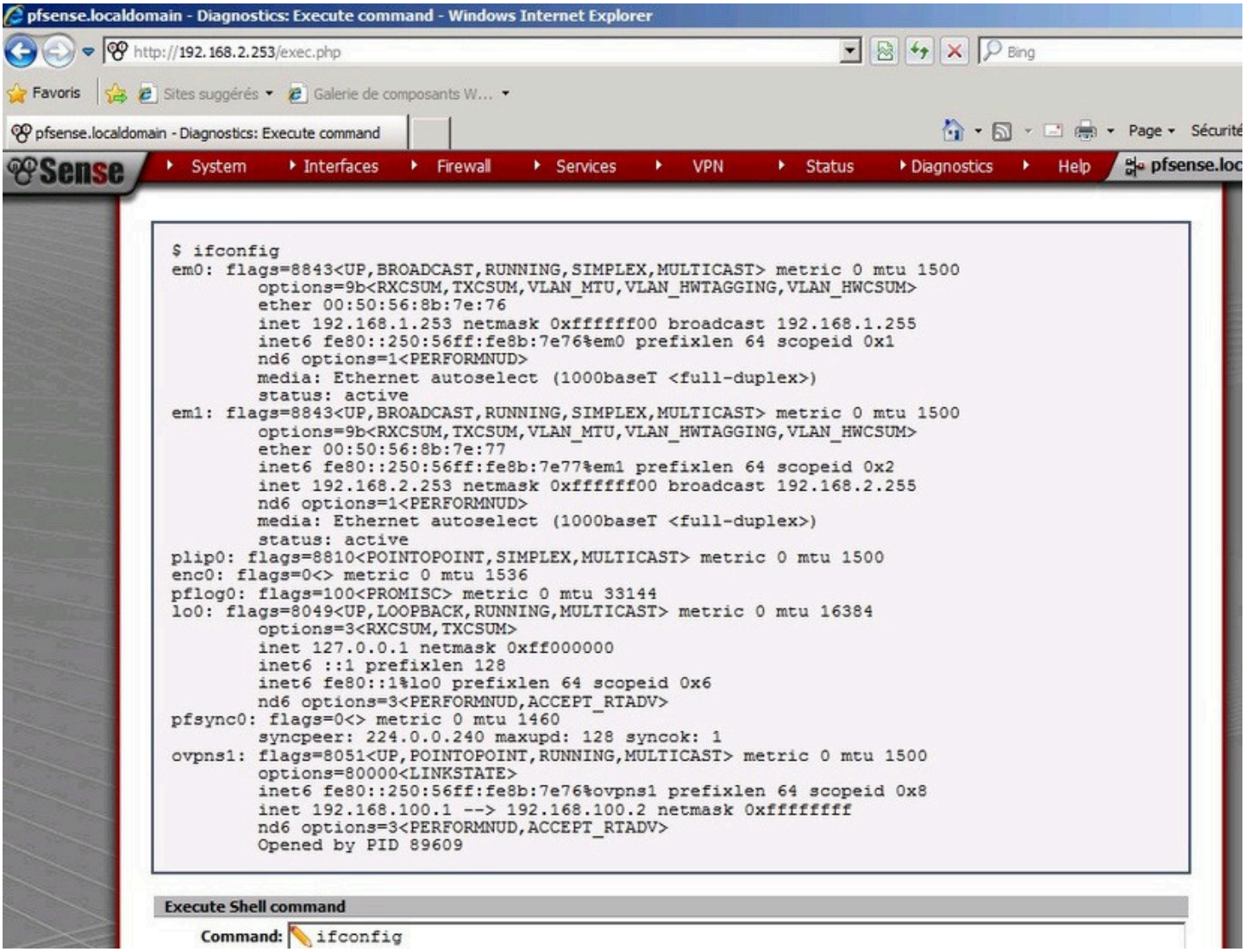
Serveur VPN local UDP:1194 Routing Table

Common Name	Real Address	Target Network	Last Used
User_VPN	192.168.1.50:56769	192.168.100.6	Sat Nov 19 09:13:34 2016

An IP address followed by C indicates a host currently connected through the VPN.

