Portail captif pfSense

I – Contexte

La ville d'Olonne sur mer accueille certains élus au sein de la Mairie. Ces élus viennent avec leurs terminaux mobiles qu'ils utilisent dans le cadre de leur travail (ordinateurs portables, Smartphones, tablettes…) et ont besoin d'un accès à internet. La plupart de ces terminaux utilisent le Wi-Fi afin de se connecter à Internet. Cependant, afin d'éviter tout abus, l'usage d'Internet est réglementé. Les lois Vigipirate et Hadopi2 imposent aux administrateurs réseaux de pouvoir identifier et tracer les navigations des utilisateurs.

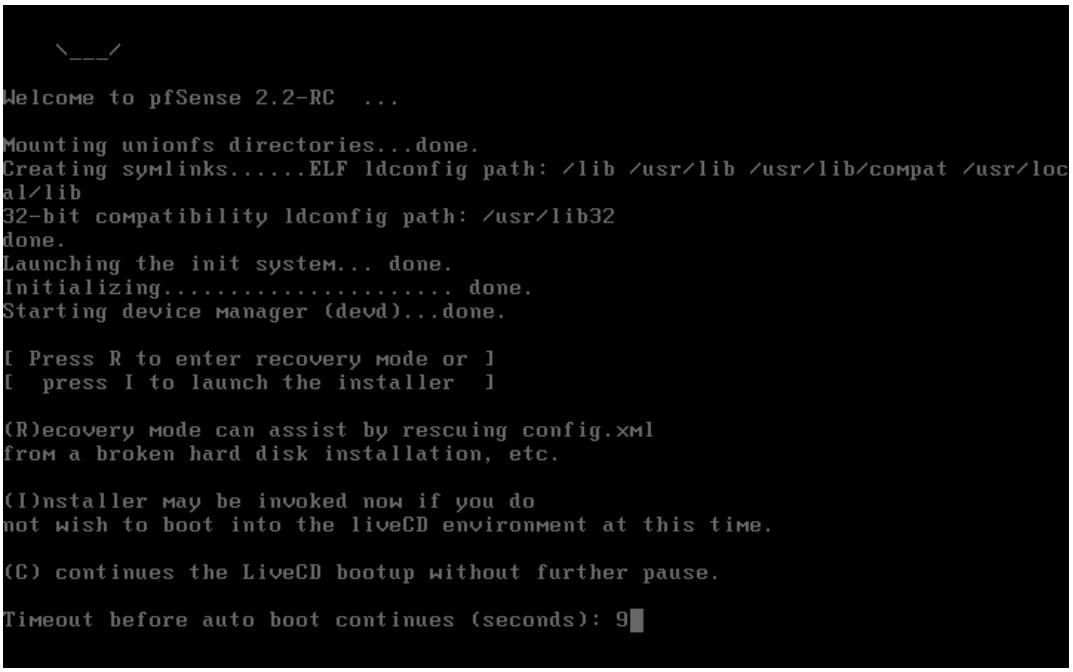
II - Définition du besoin

Les élus ayant besoin d'un accès internet sans fil, une borne wifi basique était installée. Hors la seule sécurisation était une clé WEP. Le but est de sécuriser le réseau. Pour cela, l'idée retenue a été la mise en place d'un portail captif, qui, une fois connecté au point d'accès, demande l'authentification avec les identifiants LDAP sur une page web. La borne d'accès quant à elle est remplacée par une borne avec sécurité WPA2-PSK. De plus, l'utilisation de ce portail captif permet d'obtenir des informations sur les utilisateurs. En effet, il permet d'avoir connaissance des utilisateurs connectés.

