



# Projet BMS

## (Laboratoire pharmaceutique Bristol Myers Squibb)

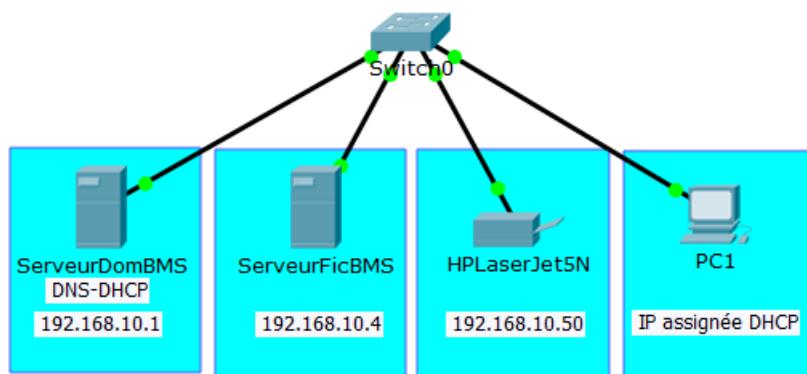


### Schéma complet du réseau

Mission 1 : Installation du serveur de domaine <i>BMS.local</i> <i>ServeurDomBMS</i> , du serveur de fichiers <i>ServeurFicBMS</i> , de l'imprimante <i>HPLaserJet5N</i> , et du PC client <i>PC1</i> .....	1
Mission 2 : Installation et configuration générale du Routeur-Pare-feu Pfsense .....	7
Mission 3 : Installation d'un serveur FOG - création et déploiement d'images .....	10
Mission 4 : Création de deux nouveaux VLANs (VLAN 20 Direction, VLAN 30 : Visiteurs) .....	15
Mission 5 : Installation du serveur de Bases de Données <i>ServeurBDBMS</i> , du serveur Web <i>ServeurWebDMZ</i> , et de l'application de gestion des frais .....	16
Mission 6 : Configuration des règles de filtrage du routeur-pare-feu Pfsense .....	18
Mission 7 : Supervision Nagios .....	22
Mission 8 : Sauvegarde journalière des dossiers personnels de base des utilisateurs .....	23
Mission 9 : Installation d'un proxy .....	23
Mission 10 : Création d'un VPN pour accéder au serveur <i>ServeurDomBMS</i> à distance .....	24
Mission 11 : Création d'un script PowerShell pour créer plusieurs utilisateurs et leur dossier personnel de base .....	25
Missions subsidiaires .....	26

### **Mission 1 : Installation du serveur de domaine *BMS.local* *ServeurDomBMS*, du serveur de fichiers *ServeurFicBMS*, de l'imprimante *HPLaserJet5N*, et du PC client *PC1***

Le but de cette mission est d'installer le domaine *BMS.local* sur un serveur contrôleur de domaine Windows Server, et de tester l'installation via un PC client Windows connecté au domaine.



#### **Mission 1 A : installation du contrôleur de domaine**

- Installer le serveur *ServeurDomBMS* qui sera contrôleur du domaine *BMS.local*, et qui sera aussi serveur DNS et serveur DHCP.

(TP SI5 de référence : [TP1 A - Création du contrôleur de domaine et connexion d'un poste au domaine](#)).

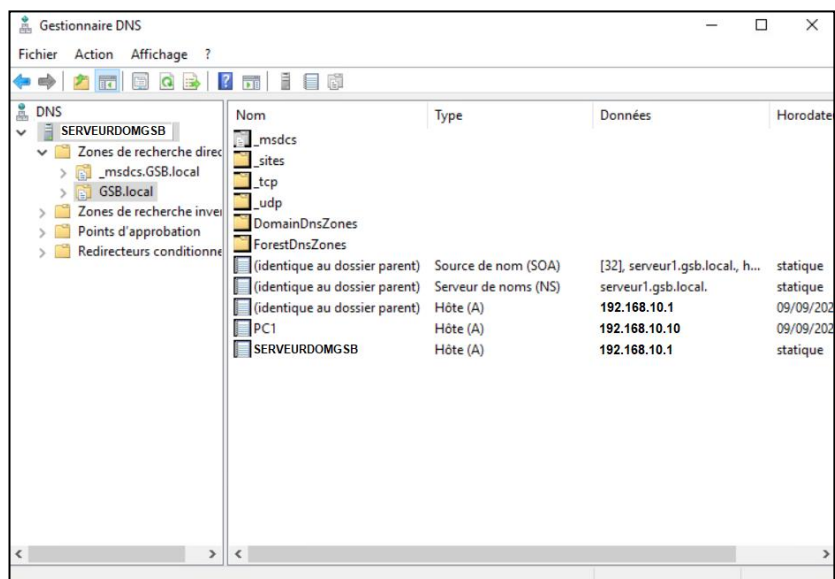
#### **Mission 1 B : installation d'un serveur de fichiers**

- Installer le serveur *ServeurFicBMS* qui sera le serveur de fichiers du domaine *BMS.local* : on stockera sur ce serveur tous les dossiers personnels de base des utilisateurs, ainsi que les dossiers partagés par les utilisateurs du domaine.

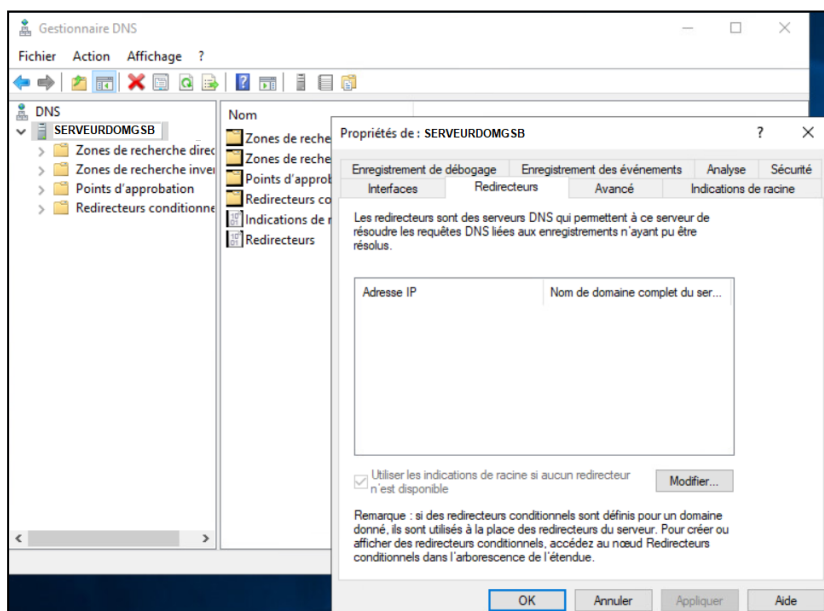
## Mission 1 C : installation du poste client PC1

- Installer le PC (sa configuration IP doit être obtenue du DHCP ; il doit être connecté au domaine).

On vérifiera en particulier, que le DNS ne comporte pas d'enregistrements d'adresses 192.168.56.X attribuées par un autre DHCP (celui de VirtualBox par exemple) aux postes du réseau BMS :



On vérifiera aussi dans les propriétés du DNS qu'il n'existe aucun redirecteur "parasite" qui se serait rajouté automatiquement (sinon les supprimer) :



## Mission 1 D : installation/déploiement de matériels et de logiciels sur les postes

- Configurer le déploiement automatique du logiciel 7-Zip sur tous les postes (serveurs et clients) du domaine BMS (TP SI5 de référence : TP5 - GPO).
- Configurer le déploiement automatique du logiciel Gantt Project uniquement sur les postes clients (PC1 et autres clients futurs) du domaine BMS.
- Installer l'imprimante LaserJet 5200 en réseau (adresse IP 192.168.10.50 ; configurer le serveur *ServeurDomBMS* comme serveur d'impression pour cette imprimante, puis configurer le déploiement automatique de cette imprimante sur tous les postes (serveurs et clients) du domaine BMS (TP SI5 de référence : TP6 - Gestion de l'impression).
- Vérifier le bon fonctionnement des déploiements de Gantt Project, 7-Zip et de l'imprimante sur le poste PC1.

Remarque : L'imprimante apparaît sur le poste client PC1 lorsqu'on ouvre une session en tant que Administrateur du domaine (BMS\Administrateur) ou utilisateur quelconque du domaine.

### Mission 1 E: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers

- Sur le serveur *ServeurFicBMS*, créer le dossier *REPBASES* et configurer ses autorisations de partage et ses autorisations de sécurité NTFS ; *REPBASES* contiendra les dossiers personnels de base de chaque utilisateur (**TP SIS de référence : TP2 A - Création de comptes-utilisateurs**).

- Créer les utilisateurs suivants (chacun avec son dossier personnel) (pour plus de simplicité, le mot de passe de chaque utilisateur ne changera jamais) ; vérifier ensuite que chaque utilisateur a son dossier dans *REPBASES* et qu'il est le seul à pouvoir y accéder, hormis les administrateurs et le système :

Nom et prénom	Nom d'ouverture de session	Nom du dossier personnel	Mot de passe
Charles Dupont	cdupont	cdupont	Windows2019
Albert Dubois	adubois	adubois	Windows2019
Clémence Rousseau	crousseau	crousseau	Windows2019
Vincent Ogier	vogier	vogier	Windows2019
Louis Ravignac	lravignac	lravignac	Windows2019

Le DSI demande ensuite de créer sur *ServeurFicBMS*, des dossiers (*DocCommerciaux*, et *DocJuridique*) pour la gestion des contrats et d'y affecter des droits d'accès NTFS différents à deux groupes d'utilisateurs (*Commerciaux* et *Juridique*).

C: \

- DocCommerciaux
- DocJuridique

- Créer les groupes d'utilisateurs et les dossiers, puis configurer les autorisations d'accès spécifiques suivantes :

Nom de groupe	Etendue	Type	Membres du groupe
Commerciaux	Domaine local	Sécurité	Charles Dupont Clémence Rousseau
Juridique	Domaine local	Sécurité	Albert Dubois Vincent Ogier

Les utilisateurs du groupe *Juridique* doivent pouvoir lire, créer, modifier et supprimer des fichiers et sous-dossiers dans le dossier *DocJuridique* ; les commerciaux ne doivent pouvoir que lire les fichiers de ce dossier ou de ses sous-dossiers.

Les utilisateurs du groupe *Commerciaux* doivent pouvoir créer des fichiers ou des sous-dossiers dans le dossier *DocCommerciaux* ; attention, un commercial ne doit pouvoir lire, modifier et supprimer que les fichiers et sous-dossiers qu'il a lui-même créés (et non ceux des autres utilisateurs).

Le groupe *Juridique* doit pouvoir lire, modifier et supprimer les fichiers et sous-dossiers de *DocCommerciaux*.

## Mission 1 F: création d'un script PowerShell et d'une GPO pour mappage automatique d'un lecteur réseau

- Créer un script PowerShell de mappage automatique d'un lecteur réseau (qui sera exécuté au démarrage d'une session utilisateur) :

- \* si l'utilisateur est membre du groupe *Commerciaux*, ce script connectera le lecteur réseau R: au dossier *DocCommerciaux*
- \* si l'utilisateur est membre du groupe *Juridique*, ce script connectera le lecteur réseau S: au dossier *DocJuridique*.

- Faire en sorte que ce script soit lancé automatiquement au démarrage de chaque session utilisateur.

### Indications concernant le module RSAT Outils Active Directory Domain Services Directory et services LDS :

Pour que ce script puisse être exécuté par le poste Windows 10, il faut installer sur celui-ci le module *RSAT Outils Active Directory Domain Services Directory et services LDS*, afin qu'il puisse exécuter les instructions concernant l'Active Directory (comme par exemple, exécuter le cmdlet *Get-ADGroupMember*).

