

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.

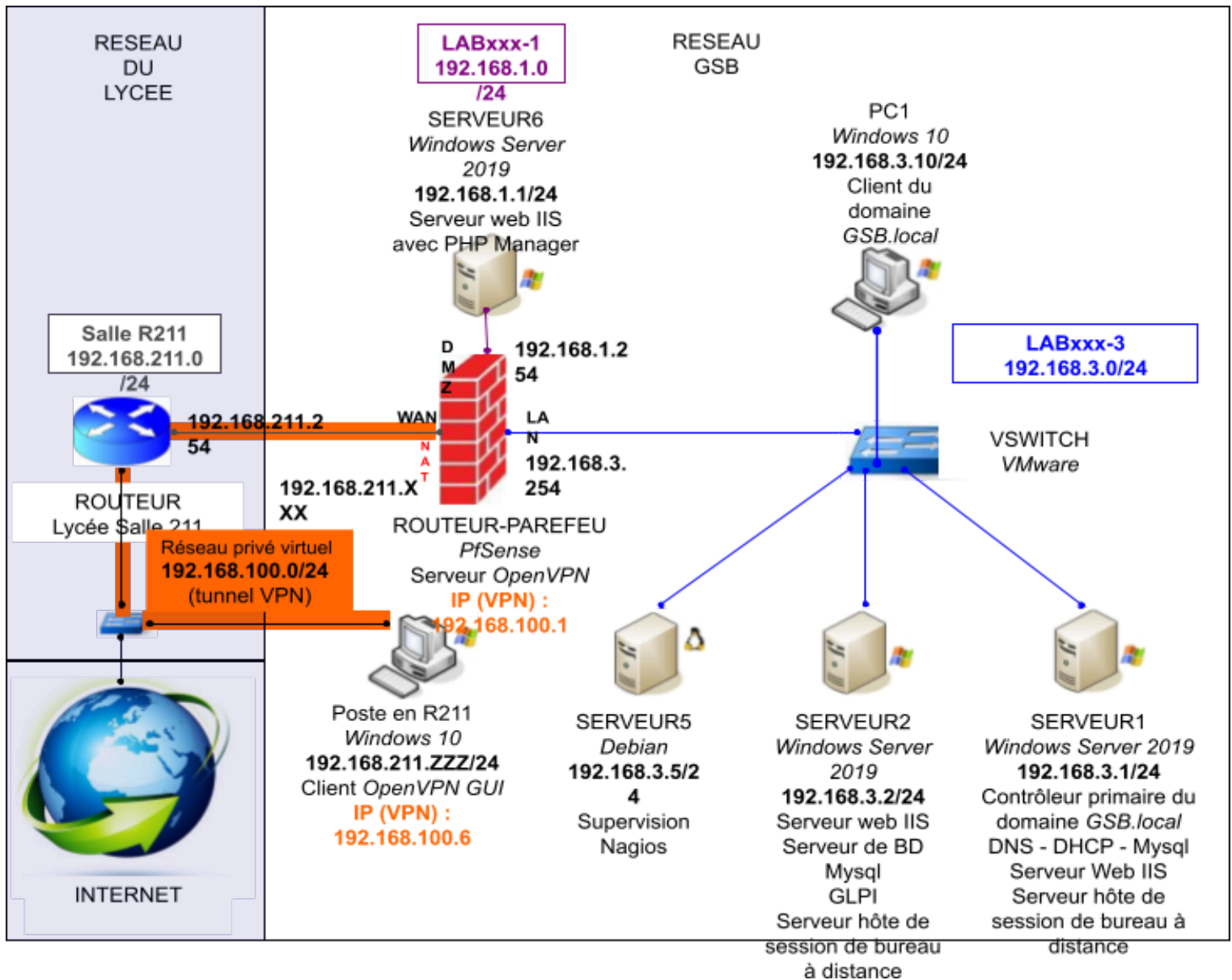
Attention : lorsqu'un client se connecte au serveur VPN, celui-ci lui présente son certificat contenant la signature par l'AC interne GSB qui a été chiffrée avec la clé privée de cette AC.

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).

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. Depuis le 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***) :

The screenshot displays the PfSense web interface for configuring a Certificate Authority (CA). The breadcrumb trail is "System / Certificate Manager / CAs / Edit". The main heading is "Create / Edit CA".

CA Configuration:

- Descriptive name:** AC_GSB_PKI
- Method:** Create an internal Certificate Authority
- Trust Store:** 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.

Internal Certificate Authority:

- Key type:** RSA
- Key Length (bits):** 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:** sha256. The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.
- Lifetime (days):** 3650
- Common Name:** AC_GSB_PKI

The following certificate authority subject components are optional and may be left blank.

- Country Code:** FR
- State or Province:** test
- City:** test
- Organization:** test
- Organizational Unit:** e.g. My Department Name (optional)

A "Save" button is located at the bottom of the form.

- 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***) :

System / Certificate Manager / Certificates / Edit ?

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name Certificat_Serveur_VPN

Internal Certificate

Certificate authority AC_GSB_PKI

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 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.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name Certificat_Serveur_VPN

The following certificate subject components are optional and may be left blank.

Country Code FR

State or Province test

City test

Organization test

Organizational Unit e.g. My Department Name (optional)

Certificate Attributes

Attribute 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 signed certificate.

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.