III – Installation

Installation de pfSense

Booter sur une clé USB contenant l'ISO de pfSense puis procéder à une installation classique :



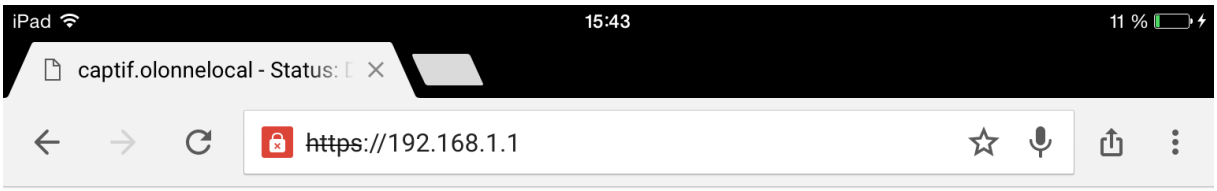
Configuration de pfSense

Une fois pfSense installé, la machine redémarre. Il faut alors débuter la configuration. Le premier élément de configuration est l'assignation des interfaces : il faut définir le LAN et le WAN. Le WAN est le côté du réseau de la Mairie, le LAN est le côté de la borne d'accès sans-fil, où viendront se connecter les postes clients.

L'adresse IP de la carte WAN va donc se configurer grâce au DHCP du réseau de la Mairie.

L'adresse IP de la carte LAN va se configurer par défaut en 192.168.1.1/24 que nous conserverons.

Une fois ceci fait, nous avons accès au tableau de bord de pfSense, configurable en mode web en tapant l'adresse de la carte LAN dans notre navigateur.



pfSense webConfigurator — captif.olonnelocal

System
Advanced
Cert Manager
Firmware
General Setup
High Avail. Sync
Logout
Packages
Routing
Setup Wizard
User Manager

Interfaces
(assign)
LAN
WAN

Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

Services
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server/RA
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP proxy
Load Balancer
NTP
PPPoE Server
SNMP
UPnP & NAT-PMP
Wake on LAN

VPN
IPsec
L2TP
OpenVPN
PPTP

Status
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
Filter Reload
Gateways
Interfaces
IPsec
Load Balancer
NTP
OpenVPN
Package Logs
Queues
RRD Graphs
Services
System Logs
Traffic Graph
UPnP & NAT-PMP

Diagnostics
ARP Table
Authentication
Backup/Restore
Command Prompt
DNS Lookup
Edit File
Factory Defaults
Halt System
Limiter Info
NDP Table
Packet Capture
pfInfo
pfTop
Ping
Reboot
Routes
SMART Status
Sockets
States
States Summary
System Activity
Tables
Test Port
Traceroute

Gold
pfSense Gold

Help
About this Page
Bug Database
Developers Wiki

Status: Dashboard

System Information

Name	captif.olonnelocal
Version	**2.2-RELEASE** (amd64) built on Thu Jan 22 14:03:54 CST 2015 FreeBSD 10.1-RELEASE-p4 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Celeron(R) CPU 1037U @ 1.80GHz 2 CPUs: 1 package(s) x 2 core(s)
Uptime	01 Hour 01 Minute 36 Second
Current date/time	Mon Feb 9 14:42:59 UTC 2015
DNS server(s)	127.0.0.1 10.0.12.1
Last config change	Mon Feb 9 14:21:09 UTC 2015
State table size	0% (8/804000) Show states
MBUF Usage	5% (1270/26584)
Temperature	27.8°C
Load average	0.00, 0.00, 0.00
CPU usage	1%
Memory usage	3% of 8049 MB
SWAP usage	0% of 16384 MB
Disk usage	/ (ufs): 1% of 39G /var/run (ufs in RAM): 3% of 3.4M

Interfaces

WAN (DHCP)	↓	none
LAN	↑	100baseTX <full-duplex> **192.168.1.1**

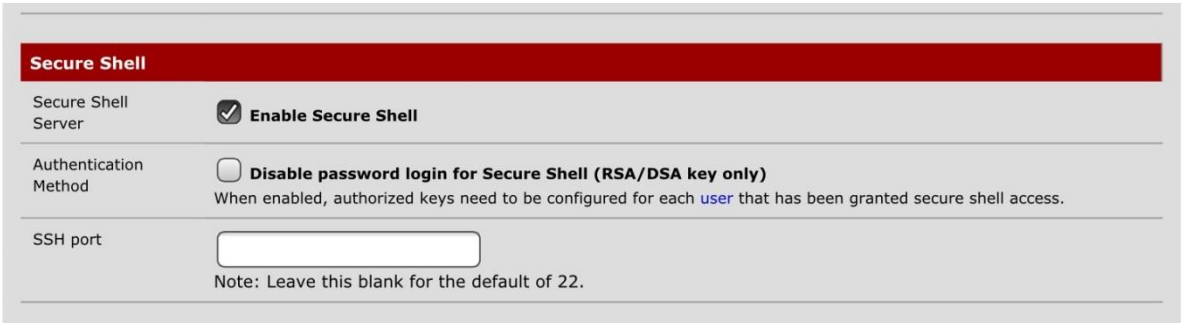
Sécurisation

Afin de sécuriser le portail captif, il est nécessaire de :