Si ce module n'est pas installé, on obtient l'erreur suivante lors de l'exécution du script :

```
Windows PowerShell
Get-ADGroupMember : Le terme «Get-ADGroupMember» n'est pas reconnu comme nom d'applet de commande, fonction, fichier de script ou programme exécutable. Vérifiez l'orthographe du nom, ou si un chemin d'accès existe, vérifiez que le chemin d'accès est correct et réessayez.
Au caractère \\192.168.3.1\Public\ConnexionLecteurReseauConditionnel.ps1:10 : 6
+ if ((Get-ADGroupMember -Identity $myGroupName | select -ExpandPropert ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Get-ADGroupMember:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

Cliquez sur Entrée pour continuer...
```

Pour vérifier si ce module est installé (attention, il faut être connecté en Administrateur) :

```
PS C:\Users\administrateur> Get-WindowsCapability -Name RSAT.ActiveDirectory* -Online

Name           : Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
State          : NotPresent
DisplayName     : RSAT: outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services)
Description    : Les outils Active Directory Domain Services (AD DS) et les services AD LDS (Lightweight Directory Services) comprennent des outils de composant logiciel enfichable et de ligne de commande pour la gestion à distance d'AD DS et d'AD LDS sous Windows Server.
DownloadSize   : 5230259
InstallSize    : 34704398
```

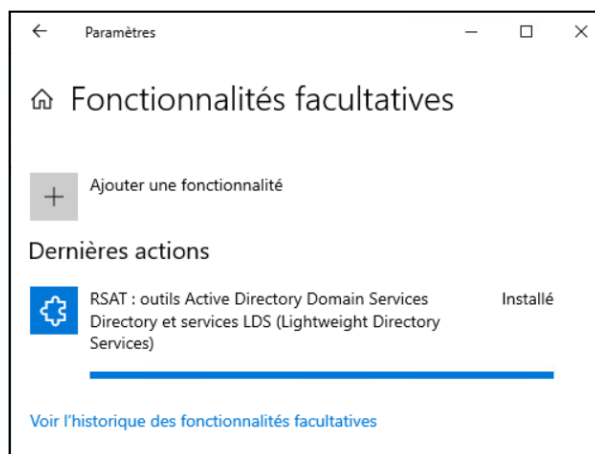
Pour installer ce module avec PowerShell (attention, il faut être connecté en Administrateur) :

```
PS C:\Users\administrateur> Get-WindowsCapability -Name RSAT.ActiveDirectory* -Online | Add-WindowsCapability -Online

Operation
Running
[ooooooooooooooooooooooooooooo]

Path      :
Online    : True
RestartNeeded : False
```

**Remarque** : on peut aussi installer ce module en ajoutant la fonctionnalité facultative RSAT dans les paramètres Windows du poste :



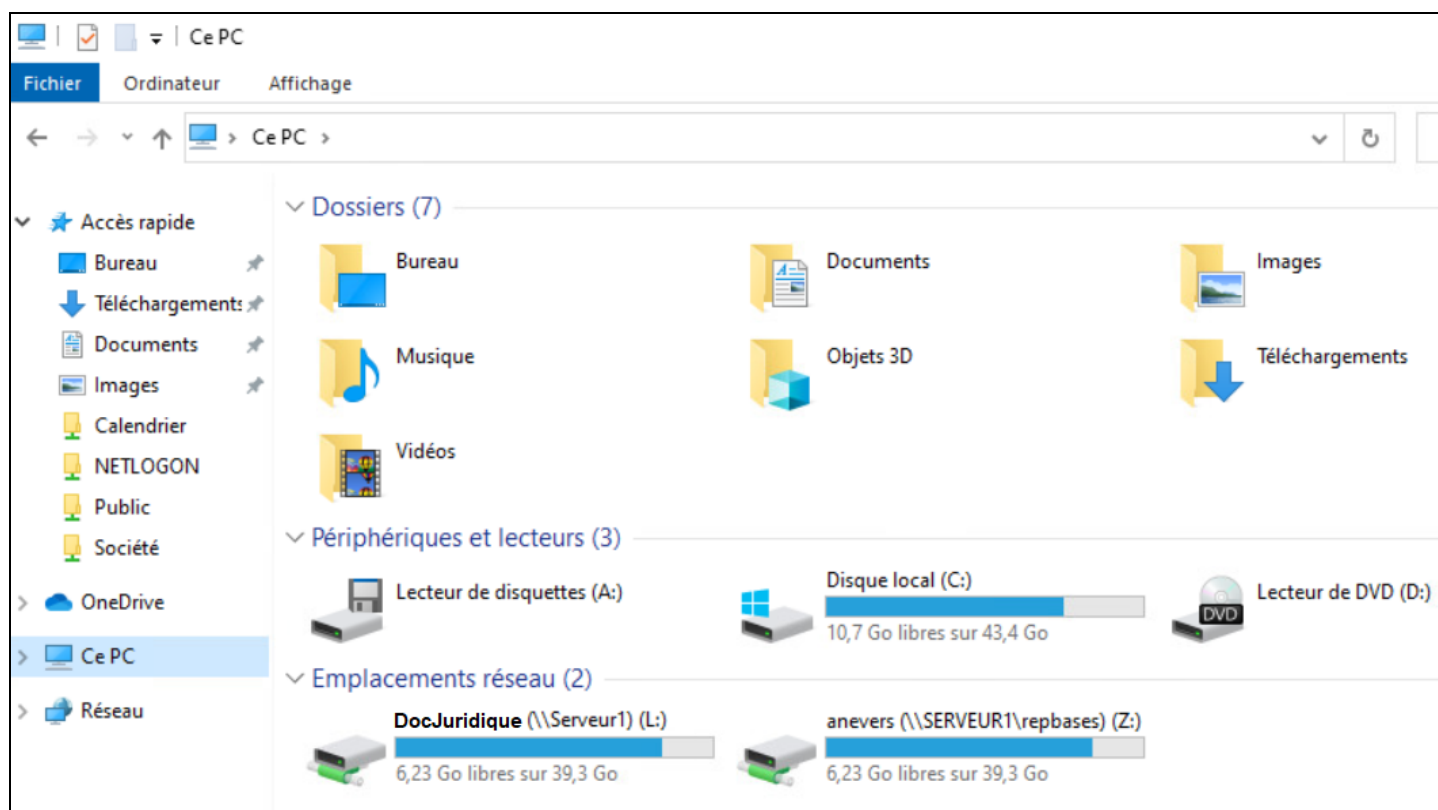
## Indications de réalisation du script :

On utilisera les 3 techniques suivantes :

- le fournisseur d'environnement **Env**: qui permet d'accéder aux variables d'environnement de Windows 10 depuis un script PowerShell en préfixant le nom de la variable d'environnement souhaitée (exemple : `$login=Env:USERNAME`) ;
- le cmdlet **New-PSDrive** qui permet de connecter un lecteur réseau en PowerShell (attention à utiliser les paramètres `-Persist` et `-Scope Global` pour que le lecteur réseau continue à exister lorsque le script PowerShell est terminé) ;
- le cmdlet **Get-ADGroupMember** et l'opérateur **contains** qui permettent de tester l'appartenance d'un utilisateur à un groupe d'utilisateurs.

Sur le poste Windows 10, on modifiera la stratégie d'exécution en tapant **T** :

```
Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse https://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la stratégie
d'exécution ?
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « N ») : T
```



Attention : dans les nouvelles mises à jour de Windows 10, l'accès depuis un poste Windows 10 au répertoire partagé **NetLogon** d'un serveur n'est plus possible avec l'Explorateur Windows !

Donc, si depuis un poste Windows 10, on souhaite exécuter un script se trouvant sur le serveur dans le dossier Netlogon :

Solution 1 : copier d'abord ce script dans un dossier partagé accessible à tous (exemple : *Public*) d'où il sera exécuté depuis le poste Windows 10. Lorsque le script aura une version définitive, il faudra penser à recopier la version définitive dans Netlogon !

Solution 2 : depuis un poste de travail connecté au domaine, on peut exécuter un script ou un programme exécutable se trouvant sur le dossier Netlogon du serveur de domaine en utilisant PowerShell.

Exemple : depuis PC1, pour exécuter le script *Factorielle.ps1* se trouvant sur le serveur *SERVEUR1* :

```
PS Z:\> Set-ExecutionPolicy RemoteSigned
PS Z:\> set-location \\SERVEUR1\Netlogon
PS Microsoft.PowerShell.Core\FileSystem: \\SERVEUR1\Netlogon> dir

Répertoire : \\SERVEUR1\Netlogon

Mode                LastWriteTime         Length Name
----                -
-a----          28/03/2014    14:51       1376768 7z920-x64.msi
-a----          15/09/2021    14:00           197 Factorielle.ps1
-a----          10/02/2013    15:56       782456 freeSSHd.exe
-a----          19/09/2013     08:19     10084352 gantt project.msi
-a----          19/09/2013    16:16       906752 jre1.7.0_40.msi
-a----          21/05/2015    14:20       7728128 khi3-3.4.7.msi
-a----          27/05/2020    17:05         134 EffaceTempo.bat

PS Microsoft.PowerShell.Core\FileSystem: \\SERVEUR1\Netlogon> .\Factorielle.ps1
```



## Mission 2 : Installation et configuration générale du Routeur-Pare-feu Pfsense

### Mission 2 A : installation du Pfsense

- Vérifier que la machine virtuelle Pfsense dispose de 5 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

OPT3 : vmx4

- 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 chaque interface).

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 suivant, noter l'adresse MAC de chaque interface réseau (fonction 8 : *Shell* sur l'écran d'interface texte du Pfsense, puis commande *ifconfig vmx0, ifconfig vmx1, ...*)

```
6) Halt system
7) Ping host
8) Shell

Enter an option: 8

[2.5.1-RELEASE][root@pfSense.localdomain/root]: ifconfig vmx0
vmx0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST>
      options=e000bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,
      ether 00:50:56:90:be:da
      inet6 fe80::250:56ff:fe90:beda%vmx0 prefixlen 64 scope
      inet 192.168.211.250 netmask 0xfffff000 broadcast 192.
```

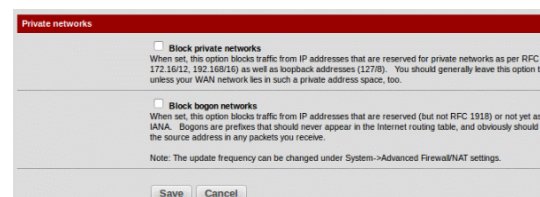
b) retrouver (sous VMware Vsphere, onglet *Résumé*, *Paramètres Matériel VM*) le numéro d'adaptateur réseau correspondant à chaque adresse MAC de cette VM, et le noter dans le tableau

Résumé	Surveiller	Configurer	Autorisations
▼ Adaptateur réseau 3			
Type d'adaptateur	VMXNET 3		
Adresse MAC	00:50:56:90:4d:03		
DirectPath I/O	Inactif		
Réseau	LAB-SISR-16-5 (connecté)		
▼ Adaptateur réseau 4			
Type d'adaptateur	VMXNET 3		
Adresse MAC	00:50:56:90:be:da		
DirectPath I/O	Inactif		
Réseau	SALLE - 211 (connecté)		

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	WAN			Salle-211
vmx1	LAN (VLAN10)			LAB-SISR-X-1
vmx2	OPT1 (VLAN20)			LAB-SISR-X-2
vmx3	OPT2 (VLAN30)			LAB-SISR-X-3
vmx4	OPT3 (DMZ)			LAB-SISR-X-4

- 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) :



- Vérifier la passerelle par défaut (Système / Routage / Passerelle).

Rappel : dans un routeur Pfsense, on ne rentre pas une route par défaut mais une passerelle par défaut : c'est l'adresse IP du prochain routeur par lequel il faut passer pour sortir sur Internet.