Add + Add

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

- a. Sélectionner la commande PfSense *System User Manager* (*Gestionnaire d'utilisateurs*), puis dans l'onglet *Users*, créer un nouvel utilisateur, de nom *User_VPN*, et de mot de passe *faure* :

The screenshot shows the PfSense web interface for editing a user. The breadcrumb trail is 'System / User Manager / Users / Edit'. The 'Users' tab is selected in the top navigation. The 'User Properties' section includes fields for 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (User_VPN), 'Password' (two masked fields), 'Full name' (empty), 'Expiration date' (empty), 'Custom Settings' (checkbox), and 'Group membership' (admins). The 'Certificate' section has a checkbox to create a certificate. The 'Keys' section has a text area for 'Authorized SSH Keys' and a field for 'IPsec Pre-Shared Key'. A 'Save' button is at the bottom.

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username: User_VPN

Password: [masked] [masked]

Full name: [empty]
User's full name, for administrative information only

Expiration date: [empty]
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 (Not member of) [empty] (Member of)

>> Move to 'Member of' list << Move to 'Not member of' list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.


Certificate: Click to create a user certificate

Keys

Authorized SSH Keys: [empty]
Enter authorized SSH keys for this user

IPsec Pre-Shared Key: [empty]

Save

- 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***) :

System / Certificate Manager / Certificates / Edit ?

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name Certificat_User_VPN

Internal Certificate

Certificate authority AC_GSB_PKI

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 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.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name Certificat_User_VPN

The following certificate subject components are optional and may be left blank.

Country Code FR

State or Province test

City test

Organization test

Organizational Unit e.g. My Department Name (optional)

Certificate Attributes

Attribute 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 User Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

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.

Add + Add

Save

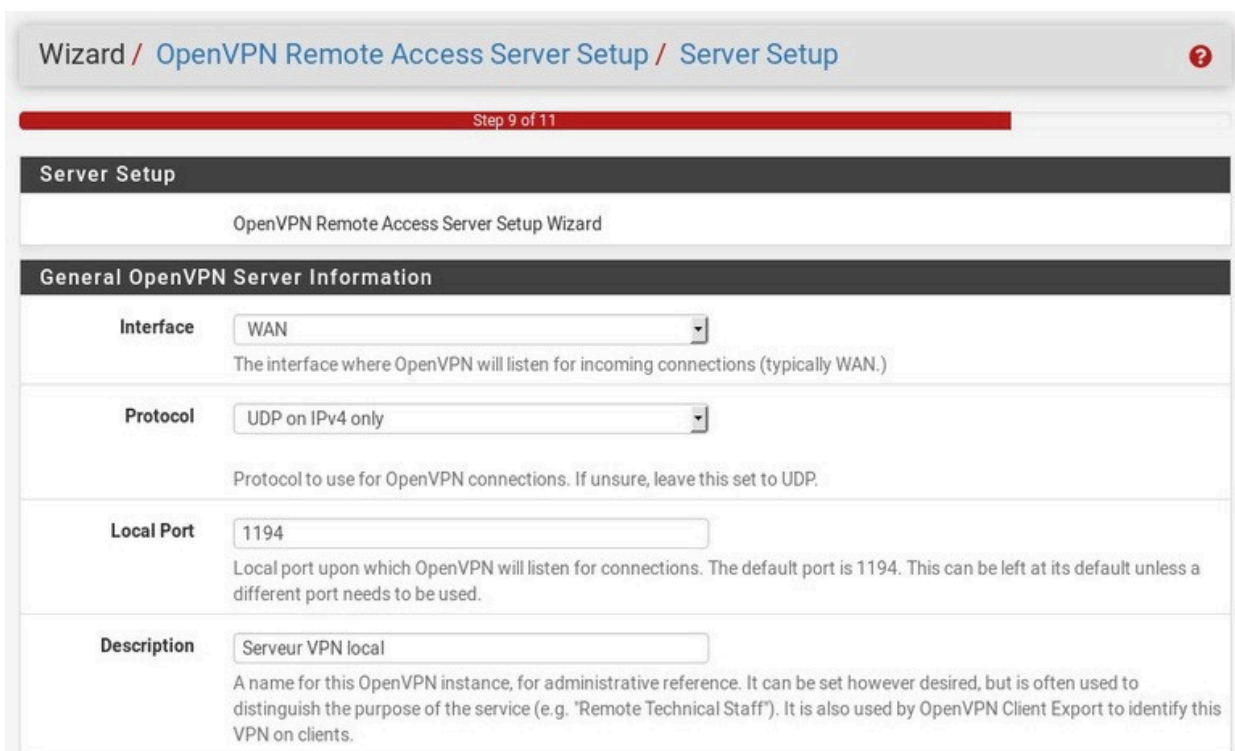
Annexe 3 : Configuration du serveur OpenVPN sur le routeur-parefeu PfSense

 **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** :

| Reserved Networks | |
|--|--|
| Block private networks and loopback addresses | <input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too. |
| Block bogon networks | <input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings. |

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

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



Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

| | | |
|--------------------|-------------------|---|
| Interface | WAN | The interface where OpenVPN will listen for incoming connections (typically WAN.) |
| Protocol | UDP on IPv4 only | Protocol to use for OpenVPN connections. If unsure, leave this set to UDP. |
| Local Port | 1194 | Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used. |
| Description | Serveur VPN local | A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients. |