- *Utiliser le protocole https lors de l'accès au configurateur Web et modifier le port :*

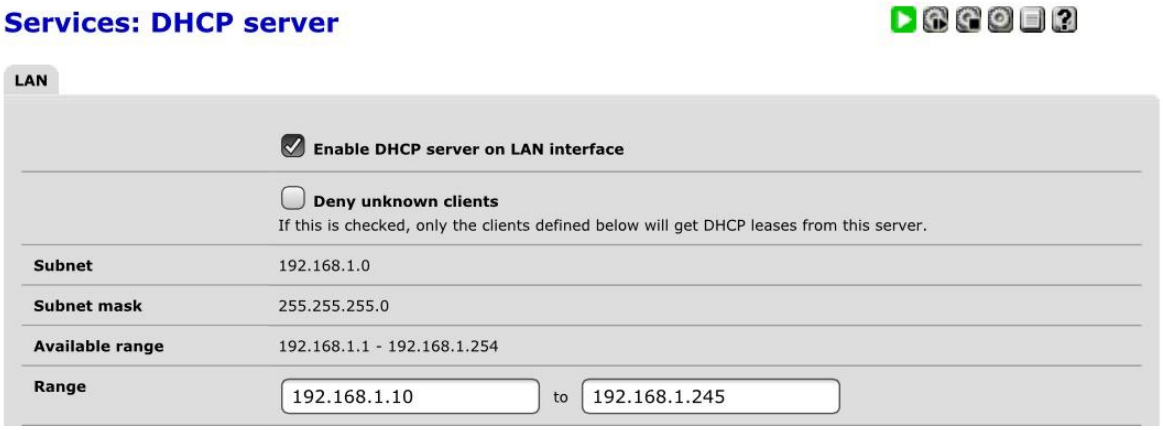
- *Activer l'utilisation du mot de passe pour protéger la console :*

- *Activer le ssh afin d'administrer le pfSense à distance :*



DHCP

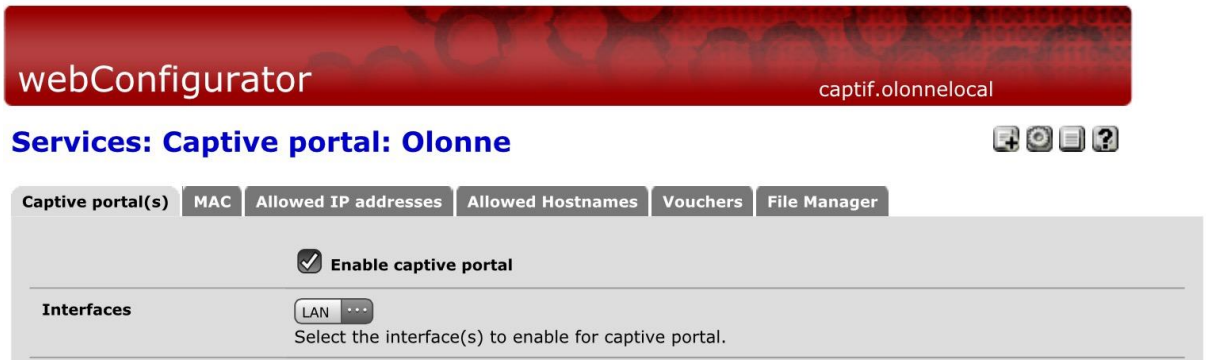
Les postes clients qui se connecteront à ce point d'accès sans fil auront besoin d'une adresse IP. Le réseau LAN (192.168.1.x) étant configuré différemment du réseau WAN (10.0.x.x) au point de vue plan d'adressage IP, il aura besoin de son propre DHCP. Il faut donc se rendre dans « DHCP Server » et activer ce service. La plage d'adresses attribuées est par défaut de 10 à 245 mais est bien sûr modifiable.



