

# 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

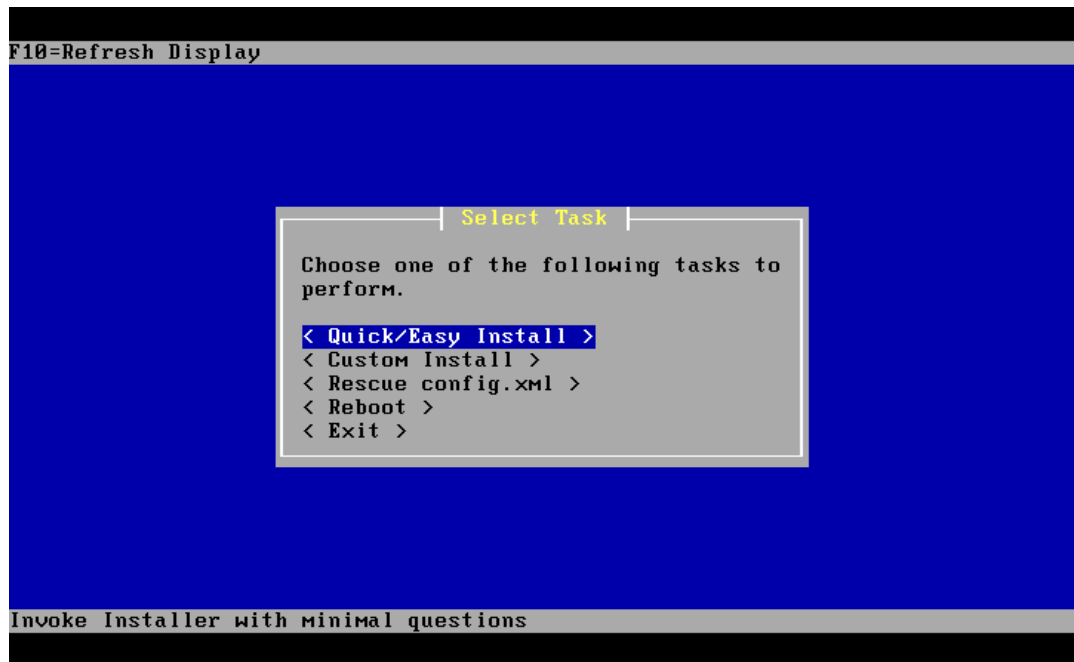
Les élus ayant besoin d'un accès internet sans fil, une borne wifi basique était installée. Hors la seule sécurisation était une clé WEP. Le but est de sécuriser le réseau. Pour cela, l'idée retenue a été la mise en place d'un portail captif, qui, une fois connecté au point d'accès, demande l'authentification 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 :

```
\_--\_/  
Welcome to pfSense 2.2-RC ...  
Mounting unionfs directories...done.  
Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib  
32-bit compatibility ldconfig path: /usr/lib32  
done.  
Launching the init system... done.  
Initializing..... done.  
Starting device manager (devd)...done.  
  
[ Press R to enter recovery mode or ]  
[ press I to launch the installer ]  
  
(R)ecovery mode can assist by rescuing config.xml  
from a broken hard disk installation, etc.  
  
(I)nstaller may be invoked now if you do  
not wish to boot into the liveCD environment at this time.  
  
(C)ontinues the LiveCD bootup without further pause.  
Timeout before auto boot continues (seconds): 9█
```



## Configuration de pfSense

*Une fois pfSense installé, la machine redémarre. Il faut alors débiter 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.*



- 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
  - pInfo
  - pTop
  - 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**