Normalement, la passerelle par défaut est la passerelle qui a été spécifiée pour l'interface WAN et son nom est GW\_WAN ; ceci est à vérifier (voire à modifier si ce n'est pas le cas) :

Système / Routage / Passerelles

Passerelles Routes statiques Groupes de passerelle

Nom	Par défaut	Interface	Passerelle	IP surveillée	Description	Actions
<input checked="" type="checkbox"/> GW_WAN (default)	Default (IPv4)	WAN	192.168.211.254	192.168.211.254	Interface wan Gateway	
<input type="checkbox"/> GW_LAN	Default (IPv4)	LAN	192.168.100.254	192.168.100.254	Interface lan Gateway	

Enregistrer + Ajouter

Passerelle par défaut

Passerelle IPv4 par défaut: GW\_WAN  
Sélectionnez la passerelle ou le groupe de passerelle à utiliser comme passerelle par défaut.

Passerelle IPv6 par défaut: Automatic  
Sélectionnez la passerelle ou le groupe de passerelle à utiliser comme passerelle par défaut.

Enregistrer

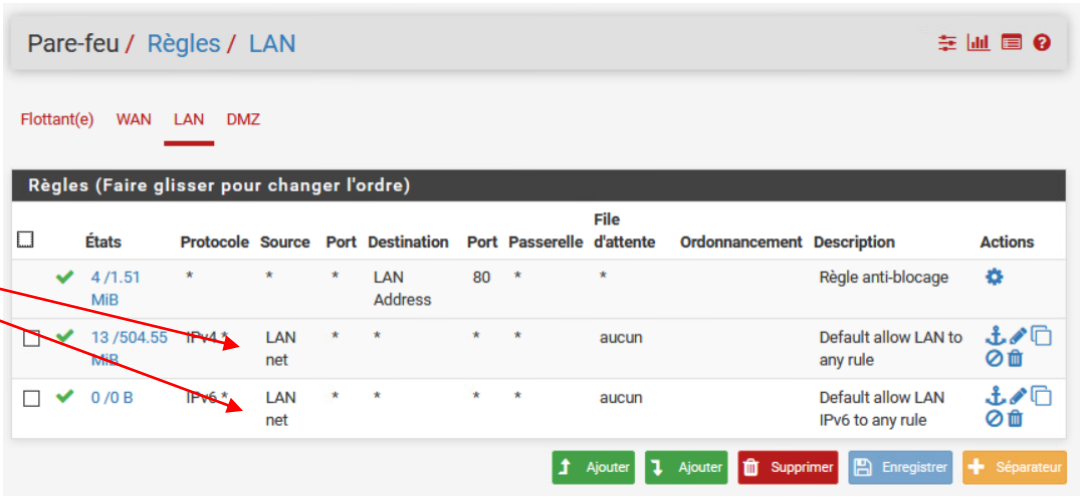


- Entrer toutes les routes nécessaires dans la table de routage du Pfsense si besoin (Système / Routage / Routes statiques).



- Modifier si besoin les règles de filtrage en entrée de l'interface VLAN10 (ou LAN) ((Pare-feu / Règles / VLAN10)) pour autoriser toute communication à partir de n'importe quel poste de ce VLAN (rappel : l'emploi de *LAN net* (adresse du réseau LAN) dans la case *Source* n'autorise que les communications à partir des postes appartenant à la même plage d'adresses que celle de l'interface LAN ;  
rappel : *LAN Address* représente l'adresse IP qui a été attribuée à l'interface LAN).

Règles à modifier



- Vérifier que la fonction NAT est bien configurée (Pare-feu / NAT / Sortant)

## Mission 3 : Installation d'un serveur FOG - création et déploiement d'images

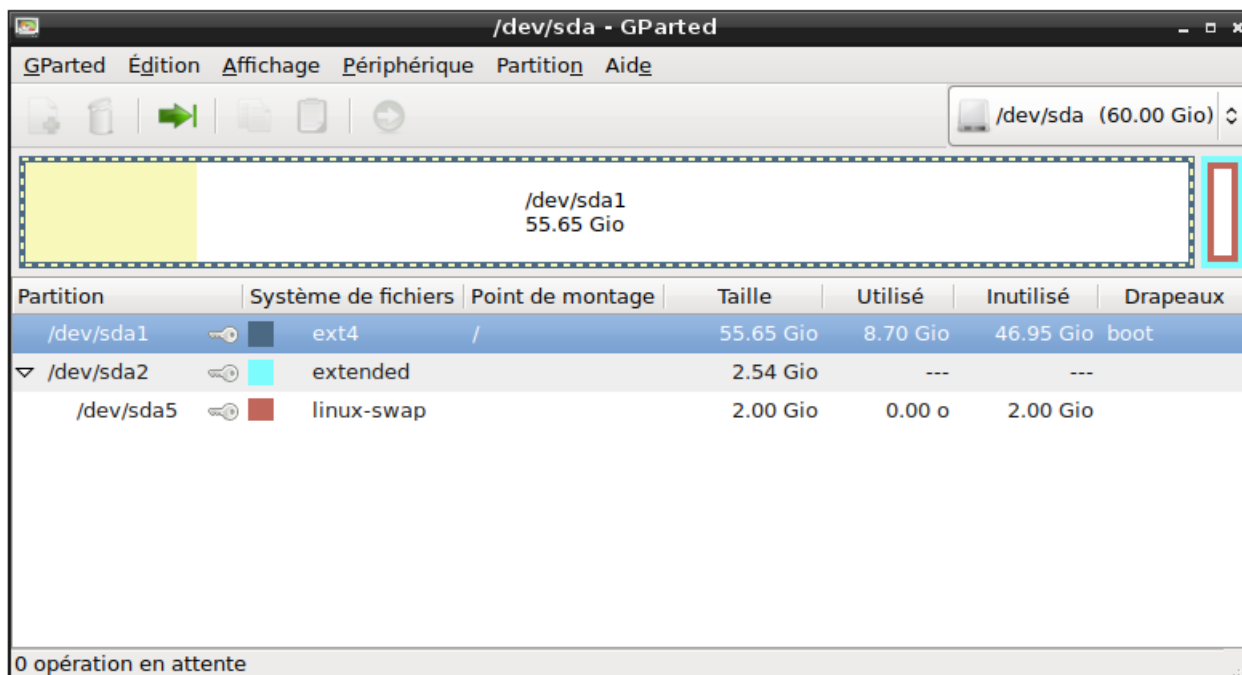
### Mission 3 A : installation et configuration du serveur FOG sous Debian

#### 3 A a) Configuration de la machine Debian

- Configurer une nouvelle machine Debian 9 qui doit avoir un disque dur de 60 GO (il doit être suffisamment grand pour y stocker plusieurs images de 10/15 GO chacune).

Consignes pour gérer la taille des partitions du disque de la machine Debian :

- utiliser l'outil graphique de gestion des partitions GParted (installer GParted sur le serveur Debian à partir des dépôts avec *apt install gparted* puis démarrer GParted) (ou démarrer le serveur FOG à partir de l'ISO GParted stocké sur la ferme de serveurs (dans le DataStore DS-COMUN\ISO))
- déplacer/réduire/agrandir si besoin la partition étendue *extended* (ici, il faut l'agrandir pour qu'elle occupe tout le disque) ;
- déplacer la partition *linux-swapp* à la fin de la partition étendue (pour déplacer/réduire/agrandir cette partition de swapp, il faut d'abord désactiver le swapp, effectuer l'opération, puis réactiver le swapp) ;
- agrandir la partition **/dev/sda1** à 55 GO (attention, on ne peut agrandir une partition que s'il y a de l'espace libre contigu à cette partition).



### 3 A b) Installation de FOG

- Effectuer la configuration IP du serveur Debian.
- Installer ensuite FOG (cf <https://fogproject.org/download>) :

```
wget https://github.com/FOGPROJECT/archive/1.5.9.tar.gz
tar -xvzf 1.5.9.tar.gz
cd fogproject-1.5.9/bin
./installfog.sh
```

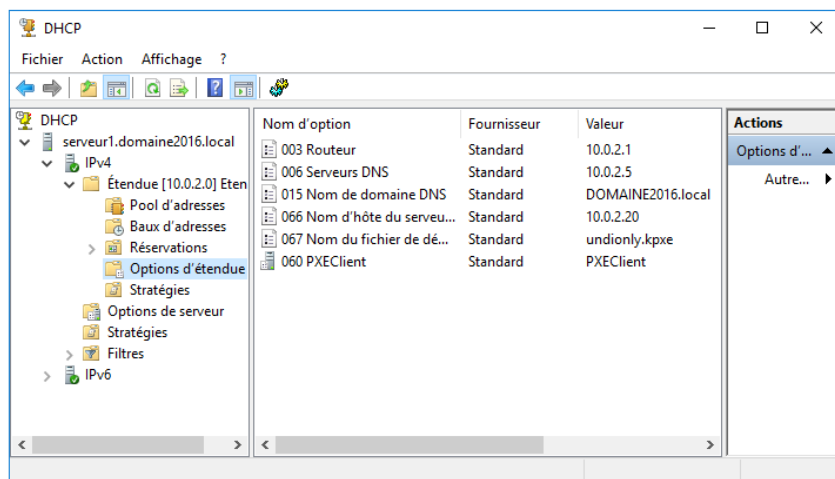
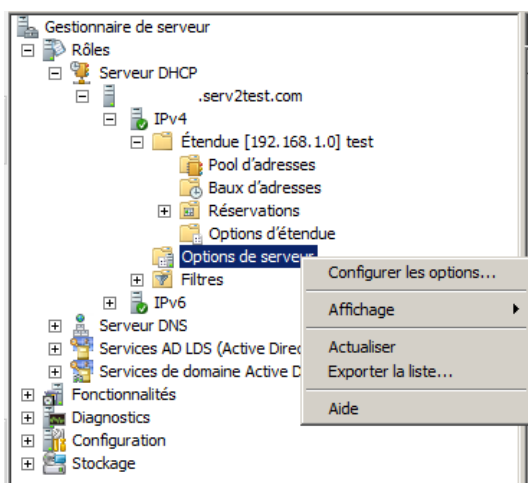
#### Consignes d'installation du serveur FOG :

- Le serveur FOG ne sera pas serveur DHCP puisque nous avons déjà un serveur DHCP sur le réseau BMS (si cela n'avait pas été le cas, il aurait fallu installer un DHCP sur le serveur FOG)
- Pour entrer dans l'interface graphique de FOG, utiliser le navigateur et l'adresse :   
*http://IP\_SERVEUR/fog/management/*
- Identifiant et Mot de passe : *fog/password* (avec un clavier non-français, taper *pqsszord*)
- Vérifier les configurations dans l'onglet *FOG Configuration*.
- Ne modifier aucun des paramètres par défaut (sinon les problèmes engendrés deviennent vite ingérables) ; par exemple, ne pas modifier le chemin par défaut des images qui seront stockées sur le serveur FOG (laisser */images*).

#### Consignes de configuration du serveur DHCP Windows :

Dans le cas d'un serveur DHCP sous Windows, il faut configurer le DHCP pour fonctionner avec FOG et le boot en PXE de nos machines : il faut utiliser l'option 66 (qui permet de spécifier le serveur qui offre les services de démarrage par le réseau pour les clients PXE) et 67 (qui permet de spécifier le nom du programme de démarrage réseau approprié à télécharger par les clients PXE) :

- Sur le serveur DHCP, dérouler le menu IPv4 puis cliquer droit sur "Options du serveur" et cliquer sur "Configurer les options" ;
- Cocher la case 66 et indiquez l'adresse du serveur FOG ;
- Cocher ensuite la case 67 et renseigner le nom du fichier de démarrage, en l'occurrence : "*undionly.kpxe*" :



### **Mission 3 B: capture d'une image d'un PC Windows 10 correctement installé (pour déploiement futur sur d'autres PC)**

- Réaliser une image d'un PC sous Windows 10 déjà installé dans le réseau BMS (exemple : PC1)(Machine déployée à partir du modèle *Windows 10 Pro - MODEL*, et surtout pas 2020 !)

