2016

PF Sense : Portail Captif

Ahmed Ibnoussina

SISR2

17/10/2016

Sommaire

PF Sense : Portail captif

Introduction

Mise en place d'un portail captif avec l'aide de PF Sense

Contexte

Dans le but de sécuriser l'accès à internet via le réseau mobile de l'entreprise et donc éviter tous connexion et/ou utilisations non désirés de cet accès à internet.

Nous allons mettre en place un portail captif qui permettra de limiter les accès internet sur le réseau aux postes sans fil, cette solution obligera les utilisateurs à indiquer leur compte utilisateur personnel pour bénéficier d'un accès à internet.

Pour cela nous utiliserons la distribution PF Sense pour mettre en place différents mode d'authentification :

- ➔ Sans authentification
- ➔ Avec authentification locale
- ➔ Authentification par l'intermédiaire d'un serveur LDAP
- ➔ Authentification par l'intermédiaire d'un serveur AD

Pré-requis

- Une machine sous PFSense avec 3 interfaces réseau
  - 3 interfaces réseau (WAN, LAN et OPT1)
  - 1 GO de mémoire vive
  - 500 Mo d'espace disque

- Une machine pour l'administration du PFSense (Windows 7)

- Une machine cliente (Windows 7)
  - Une carte Wifi est nécessaire

- Un serveur Windows 2012 R2
  - Disposant d'une AD avec des groupes utilisateurs
  - Radius

- Un serveur Ubuntu 16.04
  - Disposant d'un LDAP avec des groupes utilisateurs
  - Freeradius

Adressage IP

- PF Sense :
  - WAN : DHCP
  - LAN : 192.168.1.1/24
  - OPT1 : 192.168.2.1/24

- Machine Admin
  - ETH1 : 192.168.1.2/24

- Machine Cliente
  - ETH1 : DHCP

- Windows Serveur 2012 R2
  - ETH1 : 192.168.1.10/24

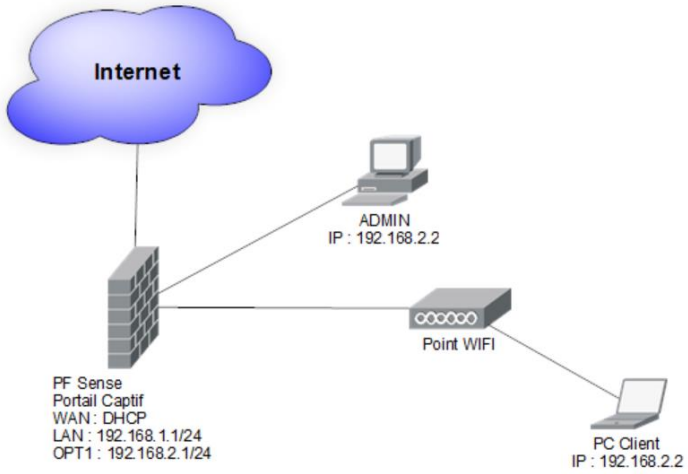
- Ubuntu Serveur 16.04
  - ENPS03 : 192.168.1.3/24

Sans authentification

La mise en place d'un portail captif sans authentification va permettre aux utilisateurs de pouvoir se connecter aux réseaux wifi de l'entreprise sans avoir besoin de fournir d'identifiant ou de mot de passe.

Elle n'est donc pas recommandée par mesure de sécurité mais elle peut être cependant très utile pour faire des tests après la mise en place du portail captif et vérifier son bon fonctionnement.

Vous pouvez voir ci-dessous un schéma illustrant l'architecture nécessaire par le déploiement d'un portail captif sans authentification



Mise en place du portail captif

Dans un premier temps nous allons devoir configurer les interfaces réseaux comme ceci :

1ere carte (WAN) en DHCP

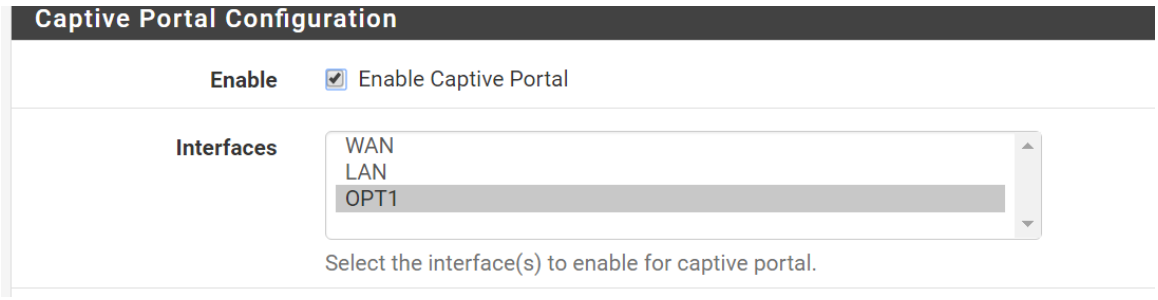
2eme carte (LAN) : 192.168.1.1/24

3eme carte (OPT1) : 192.168.2.1/24

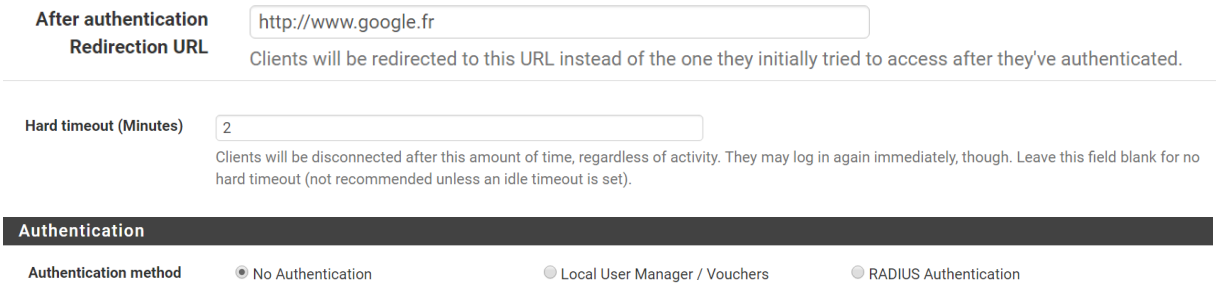
Par la suite nous allons nous connecter à l'interface navigateur via l'adresse ip LAN (192.168.1.1) pour ensuite nous rendre dans l'onglet service.