<b>Name</b>	captif.olonnelocal
<b>Version</b>	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.	
<b>Platform</b>	pfSense
<b>CPU Type</b>	Intel(R) Celeron(R) CPU 1037U @ 1.80GHz 2 CPUs: 1 package(s) x 2 core(s)
<b>Uptime</b>	01 Hour 01 Minute 36 Second
<b>Current date/time</b>	Mon Feb 9 14:42:59 UTC 2015
<b>DNS server(s)</b>	127.0.0.1 10.0.12.1
<b>Last config change</b>	Mon Feb 9 14:21:09 UTC 2015
<b>State table size</b>	<div style="width: 100%;"><div style="width: 0%; height: 10px; background-color: #ccc;"></div></div> 0% (8/804000) <a href="#">Show states</a>
<b>MBUF Usage</b>	<div style="width: 100%;"><div style="width: 5%; height: 10px; background-color: #ccc;"></div></div> 5% (1270/26584)
<b>Temperature</b>	<div style="width: 100%;"><div style="width: 27.8%; height: 10px; background-color: #ccc;"></div></div> 27.8°C
<b>Load average</b>	0.00, 0.00, 0.00
<b>CPU usage</b>	<div style="width: 100%;"><div style="width: 1%; height: 10px; background-color: #ccc;"></div></div> 1%
<b>Memory usage</b>	<div style="width: 100%;"><div style="width: 3%; height: 10px; background-color: #ccc;"></div></div> 3% of 8049 MB
<b>SWAP usage</b>	<div style="width: 100%;"><div style="width: 0%; height: 10px; background-color: #ccc;"></div></div> 0% of 16384 MB
<b>Disk usage</b>	<div style="width: 100%;"><div style="width: 1%; height: 10px; background-color: #ccc;"></div></div> / (ufs): 1% of 39G <div style="width: 100%;"><div style="width: 3%; height: 10px; background-color: #ccc;"></div></div> /var/run (ufs in RAM): 3% of 3.4M

**Interfaces**

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

## 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 :

### System: Advanced: Admin Access ?

**Admin Access** Firewall / NAT Networking Miscellaneous System Tunables Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

#### webConfigurator

Protocol  HTTP  HTTPS

SSL Certificate

TCP port

Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

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

#### Console Options

Console menu  Password protect the console menu

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

#### Secure Shell

Secure Shell Server  Enable Secure Shell

Authentication Method  Disable password login for Secure Shell (RSA/DSA key only)  
When enabled, authorized keys need to be configured for each user that has been granted secure shell access.

SSH port

Note: Leave this blank for the default of 22.

## 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.

### Services: DHCP server



**LAN**

**Enable DHCP server on LAN interface**

**Deny unknown clients**  
If this is checked, only the clients defined below will get DHCP leases from this server.

<b>Subnet</b>	192.168.1.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	192.168.1.1 - 192.168.1.254
<b>Range</b>	<input type="text" value="192.168.1.10"/> to <input type="text" value="192.168.1.245"/>

## Portail captif

### Configuration

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

**webConfigurator** captif.olonne.local

### Services: Captive portal: Olonne

**Captive portal(s)** **MAC** **Allowed IP addresses** **Allowed Hostnames** **Vouchers** **File Manager**

**Enable captive portal**

**Interfaces**  ...  
Select the interface(s) to enable for captive portal.

Nommer et décrire le portail

**Edit Captive Portal Zones**

<b>Zone name</b>	<input type="text" value="Olonne"/> Zone name. Can only contain letters, digits, and underscores (_).
<b>Description</b>	<input type="text" value="portail"/> You may enter a description here for your reference (not parsed).

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

After authentication  
Redirection URL

If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

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 :

Authentication

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   
Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port   
Leave this field blank to use the default port (1812).

Shared secret   
Leave this field blank to not use a RADIUS shared secret (not recommended).

## RADIUS

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

### System: Package Manager: Install Package



Available packages | Installed packages | **Package Installer**

---

```
freeradius2 installation completed.

Beginning package installation for freeradius2 .
Downloading package configuration file... done.
Saving updated package information... done.
Downloading freeradius2 and its dependencies...
Checking for package installation...
  Downloading https://files.pfsense.org/packages/10/All/freeradius-2.2.6_3-
amd64.pbi ... (extracting)
Loading package configuration... done.
Configuring package components...
Loading package configuration... done.
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Integrated Tab items... done.
Services... done.
Writing configuration... done.

Installation completed.
freeradius2 setup instructions:
Please visit Services: FreeRADIUS
```

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 :

### FreeRADIUS: Clients: Edit



Users MACs **NAS / Clients** Interfaces Settings EAP SQL Certificates LDAP View config XMLRPC Sync

---

**General Configuration**

Client IP Address   
Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access point, firewall, router, etc.).

Client IP Version

Client Shortname   
Enter a short name for the client. This is generally the hostname of the NAS.