| Cryptographic Settings | |
|---|---|
| TLS Authentication | <input checked="" type="checkbox"/> <p>Enable authentication of TLS packets.</p> |
| Generate TLS Key | <input checked="" type="checkbox"/> <p>Automatically generate a shared TLS authentication key.</p> |
| TLS Shared Key | <div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div> <p>Paste in a shared TLS key if one has already been generated.</p> |
| DH Parameters Length | <div style="border: 1px solid #ccc; padding: 2px;">2048 bit</div> <p>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.</p> |
| Data Encryption Negotiation | <input checked="" type="checkbox"/> <p>Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.</p> |
| Data Encryption Algorithms | <div style="border: 1px solid #ccc; padding: 2px;"> AES-256-GCM AES-128-GCM CHACHA20-POLY1305 </div> <p>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.</p> |
| Fallback Data Encryption Algorithm | <div style="border: 1px solid #ccc; padding: 2px;">AES-256-CBC (256 bit key, 128 bit block)</div> <p>The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.</p> |
| Auth Digest Algorithm | <div style="border: 1px solid #ccc; padding: 2px;">SHA256 (256-bit)</div> <p>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</p> |
| Hardware Crypto | <div style="border: 1px solid #ccc; padding: 2px;">No Hardware Crypto Acceleration</div> <p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p> |

| Tunnel Settings | |
|-----------------------------------|---|
| Tunnel Network | <input type="text" value="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 | <input type="checkbox"/> Force all client generated traffic through the tunnel. |
| Local Network | <input type="text" value="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 | <input type="text"/> Specify the maximum number of clients allowed to concurrently connect to this server. |
| Allow Compression | <input type="text" value="Refuse any non-stub compression (Most secure)"/> Allow compression to be used with this VPN instance, which is potentially insecure. |
| Compression | <input type="text" value="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 | <input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value. |
| Inter-Client Communication | <input type="checkbox"/> Allow communication between clients connected to this server. |
| Duplicate Connections | <input type="checkbox"/> 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 | <input checked="" type="checkbox"/> 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 | <input type="text"/> DNS server IP to provide to connecting clients. |
| NTP Server | <input type="text"/> Network Time Protocol server to provide to connecting clients. |
| NetBIOS Options | <input type="checkbox"/> 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 | <input type="text"/> 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 | <input type="text"/> A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks. |
| WINS Server 2 | <input type="text"/> A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks. |
| >> Next | |

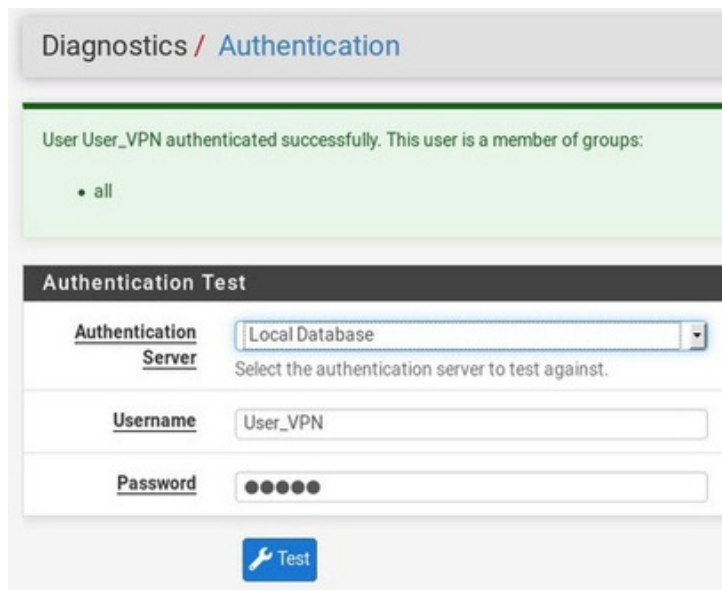
| Firewall Rule Configuration | |
|---|---|
| OpenVPN Remote Access Server Setup Wizard | |
| Firewall Rule Configuration | |
| Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected 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 | <input checked="" type="checkbox"/> Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet. |
| Traffic from clients through VPN | |
| OpenVPN rule | <input checked="" type="checkbox"/> 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.

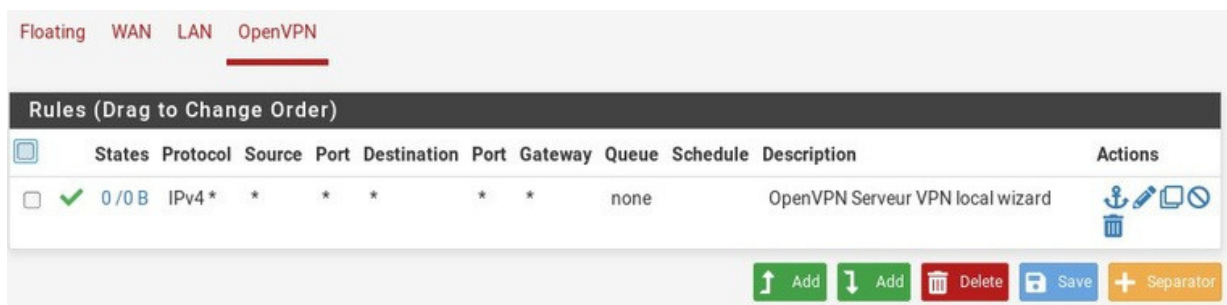
c. Vérifier avec la commande *Diagnostics Authentication*, que l'utilisateur *User_VPN* est authentifié par le serveur

OpenVPN :