Dans cet onglet il faudra cliquer sur « Captive Portal » puis sur ADD pour commencer la mise en place du portail captif.

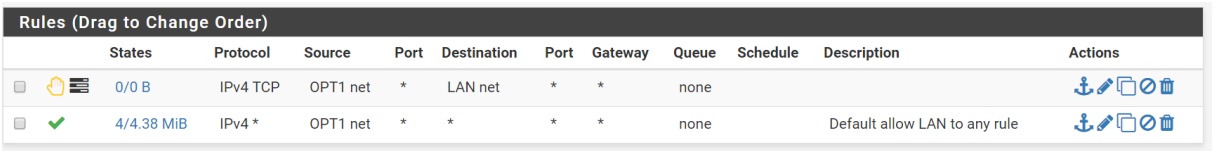
Cochez la case « enable captive portal » pour activer le portail captif par la suite il faudra choisir OPT1 comme interface pour le portail.



Pensez à mettre un temps limite de connexion et à indiquer une url de redirection, pour finir il faudra choisir le mode sans authentification et sauvegarder la configuration.



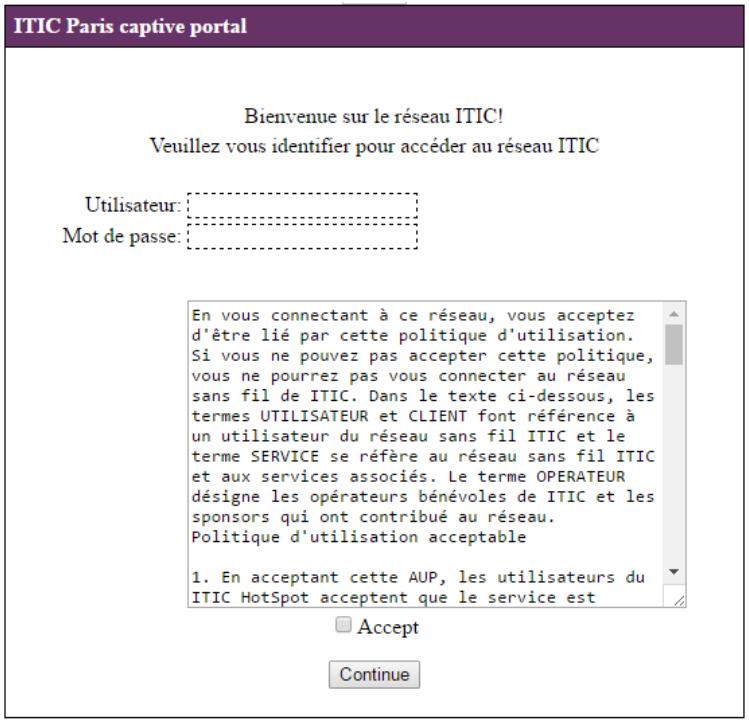
Avant de commencer à utiliser le portail captif nous allons devoir mettre en place certaines comme le montre l'image ci-dessous :



La première règle interdit les communications du réseau OPT1 vers LAN , la seconde permet d'avoir l'accès à toutes les destinations.

Test

Maintenant il faut juste lancer le navigateur depuis la machine cliente et si tout se passe bien le portail devrait apparaitre.



Ce portail ne nécessite aucune authentification vous pouvez donc juste cliquer sur « continue » pour pouvoir accéder à internet.

Avec authentification locale

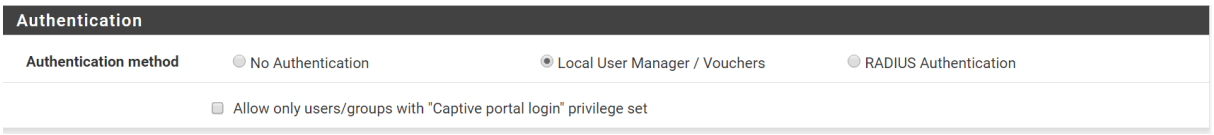
L'authentification locale est une option plus intéressante que la précédente, car elle permet de restreindre l'accès uniquement aux utilisateurs qui ont été renseigné dans la base d'utilisateurs de PF Sense.

Ce qui rend par conséquent le réseau wifi de l'entreprise moins accessible à d'éventuels intrus.

Le schéma d'infrastructure est le même que celui du mode sans authentification il y'a par conséquent aucunement besoin de modifier l'infrastructure déjà mise en place.