#### **3 B a) Exécution de sysprep sur le client Windows à capturer**

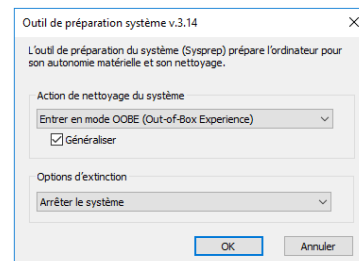
L'image d'un PC Windows à capturer doit avoir été au préalable préparée avec l'outil *sysprep* (conseillé).

Si on décide de ne pas utiliser sysprep, la machine dont on fait une image doit au moins être sortie du domaine !

Sysprep est un outil de préparation du système qui permet de remettre un PC à sa configuration d'origine (d'usine).

Lorsqu'on exécute sysprep, le PC perd donc son nom et son rattachement à un domaine, ainsi que sa clé d'activation Windows.

Sysprep permet aussi de réinitialiser le SID ; dans Windows, le SID (Security Identifier) est un identifiant unique alphanumérique qui identifie chaque système d'un domaine ; si on ne réinitialise pas le SID d'un système, il risque d'y avoir des problèmes ensuite (connexion à un domaine, ...).



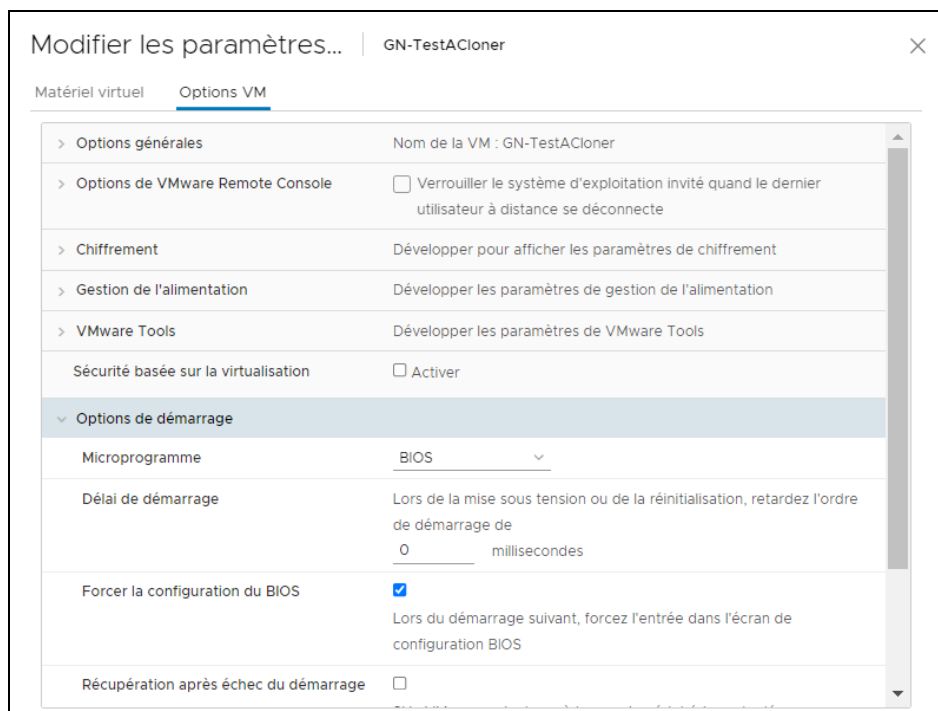
#### **3 B b) Enregistrement du client**

Démarrer le PC client dont on veut capturer l'image, en PXE (on peut utiliser la touche F12 et/ou configurer le démarrage à partir du réseau dans le setup du PC).

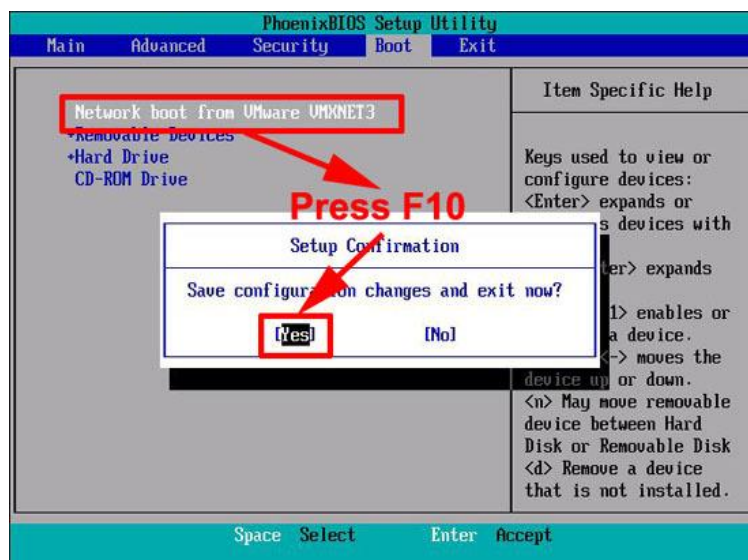
Configuration sous VMWare d'une VM devant démarrer en PXE : (<https://www.petenetlive.com/KB/Article/0000310>)

L'amorçage PXE (Pre-boot eXecution Environment) permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur (dont l'adresse IP est spécifiée dans les paramètres du serveur DHCP qui distribuera une configuration IP à la station).

- Sous VMware Vsphere, forcer le démarrage de la machine virtuelle en entrant dans la configuration du BIOS :

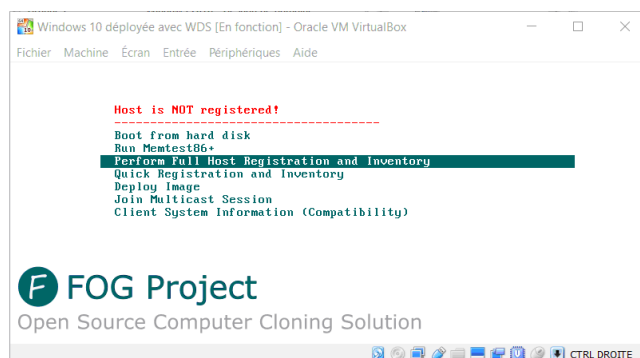


- Dans le BIOS de la machine, configurer le boot de la VM sur le réseau :



Lorsqu'on démarre le PC client dont on veut capturer l'image, en PXE, TFTP est alors utilisé pour télécharger le fichier de démarrage spécifié par DHCP (ici : *undionly.kpxe*).

Lors de l'affichage du menu FOG, enregistrer le PC auprès du serveur en sélectionnant "*Perform Full Host Registration and Inventory*". Quelques questions de configuration vont être posées telles que le nom d'hôte du client, puis il sera demandé si on veut déployer une image sur ce PC (répondre *Non*), enfin un rapide inventaire matériel sera effectué et le client sera redémarré. A ce point il sera enregistré auprès du serveur FOG ; il est possible de vérifier l'enregistrement de la machine client sur le serveur via la commande *List All Hosts* du menu *Host Management* (onglet *Hosts*).



### 3 B c) Création de l'image

Dans l'interface de gestion de FOG, sélectionner la commande *Create New Image* du menu *Image Management* (onglet *Images*). Remplir les champs comme demandé en laissant "default" pour la partie *Storage* ; le nom de fichier de l'image ne doit pas contenir de caractères spéciaux ou d'espaces !  
Cliquer sur "Add" pour terminer la création.

### 3 B d) Association de l'image avec l'hôte à figer

Sélectionner la commande *List All Hosts* du menu *Host Management* (onglet *Hosts*), puis cliquer sur le bouton "Edit" de l'hôte que l'on souhaite imager. Vérifier les champs affichés puis sélectionner l'image créée juste avant dans la liste déroulante dédiée. Cliquer sur "Update".

### 3 B e) Création de la tâche d'imaging

Toujours dans le menu d'édition de l'hôte, dans la colonne "Tasks", sélectionner la tâche "Capture" (upload image). Rebooter le client à imager en PXE ; la capture de l'image de ce client sur le serveur commence.

## Mission 3 C: déploiement d'une image Windows 10 sur un client unique

### 3 C a) Enregistrement du client

Deux solutions s'offrent à nous :

1) Démarrer le PC client vers lequel on veut déployer l'image, en PXE, puis, lors de l'affichage du menu FOG enregistrer le PC auprès du serveur en sélectionnant *"Perform Full Host Registration and Inventory"*. Quelques questions de configuration vont être posées telles que le nom d'hôte du client, puis il sera demandé si on veut déployer une image sur ce PC (répondre *Non*), enfin un rapide inventaire matériel sera effectué et le client sera redémarré. A ce point il sera enregistré auprès du serveur FOG ; il est possible de vérifier l'enregistrement de la machine client sur le serveur via la commande *List All Hosts* du menu *Host Management* (onglet *Hosts*).

2) Dans l'interface de gestion de FOG, sélectionner la commande *Create New Host* du menu *Image Management* (onglet *Images*). Il faut alors impérativement connaître l'adresse MAC du poste à ajouter (FOG utilise exclusivement l'adresse MAC pour communiquer avec les postes client) ; on peut aussi rentrer le nom de la machine ainsi que l'adresse IP.

### 3 C b) Association de l'image avec le client

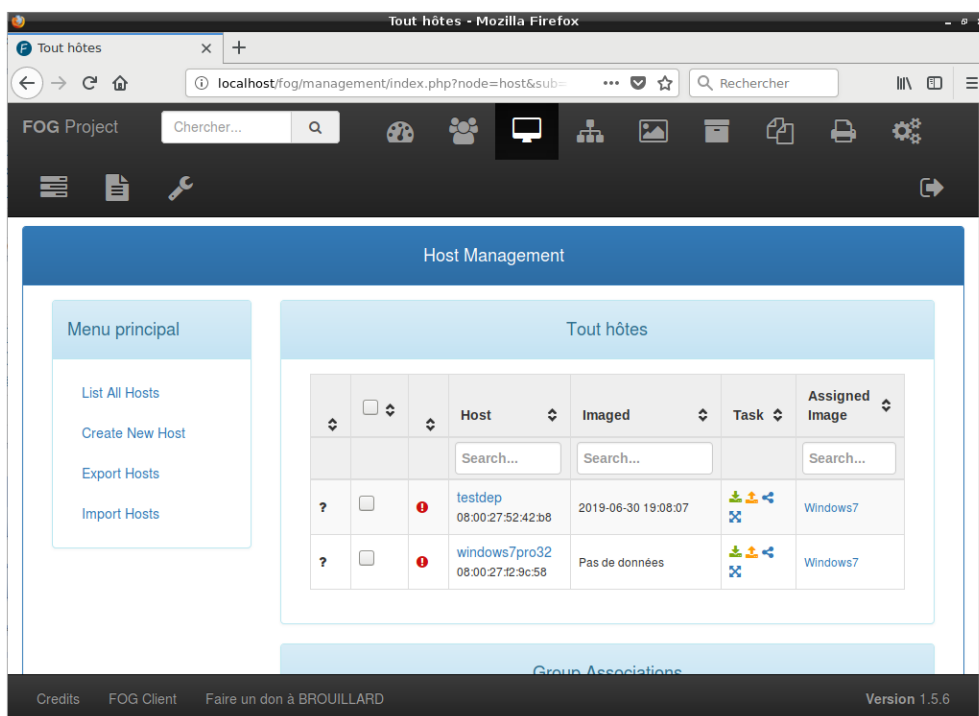
Sur l'interface de gestion, sélectionner la commande *List All Hosts* du menu *Host Management* (onglet *Hosts*), puis cliquer sur le bouton "edit" de l'hôte sur lequel vous souhaitez déployer une image. Si vous ne l'avez pas fait durant l'enregistrement du client, sélectionnez alors l'image et l'OS que vous souhaitez déployer puis cliquez sur "update".

### 3 C c) Création de la tâche de déploiement

Toujours dans le menu d'édition de l'hôte, dans la colonne *"Tasks"*, sélectionner la tâche *"Deploy"* (download image). Rebooter le client et ça devrait être bon.