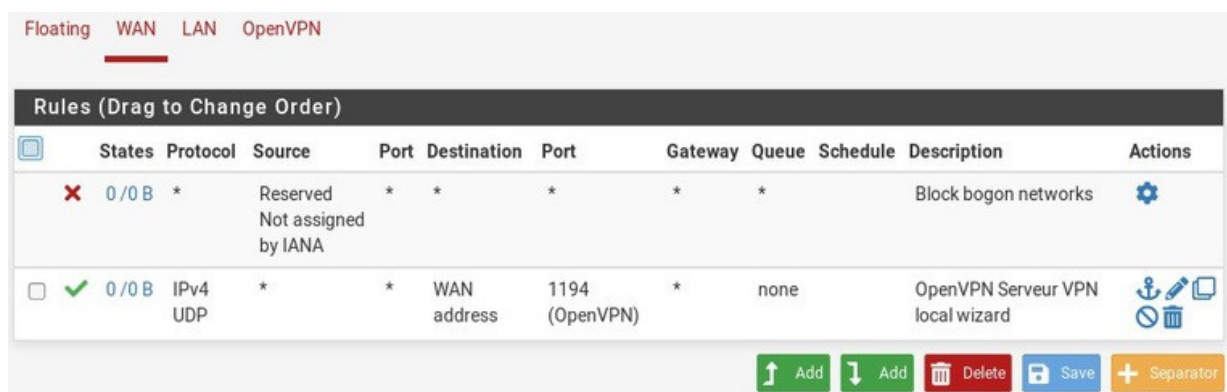


Les règles de filtrage qui ont été créées par l'assistant sont les suivantes :

- 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.

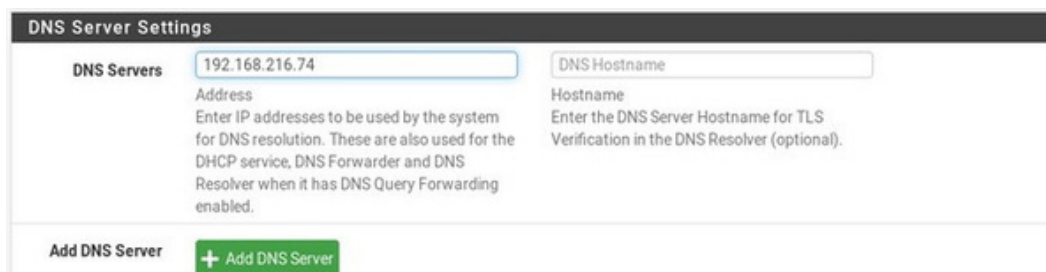
Annexe 4 : Exportation de la configuration du client depuis PfSense

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.



DNS Server Settings

| | | | |
|----------------|--|--------------|--|
| DNS Servers | 192.168.216.74 | DNS Hostname | |
| Address | Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled. | Hostname | Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional). |
| Add DNS Server | + Add DNS Server | | |

Le package *OpenVPN Client Export Utility* permet d'exporter facilement la configuration qui devra être installée 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 :

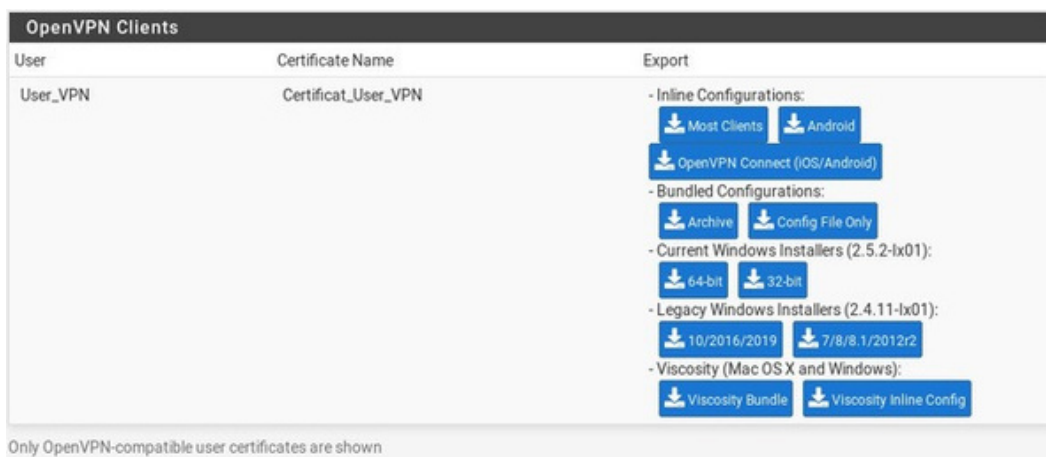
b. Installer le package *OpenVPN Client Export Utility* :

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 :



OpenVPN Clients

| User | Certificate Name | Export |
|----------|---------------------|--|
| User_VPN | Certificat_User_VPN | <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 (2.5.2-ix01):<ul style="list-style-type: none">64-bit32-bit- Legacy Windows Installers (2.4.11-ix01):<ul style="list-style-type: none">10/2016/20197/8/1/2012r2- Viscosity (Mac OS X and Windows):<ul style="list-style-type: none">Viscosity BundleViscosity Inline Config |

Only OpenVPN-compatible user certificates are shown

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.

| Nom | Modifié le | Type |
|-----------------------------------|------------------|-------------------------------------|
| pfSense-udp-1194-User-VPN.ovpn | 11/11/2016 11:04 | Fichier OVPN |
| pfSense-udp-1194-User-VPN | 11/11/2016 11:04 | Échange d'informations personnelles |
| pfSense-udp-1194-User-VPN-tls.key | 11/11/2016 11:04 | Fichier KEY |

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.