Configuration du portail captif

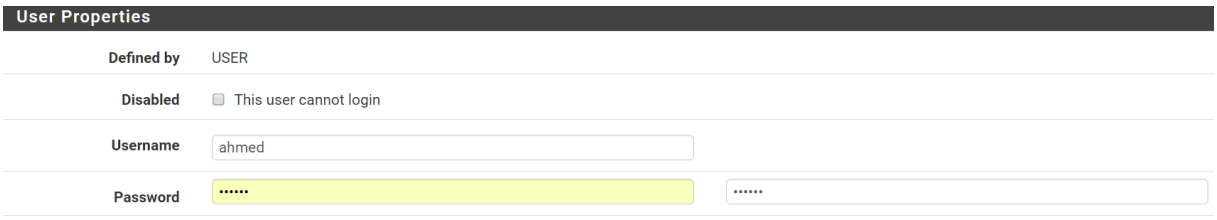
Comme dans la procédure sans authentification il faudra créer un portail avec la même configuration et les mêmes règles sauf bien sûr qu'il faudra cocher la case « Local User Manager / Vouchers »



Création des utilisateurs

Une fois ceci fait le portail demandera systématiquement un compte utilisateur pour pouvoir autoriser la connexion, pour le moment on ne peut que se connecter avec le compte ADMIN, nous allons donc devoir créer des utilisateurs pour pouvoir profiter du système d'authentification mis en place.

Pour cela nous allons devoir nous rendre dans system -> user manager et cliquer sur ADD pour lancer la création d'un nouvel utilisateur.



Nous avons juste à déclarer le nom d'utilisateur et le mot de passe.

Vous pouvez aussi mettre en place une date limite de validation pour le compte utilisateur ou encore le mettre dans un groupe d'utilisateur.

Enregistrer le nouvel utilisateur pour qu'il puisse être disponible pour une nouvelle session

Test

Sur votre machine cliente il vous suffit de lancer votre navigateur vous aurez donc un portail qui s'affiche comme avec le portail sans authentification.

La différence avec ce portail est que si vous tentez de simplement cliquer sur continuer ou de mettre un faux utilisateur un message d'erreur survient.

Invalid credentials specified.

En revanche si vous vous connecter avec l'utilisateur précédemment crée vous aurez accès à la page de redirection.

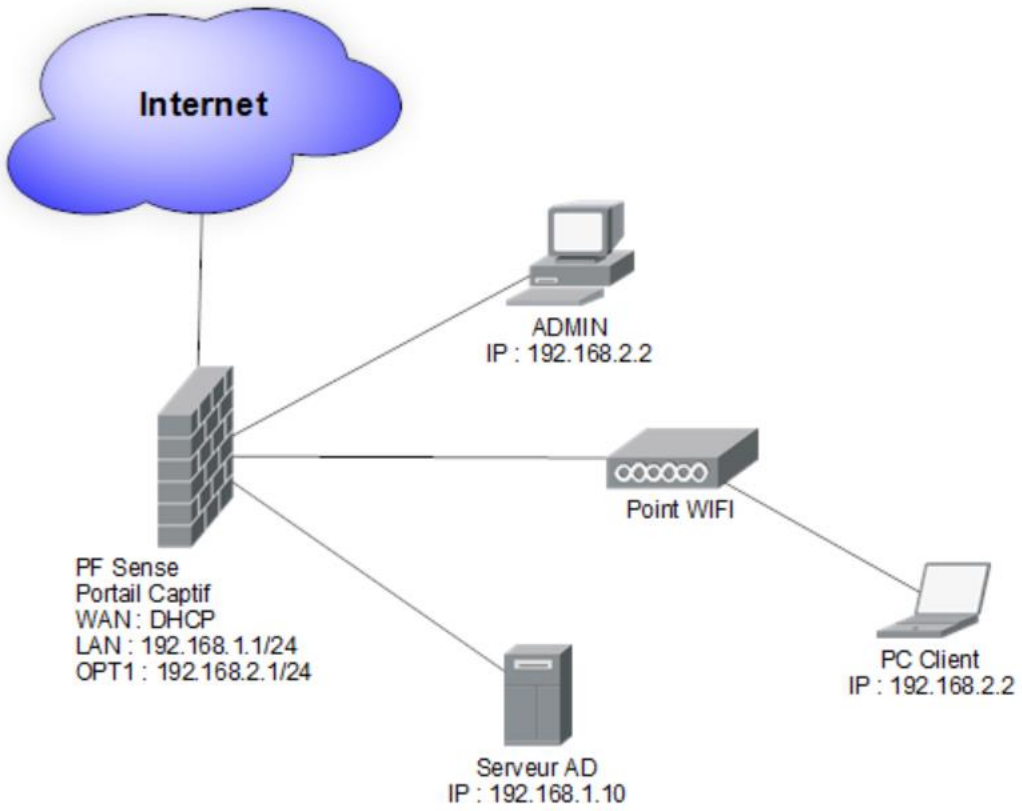
Authentification par l'intermédiaire d'une AD

Ce mode d'authentification va nous permettre d'utiliser une base d'utilisateurs/groupes déjà existant.

Il est donc recommandable d'utiliser ce mode d'authentification si vous possédez un grand nombre de groupes ou d'utilisateurs déjà présent dans un des serveurs de l'entreprise disposant d'une AD.

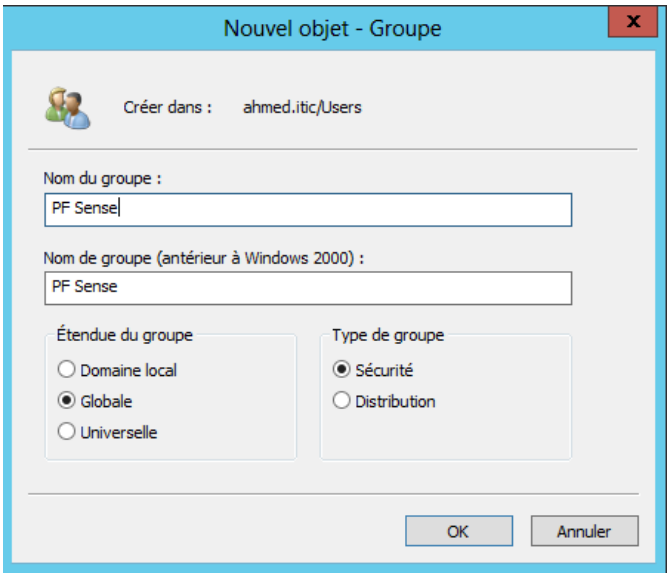
Il vous permettra d'éviter de devoir inscrire une seconde fois vos groupes/utilisateurs sur PF Sense.