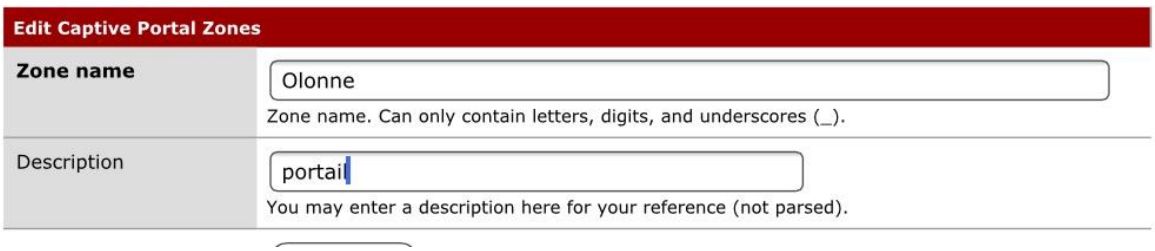
Portail captif

Configuration

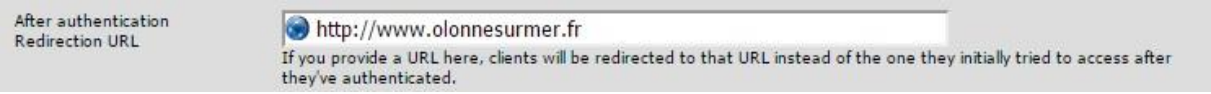
Activer le portail captif dans Services > Captive portal, puis choisir l'interface où l'on veut l'appliquer, ici le LAN



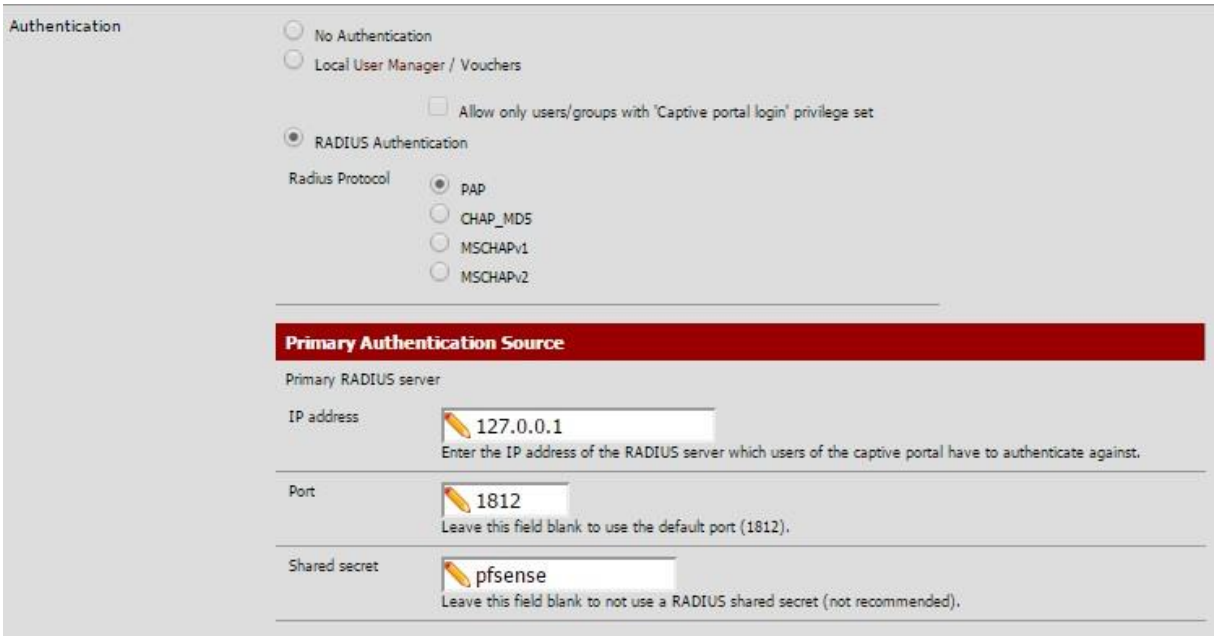
Nommer et décrire le portail



Choisir la page sur laquelle nous voulons rediriger l'utilisateur après son authentification (optionnel) :

