

## TP : Déploiement d'un WiFi public

### Sommaire :

Introduction.....	1
Mise en place de la borne.....	1
Configuration de la borne WiFi .....	2
Création du portail captif & configuration des comptes utilisateurs.....	4
Partie juridique.....	10
Problèmes rencontrés.....	12
Sources et annexes.....	12
Bloc-note (pour nous).....	13

#### > Introduction :

Notre mission consiste à travailler un nouveau service pour Selenia Software, à savoir **le déploiement d'un WiFi public** qui sera accessible aux clients et/ou aux salariés dans les locaux de l'entreprise, avec évidemment des **authentifications temporaires**. Pour cela, on utilise une borne WiFi Cisco, un poste de la salle S4 et un PC personnel pour tester le WiFi et l'authentification d'utilisateurs.

Aller sur le réseau WiFi demandera une création d'un compte temporaire et dont l'entreprise recueille les données des utilisateurs avec leur accord.

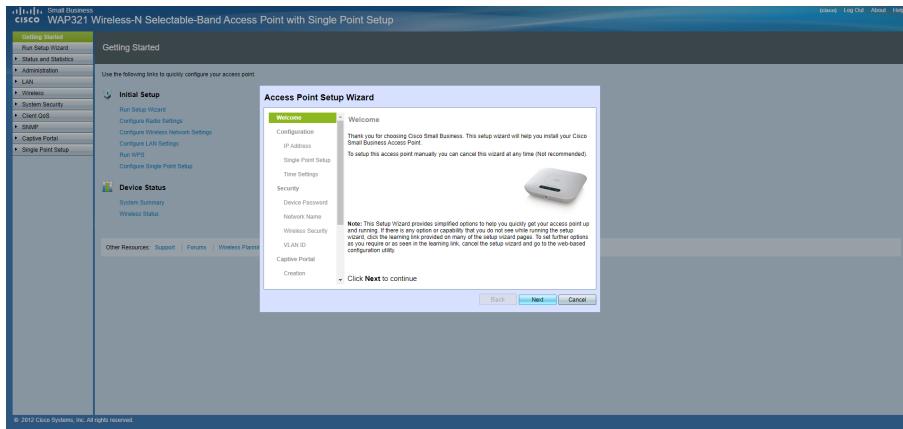
#### > Mise en place de la borne :

Nous allons prendre une **borne Cisco WAP321** dont l'alimentation de la borne est en PoE (soit **Power over Ethernet** est un équipement ne nécessitant pas beaucoup de volts et assure l'alimentation électrique et l'échange de paquets de données IP sur un même câble), avec deux câbles RJ45 (autrement appelé câble "Ethernet") d'une part pour la carte réseau Intel d'autre part pour la Broadcom qui est le réseau de la borne + la borne est reliée avec un câble rouge qui sert à alimenter la borne à partir du switch en PoE de la salle S4 et à le relier à la carte réseau Broadcom.

## > Configuration de la borne WiFi :

À partir de l'adresse IP par défaut de la borne (192.168.1.245) attribuée par le professeur (mais également trouvable dans la documentation de la borne), on peut accéder à la configuration de la borne en tapant l'adresse sur un navigateur.

Site/panneau de configuration de la borne WiFi avec l'adressage IP, le nom du réseau et les autres fonctionnalités pour la sécurité de la borne :



### Access Point Setup Wizard

**Welcome**

**Configuration**

**IP Address** (highlighted)

Single Point Setup

Time Settings

Security

Device Password

Network Name

Wireless Security

VLAN ID

Captive Portal

Creation

**Configure Device - IP Address**

Select either Dynamic or Static IP address for your device.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

