

# Projet MDL

## Sommaire:

[Mission 1 : Installation du routeur-pare-feu PfSense](#)

[Mission 2 A : création du domaine MDL.local](#)

[Mission 2 B: installation du poste client PC1](#)

[Mission 3 : Inventaire du matériel avec GLPI/FusionInventory](#)

[Travail à faire](#)

[Réalisation :](#)

[Installation du Plugin FusionInventory](#)

[Mission 4 : Installation d'un VPN](#)

[Travail à faire :](#)

[Réalisation :](#)

[Configuration du serveur OpenVPN sur le routeur-parefeu PfSense](#)

[Exportation de la configuration du client depuis PfSense](#)

[Installation du client OpenVPN sur un poste client](#)

[Mission 5 : Installation d'un serveur hôte de session Bureau à distance](#)

[Introduction de mission :](#)

[Prérequis](#)

[Configuration d'un serveur hôte de session bureau à distance](#)

[Installation d'un application pour le Bureau à distance](#)

[Ouverture d'une application RemoteApp \(à distance\)](#)

[Mission 6 : Configuration d'un cluster de deux Pfsense redondants \(en Haute Disponibilité\)](#)

[Introduction de mission :](#)

[Travail à faire](#)

[Réalisation :](#)

[PFSENSE MAITRE](#)

[PFSENSE ESCLAVE](#)

[Configuration IP virtuelle](#)

[LAN](#)

[PFSENSE Maître](#)

[PFSENSE Esclave](#)

[DMZ](#)

[PFSENSE Maître](#)

[PFSENSE Esclave](#)

[Configuration Synchro](#)

[Sur le PFSENSE Maître :](#)

[Sur le PFSENSE Esclave:](#)

## Mission 1 : Installation du routeur-pare-feu PfSense

- Créer une nouvelle machine virtuelle sous VMWare, de nom

*PM-MDL-PfSense*

- Vérifier que la machine virtuelle Pfsense dispose de 4 cartes réseau (si ce n'est pas le cas, mettre hors-tension la machine et ajouter les cartes nécessaires).

- Assigner les interfaces du Pfsense (fonction 1 : *Assign Interfaces* sur l'écran d'interface texte du Pfsense)

**WAN : *vmx0***

**LAN : *vmx1***

**OPT1 : *vmx2***

**OPT2 : *vmx3***

- Attribuer des adresses IP aux interfaces du Pfsense (fonction 2 : *Set Interface(s) IP address* sur l'écran d'interface texte du Pfsense) (ne pas oublier de spécifier la passerelle nécessaire pour l'interface WAN).

Attention : ne pas configurer de DHCP (sur aucune interface) !

- Attribuer l'étiquette réseau adéquate à chaque interface réseau selon l'adresse MAC de la carte :

a) dans le tableau ci-dessous, noter l'adresse MAC de chaque interface réseau (fonction 1 *Assign Interfaces* sur l'écran d'interface texte du Pfsense)

b) retrouver (sous VMware Vsphere, onglet *Résumé*, *Paramètres Matériel VM*) le numéro d'adaptateur réseau correspondant à chaque adresse MAC de cette VM, et le noter dans le tableau

c) attribuer l'étiquette réseau adéquate à chaque adaptateur réseau (sous VMware Vsphere, onglet *Résumé*, *Modifier les paramètres*)

Interface physique	Interface logique	Adresse MAC	N° Adaptateur réseau	Etiquette réseau
vmx0	<b>WAN</b>			<i>Salle-211</i>
vmx1	<b>LAN</b>			<i>LAB-SISR-X-2</i>
vmx2	<b>OPT1 (DMZ)</b>			<i>LAB-SISR-X-4</i>
Vmx3	<b>OPT2 (PFSYNC)</b>			<i>LAB-SISR-X-3</i>

- Rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en décochant la case *Block private networks* de l'interface WAN (sur l'écran d'interface graphique accessible via un navigateur de la machine physique hôte) :

- Modifier si besoin les règles de filtrage en entrée de l'interface LAN pour autoriser toute communication à partir de n'importe quel poste de n'importe quel VLAN de MDL.

Conseils :

- L'interface graphique du Pfsense fonctionne très bien avec le navigateur Internet Explorer ; il peut poser des problèmes avec un autre navigateur (identifiant et mot de passe parfois non-reconnus).
- Il faut rendre accessible l'interface graphique uniquement par le port 80 (ou par le port 443), mais pas par les deux simultanément (peut poser des problèmes lors de la mise en cluster de ce Pfsense avec un autre).

Attention : ne pas configurer de DHCP (sur aucune interface) !

## Mission 2 A : création du domaine MDL.local

- Créer une nouvelle machine virtuelle sous VMWare, de nom  
*PM-MDL-SERVEUR1-Contrôleur MDL.local-Windows 2019*
- Attribuer l'étiquette réseau adéquate à l'interface réseau.
- Sur cette machine, modifier le nom de l'ordinateur et sa configuration IP, puis installer le contrôleur du domaine **MDL.local** qui sera aussi serveur DNS.

## Mission 2 B: installation du poste client PC1

- Créer une nouvelle machine virtuelle sous VMWare, de nom  
*PM-MDL-PC1-Client MDL.local-Windows 10*
- Attribuer l'étiquette réseau adéquate à l'interface réseau.
- Sur PC1, modifier le nom de l'ordinateur et sa configuration IP, puis connecter cette machine au domaine MDL.local (vérifier le bon fonctionnement du DHCP).

## Mission 3 : Inventaire du matériel avec GLPI/FusionInventory

### Travail à faire

- Installer GLPI sur le contrôleur de domaine, ainsi que le plugin FusionInventory.
- Installer l'agent FusionInventory sur chaque poste du réseau MDL (**SERVEUR1**, **PC1**, **Pfsense**) pour la remontée automatique des données des postes sur le serveur.
- Importer dans GLPI tous les utilisateurs du domaine MDL.local.
- Créer dans GLPI les opérations de maintenance suivantes sur le poste SERVEUR1, et vérifier l'exactitude des TCO et VNC de ce poste :

**Clément Ogier** travaille sur SERVEUR1 et constate que le lecteur de cdrom ne fonctionne plus du tout.

- ☐ il déclare un ticket d'incident, en date du jour, d'urgence haute, sur SERVEUR1.

**Laure Dubreuil** travaille sur SERVEUR1 et constate que le logiciel Gantt Project n'est pas installé ; elle en a pourtant besoin.

- ☐ elle déclare un ticket de demande, en date du jour, d'urgence haute, sur SERVEUR1.

L'utilisateur **glpi** attribue les tickets nouveaux au technicien **tech** qui va effectuer les travaux suivants :

- ☐ Pour le premier ticket, il échange l'ancien lecteur de cdrom par un neuf (45 mn de main d'oeuvre à 160 €/h ; prix d'un lecteur : 80 €).
- ☐ Pour le deuxième ticket, il installe le logiciel Gantt Project, et ne compte aucun temps passé.

SERVEUR1 a été acheté et mis en service le 01/01/2016. Son prix d'achat était de 1800 €. Son amortissement est linéaire sur 5 ans (aucune garantie connue).