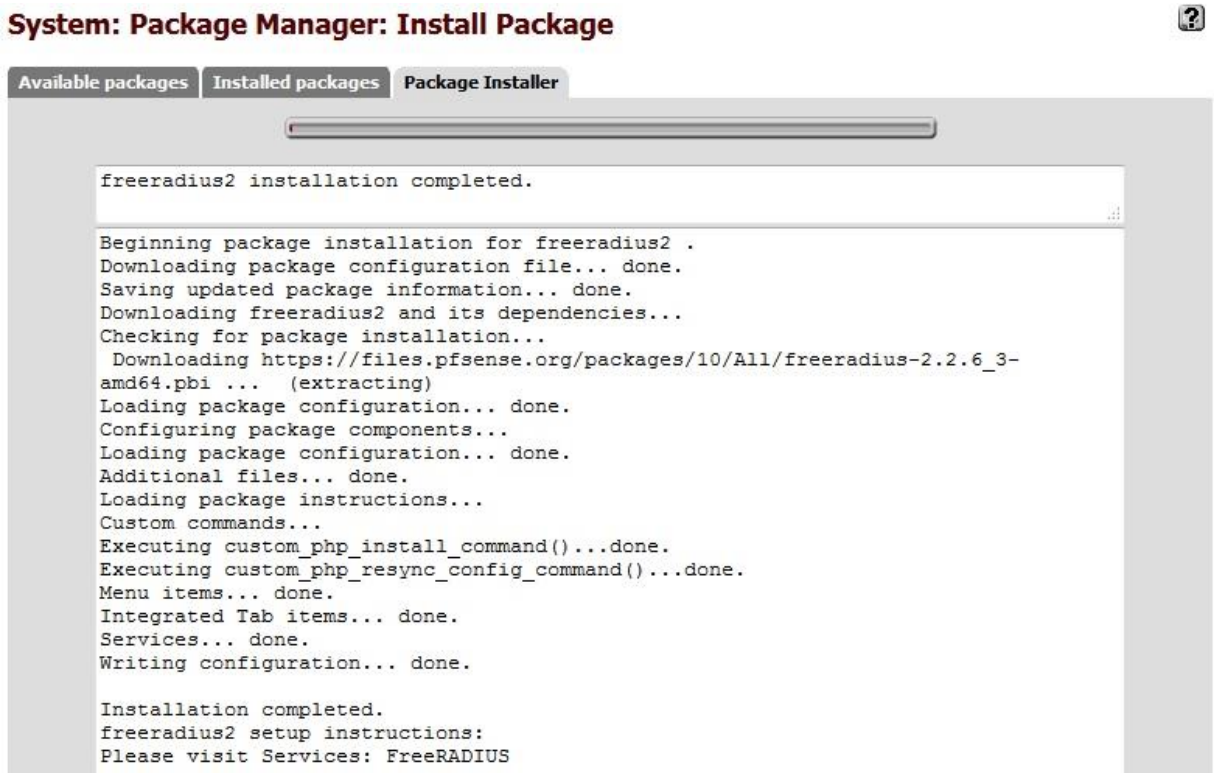


Choisir le type d'authentification, ici nous allons travailler avec RADIUS, qui sera installé en package sur la même machine. Renseigner le localhost en serveur RADIUS et 1812 pour le port. Le shared secret est au choix, il faut bien le noter car nous devront le renseigner ailleurs plus tard :