Voici un schéma illustrant la nouvelle infrastructure nécessaire



Création du groupe utilisateur

Dans un premier temps nous allons créer un groupe nommé PF Sense pour pouvoir y mettre tous les utilisateurs qui seront apte à se connecter au réseau wifi de l'entreprise.

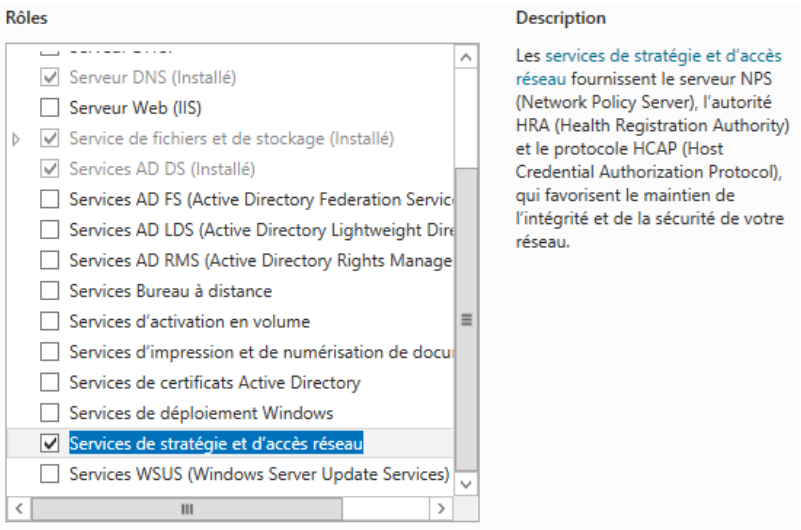


Installation du service Radius

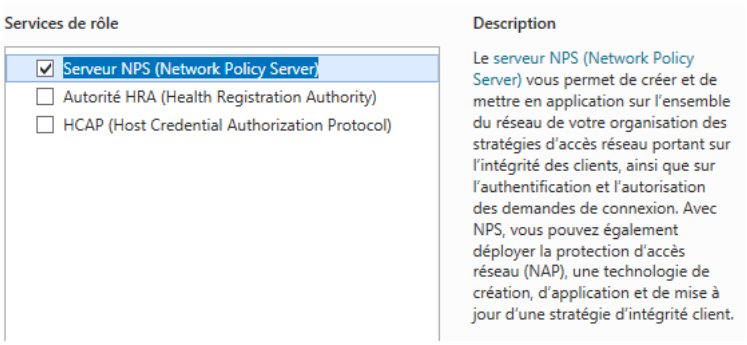
Une fois ceci fait nous allons pouvoir commencer la liaison entre l'AD et le portail captif de PF Sense grâce à l'intermédiaire du protocole Radius.

Le protocole Radius permet de rendre l'authentification possible entre l'AD et le portail captif, il a pour rôle de recevoir les données émises par le client au portail captif et de consulter l'AD pour valider ou non la véracité des données de l'utilisateur.

Nous allons donc dans un premier temps installer le rôle « Services de stratégie et d'accès réseau »



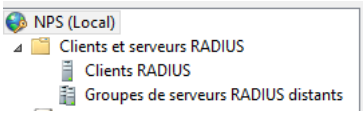
Par la suite il faut choisir le service de rôle «NPS »



Patientez pendant quelques instants jusqu'à la fin de l'installation.

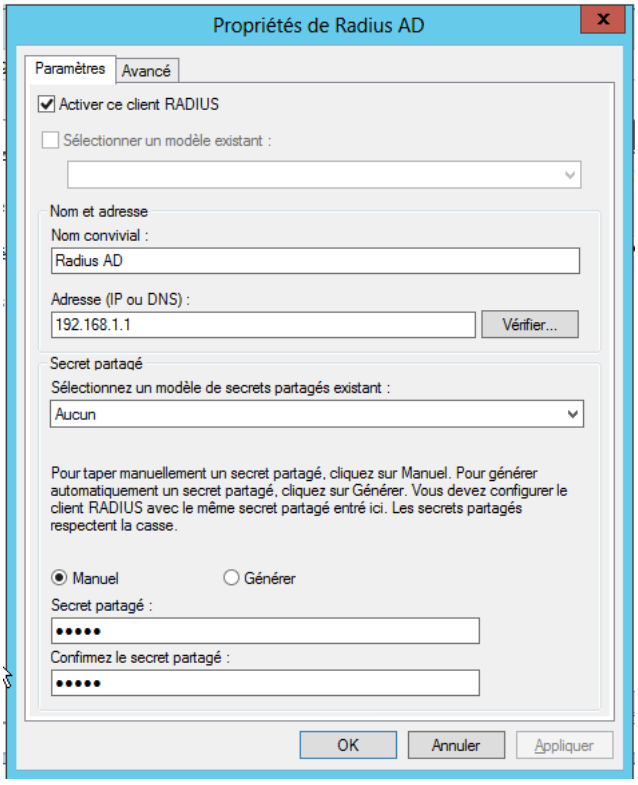
Une fois ceci fait nous allons pouvoir enfin commencer la mise en place du Radius dans un premier temps il faut se rendre sur la page du rôle que nous venons de créer.

Dans un premier temps il faut dérouler la partie « Clients et serveurs Radius »



Puis faire un clic gauche sur client Radius et cliquer sur nouveau.