### Réalisation :

- Installer le rôle **Serveur web IIS** avec les services de rôle par défaut et le service de rôle **CGI**.
- Installer ensuite PHP 7 :

Copier la dernière version (Non-Thread Safe (NTS)) du dossier **PHP 7** fourni (*php-7.2.11-nts-Win32-VC15-x64*) dans le dossier **C:\Program Files**;

Renommer le fichier **php.ini-development** en **php.ini** ;

Ajouter le chemin du dossier **C:\Program Files\php-7.2.11-nts-Win32-VC15-x64** à la variable d'environnement **Path** (*Panneau de configuration / Système et sécurité, Système, lien Paramètres système avancés* ; dans la fenêtre qui s'ouvre, sélectionner l'onglet **Avancé**, puis le bouton **Variables d'environnement** ; dans **Variables système**, sélectionner la ligne **Path**, puis cliquer sur le bouton **Modifier** ; cliquez sur le bouton **Nouveau** pour ajouter le chemin **C:\Program Files\php-7.2.11-nts-Win32-VC15-x64** à la variable Path) ;

Dans le **Gestionnaire IIS**, configurer **PHP** comme suit : cliquer sur le nom du serveur, puis double-cliquer sur l'icône **Mappages de gestionnaires** ; dans le panneau **Action**, cliquer sur le lien **Ajouter un mappage de module** :

**Chemin demandes** : \*.php  
**Module** : FastCgiModule  
**Exécutable** : taper le chemin d'accès complet à **Php-cgi.exe** :

*C:\ProgramFiles\php-7.2.11-nts-Win32-VC15-x64\php-cgi.exe*

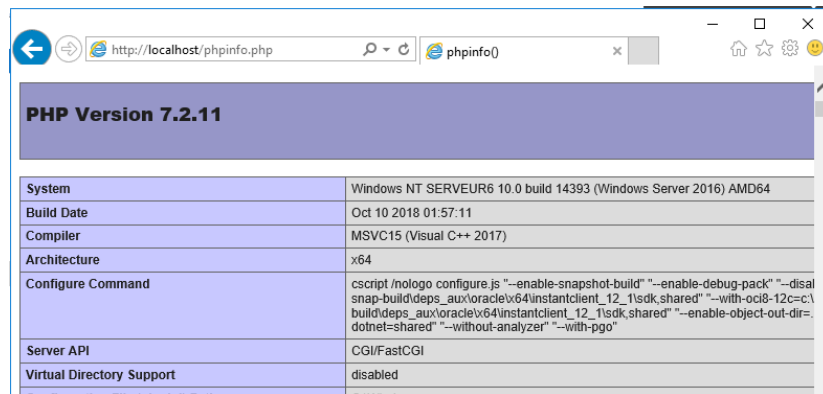
Cliquez ensuite sur le bouton **Restrictions des demandes** et cocher **Fichier ou dossier**.

Ainsi, tous les fichiers d'extension **.php** seront envoyés au module **FastCGIModule** pour y être exécutés par le programme **php-cgi.exe**.

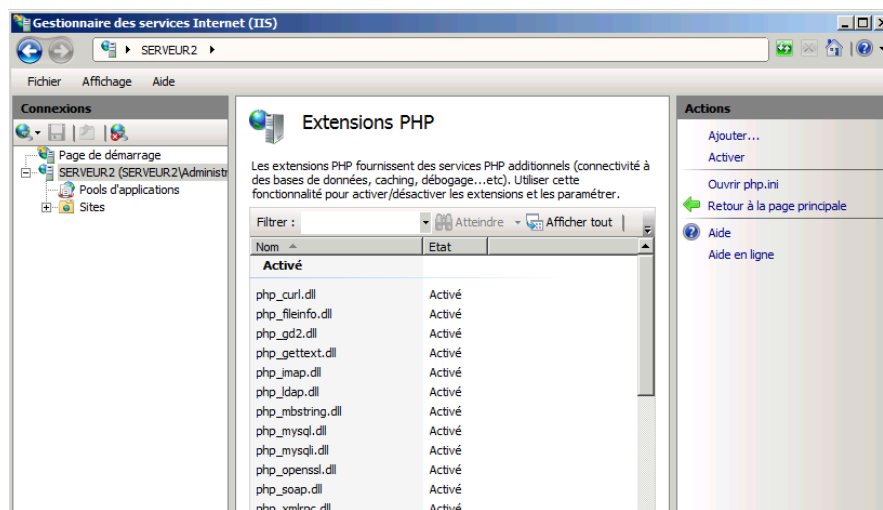
- Pour les anciennes versions de Windows, installer le package redistribuable **Microsoft Visual C++ vc\_redist.x64-2015.exe**
- Pour vérifier l'installation de PHP, créer le fichier suivant avec le bloc-notes :

```
<?php
phpinfo();
?>
```

enregistrer ce fichier dans **C:\inetpub\wwwroot\phpinfo.php**  
puis ouvrir le navigateur et entrer l'URL suivante : **http: //localhost/phpinfo.php** :  
une page Web bien formatée doit s'afficher et présenter les paramètres PHP actuels :



- Installer **PHPManager version 1.5**, qui fonctionne bien avec **IIS version 10**, avec le **.msi** fourni.
- Redémarrer le serveur
- Installer le SGBD Mysql :
  - Si l'installation se fait sur un serveur **Windows Server 2008**, installer d'abord le **framework .NET Framework 4.5** nécessaire pour le fonctionnement de Mysql
  - Installer la version **MySQL Community Server** (*installer le serveur uniquement (et non tout le package)*).
  - Si besoin, installer **PHPMyAdmin** (qui nécessite PHP déjà installé).



- Dans **PHP Manager**, activer les extensions suivantes (utilisées par GLPI) :
  - **php\_fileinfo.dll**
  - **php\_gd.dll**



- php\_intl.dll
- php\_ldap.dll
- php\_imap.dll
- php\_mysqli.dll

- Installer GLPI :

copier le dossier **glpi** dans **inetpub\wwwroot**

Dans l'explorateur Windows, attribuer l'autorisation Modification à Utilisateurs pour le dossier **C:\inetpub\wwwroot\glpi**

sous **IIS**, si besoin, créer le site web sous le nom **glpi** avec le nom d'hôte **www.glpi.fr**

## Installation du Plugin FusionInventory

copier le dossier fusionInventory dans **inetpub\wwwroot\glpi\plugins**

Dans **GLPI**, sélectionner la commande **Configuration / Plugins** ; dans la ligne du plugin FusionInventory, cliquer sur le lien **Installer**, puis ensuite sur le lien **Activer** ;

Toujours dans **GLPI**, sélectionner la commande **Administration / Entités**, puis cliquer sur le lien **Root entity**, puis sur le lien Fusioninventory : saisir l'URL d'accès au service :

<http://192.168.3.2/glpi/plugins/fusioninventory/>

- Déployer l'agent **FusionInventory Windows** sur chaque poste Windows du réseau *installer manuellement et configurer l'agent FusionInventory Windows sur chaque poste Windows.*

Pour installer l'agent **FusionInventory** sous Windows et Pfsense, suivre les indications de l'Annexe 3

- Vérifier dans **GLPI**, l'historique des remontées des données par les agents ; pour cela sélectionner **Plugins / FusionInventory**, sélectionner alors **Général / Gestion des agents** : on voit ainsi les dernières remontées.

Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation	Dernière modification	Composants - Processeur	Réseau - IP
PC1		VMware, Inc.	VMware-42 0b 08 fa 6e 5f 94 71-c7 74 bc df ee 63 af 68	Other	VMware Virtual Platform	Microsoft Windows 7 Professionnel	2017-02-06 14:42	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.3.12 fe80::608a:5f32:ae64:db50
SERVEUR1		VMware, Inc.	VMware-42 0b 6d 8a 41 57 02 71-63 67 12 9d fe f7 e6 a0	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:31	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	fe80::ad1f:778a:fc7d:da6 192.168.3.1
SERVEUR2		VMware, Inc.	VMware-42 0b 68 44 71 f4 ab 5d-87 69 c5 3a 27 4e c3 47	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:33	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.3.2 fe80::959b:2e3:db4c:53e6
SERVEUR6		VMware, Inc.	VMware-42 0b 51 ff 54 25 f4 7d-4f cd 3c c4 77 4b a0 fb	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:36	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.1.1 fe80::1042:9d2d:cf28:5839

## Mission 4 : Installation d'un VPN

### Travail à faire :

Le serveur VPN OpenVPN, configuré sur le PfSense qui intègre d'origine OpenVPN, gèrera sa propre autorité de certification ainsi que le certificat de l'autorité de certification.

Chaque machine Windows souhaitant se connecter au serveur OpenVPN utilisera le client VPN *OpenVPN GUI for Windows*.

On configurera le serveur OpenVPN avec authentification des utilisateurs par un serveur LDAP (**SERVEUR1**).

L'adresse IP réseau du VPN sera **192.168.10.0/24**. On utilisera le port **1196** du Pfsense pour créer la liaison VPN.



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 :

**Private networks**

☐ **Block private networks**  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned off unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not be the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Save Cancel

## Réalisation :

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 **CA\_Acces\_VPN**, 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**) :

System / Certificate Manager / CAs / Edit

[CAs](#)
[Certificates](#)
[Certificate Revocation](#)

### Create / Edit CA

**Descriptive name**

**Method**

**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**

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**   
 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)**

**Common Name**

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


**Country Code**

**State or Province**

**City**

**Organization**

**Organizational Unit**

 Save

- Toujours dans la commande **System Cert Manager**, mais dans l'onglet **Certificates**, créer un nouveau certificat, le certificat **SSL** du serveur Pfsense **OpenVPN** (*dont la clé publique permettra de chiffrer le trafic entre client et serveur VPN*), de nom **Certificat\_Acces\_VPN**, de type **Server Certificate**, et en choisissant la méthode **Create an internal Certificate** ; sélectionner l'autorité de certification créée précédemment **CA\_Acces\_VPN** 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

CAAs Certificates Certificate Revocation

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

Certificat\_Acces\_VPN

Internal Certificate

Certificate authority

CA\_Acces\_VPN

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\_Acces\_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

## Configuration du serveur OpenVPN sur le routeur-parefeu PfSense

- Sur le poste SERVEURDOMMDL, créer l'utilisateur suivant dans l'Active Directory du domaine MDL

Nom	Nom d'ouverture de session	Mot de passe
User_VPN_LDAP	User_VPN_LDAP	Windows2019

Cet utilisateur User\_VPN\_LDAP permettra au firewall de s'authentifier sur l'Active Directory.

- Configurer l'authentification depuis l'Active Directory, avec la commande System **User Manager**, dans l'onglet **Authentication Servers**, pour créer un nouveau serveur d'authentification de nom Serveur AD GSB, de type LDAP, et de modèle initial OpenLDAP, qui sera le serveur de domaine MDL.local :

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

### Server Settings

**Descriptive name**

**Type**

### LDAP Server Settings

**Hostname or IP address**   
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

**Port value**

**Transport**

**Peer Certificate Authority**   
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

**Protocol version**

**Server Timeout**   
Timeout for LDAP operations (seconds)

**Search scope**   
  
**Base DN**

**Authentication containers**  [Select a container](#)  
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.  
Example: CN=Users,DC=example,DC=com or OU=Staff; OU=Freelancers

**Extended query** ☐ Enable extended query

**Bind anonymous** ☐ Use anonymous binds to resolve distinguished names

**Bind credentials**

**Initial Template**

**User naming attribute**

**Group naming attribute**

**Group member attribute**

**RFC 2307 Groups** ☐ LDAP Server uses RFC 2307 style group membership  
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

**Group Object Class**   
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

**Shell Authentication Group DN**   
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.  
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

**UTF8 Encode** ☐ UTF8 encode LDAP parameters before sending them to the server.  
Required to support international characters, but may not be supported by every LDAP server.

**Username Alterations** ☐ Do not strip away parts of the username after the @ symbol  
e.g. user@host becomes user when unchecked.

**Allow unauthenticated bind** ☒ Allow unauthenticated bind  
Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

[Save](#)

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name

Serveur AD GSB

Type

LDAP

LDAP Server Settings

Hostname or IP address

192.168.3.1

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value

389

Transport

Standard TCP

Peer Certificate Authority

CA\_Acces\_VPN

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version

3

Server Timeout

25

Timeout for LDAP operations (seconds)

Search scope

Level

Entire Subtree

Base DN

DC=GSB,DC=local

Authentication containers

CN=Users,DC=GSB,DC=local

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.  
Example: CN=Users,DC=example,DC=com or OU=Staff; OU=Freelancers

Select a container

Extended query

☐ Enable extended query

Bind anonymous

☐ Use anonymous binds to resolve distinguished names

Bind credentials

CN=User\_VPN\_LDAP,CN=Users,DC=GSB,DC=local

Initial Template

OpenLDAP

User naming attribute

samAccountName

Group naming attribute

cn

Group member attribute

member

RFC 2307 Groups

☐ LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class

posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN

If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.  
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode

☐ UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

Username Alterations

☐ Do not strip away parts of the username after the @ symbol

e.g. user@host becomes user when unchecked.

Allow unauthenticated bind

☒ Allow unauthenticated bind

Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Save

15

- Valider et tester le serveur d'authentification, avec la commande **System User Manager**, dans l'onglet **Settings** :

**Authentication Server :**

**Serveur AD GSB**

System / User Manager / Settings

Users Groups **Settings** Authentication Servers

### Settings

**Session timeout**

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions.  
NOTE: This is a security risk!