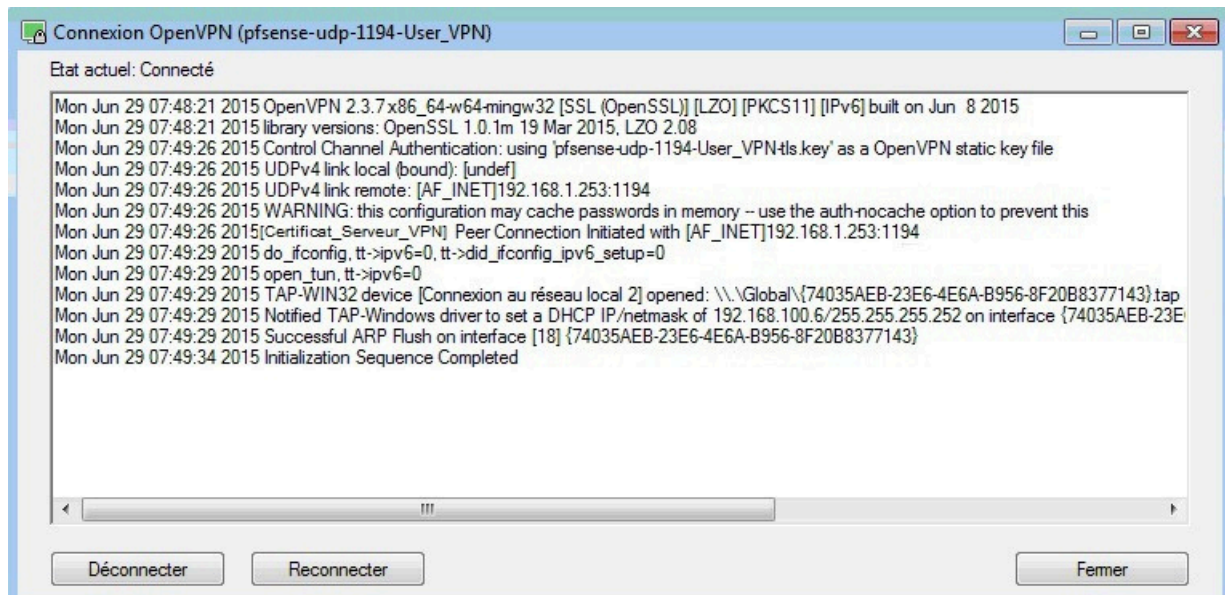
Cliquer-doit sur l'icône de l'application OpenVPN GUI et sélectionner la commande *Régler les problèmes de*

- d. *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.

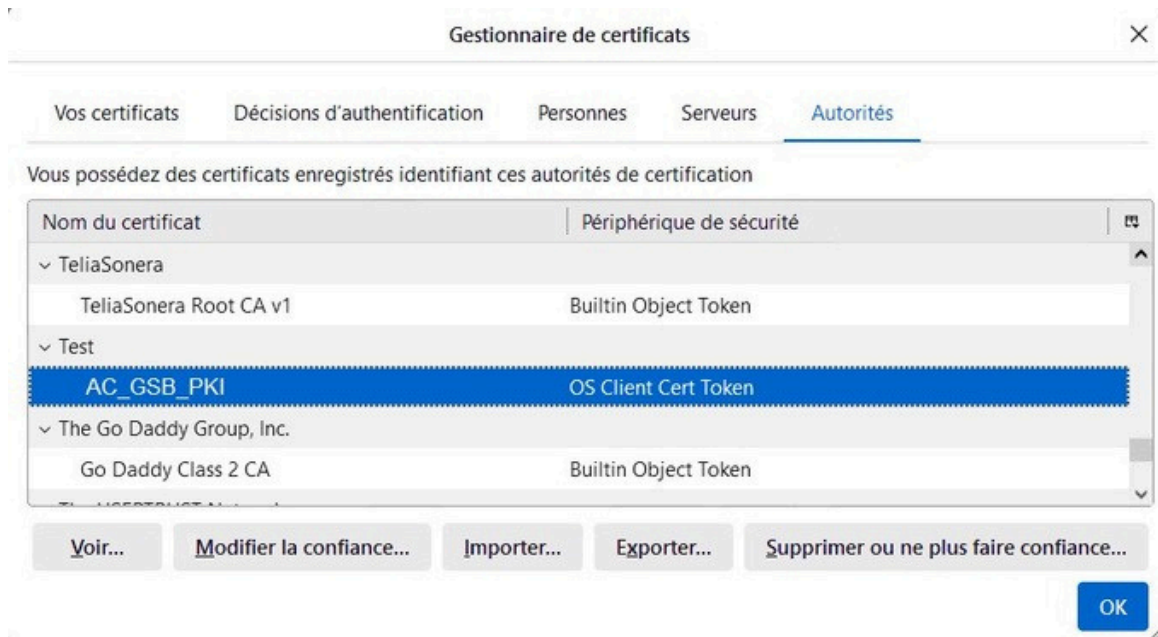
- f. Se connecter avec l'utilisateur *User_VPN* et le mot de passe *faure* :