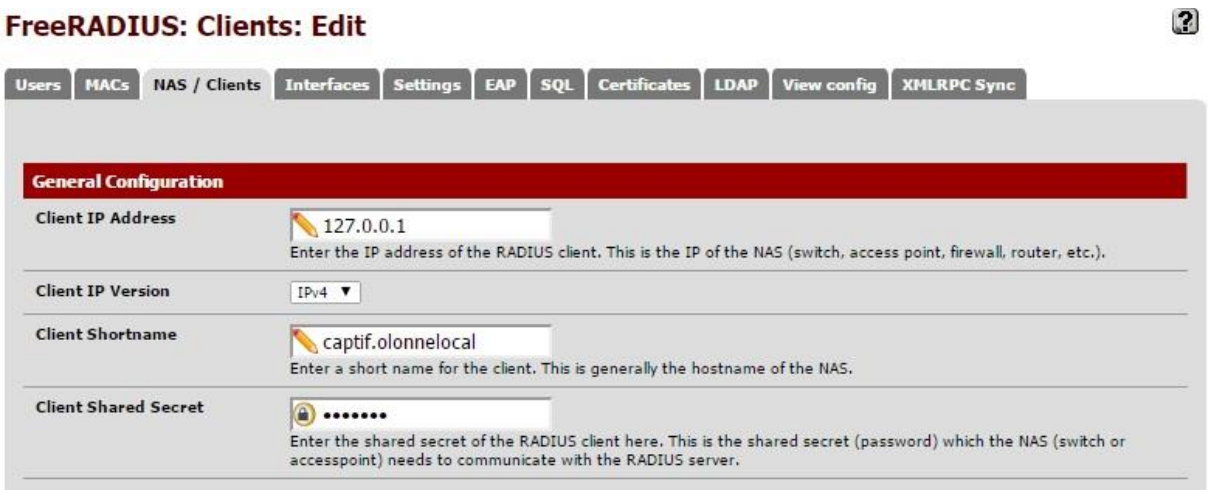


RADIUS

Dans System > Packages, télécharger et installer le paquet « freeradius2 »



Se rendre dans Services > FreeRADIUS puis dans l'onglet « NAS/Clients » puis ajouter un client avec l'adresse 127.0.0.1, le hostname du pfSense, ainsi que le SharedSecret renseigné précédemment :