**Authentication Server**

**Shell Authentication** ☐ Use Authentication Server for Shell Authentication  
If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

**Auth Refresh Time**

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

**En cliquant sur Save & Test, on devrait constater le succès complet du test**

- Configurer une nouvelle connexion **VPN**, de type **Remote Access (User Auth)** avec la commande **VPN OpenVPN**, dans l'onglet **Wizards** :
  - **Type of Server** : LDAP
  - **LDAP Servers** : Serveur AD GSB
  - **Certificate Authority** : CA\_Access\_VPN
  - **Certificate** : Certificat\_Acces\_VPN
  - **Description** : Serveur VPN avec authentification LDAP MDL
  - **Local Port** : 1195



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	<div>WAN</div>
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Protocol	<div>UDP on IPv4 only</div>
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Local Port	<div>1195</div>
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	<div>Serveur VPN avec authentification LDAP GSB</div>
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	
<b>TLS Authentication</b>	<input checked="" type="checkbox"/> <p>Enable authentication of TLS packets.</p>
<b>Generate TLS Key</b>	<input checked="" type="checkbox"/> <p>Automatically generate a shared TLS authentication key.</p>
<b>TLS Shared Key</b>	<div style="border: 1px solid #ccc; height: 50px; width: 100%;"></div> <p>Paste in a shared TLS key if one has already been generated.</p>
<b>DH Parameters Length</b>	<div>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>
<b>Data Encryption Negotiation</b>	<input checked="" type="checkbox"/> <p>Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.</p>
<b>Data Encryption Algorithms</b>	<div> <div>AES-256-GCM</div> <div>AES-128-GCM</div> <div>CHACHA20-POLY1305</div> </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>
<b>Fallback Data Encryption Algorithm</b>	<div>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>
<b>Auth Digest Algorithm</b>	<div>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>
<b>Hardware Crypto</b>	<div>No Hardware Crypto Acceleration</div> <p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p>

Tunnel Settings	
<b>Tunnel Network</b>	<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.
<b>Redirect Gateway</b>	<input type="checkbox"/> Force all client generated traffic through the tunnel.
<b>Local Network</b>	<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.
<b>Concurrent Connections</b>	<input type="text"/> Specify the maximum number of clients allowed to concurrently connect to this server.
<b>Allow Compression</b>	<input type="button" value="Refuse any non-stub compression (Most secure)"/> Allow compression to be used with this VPN instance, which is potentially insecure.
<b>Compression</b>	<input type="button" 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.
<b>Type-of-Service</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
<b>Inter-Client Communication</b>	<input type="checkbox"/> Allow communication between clients connected to this server.
<b>Duplicate Connections</b>	<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	
<b>Dynamic IP</b>	<input checked="" type="checkbox"/> <p>Allow connected clients to retain their connections if their IP address changes.</p>
<b>Topology</b>	<div>Subnet -- One IP address per client in a common subnet</div> <p>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".</p>
<b>DNS Default Domain</b>	<input type="text" value="GSB.local"/> <p>Provide a default domain name to clients.</p>
<b>DNS Server 1</b>	<input type="text" value="192.168.3.1"/> <p>DNS server IP to provide to connecting clients.</p>
<b>DNS Server 2</b>	<input type="text"/> <p>DNS server IP to provide to connecting clients.</p>
<b>NTP Server</b>	<input type="text"/> <p>Network Time Protocol server to provide to connecting clients.</p>
<b>NetBIOS Options</b>	<input type="checkbox"/> <p>Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</p>
<b>NetBIOS Node Type</b>	<div>none</div> <p>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).</p>
<b>NetBIOS Scope ID</b>	<input type="text"/> <p>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.</p>
<b>WINS Server 1</b>	<input type="text"/> <p>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</p>
<b>WINS Server 2</b>	<input type="text"/> <p>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</p>
<div>&gt;&gt; Next</div>	

Firewall Rule Configuration	
OpenVPN Remote Access Server Setup Wizard	
Firewall Rule Configuration	
<p>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.</p>	
Traffic from clients to server	
<b>Firewall Rule</b>	<input checked="" type="checkbox"/> <p>Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.</p>
Traffic from clients through VPN	
<b>OpenVPN rule</b>	<input checked="" type="checkbox"/> <p>Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.</p>

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

- Vérifier avec la commande Firewall Rules que ces règles ont bien été créées.
- Vérifier avec la commande Diagnostics Authentication, que l'utilisateur *anevers* est authentifié par *Serveur AD MDL*:

Diagnostics / Authentication


User anevers authenticated successfully. This user is a member of groups:

**Authentication Test**

Authentication Server   
Select the authentication server to test against.

Username

Password





 Test






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

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

Floating WAN LAN **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none		OpenVPN Serveur VPN avec authentificat wizard	   

 Add
  Add
  Delete
  Save
  Separator

- sur l'interface **WAN** :

Floating	WAN	LAN	OpenVPN
----------	-----	-----	---------

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗	0/0 B	*		Reserved Not assigned by IANA	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	1195	*	none	OpenVPN Serveur VPN avec authentificat wizard	   

Add
 Add
 Delete
 Save
 Separator

## 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**.

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

**DNS Server :**                      **192.168.216.74**

**Save. Redémarrer** ensuite le Pfsense.

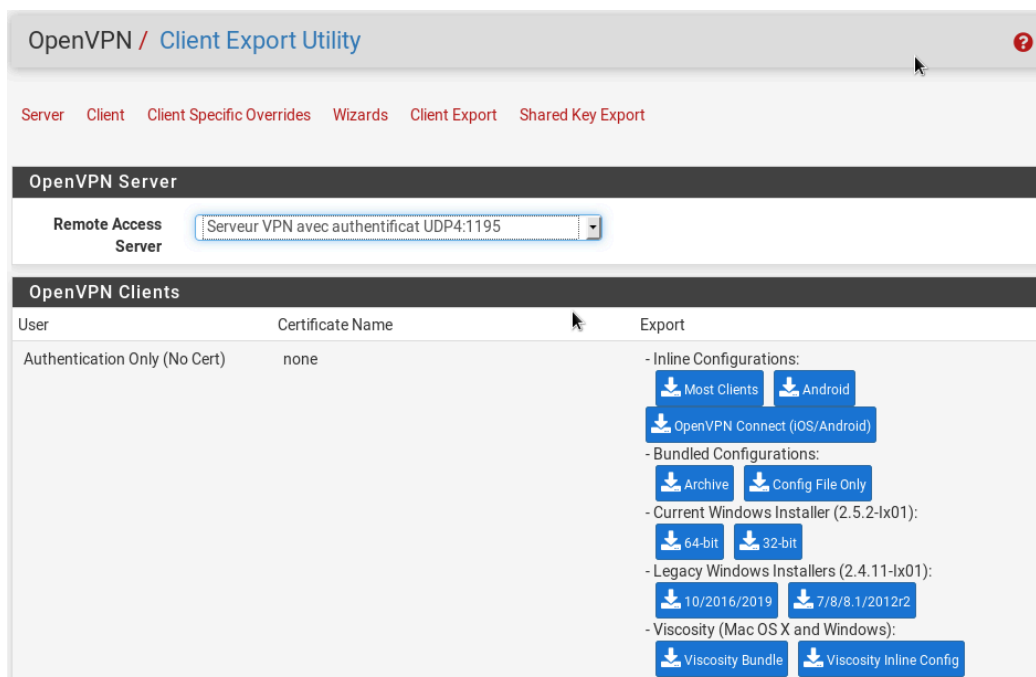
DNS Server Settings	
<b>DNS Servers</b> <input type="text" value="192.168.216.74"/> <small>Address</small> Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	<input type="text"/> <small>DNS Hostname</small> <small>Hostname</small> Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
<b>Add DNS Server</b> Add DNS Server	

Le package *OpenVPN Client Export Utility* permet d'exporter facilement la configuration qui devra être installée sur l'ordinateur client. Nous allons donc déjà installer ce package sur le PfSense serveur :

- 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.

- Sélectionner la commande VPN OpenVPN, dans l'onglet Client Export, pour le type d'utilisateur **Authentication Only (No Cert)**, afin de vérifier la présence de l'archive



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.