Il faudra donc remplir les cases comme l'exemple ci-dessous :

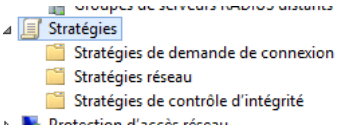


Dans la partie « Adresse » il faut renseigner l'adresse IP du client qui est pour notre part l'adresse de l'interface LAN de PF Sense.

Pour finir il faudra renseigner un « secret partagé » qui permettra la liaison avec le portail captif.

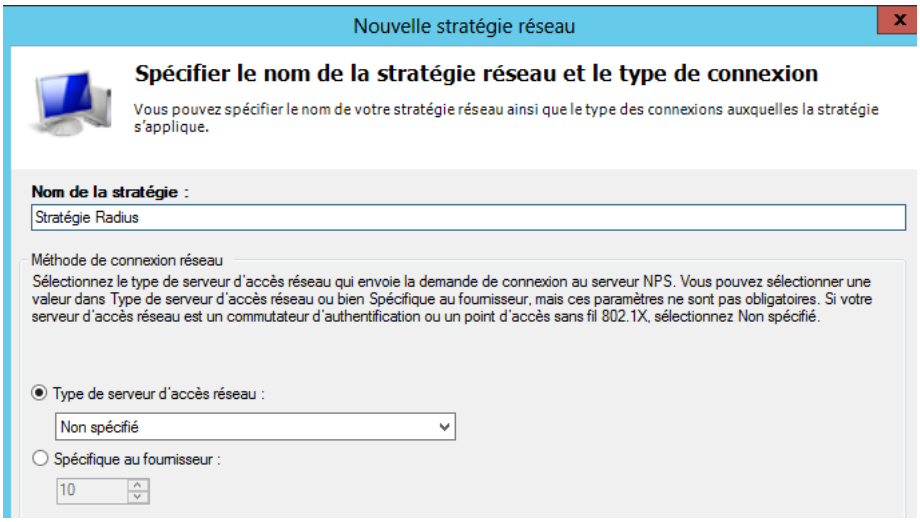
Nous allons maintenant devoir créer une stratégie pour le serveur Radius

Pour cela déroulez la partie « Stratégies »

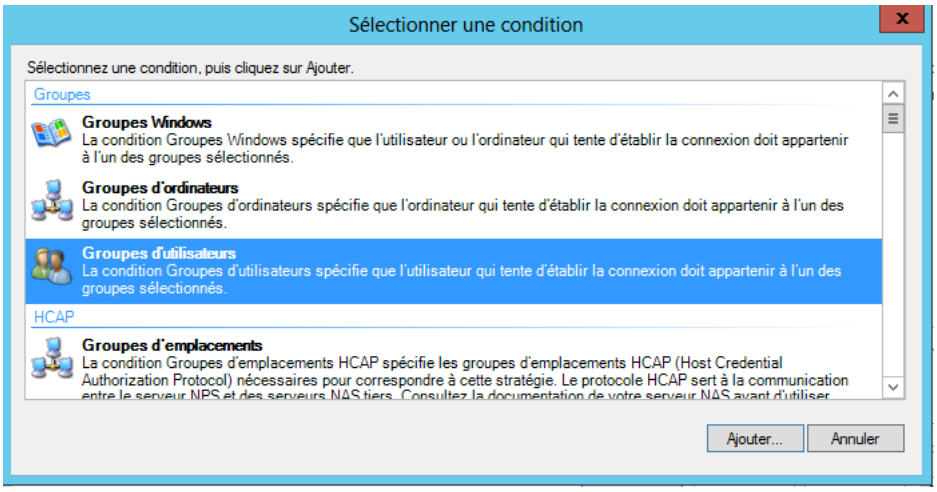


Et faites un clic droit sur « Stratégies réseau » et cliquez sur nouveau.

Choisissez un nom pour votre stratégie et laissez-le reste par défaut.

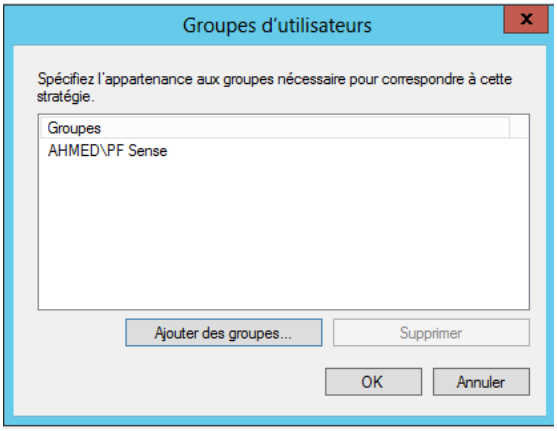


Par la suite vous devrez cliquer sur « ajouter » pour inscrire le groupe précédemment crée en choisissant la condition « Groupe d'utilisateurs »



Taper le nom du groupe concerner en utilisant la fonction « vérifier les noms » pour bien inscrire le bon groupe et éviter toute erreur.

Pour finir, cliquez sur « OK » pour valider la stratégie

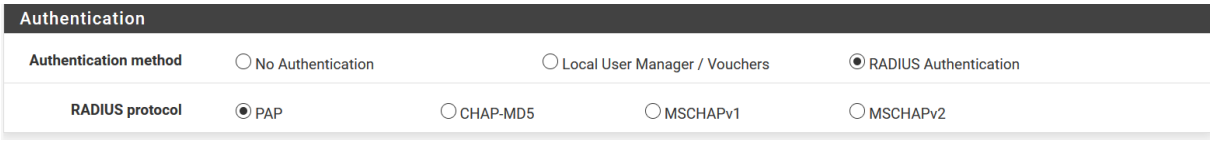


Configuration du Portail Captif

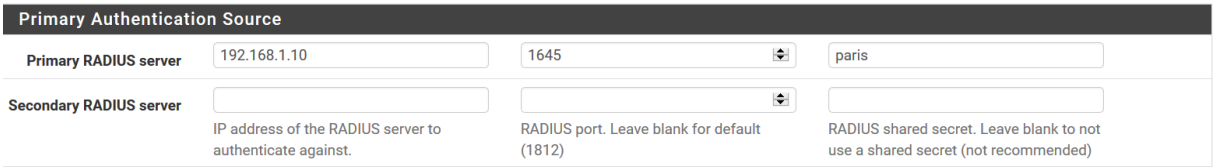
Maintenant nous allons devoir repartir sur PF Sense pour renseigner le nouveau serveur Radius pour qu'il soit enfin effectif.