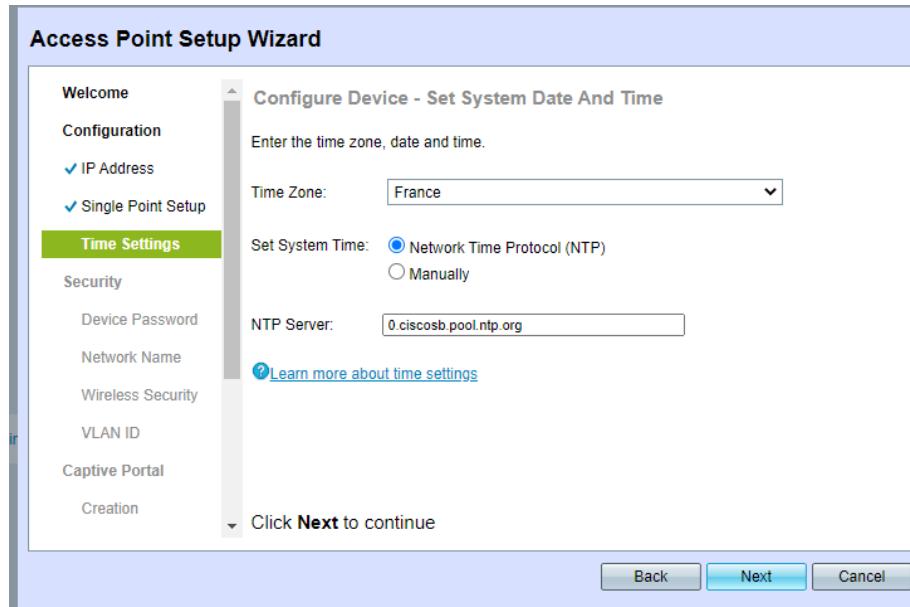
Secondary DNS (optional):  .  .  .

[? Learn more about the different connection types](#)

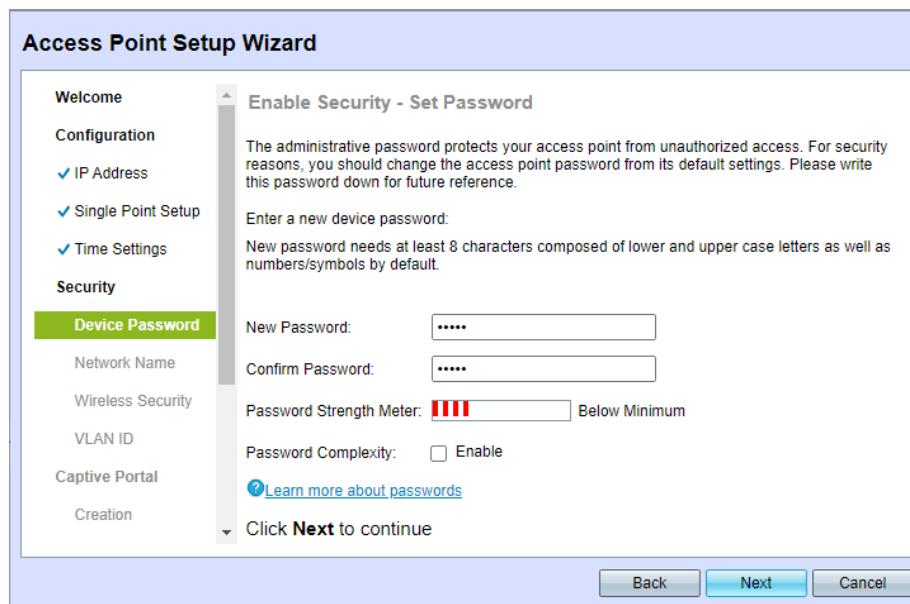
Click **Next** to continue

Back Next Cancel

Ensute on met en place le serveur NTP = Network Time Protocol (qui n'est pas obligatoire mais c'est mieux de le mettre) qui permet de mettre à jour automatiquement l'horloge de la borne, sur un réseau informatique.



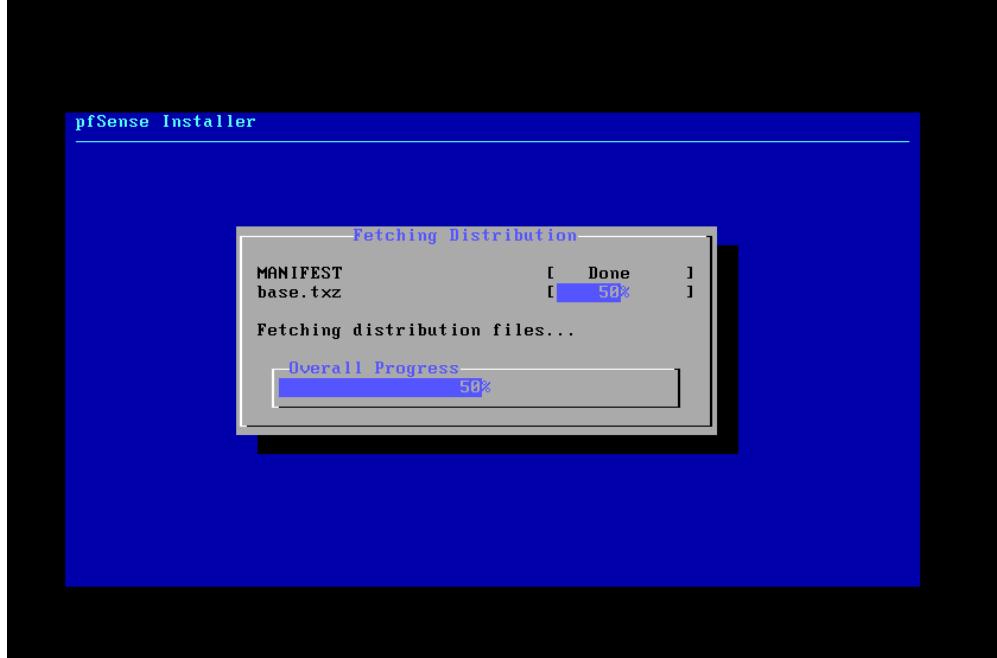
Ensute on écrit le mot de passe d'administrateur.