**Remarque** : Le fichier .ovpn contient la configuration à installer sur chaque poste client OpenVPN. Le fichier .key contient la clé TLS supplémentaire. Le fichier .crt contient le certificat de l'autorité de certification CA\_Acces\_VPN.

Nom ^	Modifié le	Type	Taille
pfSense-udp-1195.ovpn	19/11/2016 13:41	Fichier OVPN	1 Ko
pfSense-udp-1195-ca.crt	19/11/2016 13:41	Certificat de sécurité	2 Ko
pfSense-udp-1195-tls.key	19/11/2016 13:41	Fichier KEY	1 Ko

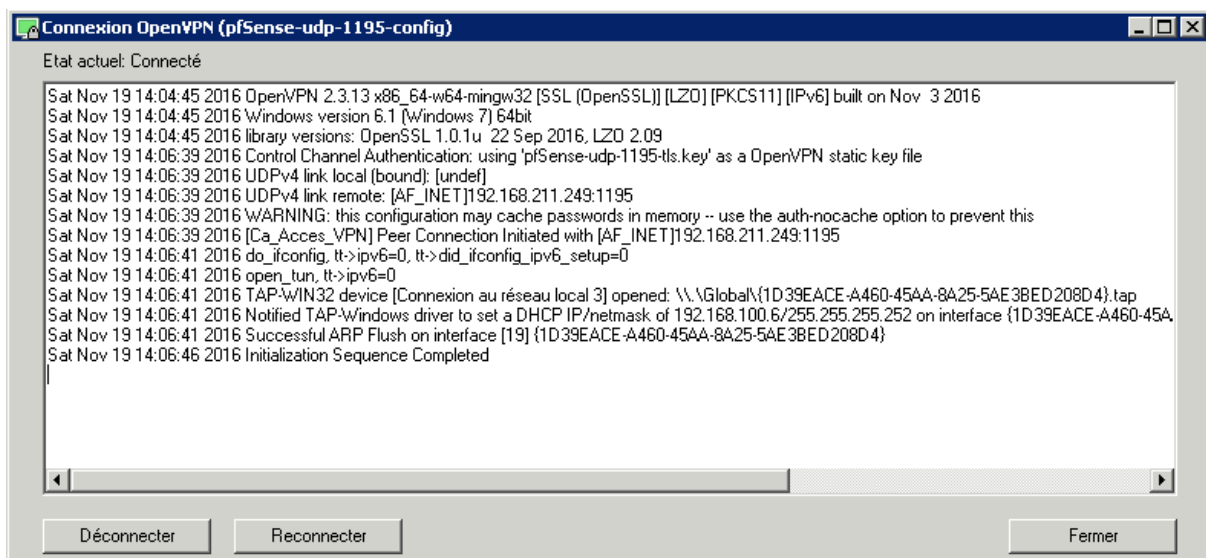
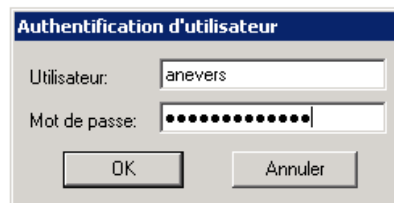
## Installation du client OpenVPN sur un poste client

- Sur le poste client, télécharger le client OpenVPN depuis le site suivant:

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

- 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-droit 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.

On va se connecter avec l'utilisateur **anevers** et le mot de passe **Windows2019** :





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

```

C:\Users\sio>ipconfig

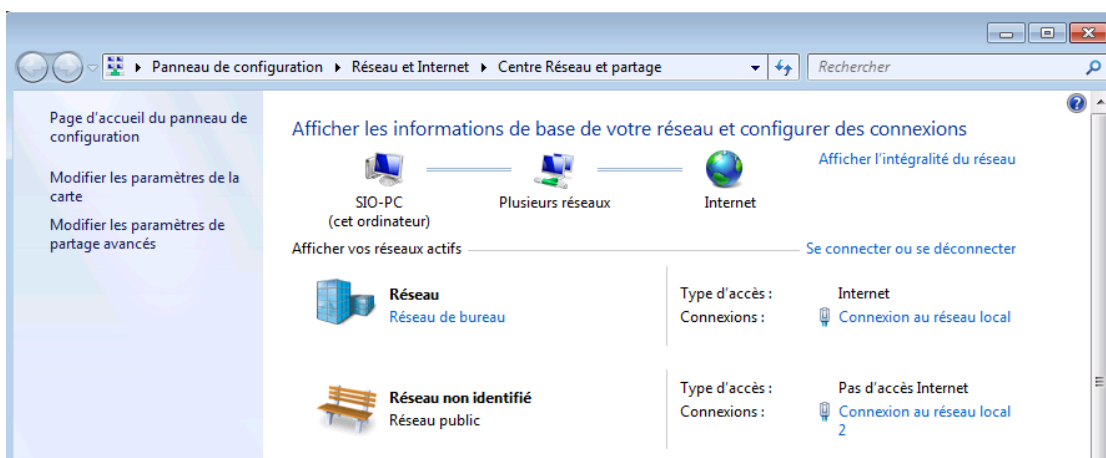
Configuration IP de Windows

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
  
```



```

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
    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
  
```

## Mission 5 : Installation d'un serveur hôte de session Bureau à distance

### Introduction de mission :

Installer et configurer SERVEUR1 pour qu'il soit serveur hôte de session de bureau à distance

Configurer Cisco Packet Tracer en tant que application Remote App accessible aux deux utilisateurs Clément Ogier et Laure Dubreil (sur les postes distants, penser à ouvrir une session de bureau à distance en utilisant le nom du serveur et non son adresse IP).

### Prérequis

Vérifier que les utilisateurs suivants sont créés (sinon les créer en décochant la case L'utilisateur doit changer de mot de passe à la prochaine ouverture de session) :

<i>Nom et prénom</i>	<i>Nom d'ouverture de session</i>	<i>Mot de passe</i>
<b>Alex Durois</b>	<b>adurois</b>	Windows2016
<b>Alice Nevers</b>	<b>anevers</b>	Windows2016
<b>Arthur Rabelais</b>	<b>arabelais</b>	Windows2016
<b>Kevin Berry</b>	<b>kberry</b>	Windows2016

### Configuration d'un serveur hôte de session bureau à distance

- Ouvrir le Gestionnaire de serveur > gérer > puis le lien Ajouter des rôles et fonctionnalités.
- Dans la fenêtre Assistant **Ajout des rôles**, choisir le type d'installation Installation des services Bureau à distance, puis le type de déploiement **Démarrage rapide** et le scénario de déploiement Déploiement de bureaux basés sur une session.
- Sélectionner le serveur concerné parmi le pool de serveurs sur lequel seront installés les services.

- Pensez à cliquer sur la case Redémarrer automatiquement le serveur de destination si nécessaire

Après le redémarrage du serveur:

- Dans le rôle **Services Bureau à distance**, sélectionner le "**sous-rôle**" à installer : Gestionnaire de licences des services Bureau à distance (remarquer que les sous-rôles Hôte de session Bureau à distance, Accès Bureau à distance par le Web, et Service Broker pour les connexions Bureau à distance sont déjà installés).

