

Mise en place d'un portail captif avec une distribution pfSense



Présentation :

pfSense est une distribution routeur/pare-feu OpenSource basée sur FreeBSD, pouvant être installée sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (packet filter), comme iptables sur GNU/Linux, il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN.

I. Installation :

Afin d'installer pfSense, il faut tout d'abord télécharger une image ISO.

Sur la page suivante se trouvent différentes images pfSense :

<http://pfsense.mirrors.ovh.net/pfsense.org/downloads/>

Il faut en choisir une compatible avec l'architecture de votre machine (i386 pour du 32bits, amd64 pour du 64bits). Il faut aussi choisir une ligne portant la mention « Live CD ».

Ici, j'ai téléchargé le fichier [pfSense-LiveCD-2.0.2-RELEASE-i386.iso.gz](#).

C'est un fichier compressé, il faudra le décompresser pour obtenir l'image ISO prête à graver. Une fois l'image gravée et le disque inséré dans la machine, cet écran apparaît. On appuie sur Entrée pour lancer pfSense.

```

Welcome to pfSense!

1. Boot pfSense [default]
2. Boot pfSense with ACPI disabled
3. Boot pfSense using USB device
4. Boot pfSense in Safe Mode
5. Boot pfSense in single user mode
6. Boot pfSense with verbose logging
7. Escape to loader prompt
8. Reboot

Select option, [Enter] for default
or [Space] to pause timer 5 _

```

Après de nombreuses lignes affichées, le programme demandera votre attention. On appuie alors sur la lettre « i » avant la fin du compteur afin de lancer l'installation.

```

Welcome to pfSense 2.0.2-RELEASE ...
Mounting unionfs directories...done.
Creating symlinks.....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): 6

```

Sur cet écran, « Accept these Settings ».

```
Configure Console
Your selected environment uses the
following console settings, shown in
parentheses. Select any that you wish
to change.
< Change Video Font (default) >
< Change Screenmap (default) >
< Change Keymap (fr.iso) >
< Accept these Settings >
```

Puis « Quick/Easy Install ».

```
Select Task
Choose one of the following tasks to
perform.
< Quick/Easy Install >
< Install pfSense >
< Rescue config.xml >
< Reboot >
< Exit >
```

Le programme prévient que le disque dur sera entièrement effacé, et tout l'espace disponible sera utilisé par pfSense. Entrée pour valider.

L'assistant vous parle d'installation d'un Kernel. Il est possible que l'écran change en fonction de l'architecture de votre système.

On choisit l'option par défaut. Voici la copie d'écran sous pfSense i386 :

```
Install Kernel
You may now wish to install a custom Kernel configuration.
< Standard Kernel >
< Embedded kernel (no UGA console, keyboard) >
```

Un écran nous informe qu'après avoir appuyé sur Entrée, la machine redémarrera. Il faudra alors retirer le disque d'installation, de façon à ce que la machine démarre sur le disque dur. L'installation de pfSense est ensuite terminée.

II. Configuration de cartes réseaux :

Il faut maintenant configurer les cartes réseaux. Les cartes réseaux sont affichées comme ceci.

```
Valid interfaces are:  
em0  08:00:27:12:5f:9d  (up) Intel(R) PRO/1000
```

Il faut bien retenir les noms de ces interfaces, car ils seront demandés plus tard.

ATTENTION, LE CLAVIER EST EN QWERTY.

La question suivante est

```
Enter the WAN interface name or 'a' for auto-detection: █
```

L'interface WAN (Wide Area Network) c'est-à-dire le réseau étendu, correspond à l'interface qui est reliée au réseau administratif. Dans notre cas, il s'agit de l'interface em0. Il faut donc rentrer em0 puis Entrée. On indique ensuite notre interface LAN (Local Area Network), c'est-à-dire le réseau pédagogique, en em1.

Il faut maintenant configurer des adresses IP fixes à nos interfaces réseau.

Avec l'option 2, on choisit ensuite l'interface WAN en tapant 1.