Nous allons donc devoir modifier les paramètres de notre portail captif avec les éléments suivants :

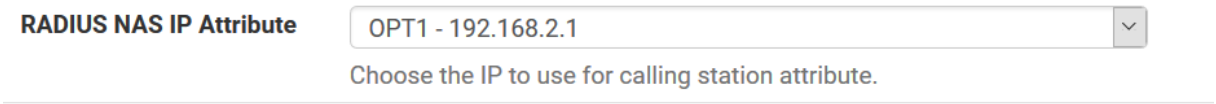
Cochez cette fois-ci « RADIUS Authentification et laissez le protocole par défaut « PAP »



Il faudra par la suite renseigner l'adresse IP du serveur Radius ainsi que le port 1645 et ne pas oublier de renseigner le secret partagé que nous avons choisi précédemment.



Pour finir il faudra juste choisir dans Radius IP NAS l'interface OPT1



C'est bon, vous devriez maintenant pouvoir vous identifiez via un compte utilisateur du groupe PF Sense de votre AD depuis la machine cliente.

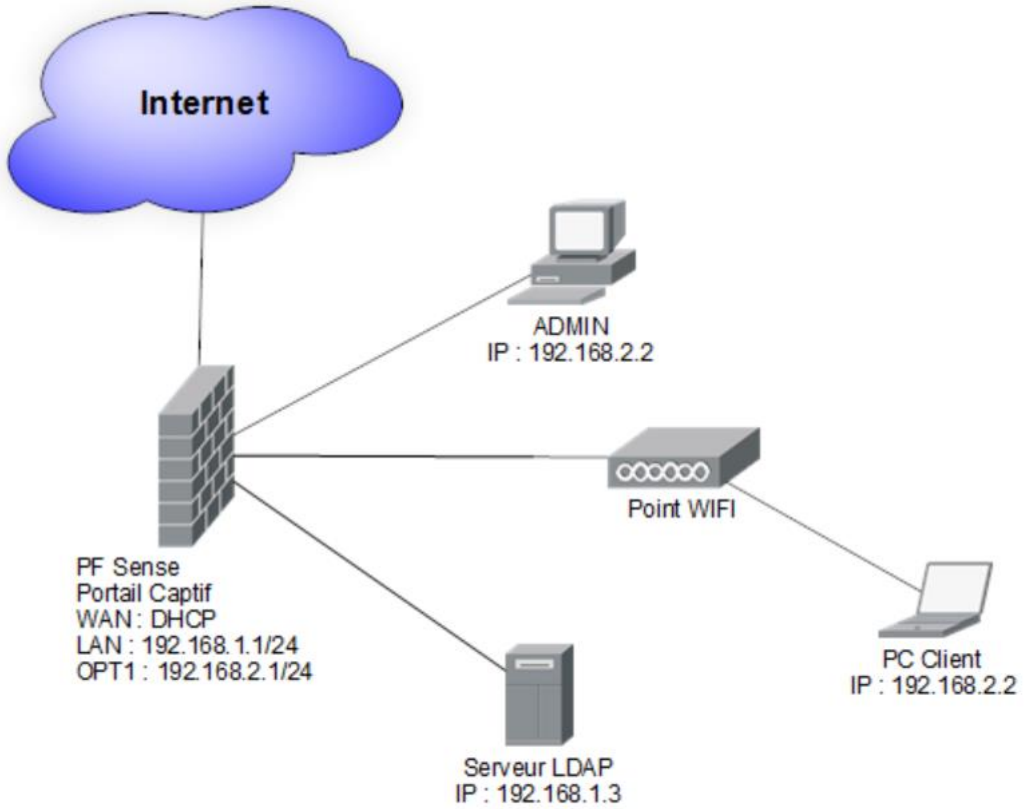
Authentification avec un serveur LDAP

Comme avec l'authentification avec AD, cette solution nous permet d'utiliser une base d'utilisateurs/groupes déjà existante.

La différence est que nous utilisons un système différent, une distribution Linux nommé Ubuntu Serveur. Par conséquent le paramétrage de ce dernier est très différent et moins accessible.

L'intérêt reste le même car il nous permettra de ne pas perdre du temps à taper un à un les utilisateurs mais plutôt d'utiliser l'un des serveur LDAP déjà existant de l'entreprise.

L'architecture est la même sauf que nous utilisons un serveur LDAP et non un serveur AD comme on peut le voir sur le schéma ci-dessous.



Installation de phpldapadmin

Avant de commencer nous allons installer le module phpldapadmin qui va nous permettre de manipuler le LDAP via une interface graphique.