#### Remarque

**Pour déployer une image sur un groupe de clients**, il suffit de créer un groupe d'hôtes dans le menu correspondant et d'appliquer la procédure ci-dessus au groupe plutôt qu'à un hôte seul.



## **Mission 4 : Création de deux nouveaux VLANs (VLAN 20 Direction, VLAN 30 : Visiteurs)**

### **Travail à faire**

#### **Mission 4 A : Configuration du DHCP**

- sur le serveur DHCP, créer une nouvelle étendue pour chacun des VLAN 20 et 30.

#### **Mission 4 B : Configuration du Pfsense**

- Configurer les interfaces VLAN20 et VLAN30 du Pfsense.
- Faire en sorte que les postes des VLAN 20 et 30 puissent envoyer des requêtes DHCP au serveur DHCP et recevoir des configurations IP de ce serveur DHCP.
- Configurer les règles de filtrage suivantes :
  - les visiteurs ne doivent pas pouvoir accéder aux différents VLANs de l'entreprise (une seule exception : les visiteurs doivent pouvoir adresser des requêtes DHCP au serveur DHCP du VLAN 10).
  - les visiteurs doivent pouvoir accéder à Internet.
  - les directeurs doivent pouvoir accéder aux différents serveurs du VLAN 10 Serveurs, mais ne doivent pas pouvoir accéder aux autres VLANs de l'entreprise.
  - les directeurs doivent pouvoir accéder à Internet.

#### **Mission 4 C : Configuration de postes-clients dans chaque VLAN**

- Installer et configurer un poste dans chacun des VLAN 20 et 30 (chacun doit avoir une configuration IP dynamique).
- Vérifier que les règles de filtrage fonctionnent.



## Mission 5 : Installation du serveur de Bases de Données *ServeurBDBMS*, du serveur Web *ServeurWebDMZ*, et de l'application de gestion des frais

Le but de cette mission est d'installer les machines, et l'application de gestion des frais BMS en mode client-serveur :

- le site Web sera installé sur le serveur Web DMZ ; on utilisera IIS pour le serveur Web.
- la base de données sera installée sur le serveur de Bases de Données du réseau local ; on utilisera Mysql pour le SGBD.

### Travail à faire

#### Mission 5 A : installation et configuration du serveur de Bases de Données

- Installer le serveur *ServeurBDBMS* Windows 2019. Cette machine doit être connectée au domaine BMS.local (*ServeurBDBMS* sera donc un serveur membre du domaine BMS mais il ne sera pas contrôleur de domaine).
- Installer le serveur de Bases de données Mysql (**TP SISR de référence : TP6 - DMZ Pfsense**).
- Créer la base de données *BMS\_frais*, puis créer les tables et leurs enregistrements à l'aide des scripts de création fournis.

#### Exemples de commandes à utiliser :

```
create database BMS_frais;
use BMS_frais;
show tables;
source c:/BMS_frais_structure.sql
show tables;
source c:/BMS_frais_insert_tables_statiques.sql
select * from visiteur;
```

- penser à configurer le SGBD Mysql en accordant tous les droits d'accès à la base de données *BMS\_frais* à l'utilisateur nommé *utilisateurWeb* (qui est à créer) et ayant le mot de passe *secret* (c'est cet utilisateur qui est utilisé dans les scripts PHP du site Web *bmsMVC* qui permettent à un internaute de se connecter à la base de données) :

```
create user "utilisateurweb" identified by "secret";
grant all privileges on BMS_frais.* to "utilisateurweb";
flush privileges;
select user from mysql.user;
show grants for "utilisateurweb";
...
```

#### Mission 5 B : installation et configuration du serveur Web DMZ

- Installer le serveur *ServeurWebDMZ* Windows 2019. Cette machine ne doit pas être connectée au domaine BMS.local.
- installer le rôle *Serveur Web IIS* avec le service de rôle *CGI* ;
- installer PHP (**TP SISR de référence : TP6 - DMZ Pfsense**) ;

- vérifier que l'extension *mysql* (bibliothèque *dll*) correspondant à la technologie utilisée dans les pages PHP du site web hébergé, est bien activée dans PHP :

- l'extension **php\_mysqli.dll** **doit être activée** si le site utilise la technologie *mysqli* :

```
$hote="192.168.10.2";
$utilisateur="utilisateurweb";
$motDePasse="secret";
$nomBase="gsb_frais";
$connexion= new mysqli($hote, $utilisateur, $motDePasse, $nomBase);
if ($connexion->connect_errno) {
    // La connexion a échoué.
    echo "Erreur : Impossible d'établir une connexion MySQL<br>";
    echo "Erreur " . $connexion->connect_errno . " : " . $connexion->connect_error . "<br>";
    exit;}
}
```

- l'extension **pph\_pdo\_mysql.dll** **doit être activée** si le site utilise la technologie *pdo* :

```
class PdoGsb{
    private static $serveur='mysql:host=192.168.10.2';
    private static $bdd='dbname=gsb_frais';
    private static $user='utilisateurweb' ;
    private static $mdp='secret' ;
    private static $monPdo;
    private static $monPdoGsb=null;

    private function __construct(){
        PdoGsb::$monPdo = new PDO(PdoGsb::$serveur.'.PdoGsb::$bdd, PdoGsb::$user, PdoGsb::$mdp);
        PdoGsb::$monPdo->query("SET CHARACTER SET utf8");
    }
    public function __destruct(){
        PdoGsb::$monPdo = null;
    }
}
```

- installer les pages du site *bmsMVC* (copier le dossier fourni *bmsMVC* dans *wwwroot*).

Ce site Web installé sur le serveur Web DMZ devra utiliser la base de données *BMS\_frais* installée sur le serveur de Bases de Données. En conséquence, il est nécessaire de modifier le script PHP de connexion au serveur Mysql et à la base de données :

- adresse IP du serveur Mysql : 192.168.10.2
- nom de la base de données : *BMS\_frais*
- identifiant et mot de passe de l'utilisateur : *utilisateurweb / secret*

#### **RAPPEL :**



Pour que le site Web *bmsMVC* fonctionne correctement, il est indispensable d'installer et de configurer auparavant le routeur-pare-feu Pfsense, afin que **le serveur Web ait accès au serveur de bases de données**.

## Mission 6 : Configuration des règles de filtrage du routeur-pare-feu Pfsense

### Travail à faire

Configurer le Pfsense et implanter les règles de filtrage nécessaires pour protéger au maximum le réseau local, et protéger au mieux la DMZ.

Rappel : le serveur Web de la DMZ ne dispose pas d'adresse IP publique. On devra néanmoins pouvoir accéder à ce serveur à partir d'un poste de la salle R211.

Indication : penser à rendre accessible le Pfsense depuis un poste ayant une adresse IP privée (par exemple un poste de la salle R211) en décochant la case *Block private networks* de l'interface WAN :

**Private networks**

☐ **Block private networks**  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on 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 appear as the source address in any packets you receive.

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

Save Cancel

## Mission 6 A : Règles minimum à configurer sur l'interface DMZ du Pfsense

- le serveur Web DMZ peut interroger le serveur de BD sur le port 3306 ;
- le serveur Web DMZ ne peut émettre aucun autre trafic vers le LAN ;
- le serveur Web DMZ peut accéder à Internet (HTTP, HTTPS, FTP, messagerie électronique, ...).

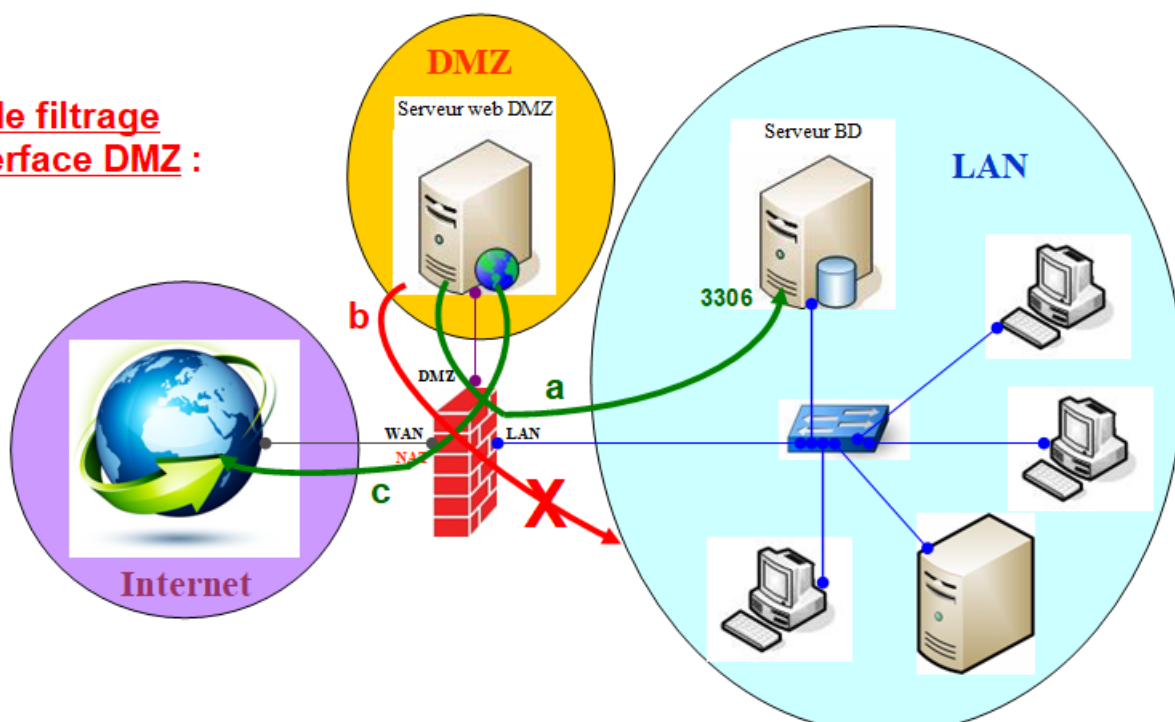


Pour la règle b, attention à bien résumer l'adresse du LAN (incluant tous les VLAN) sous peine de bloquer l'accès de tout le réseau à Internet !

### Interface DMZ

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	DMZ	E							
b	DMZ	E							
c	DMZ	E							
Def	DMZ	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

### Règles de filtrage sur l'interface DMZ :



**a** : Autoriser les nouvelles connexions entrantes de certains serveurs de la DMZ (exemple : serveur web) vers certains serveurs du LAN (ex : serveur BD) sur des ports nécessaires (par exemple, ports utilisés par MySQL, SQL Server...).

**b** : Interdire toute autre connexion entrante de la DMZ vers le LAN.

**c** : Autoriser si besoin les connexions entrantes des serveurs de la DMZ vers Internet.

Remarque : toute réponse venant de la DMZ et correspondant à une demande faite par un poste Internet ou du LAN est autorisée à entrer sur cette interface DMZ.

Remarque : on peut aussi rajouter une règle de filtrage qui permet au serveur Web DMZ de ping le serveur de BD.

