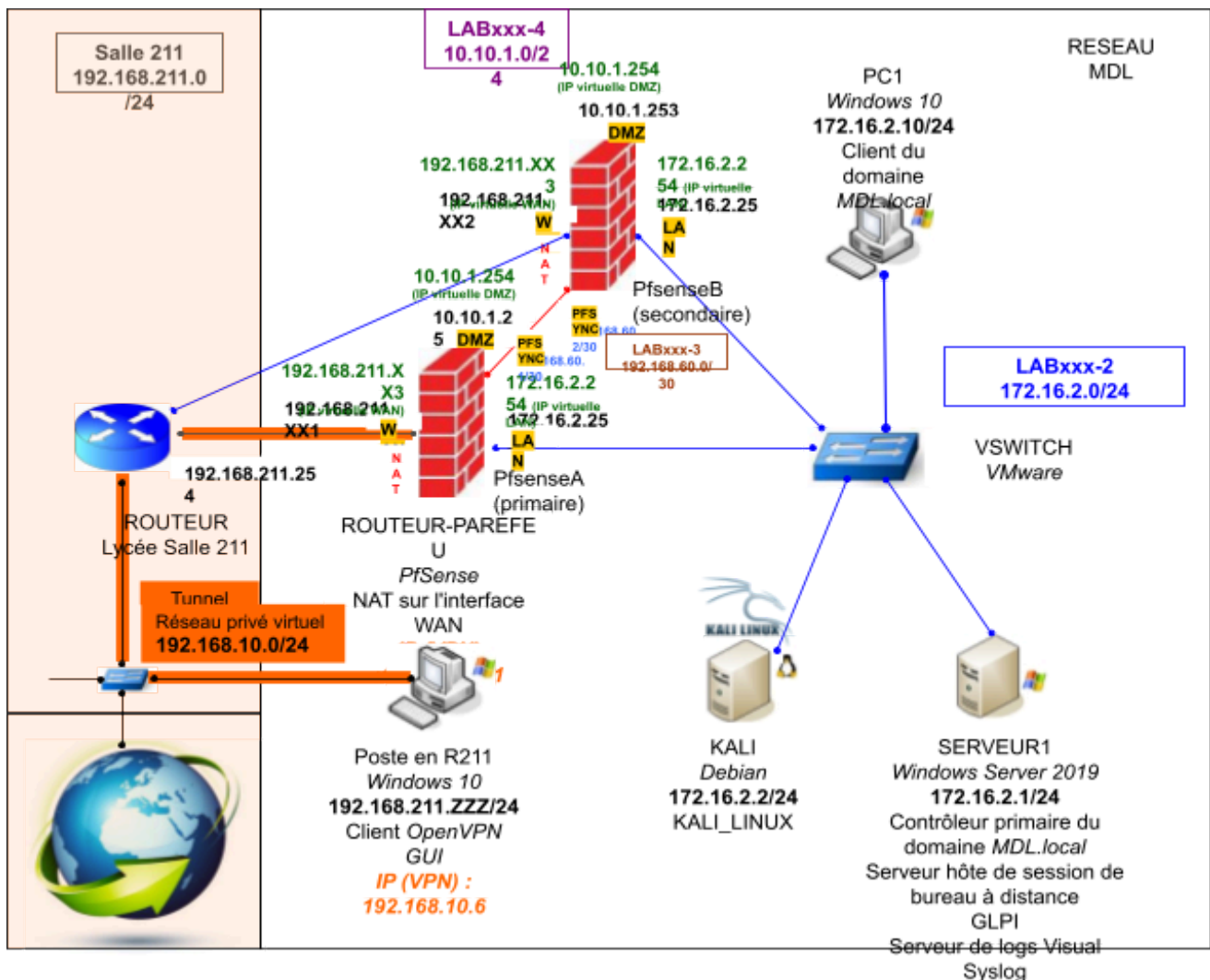


Schéma de notre réseau :



- Mission 1 : Installation du routeur-pare-feu PfSense
- Mission 2 : Installation du serveur de domaine
- Mission 3 : Inventaire du matériel avec GLPI/FusionInventory
- Mission 4 : Installation d'un VPN
- Mission 5 : Installation d'un serveur hôte de session Bureau à distance
- Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

Mission 1 : Installation du routeur-pare-feu PfSense

- Créer une nouvelle machine virtuelle sous VMware, de nom :

XX-MDL-PfSense

- Vérifier que la machine virtuelle Pfsense dispose de 4 cartes réseau machine :

> Adaptateur réseau 1	SALLE - 211 (déconnecté)
> Adaptateur réseau 2	LAB-SISR-11-2 (déconnecté)
> Adaptateur réseau 3	LAB-SISR-11-4 (déconnecté)
> Adaptateur réseau 4	LAB-SISR-11-5 (déconnecté)

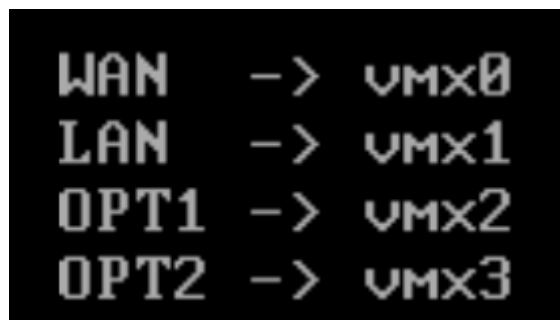
- Assigner les interfaces du Pfsense (fonction 1 : Assign Interfaces)

WAN : vmx0

LAN : vmx1

OPT1 : vmx2

OPT2 : vmx3



```
WAN -> vmx0
LAN -> vmx1
OPT1 -> vmx2
OPT2 -> vmx3
```

- Attribuer des adresses IP aux interfaces du Pfsense (fonction 2 : Set Interface(s))

(ne pas oublier de spécifier la passerelle nécessaire pour chaque interface).

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

WAN (wan)	-> vmx0	-> v4: 192.168.211.236/24
LAN (lan)	-> vmx1	-> v4: 172.16.2.254/24
OPT1 (opt1)	-> vmx2	-> v4: 10.10.1.254/24
OPT2 (opt2)	-> vmx3	->


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



> Adaptateur réseau 1	LAB-SISR-11-2 (connecté)
> Adaptateur réseau 2	LAB-SISR-11-4 (connecté)
> Adaptateur réseau 3	LAB-SISR-11-5 (connecté)
> Adaptateur réseau 4	SALLE - 211 (connecté)

Mission 2 : Installation du serveur de domaine

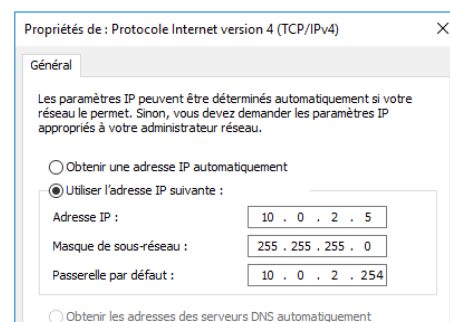
Windows Server 2019 est normalement déjà installé sur le poste.

- Démarrer la machine *Windows Server 2019*.
- Ouvrir une session avec l'utilisateur *Administrateur* et le mot de passe *Windows2019*

Après installation, un nouvel écran apparaît : le gestionnaire de serveur . Celui-ci permet d'effectuer les principales opérations de configuration d'un serveur :


- Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration  / Réseau et Internet / Centre Réseau et partage (ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage) ;


cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :



cocher la case *Utiliser l'adresse IP suivante* :

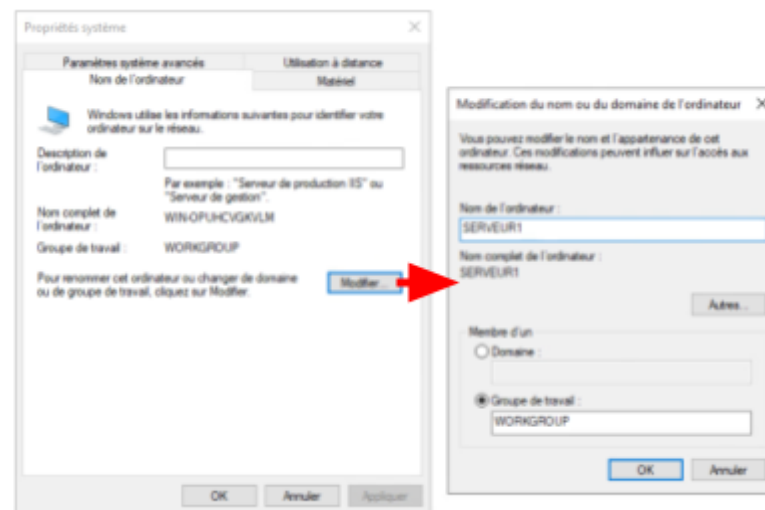
Adresse IP : 10.0.2.5
Masque de réseau : (à déterminer)
Passerelle : (à déterminer)
DNS : 10.0.2.5 (c'est-à-dire lui-même)

- d. Modifier le nom de cette machine (Panneau de configuration  / Système et sécurité, Système, lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Nom de l'ordinateur, puis le bouton Modifier)

(ou Paramètres  / Système / Informations système / Renommer le PC) :


Nom de l'ordinateur : *SERVEUR1*


- e. Laisser redémarrer le serveur.



Nous allons configurer le serveur *SERVEUR1* pour qu'il soit contrôleur d'un domaine *DOMAINE2019*.