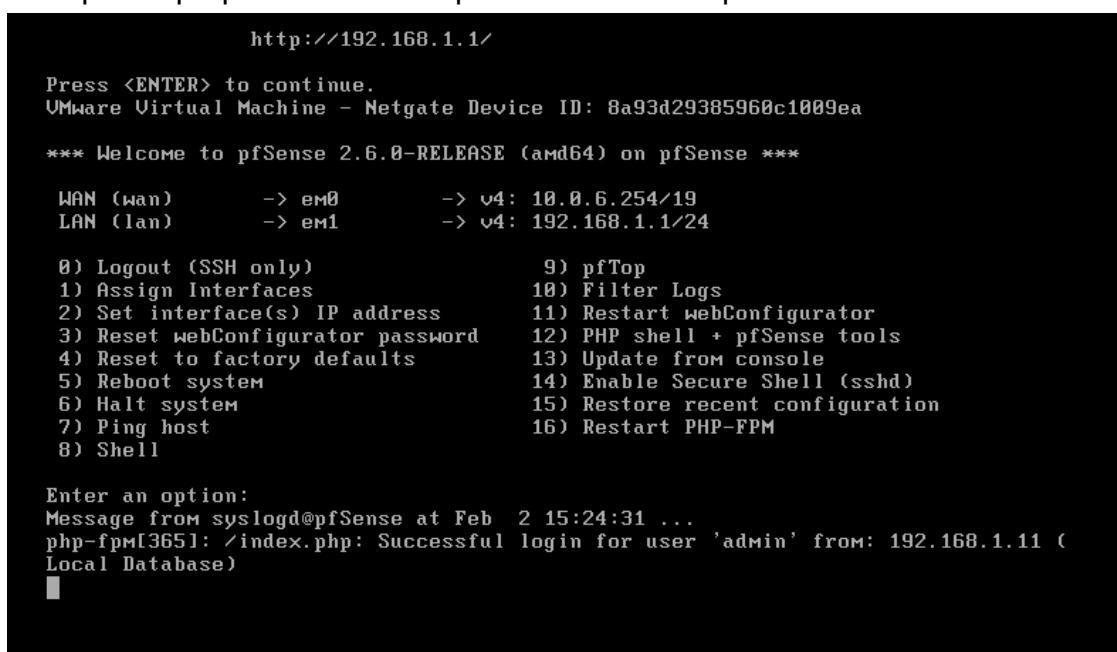
## > Création du portail captif & configuration des utilisateurs :

On souhaite que des utilisateurs s'authentifient via un portail captif pour accéder au WiFi. Pour cela, on va utiliser Pfsense (étant donné qu'il est utilisé pour le réseau EGNOM-BYOD...) sur une machine virtuelle (sous VMWare car c'est l'hyperviseur de préférence pour nous). Sur le site officiel de Pfsense, il faudra récupérer l'ISO de Pfsense. Il faudra extraire l'ISO qui est en .zip pour ainsi le convertir en extension .gz (format de compression pour les systèmes d'exploitation Linux et Unix.)

Installation de Pfsense :

