Documentation technique Pfsense

Table des matières

[Introduction 3](#_Toc135492913)

[1.Configuration de la machine 3](#_Toc135492914)

[2. Configuration des interfaces 4](#_Toc135492915)

[3. Configuration des règles 5](#_Toc135492916)

[3.1 Règle NAT 5](#_Toc135492917)

[3.2 Règle WAN 5](#_Toc135492918)

[3.3 Règle LAN 6](#_Toc135492919)

[3.4 Règle Lan-DMZ 6](#_Toc135492920)

[4. Configuration du LDAP 6](#_Toc135492921)

[4.1 Déclarer l’annuaire Active Directory sur pfSense 6](#_Toc135492922)

[4.2. Tester l'authentification AD 9](#_Toc135492923)

[4.3 Déclarer le groupe local dans pfSense 10](#_Toc135492924)

[4.4 Attribution des droits au groupe local 11](#_Toc135492925)

[4.5 Définir notre serveur AD pour l’authentification 12](#_Toc135492926)

[4.6 Tester la connexion à la WebGUI pfSense avec un compte AD 13](#_Toc135492927)

[5. OpenVPN 14](#_Toc135492928)

[5.1 Certificat d’autorité 14](#_Toc135492929)

[5.2 Certificat de serveur 15](#_Toc135492930)

[5.3 Serveur VPN 17](#_Toc135492931)

[5.4 Création du VPN Client 20](#_Toc135492932)

[5.5 Exporter notre configuration vpn 23](#_Toc135492933)

[6. Backup 25](#_Toc135492934)

[7. Restauration 26](#_Toc135492935)

[8. Bonne pratique 26](#_Toc135492936)

# Introduction

La VM Pfsense sers de pare-feu entre notre infrastructure et internet.

Sur la VM nous avons 4 cartes réseaux, 3 pour notre réseaux interne et un pour notre réseaux wan.

# 1.Configuration de la machine

Voici les caractéristiques de la machine Pfsense :

Processors :

1 Processeur

1 Cœur par processeur

2GB de memoire ram

Disque de 30 Go

Voici la configuration des interfaces Pfsense à nos cartes réseaux :

em0    = Bridged (WAN)      = 192.168.1.0/24     = Le réseau de ma machine hôte

em1    = LAN-Serveurs       = 192.168.10.1/24    = Le réseau LAN pour les serveurs

em2    = LAN-Users          = 192.168.20.1/24    = Le réseau LAN pour les Utilisateurs

em3    = LAN-DMZ            = 192.168.99.1/24    = Le réseau de la DMZ

Voici la configuration de nos 4 cartes réseaux :

NetWork Adapter      = Bridged            = 192.168.1.99/24

NetWork Adapter 2    = LAN\_Serveurs       = 192.168.10.1/24

NetWork Adapter 3    = LAN\_Users          = 192.168.20.1/24

NetWork Adapter 4    = LAN\_DMZ            = 192.168.99.1/24

# 2. Configuration des interfaces

Une image contenant texte

Description générée automatiquement

Tapez «**1** » pour «**Assign Interfaces**» <Entrée> pensez à activer le pavé numérique. Les 4 cartes réseaux, (WAN y compris) devrait s’afficher.

Should VLANs be set up now [y|n]? **n**

Enter the WAN interface name or 'a' for auto-detection: **em0**

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(em1 em2 em3 em4 a or nothing if finished): **em1**

Enter the Optional 1 interface name or 'a' for auto-detection

(em2 em3 em4 a or nothing when finished): **em2**

Enter the Optional 2 interface name or 'a' for auto-detection

(em3 em4 a or nothing when finished): **em3**

Enter the Optional 4 interface name or 'a' for auto-detection

( a or nothing when finished): **<Entrée>**

The interfaces will be assigned as follows:

WAN  -> em0

LAN  -> em1

OPT1 -> em2

OPT2 -> em3

Do you want to proceed [y|n]? y

Tapez « **2**» pour « **Set interface(s) IP address**» <Entrée>

Enter the number of the interface you wish to configure: **1**

Configure IPv4 address WAN interface via DHCP? (y/n) **n**

Enter the new WAN IPv4 address. Press <ENTER> for none:

> **192.168.1.41**

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.