Nous allons d'abord ajouter le rôle de serveur de domaine au serveur :

- a. Dans le tableau de bord *Gestionnaire de serveur* (cliquer sur  s'il n'est pas déjà ouvert), sélectionner *Gérer*, puis le lien *Ajouter des rôles et fonctionnalités*.
- b. Dans la fenêtre *Assistant Ajout de rôles et de fonctionnalités*, choisir une *Installation basée sur un rôle ou une fonctionnalité*.
- c. Sélectionner le serveur de destination sur lequel sera installé le rôle : *SERVEUR1*.
- d. Dans la liste des rôles, cocher le rôle *Services AD DS* (qui signifie *Services Active Directory Domain Services*), puis ajouter les fonctionnalités requises proposées par défaut pour ce rôle ;
cocher aussi le rôle *Serveur DNS*.
- e. Ne pas sélectionner d'autres fonctionnalités.
- f. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* (si un redémarrage est nécessaire, le serveur redémarrera automatiquement), puis confirmer l'autorisation de redémarrage automatique.
- g. Confirmer l'installation de ce rôle en cliquant sur *Installer*.

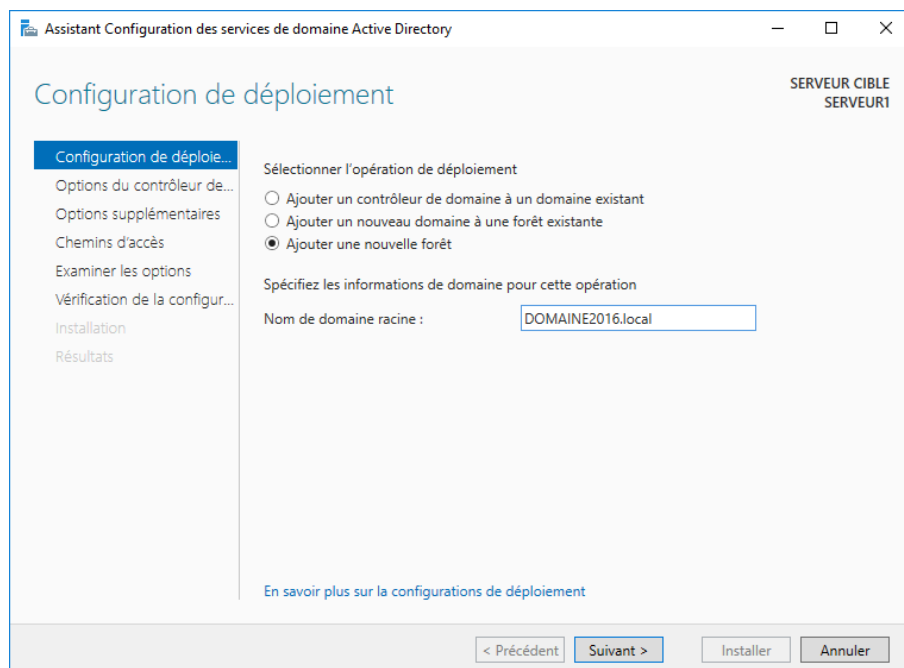
Pour faire de cette machine Windows Server 2019 un contrôleur de domaine, il faut ensuite utiliser l'icône d'avertissement représentée par le triangle jaune (Notifications)  qui apparaît dans la fenêtre *Gestionnaire de serveur* :



Avant cela, dans un vrai réseau physique, Il faudrait s'assurer que le câble Ethernet est branché entre la carte réseau du serveur et le commutateur.

h. Cliquer sur l'icône d'avertissement représentée par le triangle jaune (Notifications), puis sur le lien Promouvoir ce serveur en contrôleur de domaine :

- Ajouter une nouvelle forêt
- Nom de domaine racine : **DOMAINE2019.local**



- Choisir le niveau fonctionnel de la forêt et du domaine : *Windows Server 2016*
- Cocher les cases
 - Serveur DNS* pour installer le service Serveur DNS sur ce contrôleur de domaine
 - Catalogue global* (annuaire central regroupant des éléments de tous les domaines de la forêt)
- Entrer à nouveau le mot de passe administrateur : *Windows2019*
- Ne pas tenir compte du message "Il est impossible de créer une délégation pour ce serveur DNS, ..."
- Nom de domaine NetBIOS : **DOMAINE2019**


- Accepter les noms de dossiers proposés pour la base de données, les fichiers journaux, et le dossier SYSVOL
 - Cliquer sur *Installer* lorsque la configuration requise a bien été validée.
- i. Laisser redémarrer la machine ; ouvrir une session avec l'utilisateur *DOMAINE2019\Administrateur* (ou plus simplement *Administrateur*) et le mot de passe *Windows2019*.

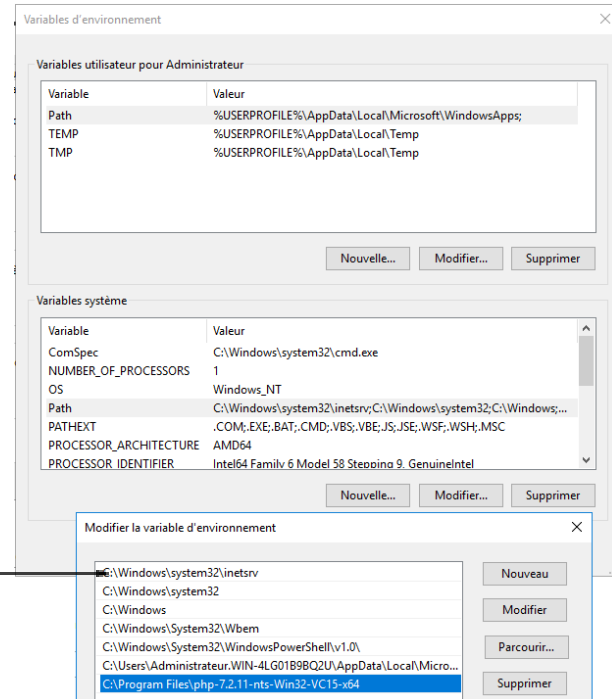
Mission 3 : Inventaire du matériel avec GLPI/FusionInventory

Etapes à suivre :

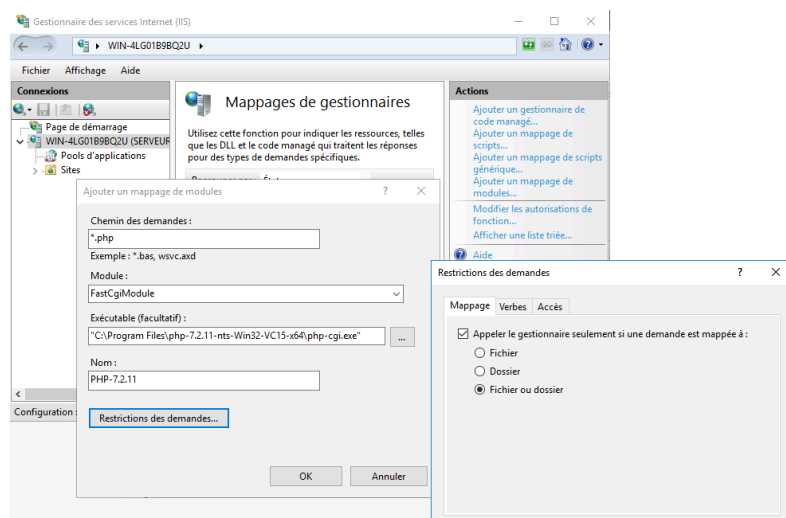
a. Installer le rôle *Serveur web IIS* avec les services de rôle par défaut et le service de rôle *CGI*.

b. 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* (en Français *Programmes*) ;
- 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* ; cliquer 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* :



DONMEZ
Okan
SIO2

[Documentation Projet MDL](#)

C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\php-cgi.exe

Nom : entrer un nom pour le
 mappage : *php-7.2.11*

cliquer 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*.