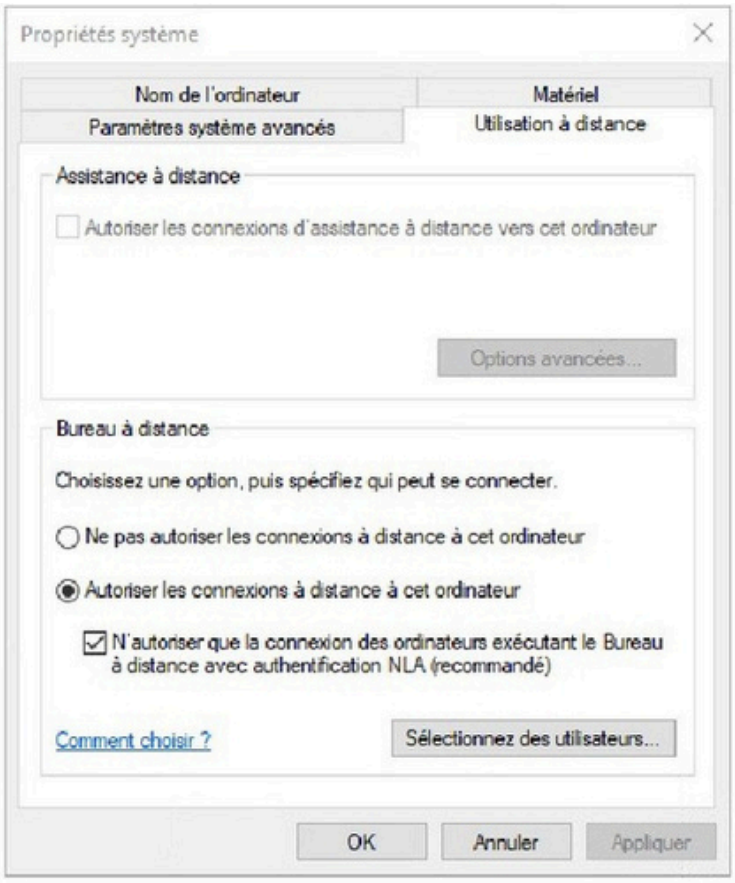
j. Vérifier que le serveur OpenVPN lui-même a bien aussi une connexion ovpns1 d'adresse 192.168.100.1 :

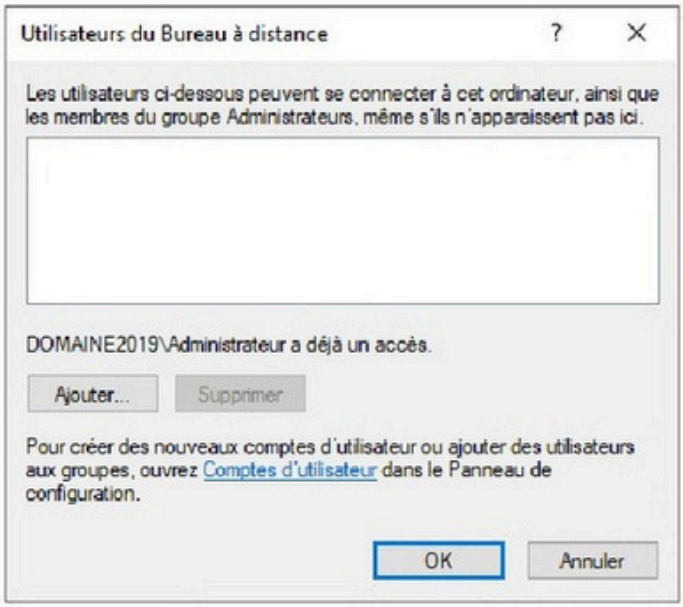
Aucune route n'a été rajoutée pour ce réseau 192.168.100.0 dans le routeur puisqu'il s'agit d'une adresse "fictive".