Pour cela taper la commande suivante :

```
sudo apt-get phpldapadmin
```

Maintenant vous n'avez plus qu'à vous rendre à l'adresse suivante via votre navigateur web pour accéder de manière graphique au LDAP.

```
https://ipduserveur/phpldapadmin
```

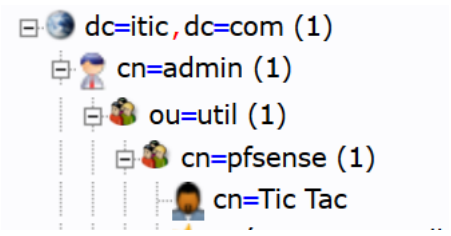
Vous devriez donc tomber sur cette page si tout se passe bien

Vous n'avez donc plus qu'à vous connecter avec le compte admin du nom de domaine de votre serveur LDAP

Création du groupe utilisateur

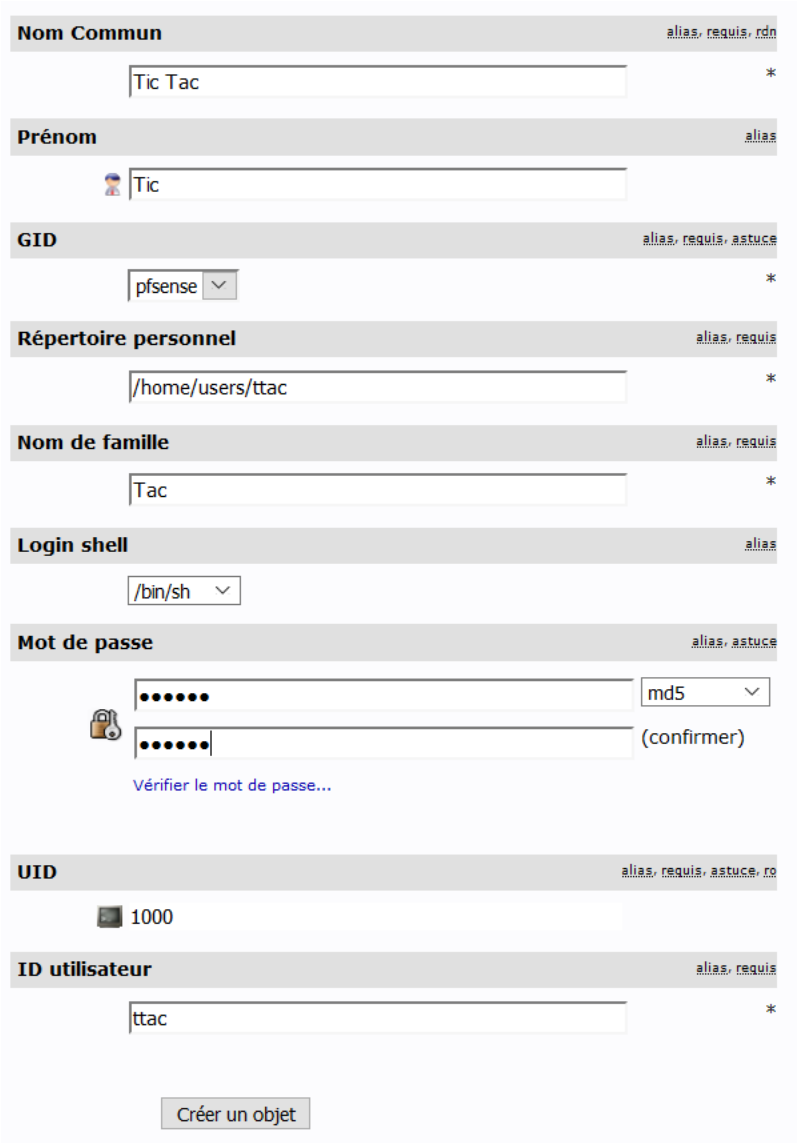
Nous allons maintenant pouvoir créer des utilisateurs et des groupes au sein du LDAP pour s'en servir comme compte utilisateur de notre portail captif.

Pour cela il faudra faire comme l'arborescence suivante :



C'est-à-dire qu'il faut dans premier temps créer une unité organisationnelle sous « cn=admin » et dans cette même unité créer un groupe posix avec un utilisateur.

Pour la création de l'utilisateur, vous pouvez suivre l'exemple suivant :



Une fois ceci fait nous allons pouvoir nous lancer dans l'installation de Freeradius

Installation de Freeradius

Comme le Radius de Windows Server, Freeradius va nous permettre de faire la liaison entre le LDAP et notre portail captif.

Sa mise en place est un peu plus complexe que son homologue Windows mais il a le même but que ce dernier.

Pour l'installer il va falloir sur votre serveur LDAP taper cette commande :

```
sudo apt-get install freeradius freeradius-ldap
```

Une fois ceci fait nous allons devoir modifier le fichier client.conf pour cela utiliser cette commande :

```
sudo nano /etc/freeradius/clients.conf
```

Puis il faudra ajouter les informations suivantes :

```
client 192.168.1.1/24 {
        secret          = paris
        shortname       = admin
}
```

Le client est l'interface LAN du PF Sense soit 192.168.1.1 et le secret est le fameux « secret partagé » qui va permettre la liaison entre le LDAP et le portail captif.

Par la suite nous allons devoir modifier le fichier LDAP dans le répertoire module de Freeradius

```
sudo nano /etc/freeradius/modules/ldap
```

Cherchez la partie LDAP du fichier et suivez l'exemple ci-dessous :

```
ldap {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = "192.168.1.3"
        identity = "cn=admin,dc=itic,dc=com"
        password = azerty
        basedn = "dc=itic,dc=com"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        #base_filter = "(objectclass=radiusprofile)"
```

Server = l'adresse du serveur LDAP

Identity = Compte qui va permettre au Radius de se connecter au LDAP

Password = le mot de passe de ce même compte

Basedn = La où se trouve l'annuaire LDAP

Par la suite il faudra modifier le fichier default

```
sudo nano /etc/freeradius/sites-available/default
```