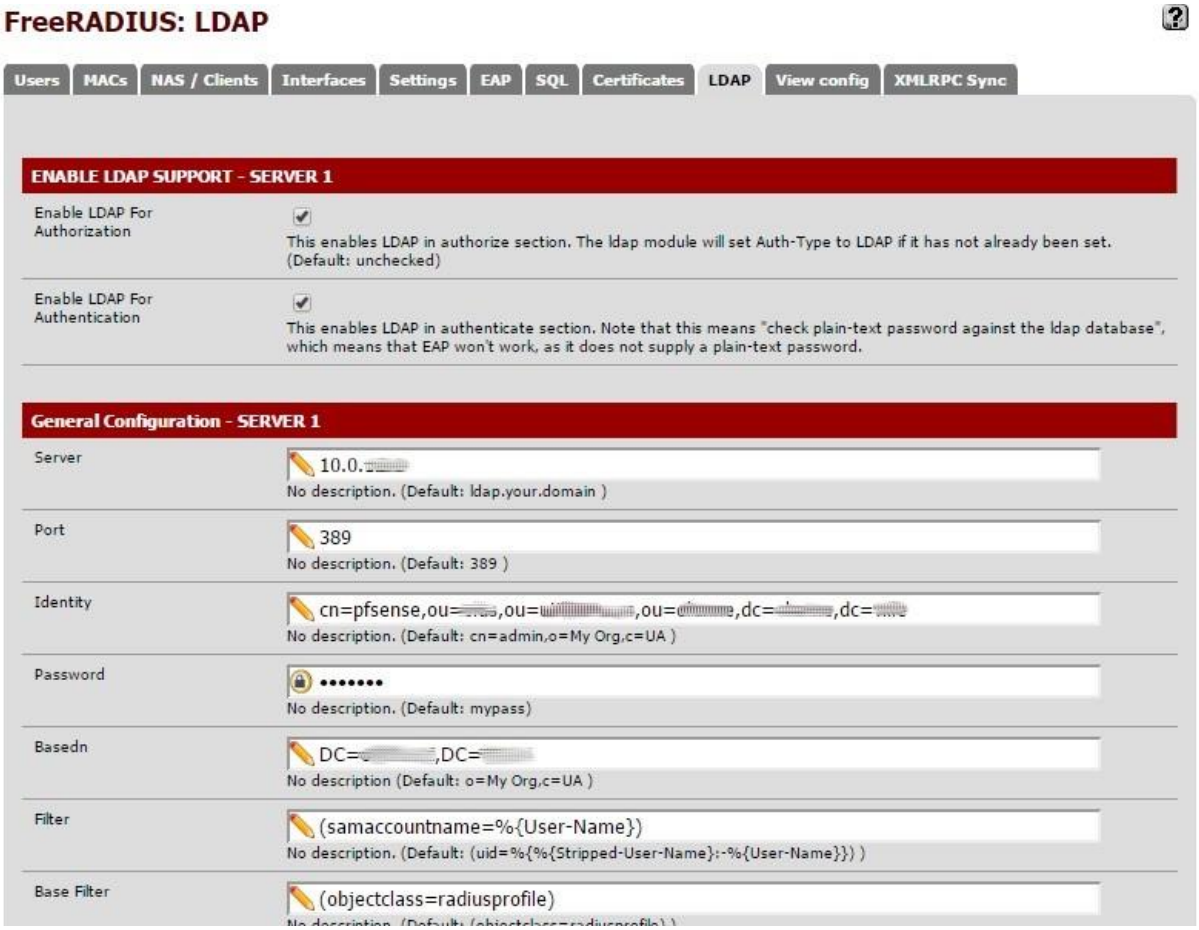


Dans l'onglet « Interfaces », renseigner l'interface sur lequel pfSense doit écouter pour le serveur RADIUS. Ici nous renseignerons 127.0.0.1 puisqu'il est lui-même serveur RADIUS :

Puis dans l'onglet LDAP, cocher « Enable LDAP For Authorization » et « Enable LDAP For Authentication ». Ensuite renseigner les champs suivants :

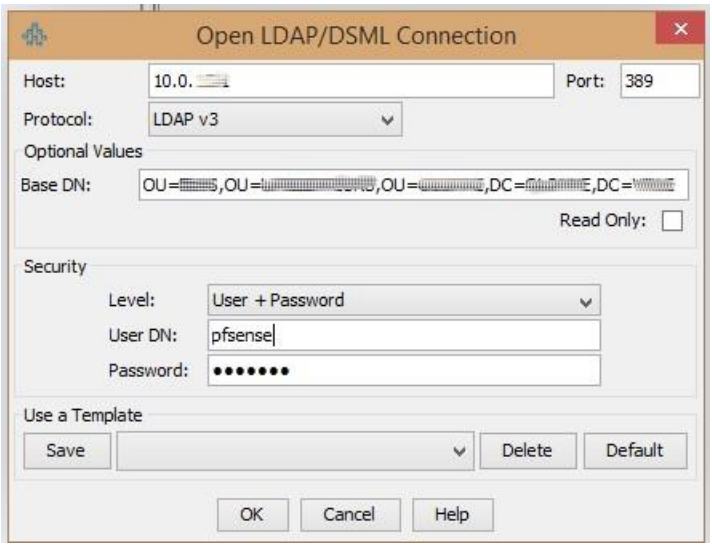
- *Server : adresse IP du serveur LDAP*
- *Port : par défaut 389*
- *Identity : chaine LDAP du compte qui permet l'accès au LDAP (doit être créé dans l'AD), attention, bien renseigner cette adresse, la plus part des problèmes de connexion peuvent potentiellement venir de là*
- *Password : mot de passe du compte pfsense dans l'AD*
- *BaseDN : Nom de domaine*

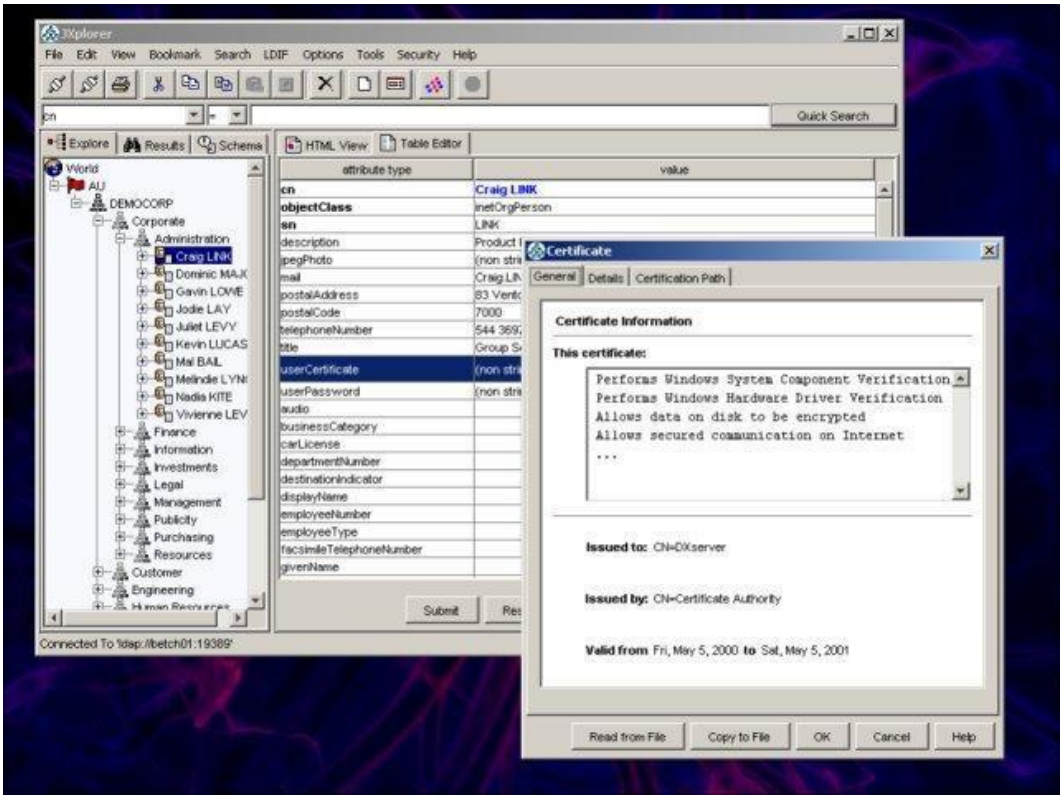
- *Filter : défini le User-Name*
- *Base Filter : laisser par défaut*



Diagnostiques d'erreurs

*En cas de problèmes de connexion LDAP, l'utilitaire d'exploration « **Jxplorer** » peut permettre de tester la connexion avec le compte « pfsense » créé dans l'AD. Cela permet également de vérifier l'exactitude des chaînes LDAP :*





Connexion

Une fois le portail captif configuré, l'utilisateur se connecte au réseau avec son terminal. Pour l'exemple nous utiliserons un Smartphone.

1. *L'utilisateur cherche le SSID du réseau et le sélectionne*
2. *L'utilisateur entre la clé WPA2-PSK*
3. *Après avoir « rejoint » le réseau, la page du portail captif apparait, l'utilisateur entre ses identifiants de connexion qu'il entre d'habitude lors de sa connexion à une session Windows*
4. *L'utilisateur est connecté au réseau et redirigé sur la page voulue*

Page de connexion

Il est possible de modifier la page qui permet à l'utilisateur de s'authentifier, pour cela, il faut se rendre dans Services > Captive Portal > Portal Page Contents et uploder la page html voulue :

Voici le code que nous allons uploader :

```
<html>
<head>
   <title>Olonne sur Mer</title>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
</head>
<body style = "background-color : #000000;">
    <center>
        <p><img src="logo.png" alt="logo" /></p>
        <h1><font color = "#FFFFF">Bienvenue sur le portail captif</font></h1>
        <h1><font color = "#FFFFF">de la ville d'Olonne sur Mer</font></h1>
        <form method="post" action="$PORTAL_ACTION$">
        <table width=225 border=0 cellpadding=3>
        <tr><td colspan=2><center><font size="+2"><b><font color = "#FFFFF">Accès réservé</b></font></center></td></tr>
        <tr><td><center><font color = "#FFFFF">Identifiant : <input name="auth_user" type="text"></font></center></td></tr>
        <tr><td><center><font color = "#FFFFF">Mot de passe :  <input name="auth_pass" type="password"></center></td></tr>
        <tr><td colspan=2 align="center"><input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
        <input name="accept" type="submit" value="Connexion"></td></tr></table>
        </form>
    </center>
</body>
</html>
```

Désormais, lorsque le client se connecte, il s'identifie sur cette page :