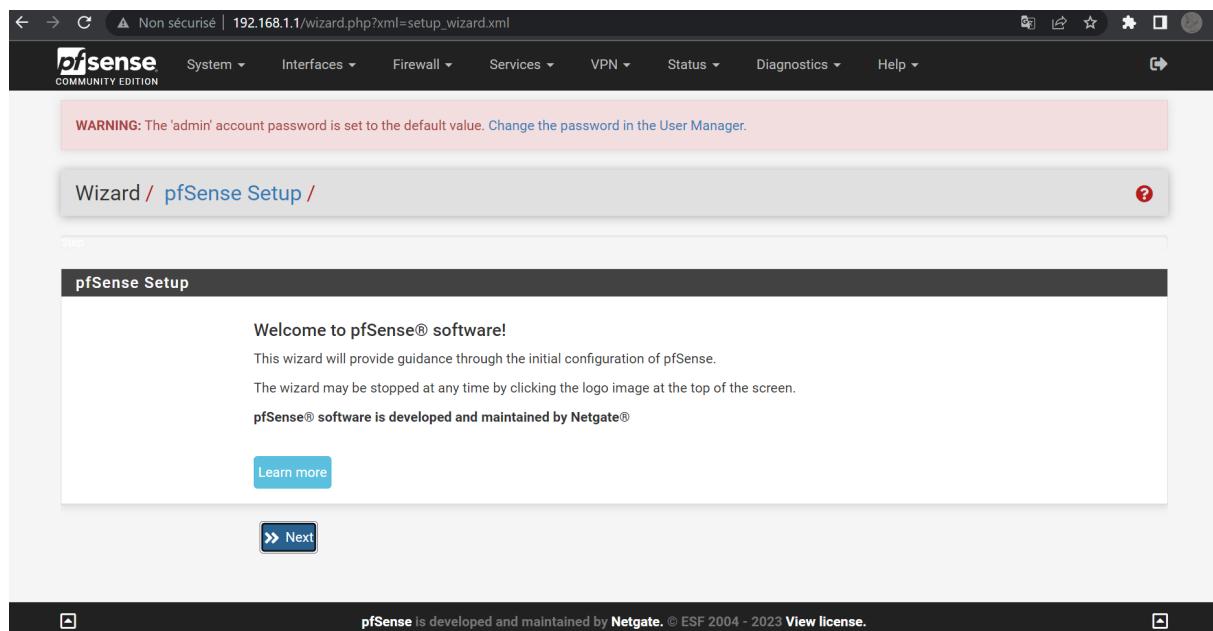
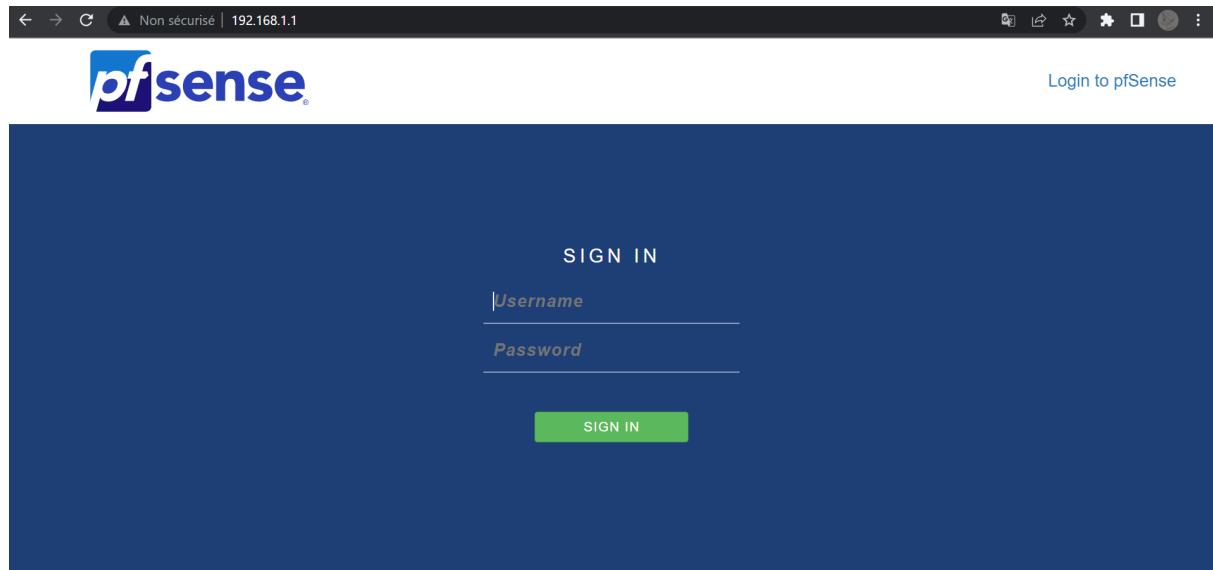


Après le bootage de Pfsense, il est possible de configurer le LAN, WAN et le reste des options proposées sur la capture d'écran en tapant un nombre entre 0 à 16.