**255.255.255.0 = 24**

255.255.0.0   = 16

255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):

> **24**

For a WAN, enter the new WAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

> **192.168.1.254**

Configure IPv6 address WAN interface via DHCP6? (y/n) **n**

Enter the new WAN IPv6 address. Press <ENTER> for none:

> **<Entrée>**

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) **y**

Please wait while the changes are saved to WAN...

Reloading filter...

Reloading routing configuration...

DHCPD...

Restarting webConfigurator...

**The IPv4 address has been set to 192.168.1.41/24**

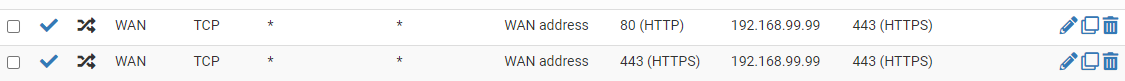
Press <Enter> to continue. **<Entrée>**

Faire pareil pour les 3 autres interfaces.

# 3. Configuration des règles

## 3.1 Règle NAT

Pour nos règles on va rediriger les requêtes http et https du port Wan vers notre serveur web avec des règles NAT :



On fait cela pour recevoir les certificats SSL pour notre serveur web.

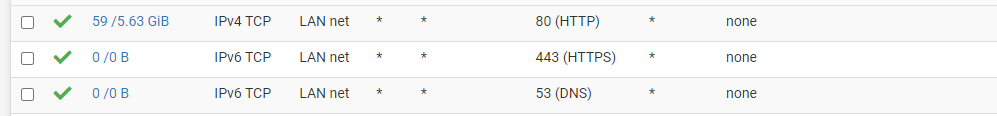
## 3.2 Règle WAN

Ensuite nous avons fait une règle pour autoriser le VPN SSL du coté de notre Wan :



## 3.3 Règle LAN

Pour les règles LAN on autorise les requêtes http, https et dns pour internet.



## 3.4 Règle Lan-DMZ

Pour les règles Lan-DMZ on fait passer les requêtes pour le serveur mail et aussi les requêtes pour

Internet.

Une image contenant texte, capture d’écran, Police, nombre

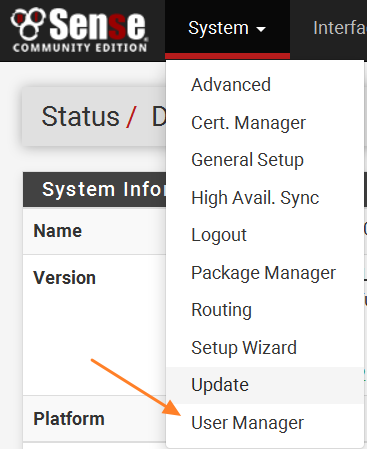
Description générée automatiquement

# 4. Configuration du LDAP

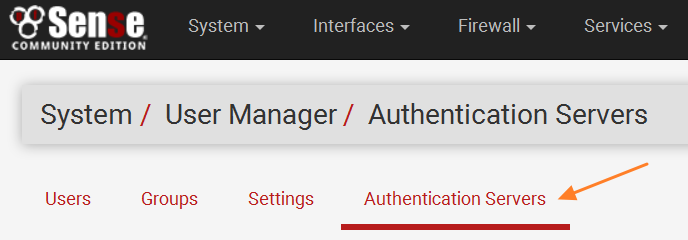
## 4.1 Déclarer l’annuaire Active Directory sur pfSense

Se connecter au WebGUI du pfSense avec un compte administrateur.

Cliquez sur le bouton "System" puis "User Manager" qui permet de gérer les utilisateurs et les groupes pfSense, ainsi que de configurer un serveur d'authentification.



Cliquez ensuite sur "*Authentication Servers*".



Les trois copies d'écran qui suivent font partie de la même page de configuration. Tous les paramètres n'ont pas besoin d'être modifiés.