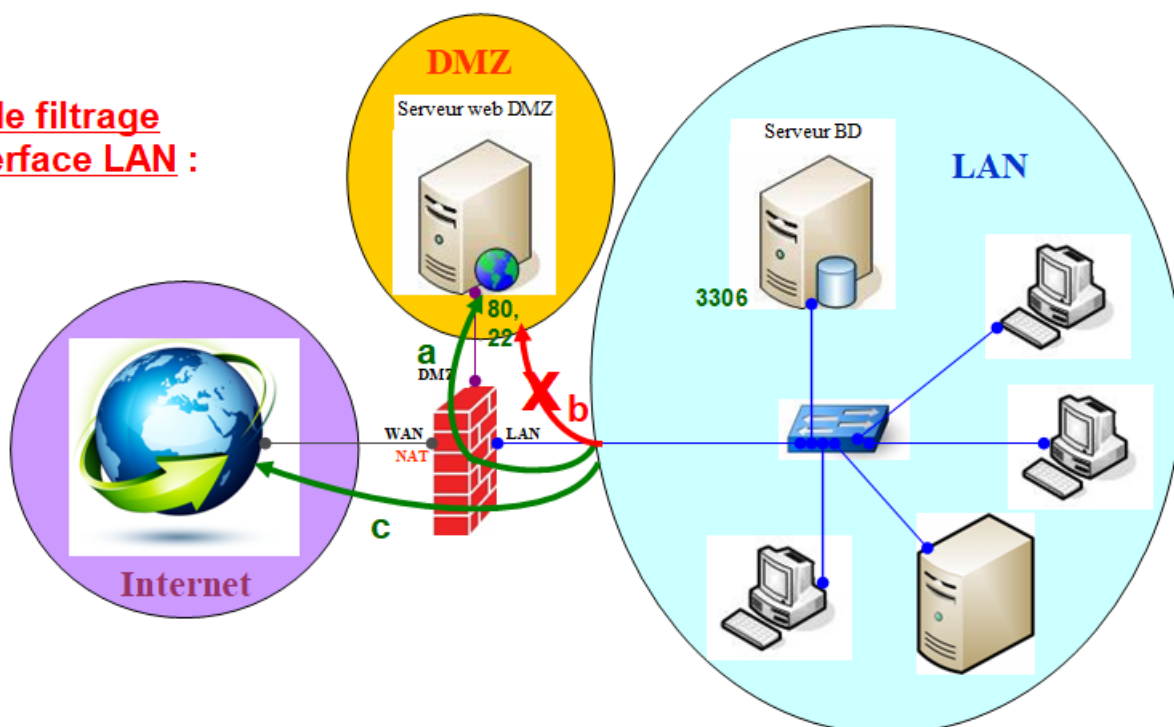
## Mission 6 B : Règles minimum à configurer sur l'interface LAN du Pfsense

- a. le LAN peut interroger le serveur Web DMZ sur le port 80 ;
- b. le LAN ne peut émettre aucun autre trafic vers le serveur Web DMZ ;
- c. le LAN peut accéder à Internet (HTTP, HTTPS, FTP, messagerie électronique, ...).

### Interface LAN

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	LAN	E							
b	LAN	E							
c	LAN	E							
Def	LAN	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

### Règles de filtrage sur l'interface LAN :



**a** : Autoriser les nouvelles connexions entrantes du LAN vers les serveurs de la DMZ sur des ports prédéfinis pour utiliser normalement ces serveurs (par exemple, STMP, FTP, POP, HTTP...), ou seulement pour les mettre à jour (SSH, FTP, ...) depuis certains postes autorisés.

**b** : Interdire toute autre connexion entrante du LAN vers la DMZ.

**c** : Autoriser toute connexion entrante du LAN vers Internet.

Remarque : toute réponse venant du LAN (du serveur BD) et correspondant à une demande faite par un serveur de la DMZ est autorisée à entrer sur cette interface LAN.

Remarque : on peut aussi rajouter une règle de filtrage qui permet à toute machine du LAN de pinguer le serveur Web DMZ.

## Mission 6 C : Règles minimum à configurer sur l'interface WAN du Pfsense

- Internet peut interroger le serveur Web DMZ sur le port 80 ;
- Internet ne peut émettre aucune autre connexion entrante vers le LAN ou la DMZ.

### Interface WAN (règles de redirection de port)

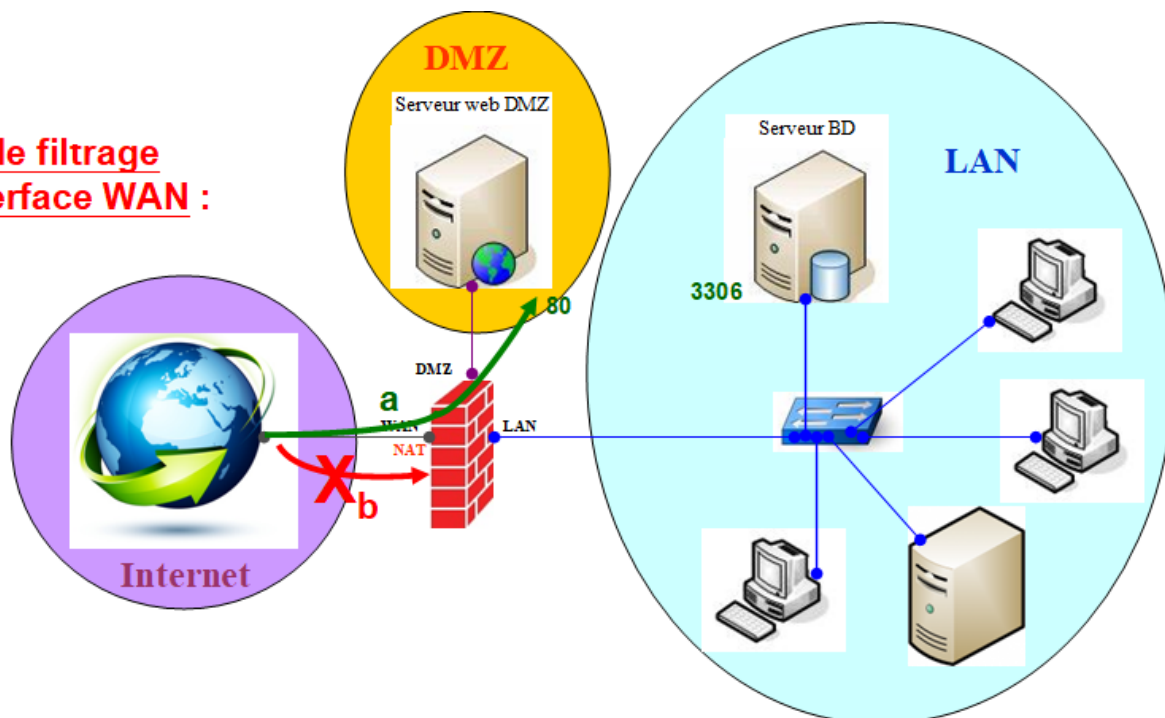
Interface d'arrivée - Adresse publique	Port public	Adresse privée	Port privé

*La règle de filtrage a est créée automatiquement lorsqu'on crée la redirection de port !*

### Interface WAN

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	WAN	E							
b	WAN	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

### Règles de filtrage sur l'interface WAN :



**a** : Autoriser les nouvelles connexions entrantes d'Internet vers les serveurs de la DMZ sur les ports nécessaires (HTTP, SMTP, FTP, POP, ...).

**b** : Interdire toute autre connexion entrante d'Internet vers la DMZ ou le LAN.

Remarque : toute réponse venant d'Internet et correspondant à une demande faite par un poste du LAN ou de la DMZ est autorisée à entrer sur cette interface WAN (connexion déjà existante et établie par ce poste).

Si l'adressage IP de la DMZ est privé :

- NAT dynamique/PAT
- NAT statique avec redirection de port

# Mission 7 : Supervision Nagios

Le but de cette mission est de réaliser la supervision des serveurs de BMS, ainsi que du Pfsense.

## Travail à faire

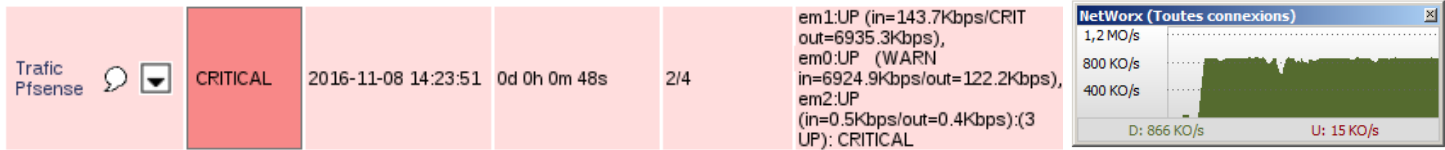
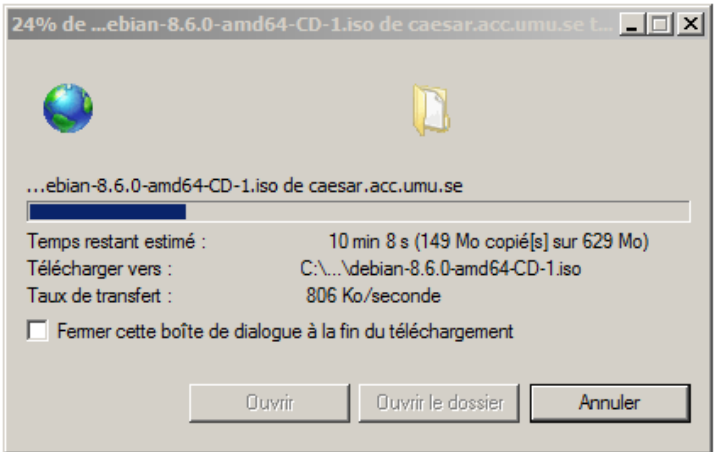
- Installer Nagios sur un serveur Debian (TP SISR de référence : [TP1 SISR5 - Installation de Nagios 4](#)) ;
- Configurer la supervision des éléments du réseau dans le fichier *monReseau.cfg*
- Déclarer tous les postes de ce projet et superviser l'affichage de la description du système, ainsi que le taux d'occupation du disque dur de chacun.

On pourra aussi superviser en temps réel la bande passante (mesure du débit instantané du trafic réseau) des principales interfaces du routeur Pfsense pour surveiller tout trafic excessif sur ces interfaces, en utilisant le plugin *check\_snmp\_netint.pl*

Exemple : lors du téléchargement d'un fichier depuis Internet sur un serveur du LAN :

- vitesse de téléchargement : 850 KO/s  
soit : 6800 Kbits/s

Ce téléchargement s'observe en mesurant en temps réel le débit du trafic réseau sur les interfaces suivantes :  
- en entrée (IN) sur l'interface externe Pfsense *em0*  
- en sortie (OUT) sur l'interface interne Pfsense *em1*





## Mission 8 : Sauvegarde journalière des dossiers personnels de base des utilisateurs

Le but de cette mission est de réaliser la sauvegarde journalière du dossier REPBASES.

### Travail à faire

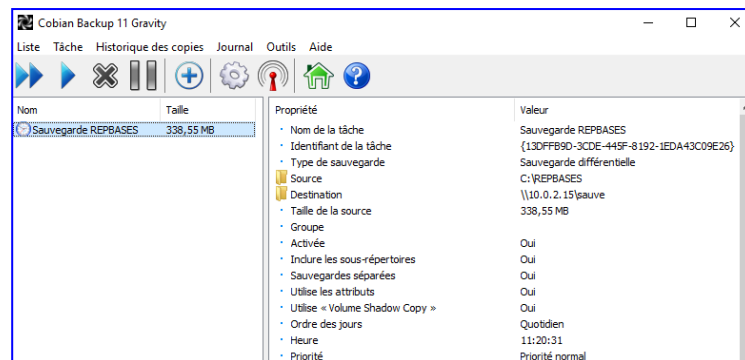
- Effectuer l'installation du logiciel de sauvegarde de votre choix (logiciel conseillé : COBIAN)
- Configurer une tâche permettant de sauvegarder le dossier REPBASES (et tous ses sous-dossiers) :
  - sur le support destination de votre choix
  - de manière périodique (tous les jours à l'heure de votre choix)
  - type de sauvegarde différentielle, mais en faisant une sauvegarde complète toutes les trois sauvegardes
  - avec compression (essayer d'abord sans compression).

Exemple de logiciel de sauvegarde : [Cobian Backup 11](#)

Tutoriels :

<http://www.logicielgratuit-tuto.com/cobian-backup.php>

<http://www.it-connect.fr/comprendre-la-sauvegarde-incrementielle-et-differentielle/>



## Mission 9 : Installation d'un proxy

Le but de cette mission est de réaliser la configuration du routeur-pare-feu Pfsense, afin qu'il joue le rôle de serveur proxy pour tous les postes du réseau LAN 192.168.0.0/16.