Dans la partie authorize{ il faudra commenter le mot « files » qui a pour rôle d'utiliser un fichier pour authentifier les utilisateurs, comme nous utilisons un serveur LDAP pour ça nous allons donc désactiver cette fonction

```
#
#  Read the 'users' file
#files

#
#  Look in an SQL database.  The schema of the database
```

Ensuite il faudra dé-commenter le mot « ldap » pour autoriser l'authentification des utilisateurs par le LDAP

```
        #
        #  The ldap module will set Auth-Type to LDAP if it has not
        #  already been set
        ldap
```

Toujours dans le même fichier, vous allez devoir dé-commenter la partie « Auth-Type LDAP {…} » qui se trouve dans la section authenticate

```
# Uncomment it if you want to use ldap for authentication
#
# Note that this means "check plain-text password against
# the ldap database", which means that EAP won't work,
# as it does not supply a plain-text password.
Auth-Type LDAP {
        ldap
}
```

Une fois ceci il faudra juste redémarrer le service Freeradius avec la commande suivante pour que les modifications soient bien prises en compte.

```
sudo /etc/init.d/freeradius restart
```

C'est bon le Radius est bien mis en place et prêt à l'utilisation

Configuration du portail captif

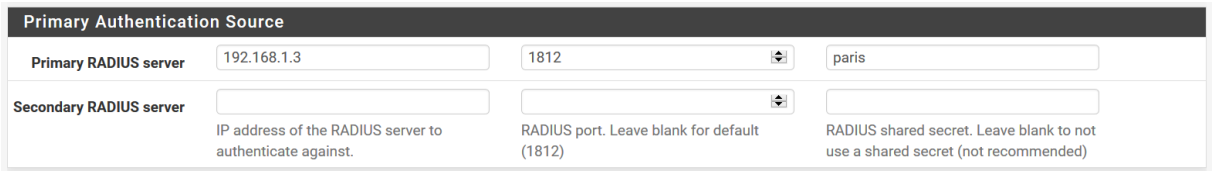
Maintenant nous allons nous occuper des quelques modifications à mettre en place directement sur PF Sense.

Nous allons donc aller sur le menu de configuration du portail captif et faire les modifications suivantes :

IP du serveur Radius : 192.168.1.3

Port : 1812

Secret partagé : paris

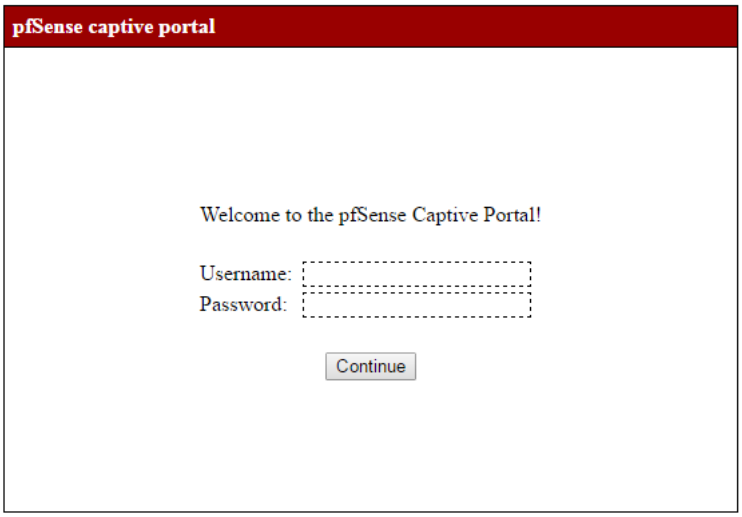


Le reste ne nécessite aucune modification et donc votre portail captif est par conséquent opérationnel.

Vous n'avez plus qu'à le tester avec votre machine cliente en utilisant l'un des compte utilisateur du LDAP.

Personnalisation de la page d'authentification

Maintenant que notre portail captif est opérationnel, vous pouvez vous rendre compte que la page par défaut de PF Sense peut paraitre sommaire.



Heureusement PF Sense propose de pouvoir importer sa propre page d'authentification, ceux qui peut être fort utile pour les entreprises souhaitent une page à l'image de leur entreprise ou encore pour passer un message à l'utilisateur comme par exemple la politique d'utilisation des ressources internet de l'organisation.

Je vais donc vous donner un bout de code que vous pourrez bien sur modifier à votre guise.

Ce bout de code contient un message de bienvenue, un encadré de saisi pour l'identifiant et le mot de passe, un encadré qui peut être utilisé pour y inscrire la politique de l'entreprise et pour finir une petite case à cocher pour attester que l'utilisateur accepte bien les règles d'utilisation.

```
<div id='loginbox'>
<table>
 <tr><td colspan="2"><center>Bienvenue sur le réseau ITIC!</td></tr>
<tr><td colspan="2"><center>Veuillez vous identifier pour accéder au réseau ITIC</td></tr>
 <tr><td> </td></tr>
 <tr><td align="right">Utilisateur:</td><td align="left"><input name="auth_user" type="text" style="border: 1px dashed;"></td></tr>
<tr><td align="right">Mot de passe:</td><td align="left"><input name="auth_pass" type="password" style="border: 1px dashed;"></td></tr>

<tr><td> </td></tr>
```

```
<tr><td></td><td><tr><td></td><td>

<tr><td></td><td><tr><td></td><td>

<P align="center"><TEXTAREA id="aup" name="aup" rows="15" cols="50">

#Politique ou règle d'utilisation…

</TEXTAREA>

</td></tr>

</tr>

</table>

<input id="iagree" type="checkbox" name="CHKBOX1" value="1">Accept</p>

<input name="accept" type="submit" value="Continue">

</div>
```

Une fois votre page créé, il faut vous rendre dans la configuration du portail captif et aller dans la section « HTML Page Contents » pour importer votre nouvelle page d'authentification.

Une fois ceci fait, voici un exemple de rendu.