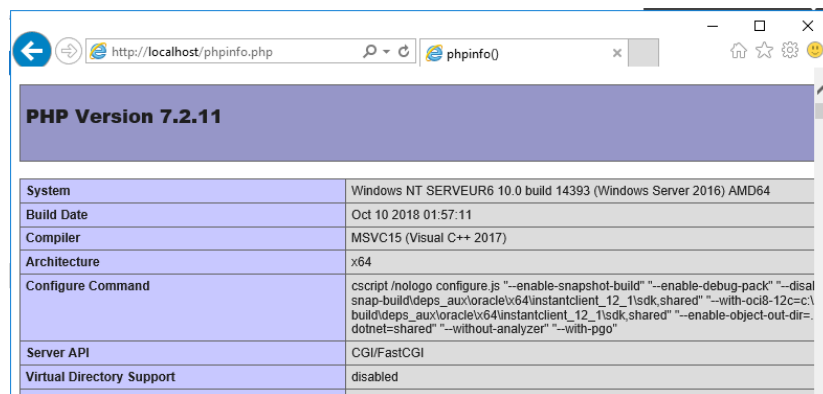
- Installer le package redistribuable Microsoft Visual C++ *vc_redist.x64-2015.exe* (c'est bien la version 2015 pour systèmes 64 bits qui est nécessaire ici) ;
- Pour vérifier l'installation de PHP, créer le fichier suivant avec le bloc-notes :

```
<?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 :



PHP Version 7.2.11	
System	Windows NT SERVEUR6 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Oct 10 2018 01:57:11
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "noloco configure.js --enable-snapshot-build --enable-debug-pack --disable-snap-build-deps_aux\oracle\64\instantclient_12_1\jdk.shared" --with-oci8-12c=c:\build\deps_aux\oracle\64\instantclient_12_1\jdk.shared --enable-object-out-dir=dotnet=shared --without-analyzer --with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled

- Installer *PHPManager* version 1.5, qui fonctionne bien avec IIS version 10, avec le .msi fourni.
- Redémarrer le serveur (indispensable pour que le programme PHP Manager apparaisse dans la liste des fonctionnalités de IIS).
- Lancer PHP Manager, puis enregistrer PHP dans IIS (*Enregistrer une nouvelle version de PHP*), puis vérifier que PHP est bien fonctionnel (*Vérifier phpinfo()*) ; si cette dernière vérification ne fonctionne pas, c'est sans doute que la version installée du package redistribuable Microsoft Visual C++ *n'est pas la bonne* !

Les trois sous-étapes suivantes permettent d'installer et d'utiliser Wincache, sensé améliorer les performances du PHP. Elles ne sont absolument pas indispensables dans le cadre de ce TP.

- Copier la dernière version du dossier de l'extension WinCache pour PHP fourni (*wincache-2.0.0.8-dev-7.2.beta2-nts-vc15-x64*) dans le sous-dossier *ext* du dossier PHP, c'est à dire *C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\ext* (en fait, seul le fichier *php_wincache.dll* sera utilisé) ;
- Avec le bloc-notes, modifier le fichier **php.ini** et ajouter la ligne suivante à la fin du fichier :

extension = php_wincache.dll
- Si besoin, modifier les directives suivantes dans *php.ini* :

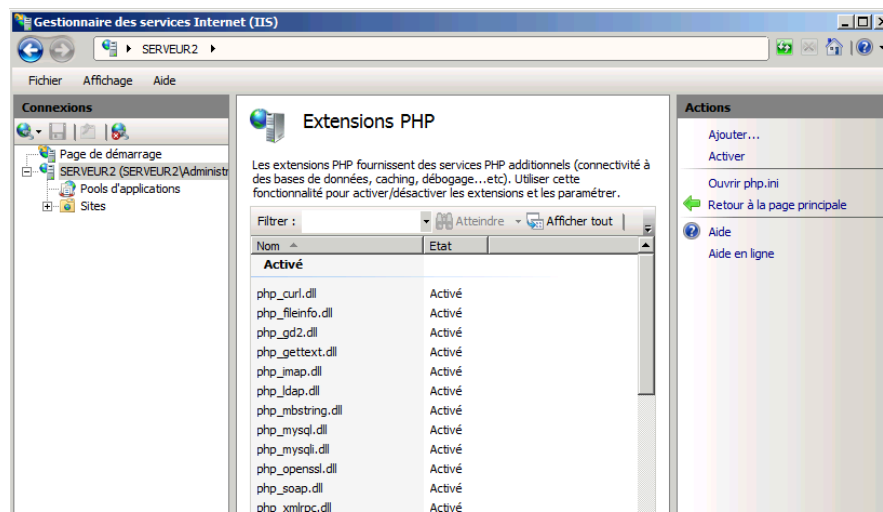
```
php.ini - Bloc-notes
Fichier Edition Format Affichage ?