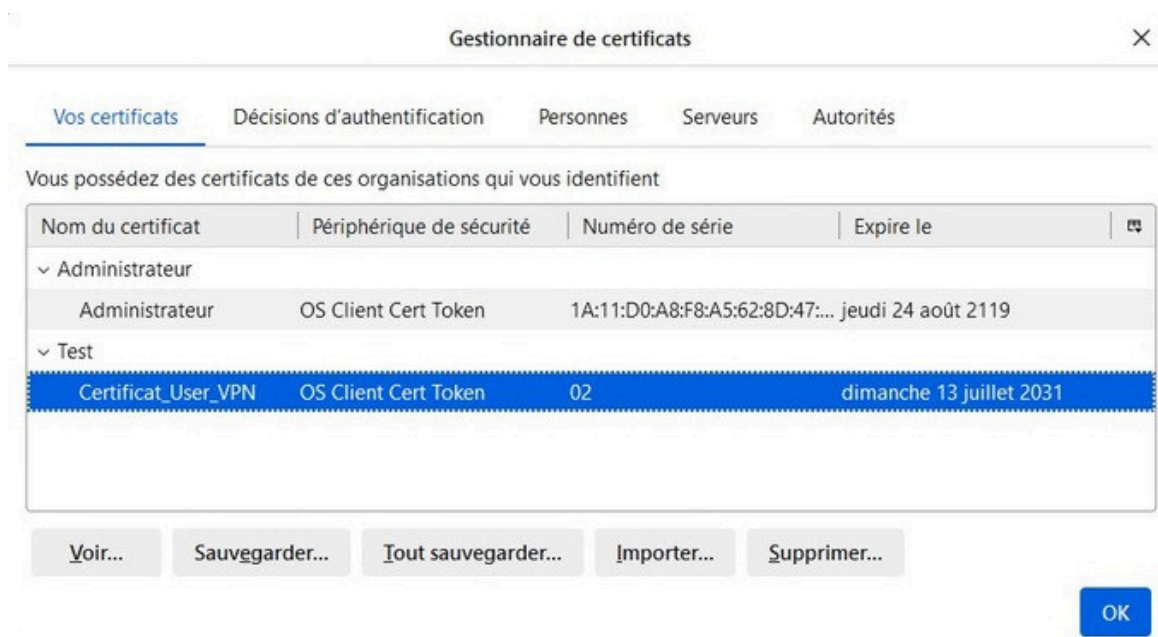
Pour info, le fichier de configuration du client OpenVPN, de nom *pfSense-udp-1194-User_VPN.ovpn* doit avoir le contenu suivant :



- 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 :

```
cmd: Invite de commandes
C:\Users\sio>ipconfig

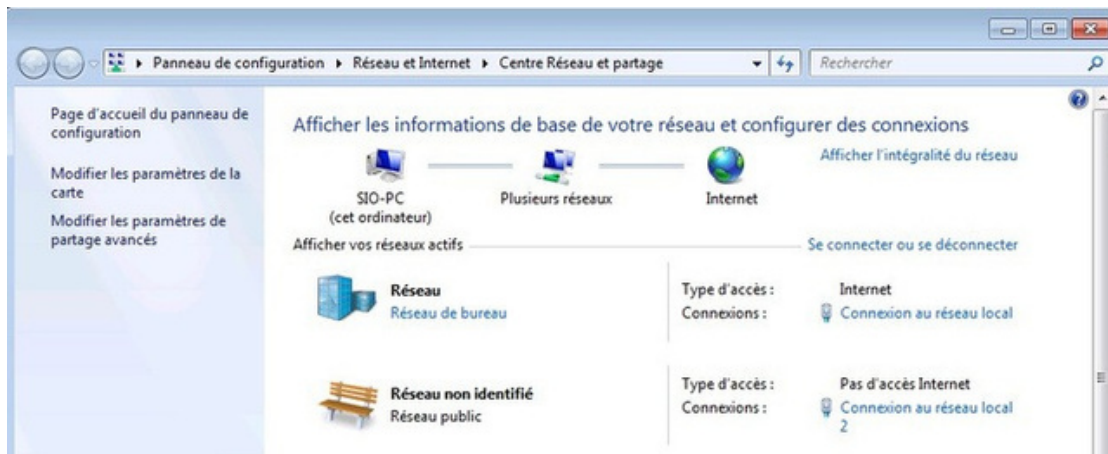
Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2 :

    Suffixe DNS propre à la connexion. . . : GSB.local
    Adresse IPv6 de liaison locale. . . . . : fe80::b14f:c9b7:a78f:ba9c%18
    Adresse IPv4. . . . . : 192.168.100.6
    Masque de sous-réseau. . . . . : 255.255.255.252
    Passerelle par défaut. . . . . :

Carte Ethernet Connexion au réseau local :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::7cca:6333:3a1d:d2b3%11
    Adresse IPv4. . . . . : 192.168.1.50
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.254
```



```
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. . . . . : IAP-Windows Adapter U9
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 ovpn1 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".

The screenshot shows the pfSense web interface with the 'Diagnostics' menu open to 'Execute command'. The command executed is `ifconfig`. The output shows the configuration for several network interfaces:

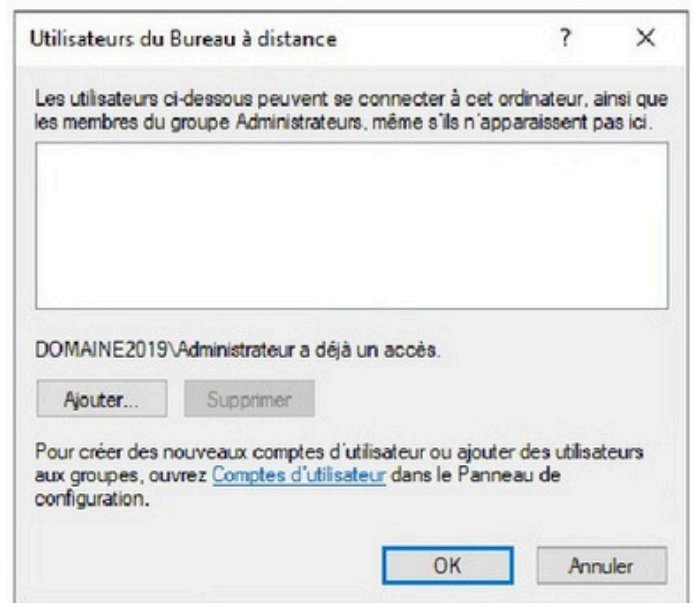
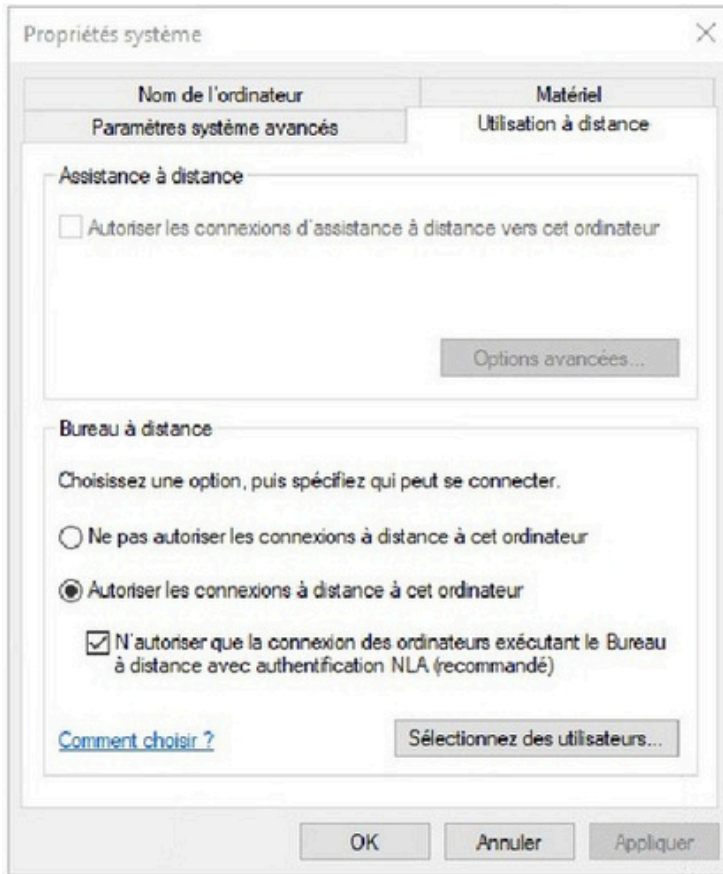
```

$ ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
  ether 00:50:56:8b:7e:76
  inet 192.168.1.253 netmask 0xffffffff broadcast 192.168.1.255
  inet6 fe80::250:56ff:fe8b:7e76%em0 prefixlen 64 scopeid 0x1
  nd6 options=1<PERFORMNUD>
  media: Ethernet autoselect (1000baseT <full-duplex>)
  status: active
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
  ether 00:50:56:8b:7e:77
  inet6 fe80::250:56ff:fe8b:7e77%em1 prefixlen 64 scopeid 0x2
  inet 192.168.2.253 netmask 0xffffffff broadcast 192.168.2.255
  nd6 options=1<PERFORMNUD>
  media: Ethernet autoselect (1000baseT <full-duplex>)
  status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
enc0: flags=0<> metric 0 mtu 1536
pflog0: flags=100<PROMISC> metric 0 mtu 33144
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
  options=3<RXCSUM, TXCSUM>
  inet 127.0.0.1 netmask 0xff000000
  inet6 ::1 prefixlen 128
  inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
  nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
pfsync0: flags=0<> metric 0 mtu 1460
  syncpeer: 224.0.0.240 maxupd: 128 syncok: 1
ovpn1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
  options=80000<LINKSTATE>
  inet6 fe80::250:56ff:fe8b:7e76%ovpn1 prefixlen 64 scopeid 0x8
  inet 192.168.100.1 --> 192.168.100.2 netmask 0xffffffff
  nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
  Opened by PID 89609
  
```

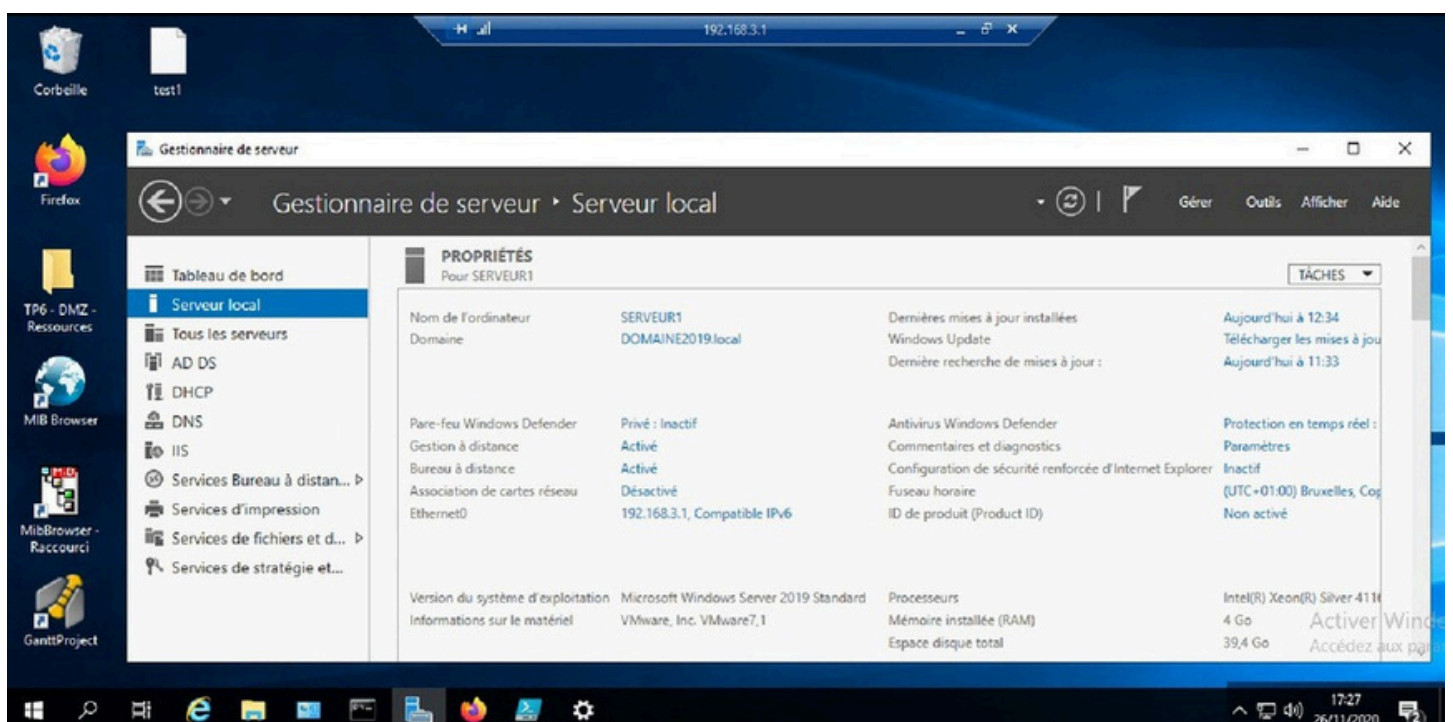
At the bottom of the terminal window, the command entered is `ifconfig`.

**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 !**

Il faut 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

- Sur le poste SERVEUR1 par exemple, seconnecter à l'interface LAN du routeur-parefeu Pfsense pour le configurer, avec le navigateur Mozilla Firefox ;
- Sur le même poste, télécharger et installer le logiciel de captures de trames Wireshark.
- Avec la commande PfSense Diagnosics Packet Capture, sélectionner les choix de capture suivants:

Interface (de capture) : WAN
Level of Detail : Full
- Lancer la capture avec *Start*.
- Depuis un poste client VPN, ouvrir une session de Connexion Bureau à distance sur SERVEUR1, puis la refermer.
- 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.