Ce proxy permettra notamment de **bloquer l'accès à tous les sites des réseaux sociaux** (facebook, twitter, linkedin, ...)

Il permettra aussi d'obtenir **un journal retraçant toute l'activité Internet des postes du réseau**.

Le proxy Pfsense sera accessible sur le port 3128.

### Travail à faire

- Sur le Pfsense, configurer l'adresse du DNS, et installer les packages *Squid*, *SquidGuard*, et *LightSquid*
- Configurer le proxy *Squid*, ainsi que les règles de blocage des sites souhaités sur *SquidGuard*.

**Indications pour configurer Squid et SquidGuard :** [Annexe 2 : mise en oeuvre de Squid et SquidGuard](#)

- Afficher l'historique de toute l'activité Internet des postes du réseau avec *LightSquid*.

Lien utile du tutorat d'installation et de configuration du proxy Pfsense : <http://sen-louis-armand.fr/index.php?id=94>  
et <https://www.pc2s.fr/pfsense-proxy-transparent-filtrage-web-url-squid-squidguard/>

### Indications

- Dans les règles de filtrage de l'interface VLAN10, il faudra s'assurer que les postes du VLAN 10 sont bien autorisés à accéder au proxy Pfsense 192.168.10.254 sur le port 3128 (idem pour les autres VLAN).
- Il faudra penser aussi à spécifier les sous-réseaux autorisés à utiliser le proxy (commande *Services Squid Proxy Server*, onglet *ACLs*). En effet, par défaut, seul le réseau connecté directement au proxy est autorisé à l'utiliser. De fait, il faudra si besoin décocher la case *Allow Users on Interface* (commande *Services Proxy Server*, onglet *General*).
- Le proxy du lycée 192.168.216.250 devra être désactivé pour la salle R211 (la règle du proxy internal → wan1 doit être activée pour la salle R211) :

▼ internal(Administration) -> wan1(Free) (8)					
1	Administration 216	all		always	ANY
2	Salle R209	all		always	ANY
3	Salle R210	all		always	ANY
4	Salle R211	all		always	ANY

- On pourra utiliser la blacklist **social\_networks** de l'université de Toulouse (<https://dsi.ut-capitole.fr/blacklists/>) qui répertorie tous les sites des réseaux sociaux connus :

[ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard\\_contrib/social\\_networks.tar.gz](ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/social_networks.tar.gz)

## **Mission 10 : Création d'un VPN pour accéder au serveur *ServeurDomBMS* à distance**

L'administrateur du réseau BMS souhaite pouvoir travailler depuis chez lui sur le serveur de domaine *ServeurDomBMS*. Il a donc besoin d'une connexion sécurisée VPN SSL/TLS de type nomade (entre un client distant et un serveur VPN). Le serveur VPN sera OpenVPN ; il sera installé sur le routeur-parefeu PfSense. Les clients VPN seront installés sur des machines Windows ; ils recevront une adresse sur le réseau par défaut **192.168.200.0/24** et auront accès au réseau 192.168.10.0/24.

OpenVPN possèdera sa propre autorité de certification. Le serveur OpenVPN et chaque client OpenVPN posséderont un certificat (avec une clé publique) et une clé privée qui leur seront propres. L'autorité de certification d'OpenVPN signera les certificats du serveur et de chaque client.

### **Travail à faire**

- Configurer le VPN SSL/TLS de type nomade
- Créer un utilisateur de nom ***User\_VPN*** et de mot de passe ***faure*** localement sur le serveur OpenVPN.
- Vérifier que cet utilisateur peut se connecter à distance au serveur *ServeurDomBMS*.

## Mission 11 : Création d'un script PowerShell pour créer plusieurs utilisateurs et leur dossier personnel de base

L'administrateur du réseau BMS souhaite pouvoir automatiser la création des utilisateurs du domaine.

Il souhaite pouvoir entrer dans un fichier .csv le prénom, le nom, le login, et le groupe d'utilisateurs de plusieurs nouveaux utilisateurs, et exécuter un script sur *ServeurDomBMS* qui permet la création de ces utilisateurs dans l'Active Directory, ainsi que la création de leur dossier personnel de base dans REPBASES sur *ServeurFicBMS*.

### Travail à faire

- on créera un fichier *NouveauxEmployes.csv* contenant toutes les données nécessaires à la création des 3 personnes ci-dessous.



#### Utilisateurs

Prénom	Nom	Login (SAMID)	Expiration password	Password	Changement password	Dossier personnel de base	Membre d'un groupe
Thierry	Joguet	tjoguet	jamais	secret1A!	non	C:\REPBASES\tjoguet	Juridique
Charlotte	Casy	ccasy	jamais	secret1A!	non	C:\REPBASES\ccasy	Commerciaux
Solène	Grime	sgrime	jamais	secret1A!	non	C:\REPBASES\sgrime	

- ces utilisateurs devront tous être créés dans une Unité d'Organisation nommée **NouveauxEntrants** (à créer si pas encore existante).

- chaque utilisateur devra être membre du groupe spécifié dans le fichier .csv (si aucun groupe n'est spécifié, ou si le groupe spécifié n'existe pas, l'utilisateur sera simplement rangé dans un groupe *Autres* (à créer si pas encore existant)).

- on devra créer pour chaque utilisateur un dossier personnel de base dans le dossier *C:\REPBASES\* (le dossier REPBASES existe déjà ; inutile de tester son existence). L'autorisation NTFS *Modifier* devra être accordée à un utilisateur sur son dossier personnel de base.

## Missions subsidiaires

### Mission 13 : Ajout d'un serveur contrôleur supplémentaire de domaine BMS ServeurDom2BMS

Le but de cette mission est d'installer un serveur contrôleur de domaine supplémentaire et de permettre ainsi une réplication de l'annuaire de "Active Directory" sur les deux serveurs afin d'améliorer la disponibilité sur le service en cas de problème.

Ainsi, si le premier contrôleur n'est pas joignable, se sera le second qui répondra et gèrera les connexions.

#### **Travail à faire**

- Installer une nouvelle machine physique sur laquelle on installera le serveur *ServeurDom2BMS* qui sera contrôleur supplémentaire du domaine BMS.
- Vérifier que les comptes-utilisateurs et le DNS sont correctement répliqués.

### Mission 14 : Connexion du serveur Debian au domaine BMS

Le but de cette mission est de joindre le serveur Debian au domaine BMS.

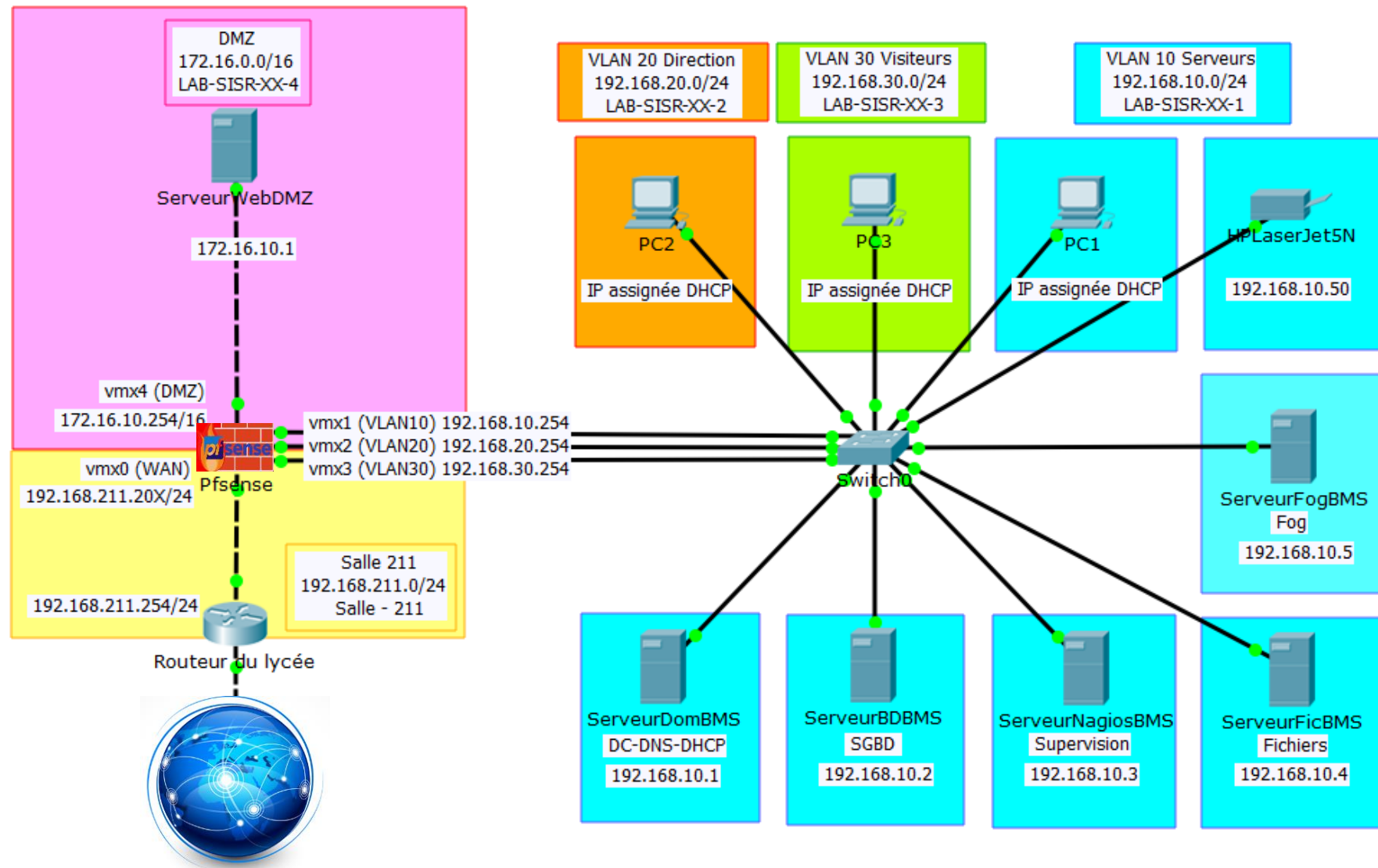
Chaque utilisateur du domaine BMS pourra ainsi ouvrir une session depuis le poste Debian et accéder à son dossier personnel de base situé sur le serveur Windows 2008 R2 *ServeurDomBMS*. Chaque utilisateur devra pouvoir aussi imprimer sur l'imprimante HP LaserJet gérée par le serveur d'impression sous Windows.

(TP SI5 de référence : [TP10 - Connexion d'un poste Linux à un domaine Windows avec PBIS](#)).

#### **Travail à faire**

- Joindre le poste Debian au domaine BMS.
- Configurer l'impression depuis le poste Debian sur l'imprimante HP LaserJet gérée par le serveur d'impression sous Windows.
- Vérifier que chaque utilisateur de l'Active Directory BMS.local peut se connecter au domaine et accéder à son dossier personnel de base ; vérifier aussi qu'il peut lancer des impressions sur l'imprimante HP LaserJet.

## Annexe 1 : schéma du réseau



## Annexe 2 : mise en oeuvre de Squid et SquidGuard

1. Activer le serveur proxy *Squid* sur les interfaces souhaitées (VLAN10, ...) **et** la boucle locale (Loopback) du Pfsense, utilisant le port 3128 (commande *Services Squid Proxy Server*) (bien cocher la case *Check to enable the Squid proxy*) :

**Squid General Settings**

**Enable Squid Proxy** ☒ Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled and stopped.

**Keep Settings/Data** ☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

**Proxy Interface(s)** LAN, DMZ, WAN, boucle locale  
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

**Proxy Port** 3128  
This is the port the proxy server will listen on. Default: 3128

2. Toujours dans l'onglet General, penser à cocher la case *Enable Access Logging* pour que les logs d'accès soient enregistrés, puis entrer la valeur 10 dans *Rotate Logs* pour définir le nombre de jours pendant lesquels les logs sont conservés (attention, le fichier des logs */var/squid/logs/access.log* risque d'être très gros au bout d'un an : vérifier qu'il y a de la place sur le disque dur ; on peut aussi fixer un nombre de jours plus petit (exemple : 30 jours), et juste avant la rotation des logs on peut transférer le fichier sur un autre disque) :

**Logging Settings**

**Enable Access Logging** ☒ This will enable the access log.  
**Warning:** Do NOT enable if available disk space is low.