## Installation d'une application pour le Bureau à distance

- Nous allons procéder à l'installation de Packet tracer **sur le serveur tout d'abord et non sur la station**
- Dans le **Gestionnaire de serveur**, sélectionner **Services Bureau à distance**, puis depuis la **vue Collections**, cliquer sur le lien **QuickSessionCollection** pour modifier cette collection existante :
  - le serveur hôte sur lequel doit s'exécuter l'application est SERVEURDOMMDL (rubrique Serveurs hôtes)
  - les utilisateurs autorisés à exécuter cette application sont **MDL\Utilisateurs** du domaine
  - l'application **Cisco Packet Tracer** doit être ajoutée à la liste Programmes RemoteApp (cliquer sur le bouton T CHES de la zone PROGRAMMES REMOTEAPP, puis sélectionner Publier des programmes RemoteApp ; dans la liste des programmes, sélectionner Cisco Packet Tracer puis cliquer sur Publier) :

Gestionnaire de serveur > Services Bureau à distance > Collections > QuickSessionCollection

**PROPRIÉTÉS**  
Propriétés de la collection

Type de collection	Session
Ressources	Programmes RemoteApp
Groupe d'utilisateurs	GSB\Utilisateurs du domaine

**PROGRAMMES REMOTEAPP**  
Dernière actualisation le 08/12/2017 12:38:18 | Programmes RemoteApp publiés : 3 au total

Nom du programme RemoteApp	Alias	Visible dans l'Accès Web des services Bureau à distance
Calculatrice	Calculatrice	Oui
Paint	Paint	Oui
WordPad	WordPad	Oui
Cisco Packet Tracer	Packet Tr	Oui

**SERVEURS HÔTES**  
Dernière actualisation le 08/12/2017 12:38:18 | Tous les serveurs | 1 au total

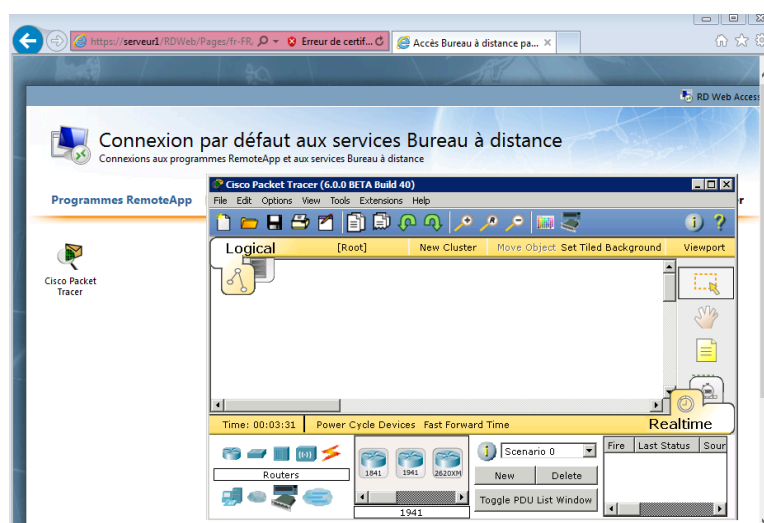
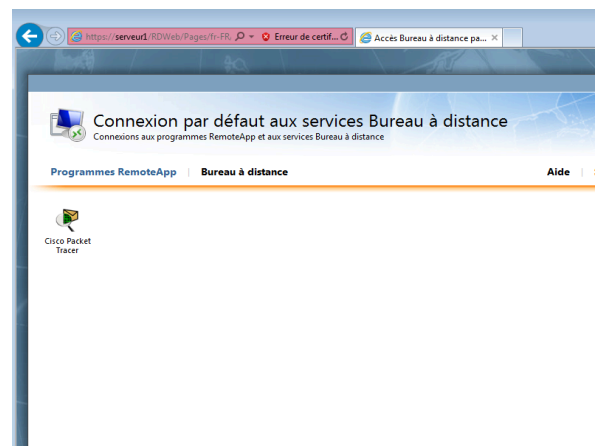
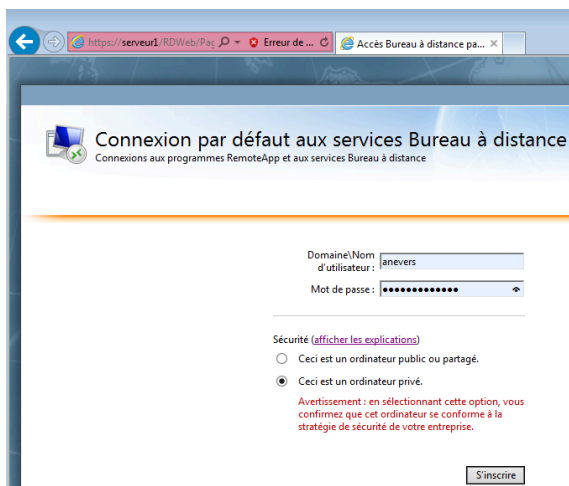
Nom du serveur	Type	Bureaux virtuels	Autoriser les nouvelles collections
SERVEUR1	Hôte de session Bureau à distance	N/A	Vrai

## Ouverture d'une application RemoteApp (à distance)

Le service de rôle **Accès Bureau à distance** par le Web, installé sur **SERVEURDOMMDL**, permet aux utilisateurs d'accéder aux programmes **RemoteApp** et aux services **Bureau à distance** via un **navigateur Web**.

- Démarrer la machine PC1 et ouvrir une session Windows avec l'utilisateur **anevers** et le mot de passe **Windows2016**
- Avec le navigateur Internet, ouvrir la page **https://SERVEURDOMMDL/rdweb** ou **https://SERVEURMDL.MDL.local/rdweb** ; après s'être authentifié (MDL\anevers / Windows2016), dans la liste des programmes RemoteApp proposés, cliquer sur **Packet Tracer** : le programme se lance dans une nouvelle fenêtre !

**Ceci doit être fait depuis un navigateur Explorer**



On peut surveiller les connexions bureau à distance ouvertes sur le serveur **SERVEURDOMMDL** :

Sur SERVEURDOMMDL, vérifier les connexions bureau à distance ouvertes: dans le **Gestionnaire de serveur**, sélectionner **Services Bureau à distance**, puis cliquer sur le **nom de la collection à surveiller** (exemple : **QuickSessionCollection**) : on constate que anevers a bien une session active en cours.

## Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

### Introduction de mission :

Le but de cette mission est de configurer un cluster de deux Pfsense pour assurer une haute disponibilité du routeur pare-feu Pfsense : en cas de défaillance du premier pfSense (pfSenseA primaire), le deuxième pfSense (pfSenseB secondaire) prend le relais sans aucune interruption de service : la bascule du pfSenseA vers pfSenseB est totalement transparente.