[opcache]
; Determines if Zend OPcache is enabled
opcache.enable=0n

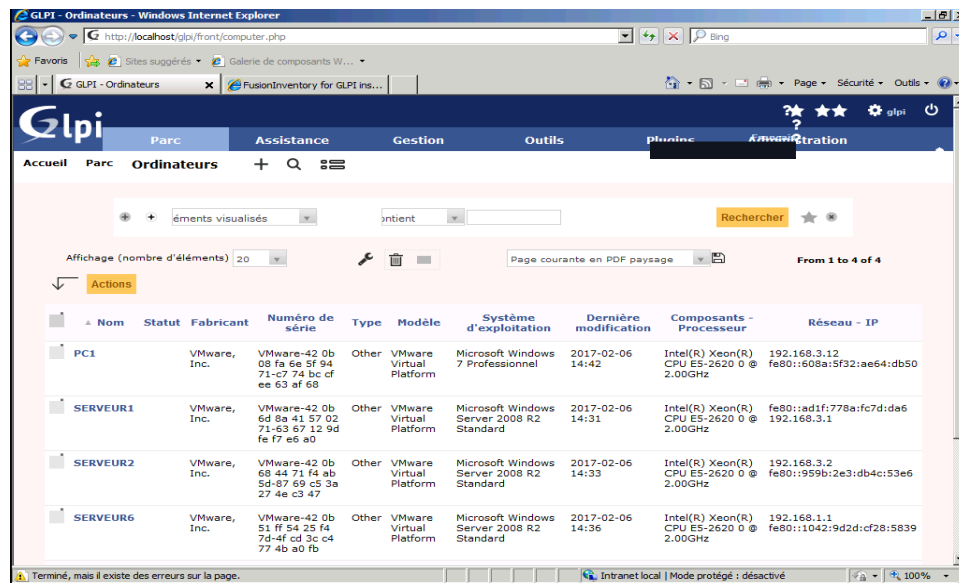
; Determines if Zend OPcache is enabled for the CLI version of PHP
opcache.enable_cli=0n
```

c. Installer le SGBD *Mysql* :

1. 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 (inutile sous Windows 2012 ou 2016).
2. Installer la version *MySQL Community Server* (installer le serveur uniquement (et non tout le package)).
3. Si besoin, installer *PHPMyAdmin* (qui nécessite PHP déjà installé).



- d. Dans PHP Manager, activer les extensions suivantes (utilisées par GLPI) :
- ***php_fileinfo.dll***
 - ***php_ldap.dll***
 - ***php_imap.dll***
 - ***php_mysqli.dll***
- (utiliser le lien *Activer ou désactiver une extension*, puis cliquer sur l'extension à activer, et enfin cliquer sur le lien *Activer* ; on peut aussi ouvrir directement le fichier *php.ini*, et supprimer le commentaire ; devant l'extension voulue).
- e. Installer GLPI :
1. copier le dossier *glpi* dans *inetpub\wwwroot*
 2. Dans l'explorateur Windows, attribuer l'autorisation *Modification* à *Utilisateurs* pour le dossier *C:\inetpub\wwwroot\glpi*
 3. sous IIS, si besoin, créer le site web sous le nom *glpi* avec le nom d'hôte *www.glpi.fr*
- f. Pour la première connexion à GLPI, suivre les indications.
- g. Installer le plugin FusionInventory :
1. copier le dossier *fusionInventory* dans *inetpub\wwwroot\glpi\plugins*
 2. Dans GLPI, sélectionner la commande Configuration / Plugins ; dans la ligne du plugin FusionInventory, cliquer sur le lien *Installer*, puis ensuite sur le lien *Activer* ;
 3. 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/
- h. Déployer l'agent FusionInventory Windows (en tant que service 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.
- i. 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 (on peut cliquer sur une machine et consulter l'historique de ses remontées, et éventuellement la restaurer si besoin !).



Importation dans GLPI des utilisateurs de l'annuaire LDAP (Active Directory) de GSB

Configurer cette importation qui sera faite périodiquement sur demande par l'administrateur de GLPI.

Tutoriel pour la première connexion à GLPI

Pour la première connexion à GLPI, procéder comme suit :

- Rentrer sous l'interface web de GLPI avec le navigateur, à l'adresse <http://localhost/glpi>
- Après avoir sélectionné la langue *Français*, configurer la connexion à la base de données :

Serveur Mysql: *localhost*
Utilisateur Mysql : *root*
Mot de passe Mysql : *root*

- Créer ensuite une nouvelle base de données de nom *glpi*
- Après avoir noté les identifiants et mots de passe, on peut maintenant utiliser GLPI et entrer dans le système avec l'identifiant *glpi* et le mot de passe *glpi*
- Modifier immédiatement les mots de passe de ces quatre utilisateurs (*glpi*, *post-only*, *tech* et *normal*) en leur donnant à tous le même : **Windows2016**

DONMEZ
Okan
SIO2

Documentation Projet MDL

GLPI - Utilisateurs - Windows Internet Explorer

http://localhost/glpi/front/user.php

GLPI - Utilisateurs

Parc Assistance Gestion Outils Plugins Administration Configuration

Utilisateurs Groupes Entités Règles Dictionnaires Profils File d'attente des courriels Maintenance Journaux

Accueil > Administration > **Utilisateurs**

Ajouter utilisateur...

Éléments visualisés: 20

contient

Rechercher

Affichage (nombre d'éléments): 20

Page courante en PDF paysage

De 1 à 5 sur 5

Actions	Identifiant	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
<input type="checkbox"/>	glpi					Oui
<input type="checkbox"/>	normal					Oui
<input type="checkbox"/>	Plugin_FusionInventory					Oui
<input type="checkbox"/>	post-only					Oui
<input type="checkbox"/>	tech					Oui

Affichage (nombre d'éléments): 20

De 1 à 5 sur 5

- f. Vérifier et valider la liste des informations devant apparaître pour chaque matériel (Informations générales) :

Tous <input type="button" value="Oui"/>					
Informations générales		Composants		Informations administratives OC SNG	
Nom	<input type="button" value="Oui"/>	Processeur	<input type="button" value="Oui"/>	Numéro d'inventaire	<input type="button" value="HARDWARE_ID"/>
Système d'exploitation	<input type="button" value="Oui"/>	Mémoire	<input type="button" value="Oui"/>	Lieu	<input type="button" value="fields_4"/>
Numéro de série du système d'exploitation	<input type="button" value="Oui"/>	Disque dur	<input type="button" value="Oui"/>	Groupe	<input type="button" value="Pas d'import"/>
Numéro de série	<input type="button" value="Oui"/>	Carte réseau	<input type="button" value="Oui"/>	Usager numéro	<input type="button" value="Pas d'import"/>
Modèle	<input type="button" value="Oui"/>	Carte graphique	<input type="button" value="Oui"/>	Réseau	<input type="button" value="Pas d'import"/>
Fabricant	<input type="button" value="Oui"/>	Carte son	<input type="button" value="Oui"/>		
Type	<input type="button" value="Oui"/>	Lecteurs	<input type="button" value="Oui"/>		
Domaine	<input type="button" value="Oui"/>	Modems	<input type="button" value="Oui"/>		
Usager	<input type="button" value="Oui"/>	Ports	<input type="button" value="Oui"/>		
Commentaires	<input type="button" value="Oui"/>				
IP	<input type="button" value="Oui"/>				
UUID	<input type="button" value="Oui"/>				
Moniteurs					
Commentaires	<input type="button" value="Oui"/>				

Tutoriel d'importation dans GLPI des utilisateurs d'un annuaire LDAP

Au lieu de créer les utilisateurs un par un dans GLPI, nous allons importer ceux déjà créés dans l'Active Directory du domaine Windows 2016 (Active Directory est en effet un annuaire LDAP).

- Dans le fichier *php.ini*, penser à supprimer le commentaire ; devant *extension=php_ldap.dll* (le module LDAP pour PHP sera ainsi installé) ; de même, penser à supprimer le commentaire ; devant *extension=php_imap.dll* (le protocole de messagerie IMAP sera ainsi installé).
- Dans GLPI, configurer le serveur LDAP à atteindre (*Configuration / Authentification* puis lien *Annuaire LDAP*) (ajouter un nouvel annuaire en cliquant sur le bouton “+” situé dans la barre de menu) :

Nom (du serveur LDAP) :	<i>SERVEUR1</i>
Serveur par défaut :	<i>Oui</i>
Actif :	<i>Oui</i>
Serveur (adresse IP) :	<i>192.168.3.1</i>
Port :	<i>389</i>
Filtre de connexion :	

(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Basedn : *CN=Users,DC=GSB,DC=local*

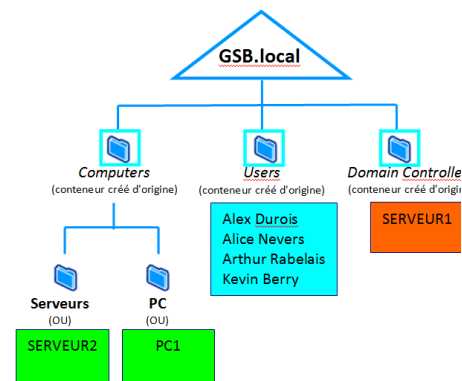
DN du compte :
CN=Administrateur,CN=Users,DC=GSB,DC=local

Mot de passe du compte : *Windows2016*

Champ de l'identifiant : *samaccountname*

Remarques :

- le *filtre de connexion* pour Windows est toujours celui donné ci-dessus.
- *Basedn* est le chemin du conteneur (ou éventuellement de l'OU) dans lequel sont stockés les utilisateurs de l'Active Directory.
- *DN du compte* est le nom du compte Active Directory qui permettra de se connecter à l'AD (ici, l'administrateur).



DONMEZ
Okan
SIO2

Documentation Projet MDL

GLPI - Annuaire LDAP - Windows Internet Explorer

http://localhost/glpi/front/authldap.form.php?id=1

GLPI - Annuaire LDAP

Parc Assistance Gestion Outils Plugins Administration Configuration

Configuration > Authentification > Annuaire LDAP

Annuaire LDAP - SERVEUR1 - ID 1

Annuaire LDAP

Tester

Utilisateurs

Groupes

Informations avanc...

Réplicats

Historique (3)

Tous

Annuaire LDAP - ID 1

Nom: SERVEUR1 Dernière modification: 2015-06-25 17:2

Serveur par défaut: Oui Actif: Oui

Serveur: 192.168.3.1 Port (par défaut 389): 389

Filtre de connexion: (&(objectClass=user)(objectCategory=person)(/userAccountControl:1.2.840.113556.1.4.803:=...

BaseDN: CN=Users,DC=GSB,DC=local

DN du compte (pour les connexions non anonymes): CN=Administrateur,CN=Users,DC=GSB,DC=local

Mot de passe du compte (pour les connexions non anonymes): [] Effacer Champ de l'identifiant: samaccountname

Commentaires

Sauvegarder

Supprimer

- c. Sauvegarder la configuration de ce serveur LDAP (bouton *Sauvegarder*), et tester la connexion à ce serveur (bouton *Tester*).

- d. Importer les utilisateurs de ce serveur LDAP (*Administration / Utilisateurs* puis bouton *Liaison annuaire LDAP* puis lien *Importation de nouveaux utilisateurs* puis bouton *Rechercher* ; cocher tous les utilisateurs puis dans *Actions*, sélectionner *Importer* ; valider avec *Envoyer*) :

Importation de nouveaux utilisateurs Mode expert

Activer le filtrage par date

Critère de recherche pour les utilisateurs

Identifiant Courriel

Nom de famille Prénom

Téléphone

Rechercher

Affichage (nombre d'éléments) 20 De 1 à 4 sur 4

Actions

Utilisateurs	Dernière mise à jour dans l'annuaire LDAP
<input type="checkbox"/> kberry	2013-07-21 14:26
<input type="checkbox"/> arabelais	2013-07-21 23:50
<input type="checkbox"/> anevers	2013-08-19 18:46
<input type="checkbox"/> adurois	2013-07-21 15:40

Actions

Affichage (nombre d'éléments) 20 De 1 à 4 sur 4

- e. Vérifier que les utilisateurs ont bien été importés (*Administration / Utilisateurs*) :

Ajouter utilisateur... Depuis une source externe Liaison annuaire LDAP

Éléments visualisés contient Rechercher

Affichage (nombre d'éléments) 20 Page courante en PDF paysage De 1 à 9 sur 9

Actions

Identifiant	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
<input type="checkbox"/> adurois	Durois				Oui
<input type="checkbox"/> anevers	Nevers				Oui
<input type="checkbox"/> arabelais	Rabelais				Oui
<input type="checkbox"/> glpi					Oui
<input type="checkbox"/> kberry	Berry				Oui
<input type="checkbox"/> normal					Oui
<input type="checkbox"/> Plugin_FusionInventory					Oui
<input type="checkbox"/> post-only					Oui
<input type="checkbox"/> tech					Oui

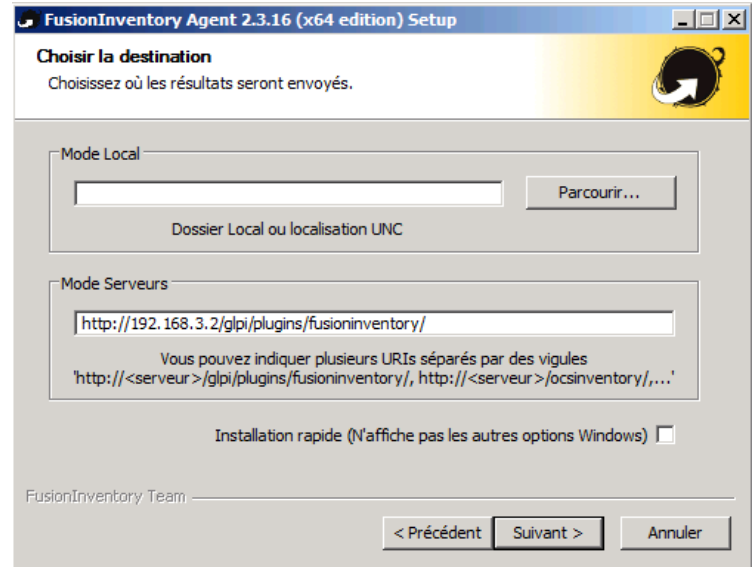
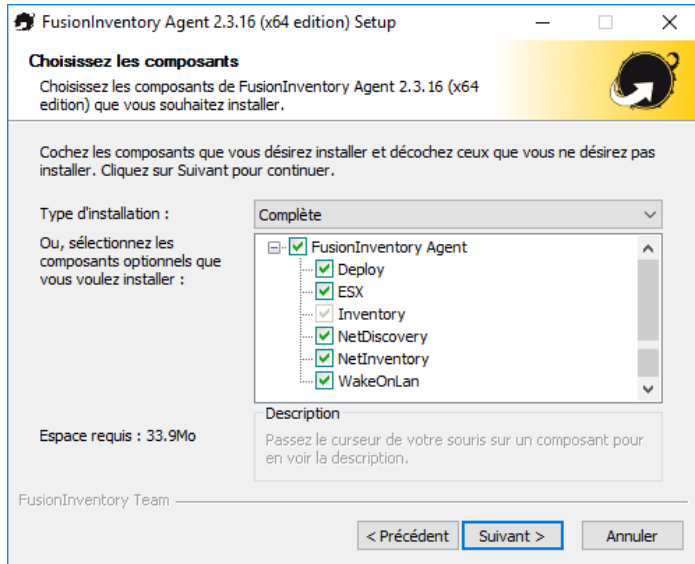
Actions

Cf documentation complète sur le site de GLPI :
<http://www.glpi-project.org/wiki/doku.php?id=fr:config:ldap>

Installation et exécution de l'agent FusionInventory sous Windows

Installation manuelle de l'agent

(toujours choisir le type d'installation **Complète**) :



Installation de l'agent par GPO :

(GPO *Configuration Ordinateur Stratégie Paramètres Windows* pour lancer automatiquement un script .bat permettant d'installer l'agent au démarrage de la machine)

Utiliser les options d'installation en ligne de commande suivantes :

/acceptlicense

Accepter par l'utilisateur les conditions d'utilisation de la licence de l'agent FusionInventory

/execmode=mode

Fixer le mode d'exécution de l'agent (en mode *Service*, l'agent s'exécutera en tant que service Windows ; en mode *Task*, l'agent s'exécutera en tant que tâche Windows)

/runnow

Lancer l'exécution de l'agent immédiatement après l'installation

/server=URI[,URI[...]]

Renvoyer les résultats de l'exécution de l'agent au serveur spécifié (ici : <http://192.168.3.2/glipi/plugins/fusioninventory/>)

/S

Exécuter l'installation de l'agent en mode silencieux

Sur chaque poste, l'agent FusionInventory doit ainsi être installé.

Exécution de l'agent **sur chaque poste du réseau** afin de remonter les données de chaque machine automatiquement vers le serveur.



Mission 4 : Installation d'un VPN

Création d'une autorité de certification CA_Acces_VPN sur le routeur-parefeu PfSense avec son certificat ; création du certificat du serveur OpenVPN

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

The screenshot shows the PfSense web interface for the 'System / Certificate Manager / CAs / Edit' page. The 'Create / Edit CA' section is active, showing fields for 'Descriptive name' (CA_Acces_VPN), 'Method' (Create an internal Certificate Authority), 'Trust Store' (unchecked), and 'Randomize Serial' (unchecked). Below this is the 'Internal Certificate Authority' section with fields for 'Key type' (RSA), 'Key length' (2048), 'Digest Algorithm' (sha256), 'Lifetime (days)' (3650), 'Common Name' (CA_Acces_VPN), and optional subject components like 'Country Code' (FR), 'State or Province' (test), 'City' (test), 'Organization' (test), and 'Organizational Unit' (e.g. My Department Name (optional)). A 'Save' button is at the bottom.

System / Certificate Manager / CAs / Edit	
CAs Certificates Certificate Revocation	
Create / Edit CA	
Descriptive name	CA_Acces_VPN
Method	Create an internal Certificate Authority
Trust Store	<input type="checkbox"/> 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	<input type="checkbox"/> 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	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	CA_Acces_VPN
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)
Save	

- c. 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