L'interface WAN correspondra à l'adresse 172.16.10.254. A la question « Configure WAN interface via DHCP ? » j'ai donc répondu non, puis indiqué cette adresse.

Ensuite est demandé « Enter the new WAN IPv4 subnet bit count », c'est-à-dire le masque de sous-réseau. Le sous réseau est 255.255.255.0, donc en notation CIDR, 24. L'interface LAN correspondra à l'adresse 172.16.30.254 et un masque en /24.

La configuration est terminée ! Il est également possible d'accéder au serveur proxy depuis un autre poste en SSH. Il faut pour cela activer l'option 14.

III. Configuration des paramètres de base :

On peut désormais accéder à l'interface web du pare-feu en saisissant son IP dans votre navigateur. Par défaut le nom d'utilisateur est admin et le mot de passe pfsense. Différents menus sont accessibles dans pfSense : System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.

On va d'abord désactiver le filtrage, afin de procéder par étape et ne pas être bloqué. On le configurera à la fin. Dans « System », on clique sur « Advanced », et dans l'onglet Firewall/NAT on coche la case « Disable all packet filtering ».

L'accès à internet étant sécurisé par un proxy, il faut indiquer ce proxy dans l'onglet « Miscellaneous ».

Sur la page de configuration des interfaces WAN et LAN, il est important de décocher les cases « Block private networks » et « Block bogon networks ».

Ensuite, dans le menu « System », on clique sur « General setup ». Il faut indiquer le nom que l'on donne à la machine, et le domaine sur lequel elle se trouve. On indique ensuite le serveur DNS auquel nos requêtes seront envoyées. On choisit ensuite le thème « pfSense », car les autres thèmes ne sont pas compatibles avec tous les navigateurs, notamment Internet Explorer.

System

Hostname pfsense
Name of the firewall host, without domain part
e.g. *firewall*

Domain pedago.local
Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. *mycorp.com, home, office, private, etc.*

DNS servers

DNS Server	Use gateway
192.168.1.2	None
	None
	None
	None

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

Do not use the DNS Forwarder as a DNS server for the firewall
By default localhost (127.0.0.1) will be used as the first DNS server where the DNS forwarder is enabled, so system can use the DNS forwarder to perform lookups. Checking this box omits localhost from the list of DNS servers.

Sous le menu « System », on clique sur « Routing », et on ajoute la passerelle permettant d'accéder à internet, c'est-à-dire l'adresse du routeur Cisco (172.16.1.253).

Dans l'onglet « Routes », on indique les sous-réseaux qui ne sont pas directement connectés, afin que pfSense puisse les contacter.

Gateways **Routes** **Groups**

Network	Gateway	Interface	Description
172.16.20.0/24	WANGW - 172.16.10.253	WAN	Réseau LAN
192.168.1.0/24	WANGW - 172.16.10.253	WAN	Résau Admin

Il faut ensuite activer le serveur DHCP sur l'interface LAN. Cliquer sur « DHCP Server » dans le menu « Services », puis sur l'onglet LAN. On coche la case « Enable DHCP server on LAN interface », puis on renseigne la plage DHCP (Range), ainsi que la liste des serveurs DNS, la passerelle et le nom du domaine.

<input checked="" type="checkbox"/>	Enable DHCP server on LAN interface
<input type="checkbox"/>	Deny unknown clients If this is checked, only the clients defined below will get DHCP.
Subnet	172.16.30.0
Subnet mask	255.255.255.0
Available range	172.16.30.1 - 172.16.30.254
Range	<input type="text" value="172.16.30.20"/> to <input type="text" value="172.16.30.245"/>
WINS servers	<input type="text"/> <input type="text"/>
DNS servers	<input type="text" value="172.16.30.254"/> <input type="text"/> NOTE: leave blank to use the system default DNS servers - the servers configured on the General page.
Gateway	<input type="text" value="172.16.30.254"/> The default is to use the IP on this interface of the firewall as not the correct gateway for your network.
Domain name	<input type="text" value="pedago.local"/> The default is to use the domain name of this system as the alternate domain name here.