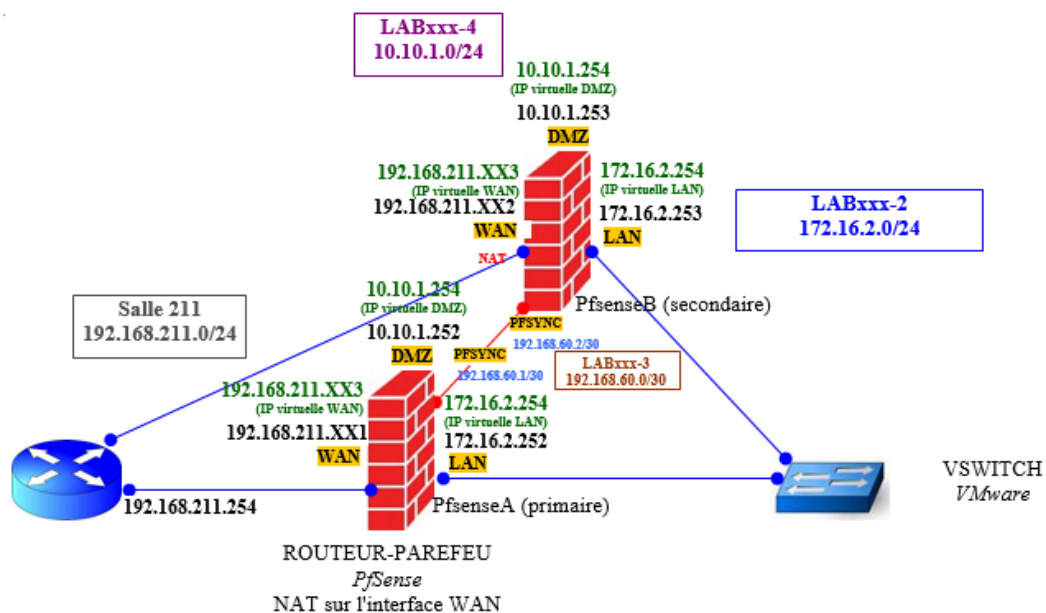
PfSense communiquera sur les réseaux LAN, WAN, et DMZ avec ses adresses IP virtuelles.

Afin d'assurer la réplication du pfSenseA vers le pfSenseB, 3 éléments doivent être configurés : CARP, pfsync et

XML-RPC :

- CARP (*Common Address Redundancy Protocol*) est un protocole permettant à plusieurs hôtes présents sur un même réseau de partager une même adresse IP virtuelle. C'est cette adresse IP *virtuelle* que pfSense va utiliser pour sa communication sur le réseau. Ainsi, en cas de défaillance du pfSense primaire (pfSenseA), le pfSense secondaire (pfSenseB) prendra le relais de manière transparente au niveau réseau (reprise de l'adresse IP virtuelle).
- PFSYNC est un protocole permettant de synchroniser entre deux pfSense l'état des connexions en cours. Ainsi, en cas de défaillance du Pfsense primaire, l'état des connexions en cours est maintenu sur le Pfsense secondaire. Il n'y a donc pas de coupure liée à la bascule des services du pfSenseA vers le pfSenseB.  
Cette synchronisation sera effectuée sur une interface dédiée sur chacun des deux Pfsense (à défaut, le lien LAN aurait pu être utilisé).
- XML-RPC est un protocole permettant la réplication de données d'un Pfsense vers un autre. Il est utilisé dans pfSense afin de répliquer la configuration du Pfsense primaire vers le Pfsense secondaire.

Pour garantir son bon fonctionnement, il est important qu'il utilise la même interface que celle utilisée par le protocole pfsync.



## Travail à faire

- Installer et configurer ce cluster de PfSense.
- Rédiger une procédure complète et détaillée (avec copies d'écran) de cette installation.

**Tutoriel** : <https://notamax.be/pfsense-creation-dun-cluster/>

**Conseil** : Pour mener cette mission efficacement sous VMware, il est fortement conseillé de cloner le **PfSense primaire** lorsque toutes les interfaces ont été correctement configurées, puis de configurer le clone comme PfSense secondaire.

## Réalisation :

**Préalable** : Partir d'un pfsense Valide (PfSense Maître)

1/ Dupliquer le PfSense Maître en PfSense Esclave

## 2/ Configuration IP de chaque PFSENSE

	Maître	Esclave
WAN	192.168.211.X	192.168.211.Y
LAN	172.16.2.252	172.16.2.253
DMZ	10.10.1.252	10.10.1.253
PFSYNC	192.168.60.1	192.168.60.2

Pour configurer les adaptateurs réseaux :

The screenshot displays the 'PM - Pfsense Esclave' interface. The top navigation bar includes 'Résumé', 'Surveiller', 'Configurer', 'Autorisations', and 'Bar'. The 'Résumé' tab is active, showing system details:

- SE invité :** FreeBSD 12 or later versions (64-bit)
- Compatibilité :** ESXi 6.7 Update 2 et versions ultérieures (VM version 15)
- VMware Tools :** En cours d'exécution, version :2147483647 (Invité géré) [Plus d'infos](#)
- Nom DNS :** pfSense.home.arpa
- Adresses IP :** 192.168.211.233 [Afficher toutes les 10 adresses IP](#)
- Hôte :** gf-esxi-02.labs-faure.ad

On the left, there is a terminal window showing system logs and links for 'Lancer la console Web' and 'Lancer Remote Console'. On the right, an 'ACTIONS' dropdown menu is open, listing the following options:

- Alimentation
- SE invité
- Snapshots
- Ouvrir Remote Console
- Migrer...
- Cloner
- Fault Tolerance
- Stratégies de VM
- Modèle
- Compatibilité
- Exporter les journaux du système...
- Modifier les paramètres...

## PFSENSE MAITRE

Modifier les paramètres...

PM-MDL-Pfsense

×

Matériel virtuel

Options VM

AJOUTER UN PÉRIPHÉRIQUE

> CPU	1	▼	
> Mémoire	1	Go	▼
> Disque dur 1	8	Go	▼
> Contrôleur SCSI 0	LSI Logic SAS		
> Adaptateur réseau 1	LAB-SISR-06-2	▼	☑ Connecté
> Adaptateur réseau 2	LAB-SISR-06-4	▼	☑ Connecté
> Adaptateur réseau 3	LAB-SISR-06-3	▼	☑ Connecté
> Adaptateur réseau 4	SALLE - 211	▼	☑ Connecté
> Lecteur CD/DVD 1	Fichier ISO banque de données	▼	☑ Connecté