CAs

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



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

- a. Sur le poste SERVEUR1, créer l'utilisateur suivant dans l'Active Directory du domaine GSB (décocher la case «L'utilisateur doit changer le mot de passe ...» et cocher la case «Le mot de passe n'expire jamais») :

<i>Nom</i>	<i>Nom d'ouverture de session</i>	<i>Mot de passe</i>
User_VPN_LDAP	User_VPN_LDAP	<i>Windows2019</i>

Cet utilisateur *User_VPN_LDAP* permettra au firewall de s'authentifier sur l'Active Directory.

- b. 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 *GSB.local* :

System / User Manager / Authentication Servers / Edit

UsersGroupsSettingsAuthentication 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

(suite de la figure : page suivante)

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.

- c. 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 [4 hours] 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!

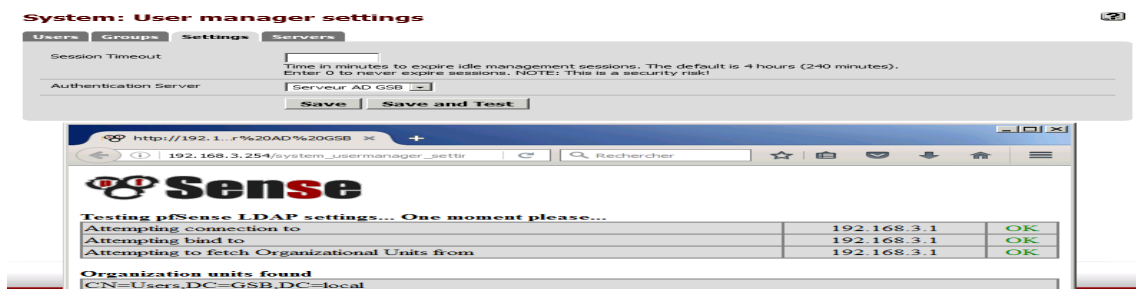
Authentication Server [Serveur AD GSB]

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 [30 seconds] 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.

Save Save & Test

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



- d. Configurer une nouvelle connexion VPN, de type *Remote Access (User Auth)* avec la commande VPN OpenVPN, dans l'onglet Wizards :

Type of Server :	<i>LDAP</i>
LDAP Servers :	<i>Serveur AD GSB</i>
Certificate Authority :	<i>CA_Access_VPN</i>
Certificate :	<i>Certificat_Acces_VPN</i>
Description :	<i>Serveur VPN avec authentication LDAP GSB</i>
Local Port :	<i>1195</i>

The screenshot shows the 'Server Setup' step of the 'OpenVPN Remote Access Server Setup Wizard'. The progress bar indicates 'Step 9 of 11'. The section is titled 'General OpenVPN Server Information' and contains the following fields:

Interface	<input type="text" value="WAN"/>	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="UDP on IPv4 only"/>	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="1195"/>	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	<input type="text" value="Serveur VPN avec authentication LDAP GSB"/>	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"/> Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key	<div></div> Paste in a shared TLS key if one has already been generated.
DH Parameters Length	<div>2048 bit</div> Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation	<input checked="" type="checkbox"/> Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	<div>AES-256-GCM AES-128-GCM CHACHA20-POLY1305</div> List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.
Fallback Data Encryption Algorithm	<div>AES-256-CBC (256 bit key, 128 bit block)</div> The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.
Auth Digest Algorithm	<div>SHA256 (256-bit)</div> The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	<div>No Hardware Crypto Acceleration</div> The hardware cryptographic accelerator to use for this VPN connection, if any.

Tunnel Settings	
Tunnel Network	<div>192.168.100.0/24</div> <p>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.</p>
Redirect Gateway	<div><input type="checkbox"/></div> <p>Force all client generated traffic through the tunnel.</p>
Local Network	<div>192.168.3.0/24</div> <p>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.</p>
Concurrent Connections	<div></div> <p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>
Allow Compression	<div>Refuse any non-stub compression (Most secure)</div> <p>Allow compression to be used with this VPN instance, which is potentially insecure.</p>
Compression	<div>Disable Compression [Omit Preference]</div> <p>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.</p>
Type-of-Service	<div><input type="checkbox"/></div> <p>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</p>
Inter-Client Communication	<div><input type="checkbox"/></div> <p>Allow communication between clients connected to this server.</p>
Duplicate Connections	<div><input type="checkbox"/></div> <p>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</p>

Client Settings

Dynamic IP

☒

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

Topology

Subnet – One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

DNS Default Domain

GSB.local

Provide a default domain name to clients.

DNS Server 1

192.168.3.1

DNS server IP to provide to connecting clients.

DNS Server 2

DNS server IP to provide to connecting clients.

NTP Server

Network Time Protocol server to provide to connecting clients.

NetBIOS Options

☐

Enable NetBIOS over TCP/IP.
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

NetBIOS Node Type

none

Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).

NetBIOS Scope ID

A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.

WINS Server 1

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

WINS Server 2

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

>> Next

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule

☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule

☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

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

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

The screenshot shows the Mikrotik WinBox interface for the 'Diagnostics / Authentication' section. At the top, there is a breadcrumb 'Diagnostics / Authentication'. Below it, a green message box states: 'User anevers authenticated successfully. This user is a member of groups:'. Underneath this is a section titled 'Authentication Test'. It contains three input fields: 'Authentication Server' (a dropdown menu currently showing 'Serveur AD GSB'), 'Username' (a text box containing 'anevers'), and 'Password' (a masked text box with 12 dots). Below these fields is a blue button with a key icon and the text '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

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.

Attention !

Dans certaines versions de Pfsense, il y a un bug qui ne permet pas d'utiliser plusieurs connexions VPN simultanément. Si une connexion VPN a déjà été configurée dans un autre TP (dans le TP 28, une connexion VPN utilisant le serveur d'authentification local Pfsense sur le port 1194 a été configurée), il faut la désactiver.

Si tel est le cas :

- e. Sélectionner la commande VPN OpenVPN Servers, puis modifier la connexion VPN utilisant le serveur d'authentification local Pfsense sur le port 1194 ; cocher la case *Désactivée* :

VPN / OpenVPN / Serveurs

Serveurs Clients Ré-écritures spécifiques au client Assistants Client Export Shared Key Export

Interface	Protocole / Port	Réseau tunnel	Chiffrement	Description	Actions
WAN	UDP / 1194	192.168.100.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	Serveur VPN local (tun)	
WAN	UDP / 1195	192.168.100.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	Serveur VPN avec aut LDAP GSB (tun)	

+ Ajouter

VPN / OpenVPN / Serveurs / Modifier

Serveurs Clients Ré-écritures spécifiques au client Assistants Client

Informations Générales

Désactivé ☒ Désactiver ce serveur
Définissez cette option pour désactiver ce serveur sans le r

Mode serveur Accès à distance (SSL/TLS + Authentification utilisateur)

Backend pour l'authentification Serveur AD GSB
Base de données locale

Seule la connexion VPN que l'on veut utiliser (ici celle utilisant le serveur d'authentification LDAP SERVEUR1 sur le port 1195) doit être active.

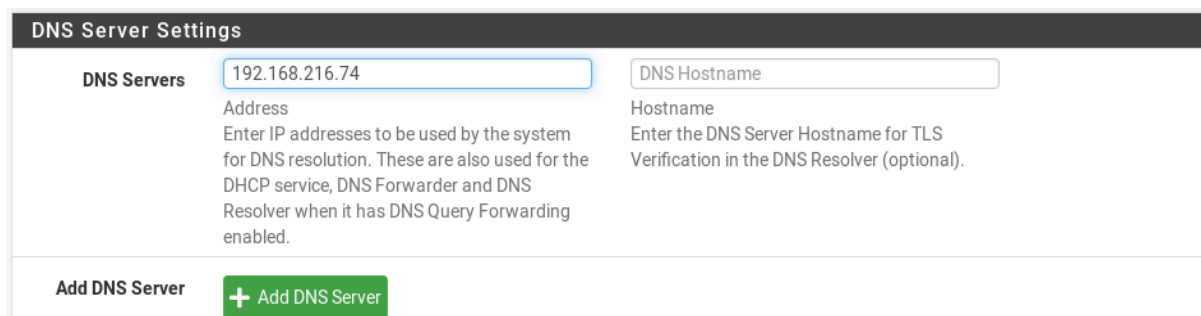
Exportation de la configuration du client depuis PfSense

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.



The screenshot shows the 'DNS Server Settings' interface. It has two input fields: 'DNS Servers' with the value '192.168.216.74' and 'DNS Hostname' which is empty. Below the 'DNS Servers' field, there is explanatory text: '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.' Below the 'DNS Hostname' field, there is explanatory text: 'Hostname: Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional)'. At the bottom left, there is a link 'Add DNS Server' and a green button with a plus sign and the text '+ 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 :

- 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 le type d'utilisateur *Authentication Only (No Cert)*, 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 (attention : sélectionner le bon serveur dans la zone *Remote Access Server*) :

OpenVPN / Client Export Utility

Server

Client

Client Specific Overrides

Wizards

Client Export

Shared Key Export

OpenVPN Server

Remote Access Server

Serveur VPN avec authentificat UDP4:1195

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	<div><div>- Inline Configurations:</div><div><div>Most Clients</div><div>Android</div></div><div><div>OpenVPN Connect (iOS/Android)</div></div><div><div>- Bundled Configurations:</div><div><div>Archive</div><div>Config File Only</div></div><div><div>- Current Windows Installer (2.5.2-lx01):</div><div><div>64-bit</div><div>32-bit</div></div><div><div>- Legacy Windows Installers (2.4.11-lx01):</div><div><div>10/2016/2019</div><div>7/8/8.1/2012r2</div></div><div><div>- Viscosity (Mac OS X and Windows):</div><div><div>Viscosity Bundle</div><div>Viscosity Inline Config</div></div></div></div></div></div></div>

DONMEZ




Okan

SIO2

Documentation Projet MDL

- 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 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.

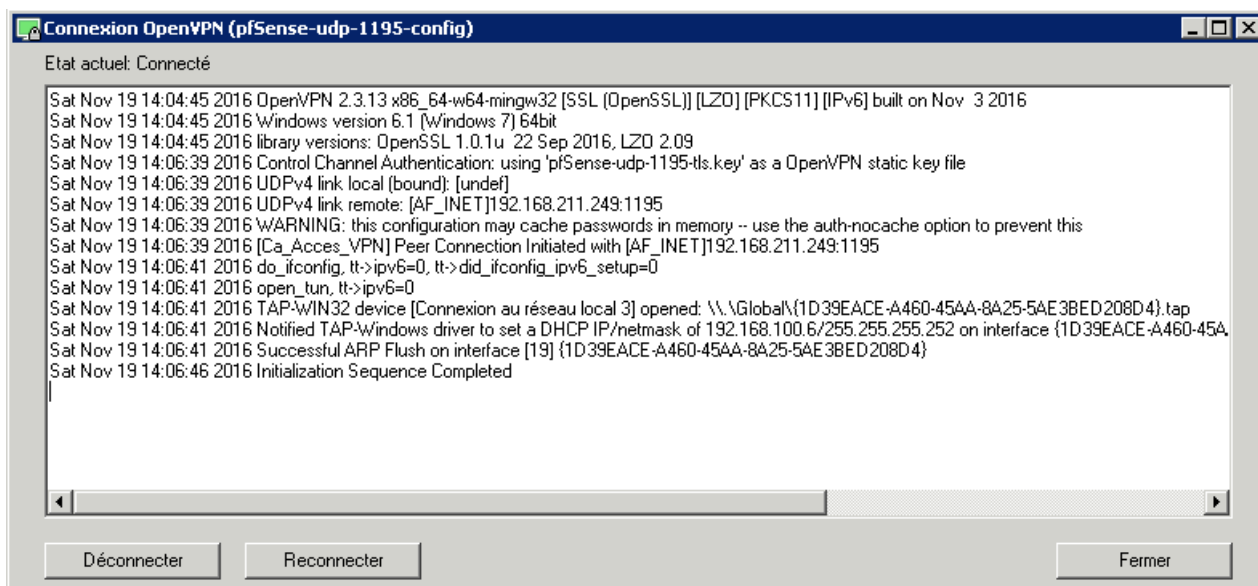
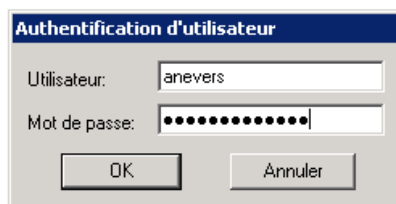
Nom ^	Modifié le	Type	Taille
 pfSense-udp-1195.ovpn	19/11/2016 13:41	Fichier OVPN	1 Ko
 pfSense-udp-1195-ca.crt	19/11/2016 13:41	Certificat de sécurité	2 Ko
 pfSense-udp-1195-tls.key	19/11/2016 13:41	Fichier KEY	1 Ko

Installation du client OpenVPN sur un poste client

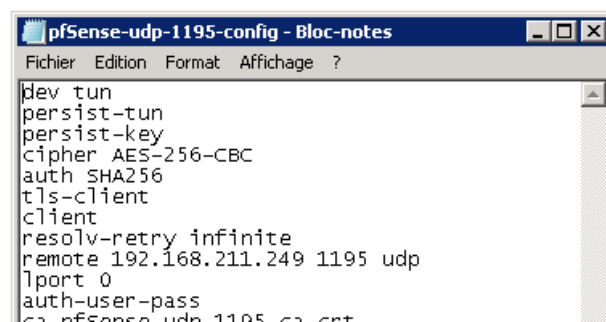
- a. Sur le poste client, télécharger le client OpenVPN depuis le site suivant (onglet *Community*, *Windows Installer 64 bits*) :

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

- b. Installer ce logiciel client sur le poste (installer aussi le logiciel *TAP-Windows Provider V9 Cartes réseau*).
- c. Recopier le fichier d'installation exécutable dans le dossier C:\Programmes\OpenVPN\Config (si la copie directe ne fonctionne pas, on pourra copier le fichier d'abord dans le dossier Documents du PC local, puis du dossier Documents vers C:\Programmes\OpenVPN\Config) puis exécuter ce fichier qui installera automatiquement les 3 fichiers de configuration dans le dossier.
- d. Cliquer-doit sur l'icône de l'application OpenVPN GUI et sélectionner la commande *Régler les problèmes de compatibilité*, puis le bouton *Essayer les paramètres recommandés* ; lancer ainsi l'application.
- e. L'application OpenVPN GUI devra ensuite toujours être lancée en mode administrateur.
- f. Se connecter avec l'utilisateur *anevers* et le mot de passe *Windows2019* :



Pour info, le fichier de configuration du client OpenVPN, de nom *pfSense-udp-1195-config.ovpn* doit avoir le contenu suivant :



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

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

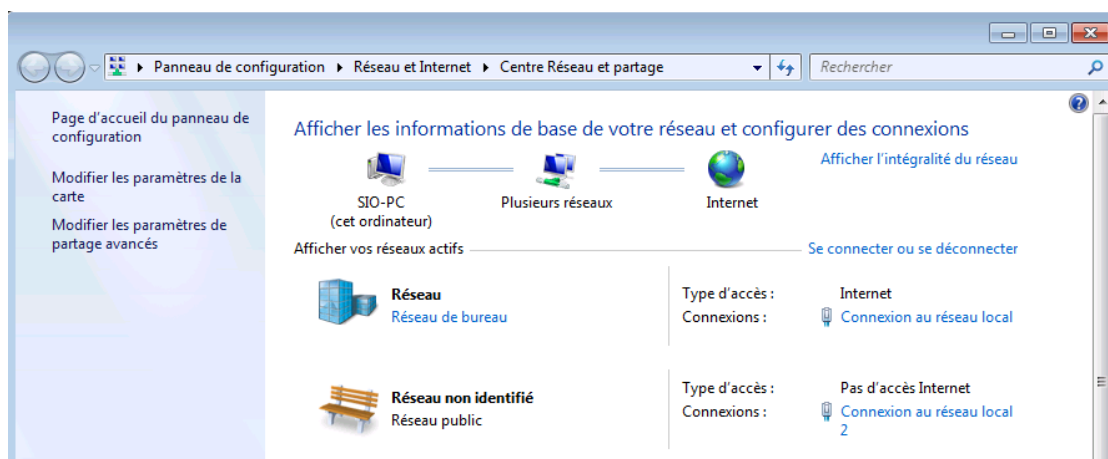
Configuration IP de Windows

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. . . . . : TAP-Windows Adapter V9
Adresse physique . . . . . : 00-FF-74-03-5A-EB
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::b14f:c9b7:a78f:ba9c%18<préféré>
>
Adresse IPv4. . . . . : 192.168.100.6<préféré>
Masque de sous-réseau. . . . . : 255.255.255.252
Bail obtenu. . . . . : lundi 29 juin 2015 07:49:29
Bail expirant. . . . . : mardi 28 juin 2016 07:49:28
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 192.168.100.5
IAID DHCPv6 . . . . . : 302055284
DUID de client DHCPv6. . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
Serveurs DNS. . . . . : 192.168.3.1
NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Connexion au réseau local :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Connexion réseau Intel(R) PRO/1000 M
T
Adresse physique . . . . . : 00-50-56-8B-7E-86
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::7cca:6333:3a1d:d2b3%11<préféré>
>
Adresse IPv4. . . . . : 192.168.1.50<préféré>
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.254
IAID DHCPv6 . . . . . : 234901590
DUID de client DHCPv6. . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
Serveurs DNS. . . . . : 192.168.216.74
NetBIOS sur Tcpip. . . . . : Activé
```

- h. Vérifier sur le serveur OpenVPN avec la commande Diagnostic OpenVPN, les connexions des clients en cours :



Status: OpenVPN



Serveur VPN avec aut LDAP GSB UDP:1195 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
anevers	192.168.1.50:56769	192.168.100.6	Sat Nov 19 12:59:28 2016	6 KB	6 KB

▶ Running



Serveur VPN avec aut LDAP GSB UDP:1195 Routing Table

Common Name	Real Address	Target Network	Last Used
anevers	192.168.1.50:56769	192.168.100.6	Sat Nov 19 13:00:02 2016

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

- i. 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".

pfsense.localdomain - Diagnostics: Execute command - Windows Internet Explorer


http://192.168.2.253/exec.php

pfsense.localdomain - Diagnostics: Execute command


System Interfaces Firewall Services VPN Status Diagnostics Help

```
$ 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
```

Execute Shell command

Command:  ifconfig

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

- a. Ouvrir le Gestionnaire de serveur (s'il n'est pas déjà ouvert) en cliquant sur le bouton  de la barre des tâches actives.
- b. Dans ce tableau de bord, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- c. 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*.
- d. Choisir le serveur *SERVEUR1* parmi le pool de serveurs sur lequel seront installés les services.
- e. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* puis cliquer sur *Déployer*.
- f. Laisser l'installation se faire et la machine redémarrer.

Remarque :

Si le message d'erreur suivant apparaît : *La communication à distance Powershell ne permet pas la connexion avec le serveur (Unable to connect to the server by using Windows PowerShell remoting)*, il faut lancer les deux commandes suivantes sous PowerShell en tant qu'Administrateur pour activer la gestion à distance et déployer RDS :

Get-service WinRM

Enable-PSRemoting

puis redémarrer la machine si nécessaire.

Voir aussi :

<https://hichamkadiri.wordpress.com/2015/03/15/how-to-fix-unable-to-connect-to-the-server-by-using-windows-powershell-remoting-rds-sur-microsoft-azure/>

<https://blog.adsl2meg.fr/administration-a-distance-dun-serveur-windows-server-2012-par-le-gestionnaire-de-serveur/>

Chaque utilisateur ou périphérique informatique qui se connecte à un serveur hôte de session Bureau à distance doit obtenir une licence d'accès client aux services Bureau à distance auprès d'un serveur de licences des services Bureau à distance (obligatoire depuis Windows 2008 R2).

Sur le serveur hôte de session bureau à distance, il faut donc spécifier le serveur de licences qui sera utilisé : ce sera le même SERVEUR1 dans notre cas

- g. Dans le Gestionnaire de serveur, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- h. Dans la fenêtre *Assistant Ajout des rôles*, choisir le type d'installation *Installation basée sur un rôle ou une fonctionnalité*.
- i. Choisir le serveur *SERVEUR1* parmi le pool de serveurs sur lequel seront installés les services.
- j. 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).
- k. Ajouter les fonctionnalités requises proposées.
- l. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* puis cliquer sur *Installer*.
- m. Laisser l'installation se terminer.

DONMEZ
Okan
SIO2

Documentation Projet MDL

Après avoir installé les rôles, il faut maintenant effectuer la configuration proprement dite des services Bureau à distance.

- n. Dans le Gestionnaire de serveur, sélectionner Services Bureau à distance.

Avec Windows Server, nous pouvons diffuser des applications qui peuvent être utilisées par des machines clientes. C'est le système «RemoteApp». Cette solution est incluse au service de Bureau à distance et permet de faire tourner des applications lourdes sur le serveur depuis des ordinateurs clients.

Les applications tournent sur le serveur et le client reçoit en réalité un «stream» de l'application. Ceci permet d'économiser de l'argent dans une entreprise en achetant un gros serveur et des clients légers pour les employés.

Les services Bureau à distance sont configurés au travers des collections. Une collection permet de déclarer des applications "Remote App" pour un serveur, et de définir les utilisateurs qui pourront les exécuter.

Une collection est déjà créée par défaut : *QuickSessionCollection* ; elle permet de déclarer les 3 applications Calculatrice, Paint, et WordPad comme applications RemoteApp exécutables sur SERVEUR1 et accessibles à tous les utilisateurs du domaine.

Nous allons soit créer une nouvelle collection, soit modifier la collection existante *QuickSessionCollection* pour permettre de déclarer l'application *Cisco Packet Tracer* comme application RemoteApp exécutable sur SERVEUR1 et accessible à tous les utilisateurs du domaine.

- o. Installer Packet Tracer sur le serveur SERVEUR1 (et non sur la station !).
- p. Dans le Gestionnaire de serveur de SERVEUR1, 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 *SERVEUR1* (rubrique *Serveurs hôtes*)
 - les utilisateurs autorisés à exécuter cette application sont *GSB\Utilisateurs du domaine* (rubrique *Propriétés*)
 - l'application Cisco Packet Tracer doit être ajoutée à la liste *Programmes RemoteApp* (cliquer sur le bouton *TÂCHES* 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

- Serveurs
- 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
SERVER01	Hôte de session Bureau à distance N/A	Vrai

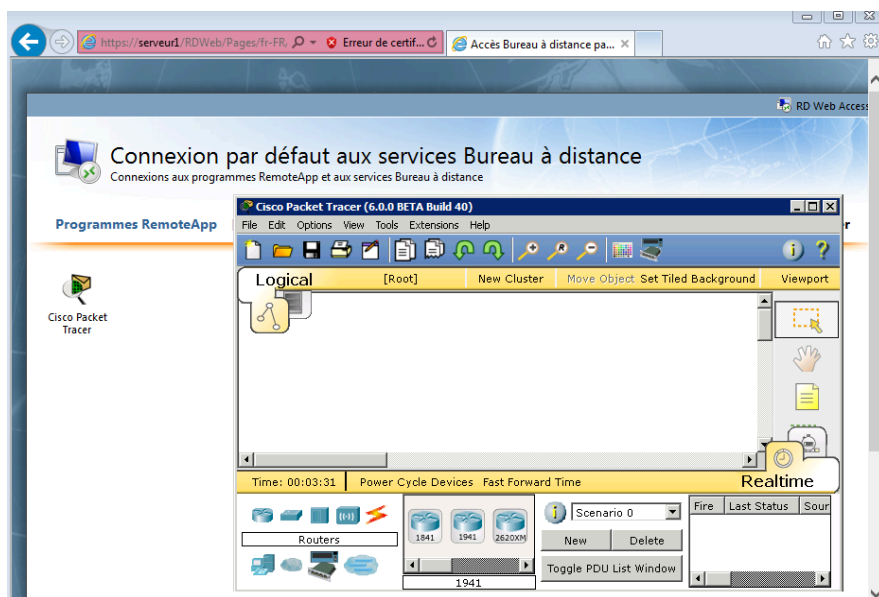
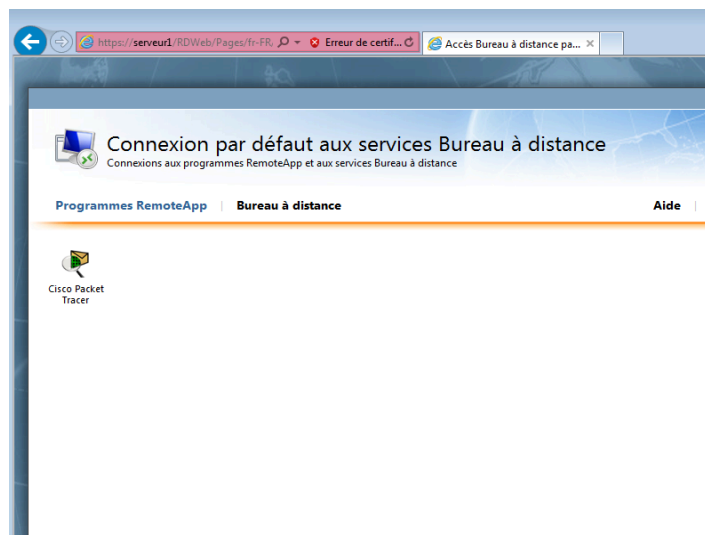
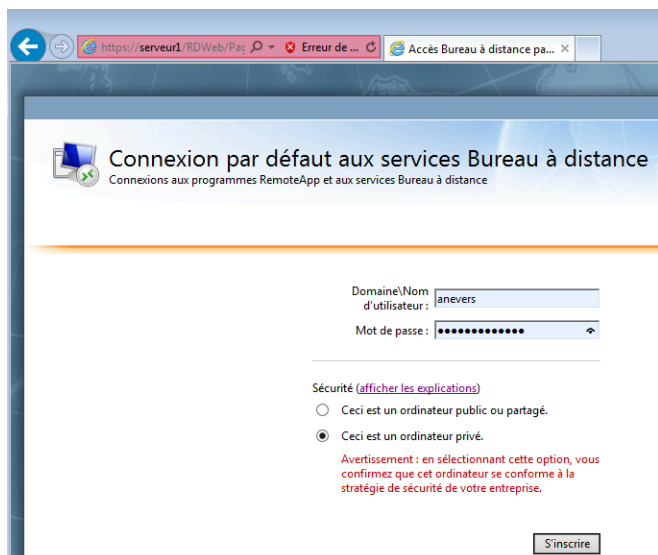
Annexe 2 : Ouverture d'une application RemoteApp (à distance) depuis PC1

Le service de rôle *Accès Bureau à distance par le Web*, installé sur SERVEUR1, permet aux utilisateurs d'accéder aux programmes RemoteApp et aux services Bureau à distance via un navigateur Web.

En effet, depuis Windows 2012, tous les utilisateurs désirant exécuter des applications RemoteApp doivent passer par le navigateur de leur poste, et se connecter au serveur hébergeant le service Broker (SERVEUR1) qui héberge aussi le service Accès Web.

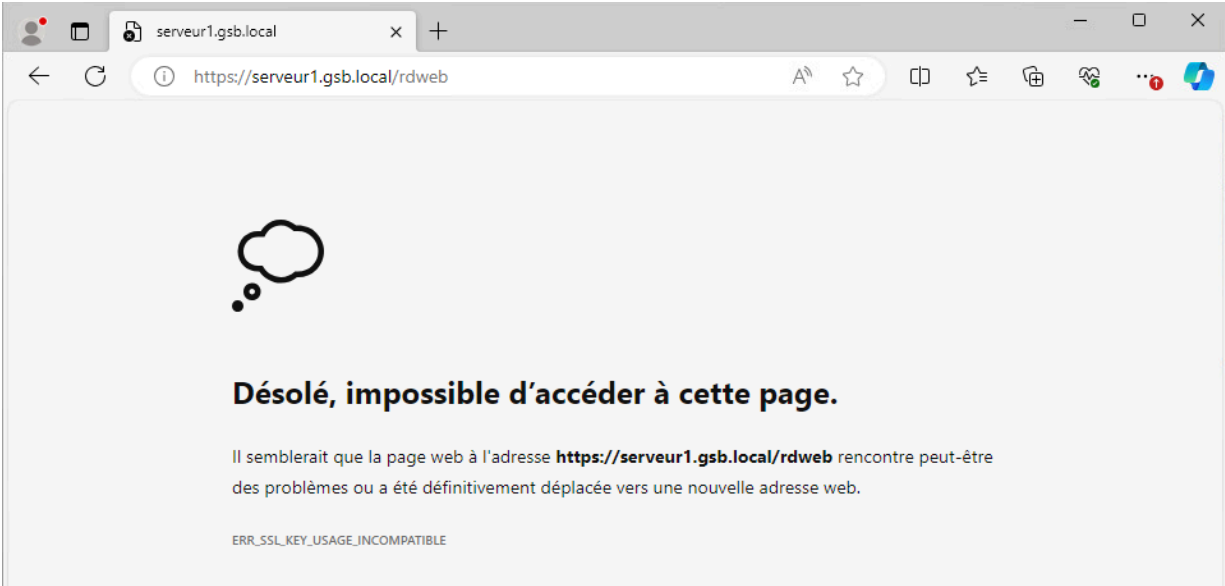
Nous allons maintenant tester l'*Accès Bureau à distance par le Web* :

- a. Démarrer la machine PC1 et ouvrir une session Windows avec l'utilisateur *anevers* et le mot de passe *Windows2022*
- a. Avec **le navigateur Internet Mozilla Firefox**, ouvrir la page ***https://SERVEUR1/rdweb*** ou ***https://SERVEUR1.GSB.local/rdweb*** ; après s'être authentifié (*GSB\anevers / Windows2022*), dans la liste des programmes RemoteApp proposés, cliquer sur Packet Tracer : le programme se lance dans une nouvelle fenêtre !



Attention :

Si on tente d'accéder aux programmes RemoteApp et aux services Bureau à distance via le navigateur Web *Edge* ou *Opéra*, on obtient le message d'erreur suivant : **ERR_SS_KEY_USAGE_INCOMPATIBLE** :



En effet, le certificat qui a été créé sur le serveur Web est un **certificat auto-signé** ; les navigateurs actuels tels que *Edge* ou *Opéra* refusent dorénavant l'accès aux sites Web https ayant un certificat auto-signé, ce qu'autorise encore Mozilla Firefox ...

On peut d'ailleurs voir ce certificat sur SERVEUR1 et vérifier qu'il est bien auto-signé :

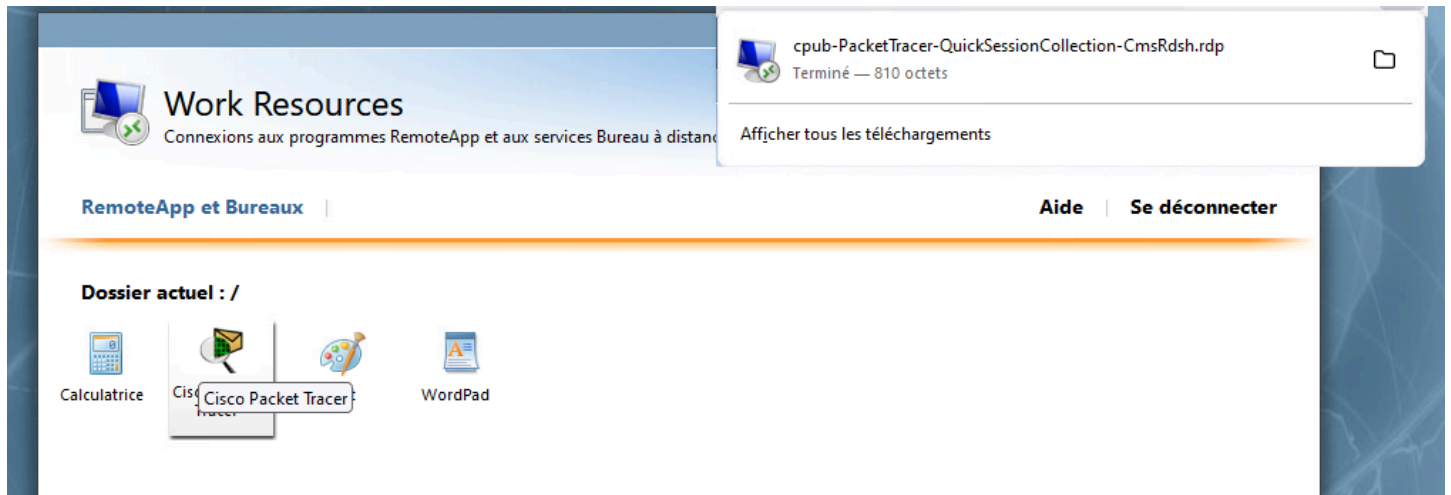
Certificat

SERVEUR1.GSB.local	
Nom du sujet	
Nom courant	SERVEUR1.GSB.local
Nom de l'émetteur	
Nom courant	SERVEUR1.GSB.local
Validité	
Pas avant	Tue, 12 Dec 2023 08:54:08 GMT
Pas après	Wed, 12 Jun 2024 08:54:08 GMT

Remarque :

Il est possible que, lorsqu'on clique sur une application distante (par exemple : Packet Tracer), le navigateur n'ouvre pas directement l'application correspondante, mais télécharge un fichier .rdp

Il suffit alors de cliquer sur ce fichier .rdp pour lancer l'application :



Un fichier RDP (Remote Desktop Protocol) contient les informations nécessaires à la connexion à un serveur de terminaux, y compris la configuration des options lors de la sauvegarde du fichier. Il est utilisé par les services de bureau à distance de Microsoft et les applications associées.

Un fichier RDP contient plusieurs paramètres, notamment l'adresse du serveur, le numéro de port, le nom d'utilisateur, le mot de passe, le domaine, la taille du bureau, le mode d'écran et plusieurs autres. Il est enregistré dans un format de texte brut pouvant être lu et modifié à l'aide d'un éditeur de texte (par exemple NotePad).

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

La première étape est donc de créer nos deux interfaces virtuelles, sur chacun de nos hôtes. Pour cela on se rend sur **Firewall** puis **Virtual IPs** puis **Add** :

Ici on choisi donc le type **CARP**, car nous avons aussi la possibilité d'utiliser l'IP Alias ou encore le Proxy ARP, mais ce n'est pas le cas ici. On choisi ensuite notre interface, **WAN** pour commencer, puis on renseigne donc notre adresse. Ensuite, on renseigne un mot de passe qui sera utilisé pour le groupe VHID. On vient ensuite justement renseigner l'ID de ce fameux groupe, car un même pfSense peut faire parti de plusieurs clusters, ici nous nous contenterons de l'ID **1**. Et enfin, nous laissons la valeur **Base** à **1** (qui correspond au nombre de secondes avant qu'un hôte soit considéré comme down) et pour la valeur **Skew**, nous la laissons à valeur à **0**. Cette valeur devra être incrémentée sur chacun des "esclaves" de notre cluster, ici nous sommes sur notre pfSense-01 qui sera le master donc nous laissons cette valeur.

Libre à vous de mettre ensuite une description ou non, puis nous réalisons la même chose pour l'IP virtuelle du LAN :

Normalement, si l'on se rend sur l'onglet **Status** puis **CARP (failover)** on devrait avoir ceci, après avoir réalisé la même manipulation sur le second pfSense

La première étape est d'activer notre interface "pfSync".

Pour cela, on se rend d'abord sur **Interfaces**, puis **Assignments** :

On va donc cliquer sur **Add** pour rajouter notre interface :

On coche bien entendu la case **Enable**, puis on rajoute la description qui va bien, on lui assigne une adresse IP (dans mon cas ce sera en /30, car je n'ai que deux hôtes mais libre à vous d'adapter au besoin), et c'est à peu près tout. Pensez à faire de même sur le second pfSense en ajustant l'adresse IP et le tour est joué !

Ensuite, on se rend dans **System**, puis **High Avail. Sync** :

On coche la case **Synchronize states**, qui permet d'activer la fonctionnalité, on choisi ensuite notre interface (LAN ou bien une interface dédiée, dans notre cas ce sera donc **pfSync**), on défini ensuite l'IP de notre second pfSense (pour rappel, toutes les actions effectuées jusqu'ici sont réalisées sur le pfSense-01 !), et ensuite on renseigne à nouveau l'IP du second dans le champ **Synchronize Config to IP**, puis on ajoute plus bas les credentials et enfin on coche les fonctionnalités à répliquer. Pensez à cocher **NAT configuration**, de

DONMEZ

Okan

SIO2

[Documentation Projet MDL](#)

cette manière vous pourrez voir par la suite si vos démarches fonctionnent en vous rendant sur le second pfSense.

Par rapport au second pfSense justement, il convient simplement de cocher la case pour activer le service, renseigner l'interface, puis l'IP du pfSense-01 dans **pfsync Synchroniez Peer IP** et rien de plus, car c'est le Master qui va répliquer les sur les slaves

nous devons nous rendre sur l'onglet **Firewall** puis **Rules** et enfin **pfSync** (ou local) pour rajouter nos règles de pare-feu histoire d'autoriser ce trafic