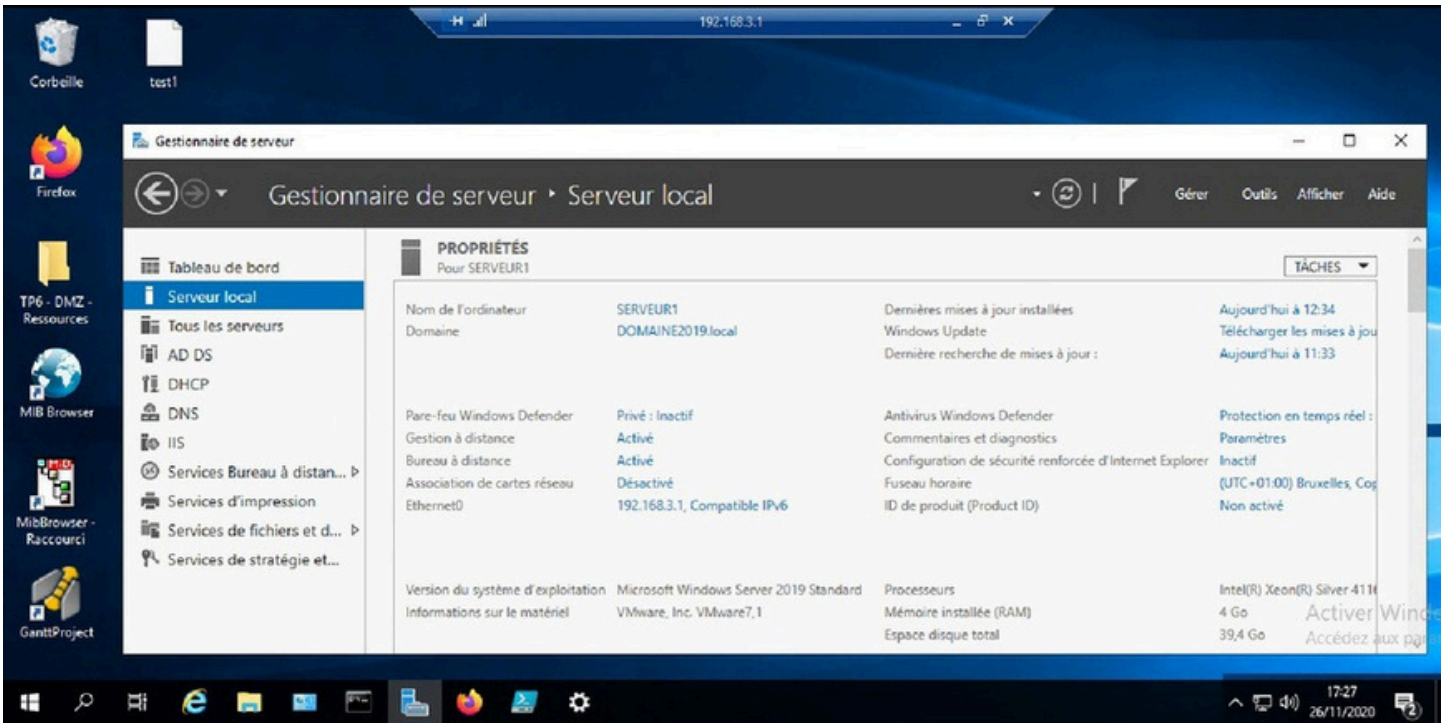
On peut maintenant, depuis le poste client,
ouvrir une Connexion Bureau à distance vers le serveur 192.168.3.1 ou toute autre machine du réseau LAN GSB !

Ilfaut évidemment que SERVEUR1 ait été configuré pour accepter les connexions à distance à cet ordinateur (lorsqu'on les autorise, par défaut seul l'Administrateur a le droit de se connecter à distance à cette machine).





Connexion Bureau à distance depuis un poste de la salle R211 :



Annexe 6 : Vérification du tunnel

a. Sur le poste SERVEUR1 par exemple, seconnecter à l'interface LAN du routeur-parefeu Pfsense pour le configurer, avec le navigateur Mozilla Firefox ;

b. Sur le même poste, télécharger et installer le logiciel de captures de trames Wireshark.

c. Avec la commande PfSense *Diagnostics Packet Capture*, sélectionner les choix de capture suivants:

Interface (de capture) : *WAN*
Level of Detail : *Full*

d. Lancer la capture avec *Start*.

e. Depuis un poste client VPN, ouvrir une session de Connexion Bureau à distance sur SERVEUR1, puis la refermer.

f. Toujours avec la commande PfSense *Diagnostic Packet Capture*, arrêter la capture avec *Stop* ; cliquer sur *Download capture*, puis sur *Ouvrir* : cela permet de lancer automatiquement Wireshark, et d'ouvrir le fichier de la capture ; vérifier que les trames échangées entre le routeur-parefeu Pfsense et le poste client VPN sont bien des trames OpenVPN.