IV. Mise en place du portail captif :

1. Réglages proxy

Afin d'accéder à internet, les clients se connectant au portail captif devront passer par le proxy. Cependant, il est trop lourd de demander à chaque utilisateur de configurer manuellement son navigateur pour utiliser un proxy. C'est pourquoi il faut utiliser une redirection ainsi qu'un fichier d'auto-configuration.

Dans la rubrique « Packages » du menu « System », on installera le paquet « squid3 ». On le configure ensuite sous « Proxy server » dans le menu « Services ». On indique l'interface LAN, le port 3128, et on coche les cases « Allow users », « Patch captive portal » et « Resolv dns v4 first ». On active les logs sur 365 jours et on sauvegarde les modifications.

Squid General Settings

Proxy interface
 The interface(s) the proxy server will bind to.

Proxy port
 This is the port the proxy server will listen on.

ICP port
 This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow users on interface
 If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent HTTP proxy
 Enable transparent mode to forward all requests for destination port 80 to the proxy server without any additional configuration necessary.
NOTE: Transparent mode will filter ssl(port 443) if enable men-in-the-middle options below.
 To filter both http and https protocol without intercepting ssl connections, enable WPAD/PAC options on your dns/dhcp.

Patch captive portal
 Enable this option to force captive portal to non transparent proxy users.
NOTE: You may need to reapply captive portal config after changing this option.

Bypass proxy for Private Address destination
 Do not forward traffic to Private Address Space (RFC 1918) **destination** through the proxy server but directly through the firewall.

Bypass proxy for these source IPs
 Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Bypass proxy for these destination IPs
 Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Resolv dns v4 first
 Enable this option to force dns v4 lookup first. This option is very usefull if you have problems to access https sites.

Use alternate DNS-servers for the proxy-server
 If you want to use other DNS-servers than the DNS-forwarder, enter the IPs here, separated by semi-colons (;).

Logging Settings

Enabled logging
 This will enable the access log. Don't switch this on if you don't have much disk space left.

Log store directory
 The directory where the log will be stored (note: do not end with a / mark)

Log rotate
 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

On va ensuite créer une règle de redirection NAT sous le menu « Firewall ». Dans l'onglet « Port Forward », ajouter une règle comme ceci :

Port Forward 1:1 Outbound

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>	LAN	TCP	LAN net	*	*	3128	192.168.1.254	3128	

Passons au fichier d'auto-configuration, fichier .PAC :

```
function FindProxyForURL(url, host)
{
  if (isInNet(dnsResolve(host), "172.16.30.0", "255.255.255.0"))
  return "DIRECT";
  else if (isInNet(dnsResolve(host), "192.168.1.0", "255.255.255.0"))
  return "DIRECT";
  else if (shExpMatch(host, "*.local"))
  return "DIRECT";
  else
  return "PROXY 172.16.30.254:3128";
}
```

Ce fichier indique que, si le site de destination se trouve dans le réseau 172.16.30.0, le navigateur ne devra pas utiliser de proxy pour y accéder. Idem pour le réseau 192.168.1.0, ou pour un site faisant partie du domaine .local

Dans les autres cas, le navigateur devra utiliser le proxy 172.16.30.254 sur le port 3128.

Pour rendre accessible ce fichier, il faut soit le taper directement sur un éditeur texte sur pfSense, soit l'uploader une fois prêt. Il est possible d'uploader ce fichier via la page de configuration du portail captif (expliqué plus loin).

Le fichier se trouvera donc dans /usr/local/captiveportal/

A l'aide du shell, copier ce fichier dans /usr/local/www/ et le renommer « wpad.dat ».

```
# cp /usr/local/captiveportal/captiveportal-proxy.pac
/usr/local/www/wpad.dat
(même ligne)
```

Le fichier est désormais accessible depuis <http://172.16.30.254/wpad.dat>

Cependant, un navigateur cherche un fichier d'auto-configuration à l'adresse <http://wpad.NOMDUDOMAINE.LOCAL/wpad.dat>

Il nous faut donc créer une redirection DNS pour cette adresse, dans la partie « DNS Forwarder » sous le menu « Services ». Vérifier que la case DNS forwarder est cochée, puis ajouter cette ligne dans la partie « Host Overrides » :

Host Overrides			
Entries in this section override individual results from the forwarders. Use these for changing DNS results or for add DNS records.			
Host	Domain	IP	Description
wpad	pedago.local	172.16.30.254	

Il faudra simplement que la case « Détecter automatiquement les paramètres proxy pour ce réseau » soit cochée dans les navigateurs.

2. Personnalisation du portail captif

Afin de rendre la page de portail captif un peu plus accueillante, il est possible de la modifier. Il reste tout de même nécessaire d'y faire figurer les champs pour le nom d'utilisateur, le mot de passe, le bouton valider, etc. La page web peut être au format html ou php, peu importe.

```
<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>
```

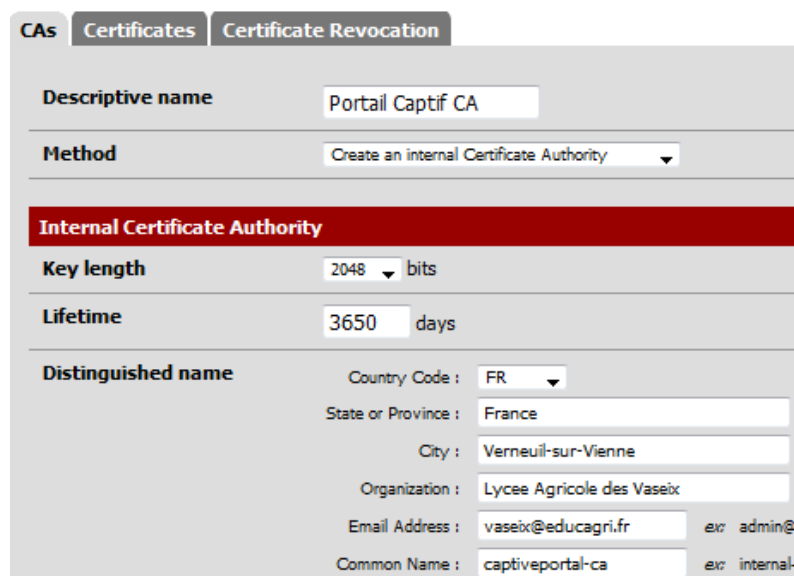
Les lignes « auth_voucher » et « redirurl » sont facultatives... Il est cependant conseillé d'utiliser « redirurl » sur chaque page afin de garder en mémoire la page que l'utilisateur souhaitait consulter à l'origine.

On peut modifier la page d'accueil, la page en cas d'erreur de connexion, et créer une page de réussite d'authentification.

Sur la page « Captive portal » du menu « Services », il est possible d'uploader des fichiers avec l'onglet « File Manager ». Tout fichier uploadé sera renommé avec le préfixe « captiveportal- ». Une fois les pages modifiées et les fichiers uploadés, on peut envoyer les pages modifiées depuis le premier onglet, à l'aide des trois derniers champs.

3. Sécurisation du portail captif

Il faut ensuite créer des certificats TLS (anciennement SSL) afin de sécuriser l'accès au portail captif en HTTPS. On clique sur « Cert Manager » dans le menu « System ». Sur l'onglet Cas, il faut créer une nouvelle autorité de certification. Indiquer un nom, par exemple « Portail Captif CA », dans la liste, choisir « Create an internal CA », puis remplir les champs. La valeur du dernier champ devra se terminer par « -ca ».



CAS	
Certificates	Certificate Revocation
Descriptive name	Portail Captif CA
Method	Create an internal Certificate Authority
Internal Certificate Authority	
Key length	2048 bits
Lifetime	3650 days
Distinguished name	Country Code : FR
	State or Province : France
	City : Verneuil-sur-Vienne
	Organization : Lycee Agricole des Vaseix
	Email Address : vaseix@educagri.fr ex: admin@
	Common Name : captiveportal-ca ex: internal-

Sur l'onglet Certificates, créer un nouveau certificat. On choisit dans la liste « Create an internal Certificate », puis on entre un nom du type « Portail Captif Cert ». Dans « Certificate authority », vérifier que l'autorité de certification précédemment créée est bien sélectionnée. Remplir les autres champs, puis dans le dernier champ, indiquer le nom-de-la-machine.domaine.local

CA	Certificates	Certificate Revocation
Method	Create an internal Certificate	
Descriptive name	Portail Captif Cert	
Internal Certificate		
Certificate authority	Portail Captif CA	
Key length	2048 bits	
Certificate Type	User Certificate Type of certificate to generate. Used for placing restrictions	
Lifetime	3650 days	
Distinguished name	Country Code : FR State or Province : France City : Verneuil-sur-Vienne Organization : Lycee Agricole des Vaseix Email Address : vaseix@educagri.fr ex: webadmin Common Name : pfsense.pedago.local ex: www.example.com	

Sur l'onglet CAs, cliquer sur le premier bouton avec une flèche vers le bas « export CA cert ». Faire de même sur l'onglet « Certificates » avec le certificat précédemment créé et les deux premières flèches « export CA » et « export key ». Il faut ensuite ouvrir ces fichiers avec un éditeur de texte et copier-coller leur contenu dans la page de configuration du portail captif.

HTTPS login **Enable HTTPS login**
 If enabled, the username and password will be transmitted over the network. This is not secure and is vulnerable to eavesdroppers. A server name, certificate and private key must be provided.

HTTPS server name
 pfsense.pedago.local
 This name will be used in the form action for the certificate (otherwise, the client browser will not resolve this name in DNS and verify on the client).

HTTPS certificate

```
-----BEGIN CERTIFICATE-----
MIICGzCCARUgAwIBAgIBATAKBggqhkjOPQQADMdGAEEUO31KvNLSRNgP9eHfLUeGeP1AUU
yeJpReQqNKrHkavP1GEBwT3MAa7x5licF+g5c
ijUkw4tGGA7WDCmI/28pAdiVwXDO/EByyVduHv
vrX8Lpe18+wB8ZjDWJadI6Pndk3qL+y2gxxxiC
9fjFfmJobWT1/2naMgINT+nn1e5HAJm6Gldf2:
57hJZHNN/3Ks+LP1xCrv2Igo
-----END CERTIFICATE-----
```

 Paste a signed certificate in X.509 PEM format here.

HTTPS private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAJwxxYE/ctYb0VQqcafgBamT9AoGBAIt64g48+I
UgDwuBXwUDqNVhcWMerL8jm9+Dohn2cIrxJMFBO
RUWXgX3cfJERU1bCAdXgd+ws2FNq/karhShwI:
h8/UyejBAqGBAQeXFCJA+c6h42u313woeKig4V
drbVpnn8Xy43+3MbqFDE+6xkWn/k4WEEFP4w8:
IieMgO3bZ/aAg513NeKuFetIa4IH82dBio3:
-----END RSA PRIVATE KEY-----
```

 Paste an RSA private key in PEM format here.

HTTPS intermediate certificate

```
-----BEGIN CERTIFICATE-----
MIICGzCCARUgAwIBAgIBATAKBggqhkjOPQQADMdGAEEUO31KvNLSRNgP9eHfLUeGeP1AUU
kS2a1HCE0U09HmAVC3q6d8QXO43KFXVrXeYyet
yG/eMaAsXN/s3B95ivLMw+6y88JGTaA78pcox
50D0yEJ2Ju8tvHxIxGX6Wv77twbgjYIXruooVn
oo2FE+LxvtQxq1qk1TT94x85XWVS+xBnO1F:
eHRLKrujg7rGBYWULoVXH4nax1rL3uX12zjk:
61P5c6dowCVH4qN9
-----END CERTIFICATE-----
```

 Paste a certificate in X.509 PEM format here.

ProjetBO ► Téléchargements
 Inclure dans la bibliothèque ▼ Partager avec ▼ Graver

Nom	Moc
netscan	28/0
Portail+ Captif+ CA	29/0
Portail+ Captif+ Cert	29/0
Portail+ Captif+ Cert.key	29/0

Afin d'être sûr que le certificat sera accessible depuis le nom nom-de-la-machine.domaine.local, il faut ajouter une redirection DNS, dans « DNS Forwarder ».

Host	Domain	IP	Description
pfsense	pedago.local	172.16.30.254	
wpad	pedago.local	172.16.30.254	

Il existe deux méthodes d'authentification possibles sur le portail captif :

- une authentification locale, avec des noms d'utilisateurs et des mots de passe à créer dans pfSense ;
- une authentification RADIUS, plus sécurisée (utilisation de certificats) permettant d'utiliser des noms d'utilisateurs existants déjà dans un annuaire OpenLDAP ou ActiveDirectory.

Ici, l'accès sans fil servant à des personnes venant de l'extérieur, nous utiliserons l'authentification locale. Il faut donc cocher le bouton « Local User Manager » dans la partie Authentification de la page de configuration portail captif, et ensuite créer des utilisateurs dans « User Manager » sous « System ».

L'onglet « Pass-through MAC » de la page de configuration du portail captif sert à autoriser les connexions directes de certaines machines, sans passer par la page de connexion du portail captif. Il faut ajouter l'adresse MAC de la machine correspondante.

V. Filtrage :

Il est alors grand temps de configurer notre table de filtrage.

Tout d'abord, on réactive le filtrage dans la partie « Advanced » du menu « System ». On se rend ensuite dans « Rules », sous « Firewall ».

Dans l'onglet WAN, on autorisera donc les requêtes web et DNS, donc ports 3128 (proxy) 53, 80 et 443. Il faut bloquer tout le reste. pfSense lis les requêtes de haut en bas : on autorise d'abord, on bloque ensuite.

Floating WAN LAN										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>		TCP	*	3128	*	*	none		Autoriser Web (Proxy)	
<input type="checkbox"/>		UDP	*	*	53 (DNS)	*	none		Autoriser DNS	
<input type="checkbox"/>		TCP	*	*	80 (HTTP)	*	none		Autoriser HTTP	
<input type="checkbox"/>		TCP	*	*	443 (HTTPS)	*	none		Autoriser HTTPS	
<input type="checkbox"/>		*	*	*	*	*	none		BLOCK ALL	

Dans l'onglet LAN, on autorisera les mêmes choses, et l'on rajoutera une ligne pour le portail captif, en port 8000.

Floating WAN LAN										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>		*	*	LAN Address	80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>		*	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>		TCP	LAN net	*	172.16.30.254	8000	none		Autoriser Portail Captif	
<input type="checkbox"/>		UDP	LAN net	*	*	53 (DNS)	none		Autoriser DNS	
<input type="checkbox"/>		TCP	LAN net	*	*	80 (HTTP)	none		Autoriser HTTP	
<input type="checkbox"/>		TCP	LAN net	*	*	443 (HTTPS)	none		Autoriser HTTPS	
<input type="checkbox"/>		TCP	LAN net	*	192.168.1.254	3128	none		NAT	
<input type="checkbox"/>		*	*	*	*	*	none		BLOCK ALL	

Le personnel extérieur n'a plus qu'à se connecter au SSID de notre borne Wi-Fi (configurée préalablement), et après avoir ouvert son navigateur, il sera redirigé automatiquement sur la page d'accueil du portail captif !

Portail Captif pfSense



Bienvenue sur le réseau Wi-Fi du Lycée Agricole des Vaseix.

Nom d'utilisateur :

Mot de passe :