* **Descriptive name** : Indiquez un nom pour ce serveur.
* **Type** : Indiquez "LDAP" qui est le choix par défaut de pfSense.
* **Hostname or IP address** : Indiquez l’IP

C'est tout pour cette première partie.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Voici la suite du paramétrage :

* **Search Scope** : Laissez "*Entire Subtree*" pour le scope de recherche, puis pour la "Base DN" indiquez la racine de votre AD.
* **Authentication containers** : Indiquez une ou plusieurs OU dans lesquelles pfSense peut regarder pour trouver les utilisateurs qui tentent de se connecter.

Ensuite décochez l'option de "*Bind anonymous*" on va plutôt s'authentifier pour requête l'AD. Au préalable, nous avons créé un compte pfsenseadmin pour pouvoir s’identifier avec.

Pour récuperer le DN de l’utilisateur on tape la commande suivante en powershell sur notre serveur AD :

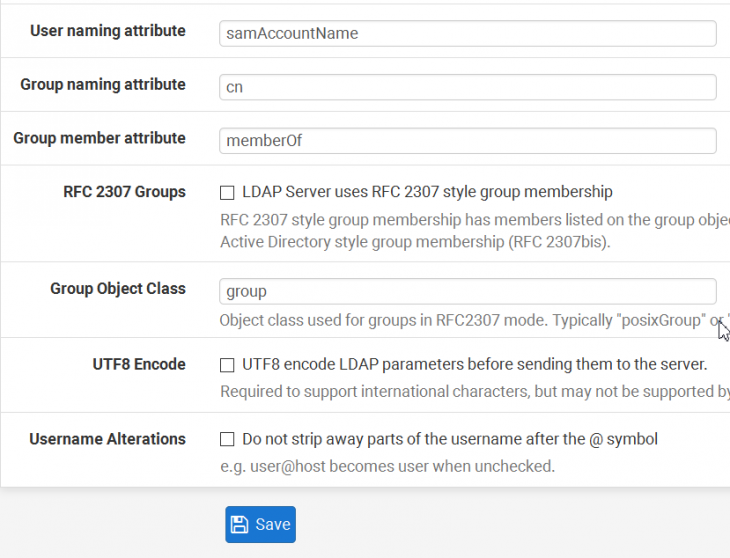
(get-aduser -filter 'samaccountname -eq "pfsense.connect"').DistinguishedName

Copiez ensuite la valeur retournée dans le champ "*Bind credentials*" de la conf pfSense, puis sur le champ juste à droite indiquez le mot de passe associé à ce compte.

Une image contenant texte, Police, capture d’écran, nombre

Description générée automatiquement

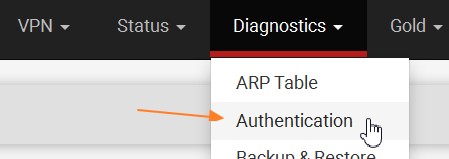
Vous pouvez seulement indiquer "*group*" à la place de "*posixGroup*", et veillez à ne pas cocher l'option "*LDAP Server uses RFC 2307 style group membership*" sinon pfSense ne pourra pas récupérer le nom du groupe auquel appartient votre utilisateur.



Sauvegardez la configuration avec le bouton "Save".

## 4.2. Tester l'authentification AD

Dans le menu "*Diagnostics*", cliquez sur "*Authentication*".



Choisissez votre AD comme serveur d'authentification puis tester un login et un mot de passe qui est censé fonctionner.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Cliquez sur "Test", si tout est OK vous devriez obtenir ce message :

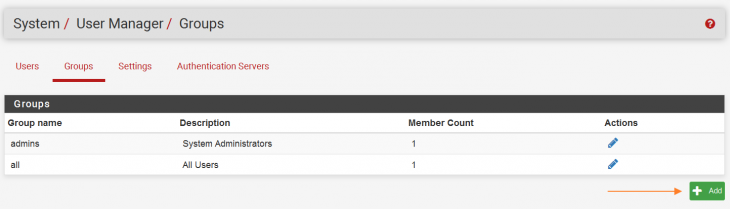
Une image contenant texte, capture d’écran, Police

Description générée automatiquement

## 4.3 Déclarer le groupe local dans pfSense

Il faut créer un groupe local qui aura le même nom que le groupe Active directory

Dans System, User Manager, accédez à l'onglet "Groups" et cliquez sur "Add".