**Log Store Directory** /var/squid/logs  
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs  
**Important:** Do NOT include the trailing / when setting a custom location.

**Rotate Logs** 365  
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

**Log Pages Denied by SquidGuard** ☐ Makes it possible for SquidGuard denied log to be included on Squid logs.  
Click Info for detailed instructions. ⓘ

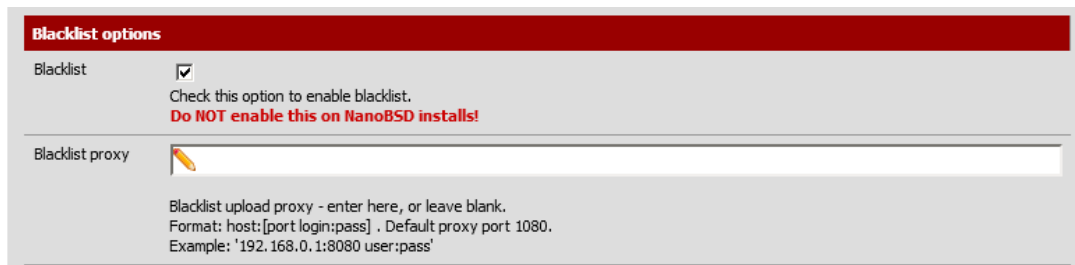
3. Passer ensuite à la configuration du filtrage du proxy *SquidGuard* (commande *Services SquidGuard Proxy Filter*) : dans l'onglet *Target categories*, créer obligatoirement au moins une catégorie (par exemple de nom *Personnel*) même si elle est vide.

### Proxy filter SquidGuard: Target categories

**General settings** **Common ACL** **Groups ACL** **Target categories** **Times** **Rewrites** **Blacklist** **Log** **XMLRPC Sync**

Name	Redirect	Description
Personnel		

4. Dans l'onglet *General Settings*, autoriser l'utilisation des blacklists en cochant la case *Blacklist*.



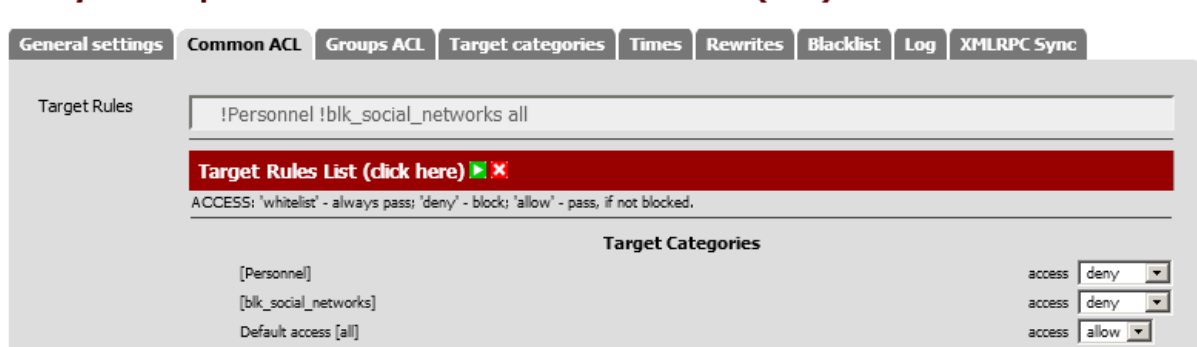
5. Dans l'onglet *Blacklist*, télécharger la blacklist voulue (entrer l'adresse du lien FTP de cette blacklist, puis cliquer sur le bouton *Download*).

blacklist **social\_networks** de l'université de Toulouse (<https://dsi.ut-capitole.fr/blacklists/>) :  
[ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard\\_contrib/social\\_networks.tar.gz](ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/social_networks.tar.gz)



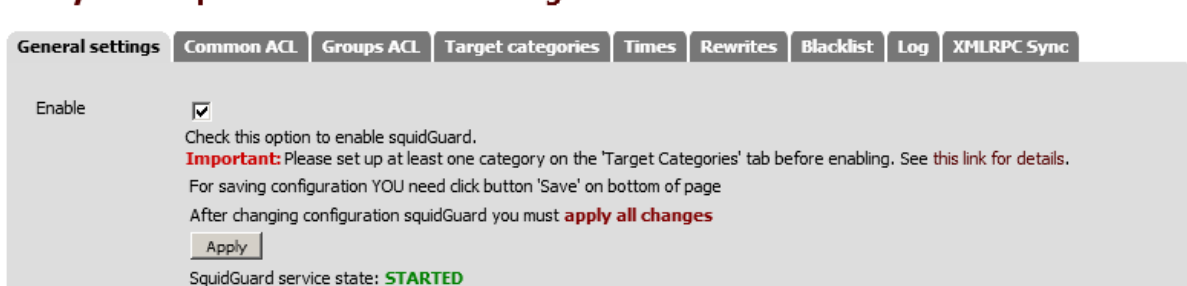
6. Dans l'onglet *Common ACL*, afficher les règles (cliquer sur le bouton + *Show Rules* de la zone *Target Rules List*), puis
- interdire l'accès aux sites référencés par la blacklist *blk\_social\_networks*
  - interdire l'accès aux sites référencés de la catégorie *Personnel*
  - autoriser tout le reste.

### Proxy filter SquidGuard: Common Access Control List (ACL)



7. Dans l'onglet *General Settings*, activer SquidGuard (en cochant la case *Check this option to enable SquidGuard*) puis appliquer tous les changements (cliquer sur le bouton *Apply*) et redémarrer si besoin le service Squid.

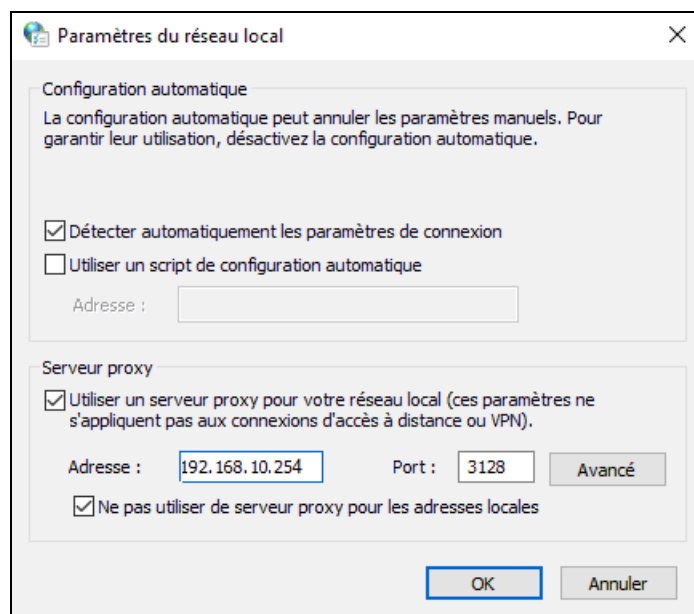
### Proxy filter SquidGuard: General settings





8. Modifier la configuration IP de chaque poste du réseau local pour qu'il utilise le proxy :

Exemple pour un poste du VLAN 10 :





9. Configurer l'outil d'analyse de logs *LightSquid* (commande *Status Squid Proxy Reports*) en décochant la case *LightSquid Web Port* (pour que le service soit accessible en HTTP sur le port 7445 et non en HTTPS qui obligerait à créer un certificat) et en sélectionnant le Français comme langue de l'outil d'analyse :

Web Service Settings	
<u>LightSquid</u> <u>Web Port</u>	7445 Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)
<u>LightSquid</u> <u>Web SSL</u>	<input type="checkbox"/> Use SSL for Lightsquid Web Access This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.
<u>LightSquid</u> <u>Web User</u>	admin Username used to access lighttpd. (Default: admin)
<u>LightSquid</u> <u>Web Password</u>	..... Password used to access lighttpd. (Default: pfsense)
Links	<a href="#">Open Lightsquid</a> <a href="#">Open sqstat</a>
Report Template Settings	
Language	Français Select report language.

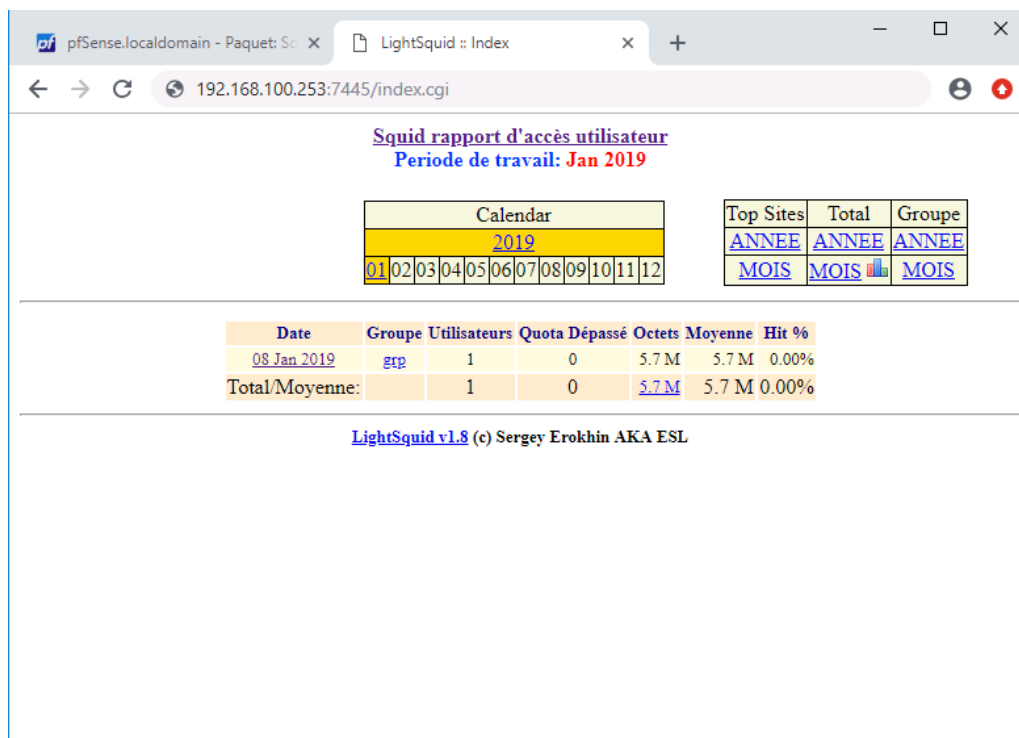
10. Cliquer sur le bouton *Refresh Full* pour reporter immédiatement tous les logs dans l'analyseur de logs LightSquid (ceci est fait par défaut toutes les 60 minutes) :

**Manual Refresh** Use these buttons to start a background refresh of the Lightsquid reports.

 **Refresh** Will (re)parse today's entries only in Squid's current access.log.

 **Refresh Full** Will (re)parse all entries in all Squid's access logs, including the rotated ones. This may take a long time to finish!

11. Visualiser ces logs dans le navigateur en tapant l'adresse LAN du PfSense suivi du numéro de port 7445 :



**Squid rapport d'accès utilisateur**  
Periode de travail: Jan 2019

Calendar												Top Sites	Total	Groupe
2019												ANNEE	ANNEE	ANNEE
01	02	03	04	05	06	07	08	09	10	11	12	MOIS	MOIS	MOIS

Date	Groupe	Utilisateurs	Quota Dépassé	Octets	Moyenne	Hit %
08 Jan 2019	grp	1	0	5.7 M	5.7 M	0.00%
Total/Moyenne:		1	0	5.7 M	5.7 M	0.00%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL