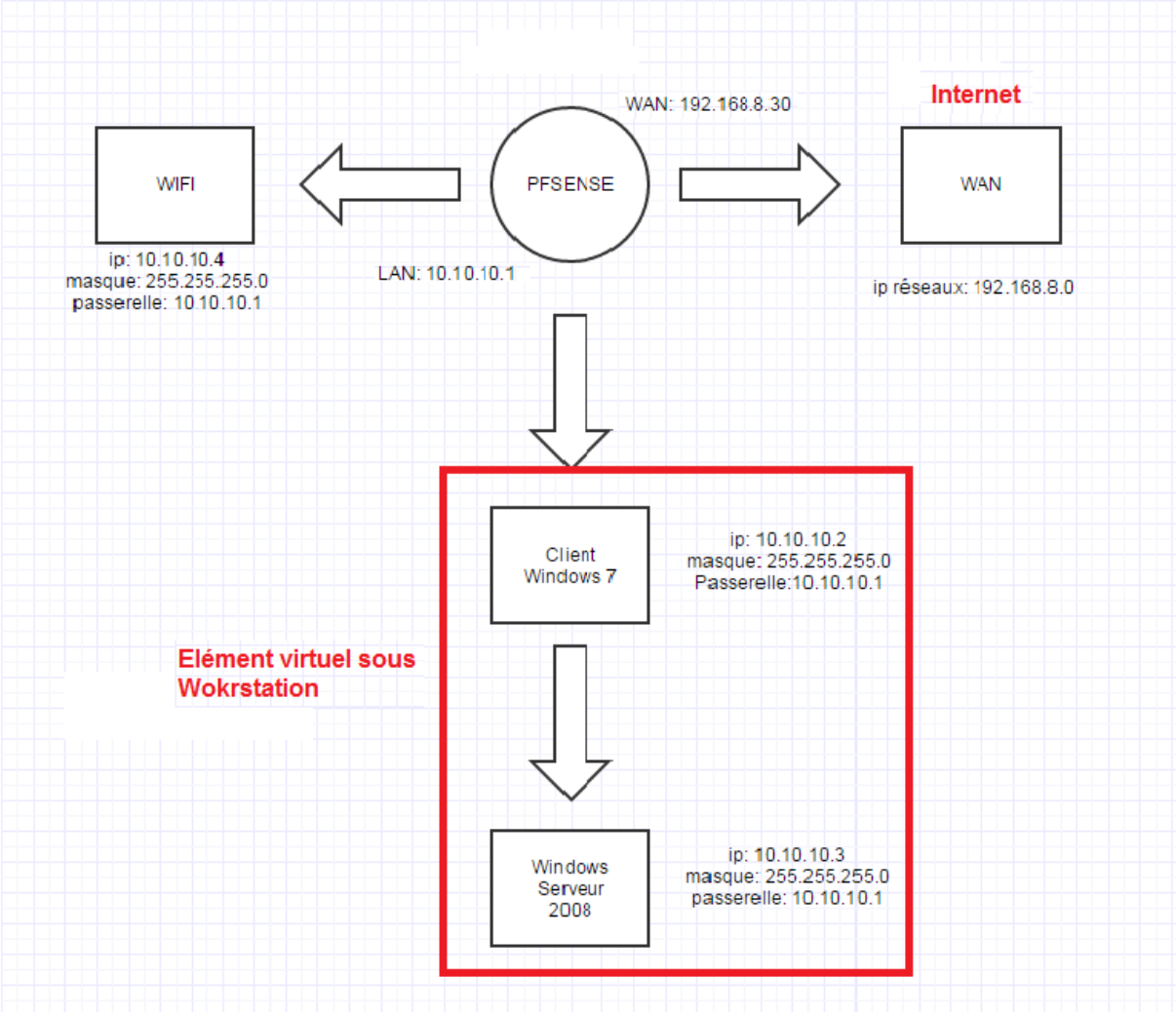
Mise en place d'un portail captif avec pfsense.

J'ai mis en place un portail captif à l'aide de Pfsense pour pouvoir sécuriser un accès sans fils (Wifi) pour que seuls les utilisateurs présents dans le répertoire AD puissent accéder à internet.

L'architecture du réseau comprend :
- Pfsense (Firewall/Routeur…) (Workstation)
- Un client Windows 7 (Workstation)
- Un Windows serveur 2008 (Workstation)
- Une borne WIFI

Voici un Schéma du réseau mise en place.



Nous prendrons comme situation un réseau d'entreprise appelé GSB qui sécurise son accès à internet à l'aide d'un portail captif, j'ai donc créé dans un répertoire Active Directory un groupe nommé « Groupe_GSB » ainsi que les utilisateurs de l'entreprise qui font partie de ce groupe sont :

Secretaire_GSB, Comptable_GSB, Inviter_GSB.

Le mot de passe que j'ai attribué à ces utilisateurs est p@ssw0rd.

1) Configuration Pfsense.

Il faut d'abord installer l'ISO pfsense, choisir le nombre d'interface que nous souhaitons installer (LAN et WAN) puis configurer ces interfaces, mes configuration sont les suivantes :

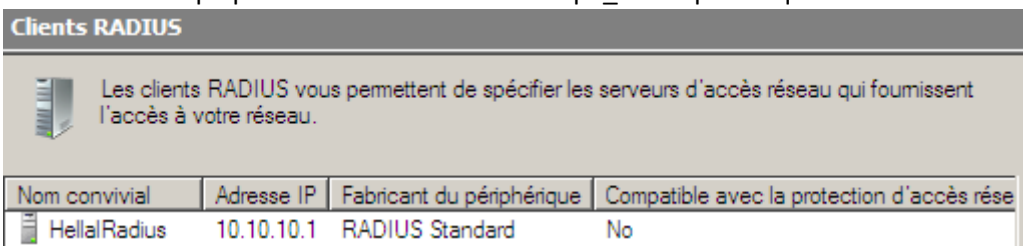
```
WAN (wan)       -> em0        -> v4: 192.168.8.30/24
LAN (lan)       -> em1        -> v4: 10.10.10.1/24
```

L'accès à l'interface graphique se fait via l'IP de l'interface LAN.

2) Installation RADIUS.

Tout d'abord il nous faut installer un serveur d'authentification (RADIUS) sur Windows Serveur 2008 qui permettra de lié Pfsense au répertoire d'Active Directory pour l'authentification, pour cela il faut ajouter un rôle :

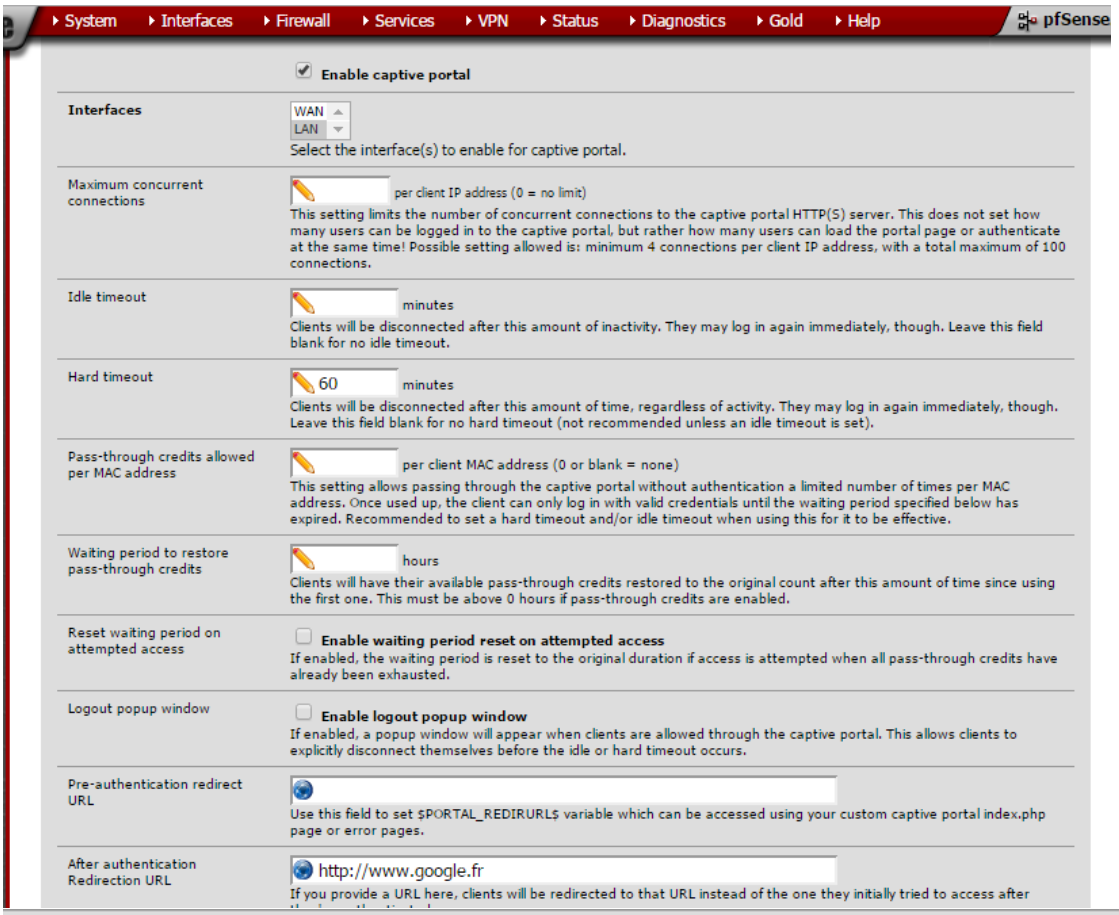
- en premier cocher « Service de stratégie et d'accès réseau »
- choisir le service NPS (Network Policy Server)
- configurer le rôle NPS « Serveur RADIUS pour les connexions câblées ou sans fils »
- choisir le type de configuration (pour nous se sera Connexions sans fils)
- attribuer un nom au client RADIUS, une adresse ip, et un secret partager qui sera à réécrire dans pfsense.
- choisir le protocole PEAP pour le transfert d'information sécurisé
- Choisir le Groupe précédemment créer « Groupe_GSB » puis cliquez sur terminer.



3) Mise en place du portail captif.

Une fois le serveur RADIUS configuré, il nous faudra configurer le portail captif dans les réglages de Pfsense. Aller dans Services > Captive Portal.

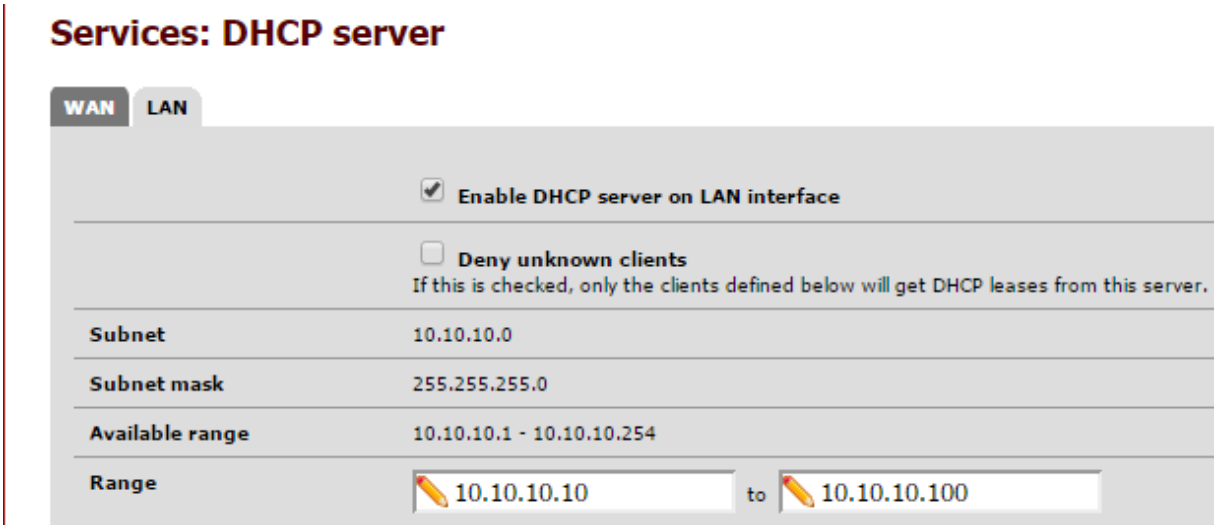
- Cocher la case « Enable captive portal » pour activer celui-ci
- Sélectionner l'interface sur lequel le portail se déploiera
- Il est possible de définir une durée limiter de connexion ainsi que de choisir une page sur laquelle nous serons rediriger après l'authentification (Redirection URL After Authentication)
- choisir la méthode d'authentification donc nous choisirons « RADIUS Authentication », il faudra entrer l'IP du RADIUS autrement dit l'adresse du serveur 2008 et mettre le même secret partager que lors de la configuration du Radius
- Il est également possible de personnaliser son portail captif et enfin sauvegarder la configuration.


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
pfSense
Enable captive portal
Interfaces
WAN
LAN
Select the interface(s) to enable for captive portal.
Maximum concurrent connections
per client IP address (0 = no limit)
This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.
Idle timeout
minutes
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout
60
minutes
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Pass-through credits allowed per MAC address
per client MAC address (0 or blank = none)
This setting allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.
Waiting period to restore pass-through credits
hours
Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.
Reset waiting period on attempted access
Enable waiting period reset on attempted access
If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
Logout popup window
Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL
Use this field to set $PORTAL_REDIRURL$ variable which can be accessed using your custom captive portal index.php page or error pages.
After authentication Redirection URL
http://www.google.fr
If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after


No Authentication
Local User Manager / Vouchers
Allow only users/groups with 'Captive portal login' privilege set
RADIUS Authentication
Radius Protocol
PAP
CHAP_MD5
MSCHAPv1
MSCHAPv2
Primary Authentication Source
Primary RADIUS server
IP address
10.10.10.3
Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.
Port
1812
Leave this field blank to use the default port (1812).
Shared secret
pfsense
Leave this field blank to not use a RADIUS shared secret (not recommended).

4) Activation serveur DHCP (Interfaces LAN)

Un serveur DHCP a été configuré pour attribuer des adresses allant de 10.10.10.10 à 10.10.10.100 pour toutes les personnes se connectant au réseau wifi.



Une fois le portail captif configuré il ne reste plus qu'à essayer en entrant dans le portail comme login un des utilisateurs créé dans le répertoire Active Directory (exemple : Secretaire_GSB) et en mot de passe p@ssw0rd.