Nommez le groupe comme celui de l’AD, donc dans notre cas on note pfsense.

Pour le scope on choisit Remote.

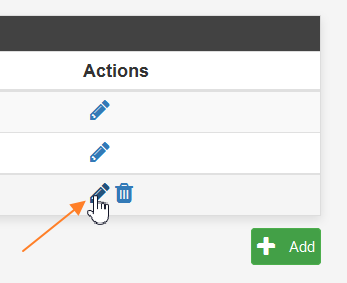
Et on sauvegarde

Une image contenant texte, capture d’écran, logiciel, nombre

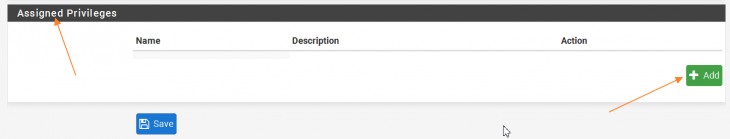
Description générée automatiquement

## 4.4 Attribution des droits au groupe local

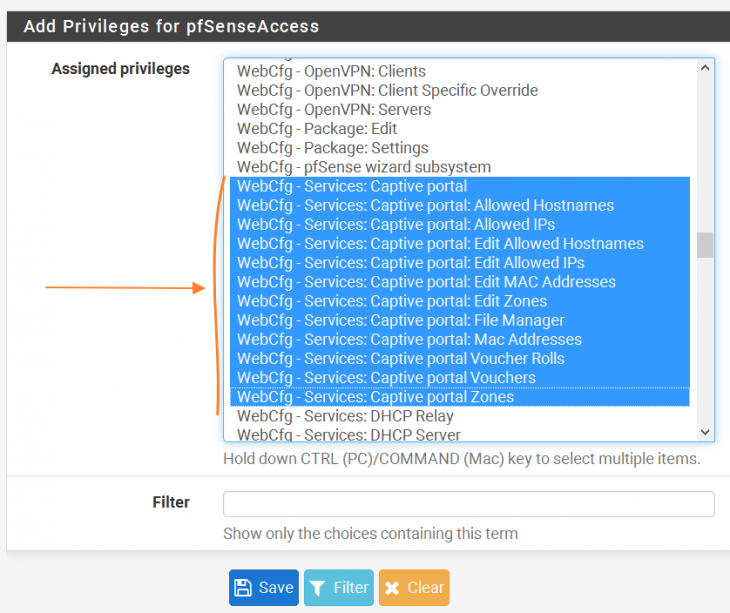
Toujours dans la gestion des groupes, cliquez sur l'icône en forme de crayon pour éditer le groupe fraîchement créé.



Descendez au niveau de la section "Assigned Privileges" et cliquez sur "Add".



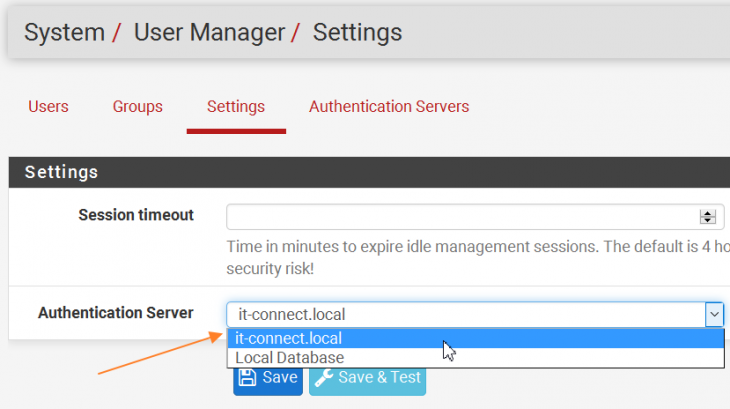
Ensuite, toute la liste des privilèges apparaît, voici ce qu'il faut sélectionner :



On aurait pu ajouter d'autres privilèges pour accéder à la partie log du portail captif. Cliquez sur "Save" dès lors que votre sélection est effectuée.

## 4.5 Définir notre serveur AD pour l’authentification

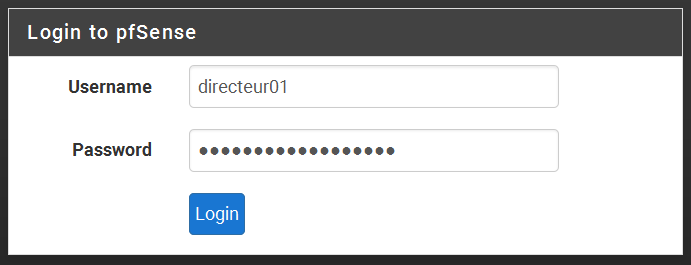
Cette étape de la configuration est indispensable sinon la connexion à pfSense s'appuiera sur la base locale et non sur l'AD. Toujours dans System / User Manager / Settings, définissez l’AD. Puis, sauvegardez.



Cette étape est déjà terminée, maintenant il va falloir tester cette config.

## 4.6 Tester la connexion à la WebGUI pfSense avec un compte AD

Ouvrez un navigateur et accédez à la page de connexion de pfSense. Ensuite, tentez de vous connecter avec un compte AD :



# 5. OpenVPN

## 5.1 Certificat d’autorité

On créé un certificat d’autorité pour créer nos certificats de serveurs et d’utilisateurs.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

## 5.2 Certificat de serveur

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

## 5.3 Serveur VPN

Le serveur VPN va utiliser la base de données server-AD qui est notre base de données AD. On utilise donc l’authentification par User Auth. On utilise aussi le port local 1360 pour faire passer les requêtes

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, document, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, ligne, Police

Description générée automatiquement

## 5.4 Création du VPN Client

Nous allons créer un VPN client pour tous nos users.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

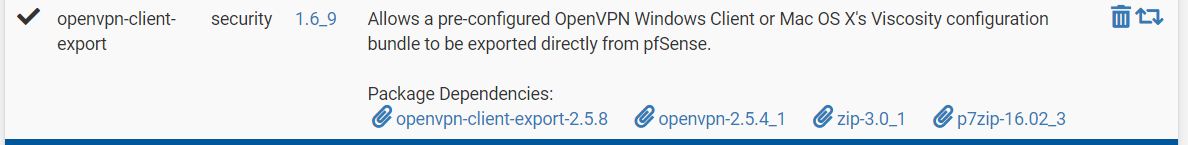
Description générée automatiquement

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## 5.5 Exporter notre configuration vpn

Il faut d’abord installer le package suivant :



Ce package va nous permettre d’exporter notre configuration pour le VPN.

Ensuite nous allons dans OpenVPN puis dans Client Export.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Puis on export le certificat

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

# 6. Backup

Créer un compte de backup :



Puis il faut lui affecter le droit suivant :

* WebCfg - Diagnostics: Backup & Restore

On crée donc un groupe backup et on attache le droit ci-dessus

On utilise un script pour récupérer la configuration du pfSense.

Ce script est fourni dans le github de blogmotion (<https://github.com/blogmotion/bm-backup-pfsense>)

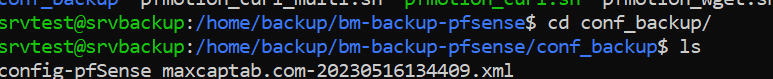
Ce script permet de récupérer la conf du pfsense et d’automatiser le backup avec du CRON.

Voici le résultat :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Si on se dirige dans le dossier on aperçoit le backup :



# 7. Restauration

Pour restaurer pfSense on a 2 choix :

* Utiliser les commandes pfSense pour restaurer une configuration récente
* Utiliser le Backup effectuer par le script pour réaliser la restauration

# 8. Bonne pratique

Nous utilisons, pour le VPN, toujours l’authentification par certificat + database.

Nous avons créé un serveur VPN exclusivement pour les administrateurs pour pouvoir utiliser le ssh et le rdp avec les machines présentes dans l’infra. Il a aussi accès en web a pfSense.

On utilise des comptes spéciaux pour les backups