Client Shared Secret   
Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch or accesspoint) needs to communicate with the RADIUS server.

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 :

### FreeRADIUS: Interfaces: Edit



Users MACs **NAS / Clients** **Interfaces** Settings EAP SQL Certificates LDAP View config XMLRPC Sync

---

**General Configuration**

Interface IP Address   
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose \* then it means all interfaces. (Default: \*)

Port   
Enter the port number of the listening interface. Different interface types need different ports.  
You could use this as an example:  
Authentication = 1812  
Accounting = 1813  
Status = 1816  
**IMPORTANT: For every interface type listening on the same IP address you need different ports.**

Interface Type   
Enter the type of the listening interface. (Default: auth)

IP Version   
Enter the IP version of the listening interface. (Default: IPv4)

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

## FreeRADIUS: LDAP



Users	MACs	NAS / Clients	Interfaces	Settings	EAP	SQL	Certificates	LDAP	View config	XMLRPC Sync
<b>ENABLE LDAP SUPPORT - SERVER 1</b>										
Enable LDAP For Authorization	<input checked="" type="checkbox"/> This enables LDAP in authorize section. The ldap module will set Auth-Type to LDAP if it has not already been set. (Default: unchecked)									
Enable LDAP For Authentication	<input checked="" type="checkbox"/> This enables LDAP in authenticate section. 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.									
<b>General Configuration - SERVER 1</b>										
Server	<input type="text" value="10.0.1.1"/> No description. (Default: ldap.your.domain )									
Port	<input type="text" value="389"/> No description. (Default: 389 )									
Identity	<input type="text" value="cn=pfsense,ou=users,ou=My Org,dc=example,dc=com"/> No description. (Default: cn=admin,o=My Org,c=UA )									
Password	<input type="password" value="*****"/> No description. (Default: mypass)									
Basedn	<input type="text" value="DC=example,DC=com"/> No description (Default: o=My Org,c=UA )									
Filter	<input type="text" value="(samaccountname=%{User-Name})"/> No description. (Default: (uid=%{%{Stripped-User-Name}}:-%{User-Name})) )									
Base Filter	<input type="text" value="(objectclass=radiusprofile)"/> No description. (Default: (objectclass=radiusprofile))									

### 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 :

Open LDAP/DSML Connection

Host:  Port:

Protocol:

Optional Values

Base DN:  Read Only:

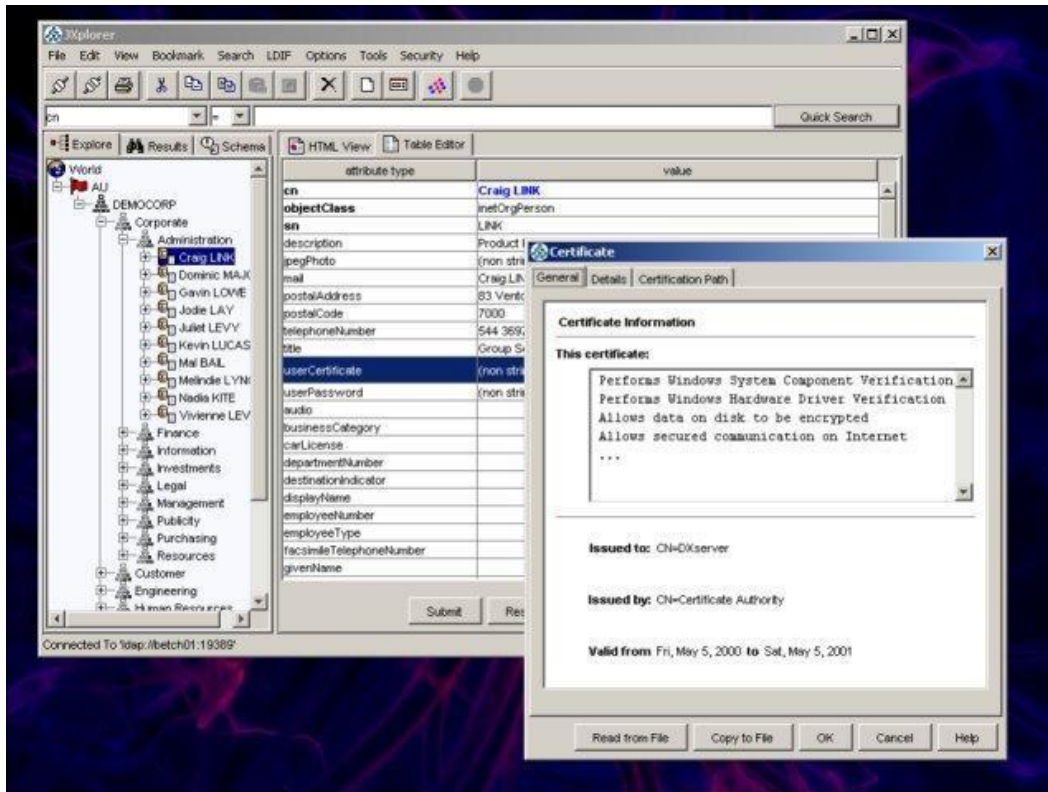
Security

Level:

User DN:

Password:

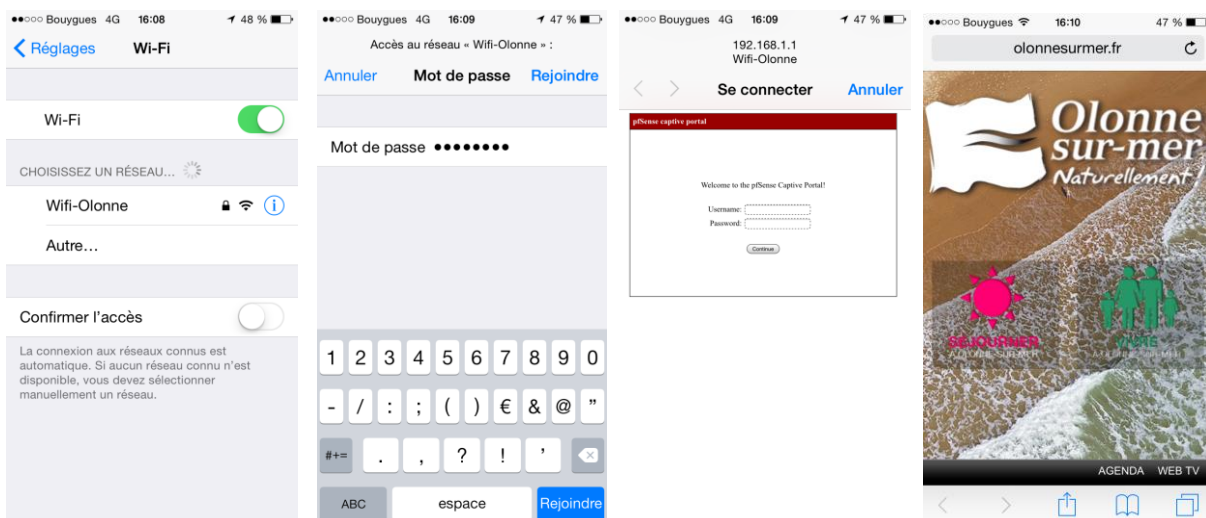
Use a Template



## 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 apparaît, 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 uploader la page html voulue :

Portal page contents Choisir le fichier aucun fichier sél.

[View current page](#)  
[Download current page](#)  
[Restore default portal page](#)

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL\_ACTION\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL\_REDIRURL\$". Include the "auth\_user" and "auth\_pass" and/or "auth\_voucher" input fields if authentication is enabled, otherwise it will always fail.  
Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="accept" type="submit" value="Continue">
</form>
```

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></p>
    <h1><font color = "#FFFFFF">Bienvenue sur le portail captif</font></h1>
    <h1><font color = "#FFFFFF">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 = "#FFFFFF">Accès réservé</font></b></font></center></td></tr>
    <tr><td><center><font color = "#FFFFFF">Identifiant : <input name="auth_user" type="text"></font></center></td></tr>
    <tr><td><center><font color = "#FFFFFF">Mot de passe : <input name="auth_pass" type="password"></font></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 :



**Bienvenue sur le portail captif**  
**de la ville d'Olonne sur Mer**

**Accès réservé**

Identifiant :

Mot de passe :