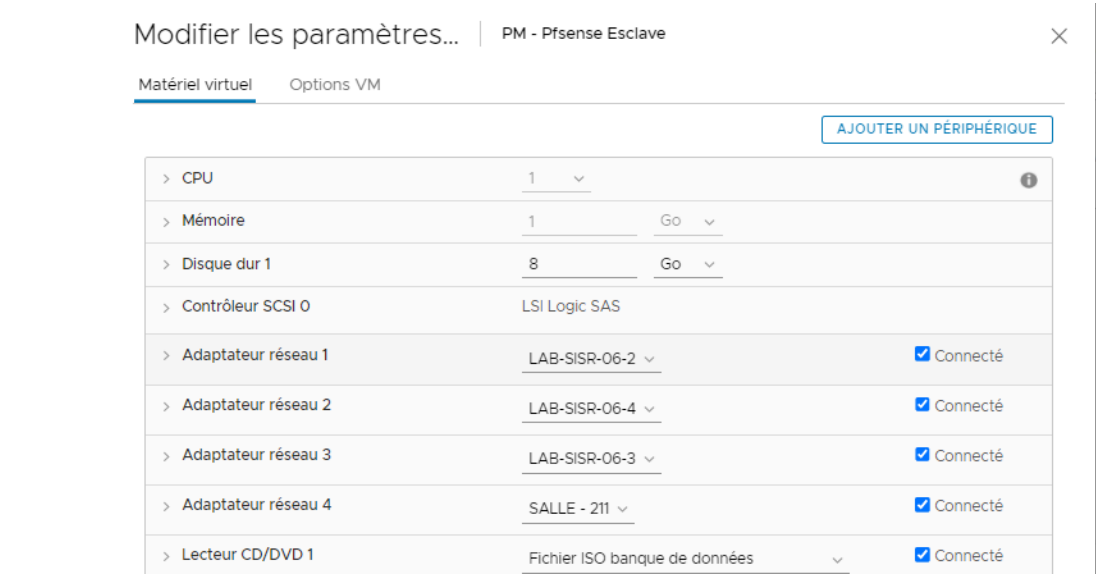
```
WAN (wan)      -> vmx0      -> v4: 192.168.211.232/24
LAN (lan)      -> vmx1      -> v4: 172.16.2.252/24
OPT1 (opt1)    -> vmx2      -> v4: 10.10.1.252/24
OPT2 (opt2)    -> vmx3      -> v4: 192.168.60.1/30
```

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
```



PFSense ESCLAVE



```
WAN (wan)      -> vmx0      -> v4: 192.168.211.233/24
LAN (lan)      -> vmx1      -> v4: 172.16.2.253/24
OPT1 (opt1)    -> vmx2      -> v4: 10.10.1.253/24
OPT2 (opt2)    -> vmx3      -> v4: 192.168.60.2/30

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
```

Configuration IP virtuelle

Création des ip virtuelles sur pfsense :

Maître et esclave	IP Virtuelle
172.16.2.254	LAN
10.10.1.254	DMZ

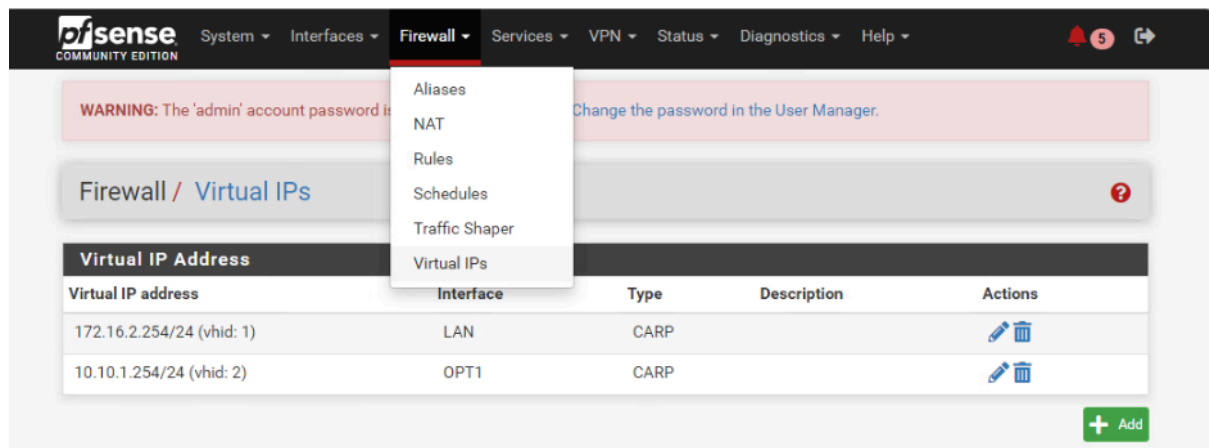
## Type CARP

VHID Group :

- 1 pour LAN
- 2 pour DMZ

Skew :

- 0 sur Maître
- 100 sur Esclave



## LAN

## PFSENSE Maître

Edit Virtual IP

Type
☐ IP Alias
☒ CARP
☐ Proxy ARP
☐ Other

Interface
LAN

Address type
Single address

Address(es)
172.16.2.254
/ 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password.
Confirm

VHID Group
1
Enter the VHID group that the machines will share.

Advertising frequency
1
0
Base
Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description
lan
A description may be entered here for administrative reference (not parsed).

Save

## PFSENSE Esclave

Firewall / Virtual IPs / Edit

### Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface

Address type

Address(es)  /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.


Advertising frequency

Base Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

 Save

## DMZ

## PFSENSE Maître

Firewall / Virtual IPs / Edit

### Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface

Address type

Address(es)  /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.


Advertising frequency

Base Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

 Save

## PFSENSE Esclave

Firewall / Virtual IPs / Edit

### Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface

Address type

Address(es)  /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.

Advertising frequency

Base Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

## Configuration Synchro

### Sur le PFSENSE Maître :

- Interface de synchro : **PFSYNC**
- IP Synchro de pair : **192.168.60.2**
- Synchro avec **192.168.60.2**

System / High Availability

### State Synchronization Settings (pfsync)

**Synchronize states** ☒ pfsync transfers state insertion, update, and deletion messages between firewalls.  
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group.  
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

**Synchronize Interface**   
If Synchronize States is enabled this interface will be used for communication.  
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.  
An IP must be defined on each machine participating in this failover group.  
An IP must be assigned to the interface on any participating sync nodes.

**Filter Host ID**   
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.  
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).  
Each node participating in state synchronization must have a different ID.

**pfsync Synchronize Peer IP**   
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

### Configuration Synchronization Settings (XMLRPC Sync)

**Synchronize Config to IP**   
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.  
  
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Username**   
Enter the webConfigurator username of the system entered above for synchronizing the configuration.  
Do not use the Synchronize Config to IP and username option on backup cluster members!

Synchronize backup cluster members:

**Synchronize admin** ☐ synchronize admin accounts and autoupdate sync password.  
By default, the admin account does not synchronize, and each node may have a different admin password.  
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

**Select options to sync**

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

☒ Toggle All

[Sur le PFSENSE Esclave:](#)

System / High Availability

### State Synchronization Settings (pfsync)

**Synchronize states** ☒ pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled (see Configuration Synchronization Settings below)

**Synchronize Interface**  If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

**Filter Host ID**  Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.

**pfsync Synchronize Peer IP**  Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

### Configuration Synchronization Settings (XMLRPC Sync)

**Synchronize Config to IP**  Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Username**  Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!

**Remote System Password**   Confirm Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Password**   Confirm Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!

**Synchronize admin** ☐ synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

**Select options to sync**

- ☐ User manager users and groups
- ☐ Authentication servers (e.g. LDAP, RADIUS)
- ☐ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☐ Firewall rules
- ☐ Firewall schedules
- ☐ Firewall aliases
- ☐ NAT configuration
- ☐ IPsec configuration
- ☐ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☐ DHCP Server settings
- ☐ DHCP Relay settings
- ☐ DHCPv6 Relay settings
- ☐ WoL Server settings
- ☐ Static Route configuration
- ☐ Virtual IPs
- ☐ Traffic Shaper configuration
- ☐ Traffic Shaper Limiters configuration
- ☐ DNS Forwarder and DNS Resolver configurations
- ☐ Captive Portal
- ☒ Toggle All

Une fois la configuration effectuée, veuillez redémarrer les machines Pfenses.

## Annexe : Schéma du réseau