The screenshot shows the Wireshark interface with the following details:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|-----------------|----------|--------|--|
| 73 | 13.182501 | 192.168.1.253 | 192.168.216.250 | TCP | 54 | 52519-8080 [ACK] Seq=3 Ack=2 win=513 Len=0 |
| 74 | 13.503204 | 192.168.1.50 | 192.168.1.253 | OpenVPN | 143 | MessageType: P_DATA_V1 |
| 75 | 13.504592 | 192.168.1.253 | 192.168.1.50 | OpenVPN | 143 | MessageType: P_DATA_V1 |
| 76 | 13.506517 | 192.168.1.50 | 192.168.1.253 | OpenVPN | 127 | MessageType: P_DATA_V1 |
| 77 | 13.506540 | 192.168.1.50 | 192.168.1.253 | OpenVPN | 175 | MessageType: P_DATA_V1 |
| 78 | 13.515049 | 192.168.1.253 | 192.168.1.50 | OpenVPN | 127 | MessageType: P_DATA_V1 |
| 79 | 13.515100 | 192.168.1.253 | 192.168.1.50 | OpenVPN | 143 | MessageType: P_DATA_V1 |
| 80 | 13.711138 | 192.168.1.50 | 192.168.1.253 | OpenVPN | 127 | MessageType: P_DATA_V1 |
| 81 | 14.169317 | 192.168.1.253 | 192.168.1.254 | ICMP | 94 | Echo (ping) request id=0x6631, seq=770/515, ttl=64 (re... |
| 82 | 14.169985 | 192.168.1.254 | 192.168.1.253 | ICMP | 94 | Echo (ping) reply id=0x6631, seq=770/515, ttl=64 (re... |
| 83 | 15.179264 | 192.168.1.253 | 192.168.1.254 | ICMP | 94 | Echo (ping) request id=0x6631, seq=1026/516, ttl=64 (re... |

Packet 74 details:

- Frame 74: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
- Ethernet II, Src: Vmware_8b:7e:86 (00:50:56:8b:7e:86), Dst: vmware_8b:7e:76 (00:50:56:8b:7e:76)
- Internet Protocol Version 4, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.253 (192.168.1.253)
- User Datagram Protocol, Src Port: 57355 (57355), Dst Port: 1194 (1194)
- OpenVPN Protocol

Packet bytes (hex and ASCII):

```

0000 00 50 56 8b 7e 76 00 50 56 8b 7e 86 08 00 45 00  .PV.~v.P V.~...E.
0010 00 81 15 1b 40 00 80 11 60 d1 c0 a8 01 32 c0 a8  ...@...  ...2.
0020 01 fd e0 0b 04 aa 00 6d 83 06 30 d0 a8 0b 49 a8  .....m ..0...I.
0030 a5 2b b1 09 ee 1b 42 a4 f8 e8 31 47 bb c7 0e 1b  .+...B. ..1G...
0040 4a 70 0a fe 9d 5f bb da f9 f7 58 7d 9d 4a 95 fc  Jp.....X}.J.
0050 1a d8 7c 3f 32 5e 99 92 55 a5 5d c7 93 06 ee fc  .]??^.. U.]....
0060 47 95 46 62 a4 38 01 b7 8f 31 73 09 33 17 f5 32  G.Fb.8. .1s.3..2
0070 41 d2 83 41 57 f9 3e 79 51 21 b6 de 80 82 02 d5  A..Aw.>y Q!.....
0080 21 c2 84 c8 32 dc 36 b6 f4 57 87 a6 61 07 76  !...2.6. .W..a.v
  
```