(Si la VM est éteinte, plus rien ne fonctionne, il faut veiller à le laisser connecté)

Après avoir configuré les paramètres du portail captif, on se connecte avec notre WiFi et on inscrit notre IP de DNS sur un navigateur (par exemple Google Chrome pour nous). Le portail captif de PfSense apparaît, demandant de s'authentifier. On va se connecter sur le compte administrateur pour créer les utilisateurs pouvant accéder à notre WiFi à partir des identifiants conçus.



**User Properties**

Defined by	SYSTEM		
Disabled	<input type="checkbox"/> This user cannot login		
Username	admin		
Password	*****		
Full name	System Administrator User's full name, for administrative information only		
Expiration date			
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY			
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.		
Group membership	<table border="1"> <tr> <td>Not member of</td> <td>admins</td> </tr> </table>	Not member of	admins
Not member of	admins		
<input list"="" member="" of"="" type="button" value="» Move to "/> <input list"="" member="" not="" of"="" type="button" value="« Move to "/>			

Après la configuration du setup, on accède à la page d'accueil qui indique les informations du système à savoir le nom de notre DNS, le système qui "maintient la connexion" et la vitesse du WiFi (ainsi que d'autres informations).

**System Information**

Name	poulet.poulet.lab
User	admin@192.168.1.11 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 8a93d29385960c1009ea
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
The system is on the latest version. Version information updated at Tue Feb 7 13:42:23 CET 2023	
CPU Type	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4 CPUs: 2 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 17 Minutes 56 Seconds
Current date/time	Tue Feb 7 13:59:33 CET 2023

**Netgate Services And Support**

Contract type	Community Support Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES	
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the <a href="#">NETGATE RESOURCE LIBRARY</a> .  You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.	
<ul style="list-style-type: none"> <li>• <a href="#">Upgrade Your Support</a></li> <li>• <a href="#">Community Support Resources</a></li> <li>• <a href="#">Netgate Global Support FAQ</a></li> <li>• <a href="#">Official pfSense Training by Netgate</a></li> <li>• <a href="#">Netgate Professional Services</a></li> <li>• <a href="#">Visit Netgate.com</a></li> </ul>	
If you decide to purchase a Netgate Global TAC Support subscription, you <b>MUST</b> have your <a href="#">Netgate Device ID (NDI)</a> from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support <a href="#">here</a> .	

Afin de créer un utilisateur, il faut aller dans "System/User Manager/Users/Edit"

**Users**

- [Users](#)
- [Groups](#)
- [Settings](#)
- [Authentication Servers](#)

**User Properties**

Defined by	USER		
Disabled	<input type="checkbox"/> This user cannot login		
Username	user1		
Password	*****		
Full name	Utilisateur 1 User's full name, for administrative information only		
Expiration date			
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY			
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.		
Group membership	<table border="1"> <tr> <td>Not member of</td> <td>admins</td> </tr> </table>	Not member of	admins
Not member of	admins		
<input list"="" member="" of"="" type="button" value="» Move to "/> <input list"="" member="" not="" of"="" type="button" value="« Move to "/>			

Pour le portail captif, il faut aller dans “Services/Captive Portal” puis créer une zone de portail captif et configurer.

Services / Captive Portal

**Captive Portal Zones**

Zone	Interfaces	Number of users	Description	Actions
poulet	LAN	0	Bonjour les pouletos !	

**Captive Portal Configuration**

Enable  Enable Captive Portal

Description: Bonjour les pouletos !  
A description may be entered here for administrative reference (not parsed).

Interfaces: WAN, LAN

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

Maximum concurrent connections:

Idle timeout (Minutes):

Hard timeout (Minutes): 15

Traffic quota (Megabytes):

Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

## Configuration du serveur DHCP :

BOOTP  Ignore BOOTP queries

Deny unknown clients: Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients:  Denied clients will be ignored rather than rejected.  
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers:  If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.  
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet: 192.168.1.0

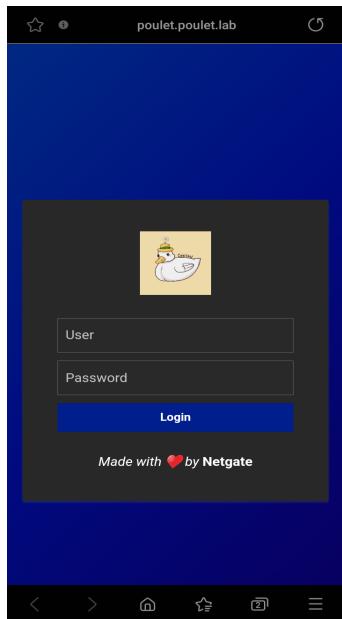
Subnet mask: 255.255.255.0

Available range: 192.168.1.1 - 192.168.1.254

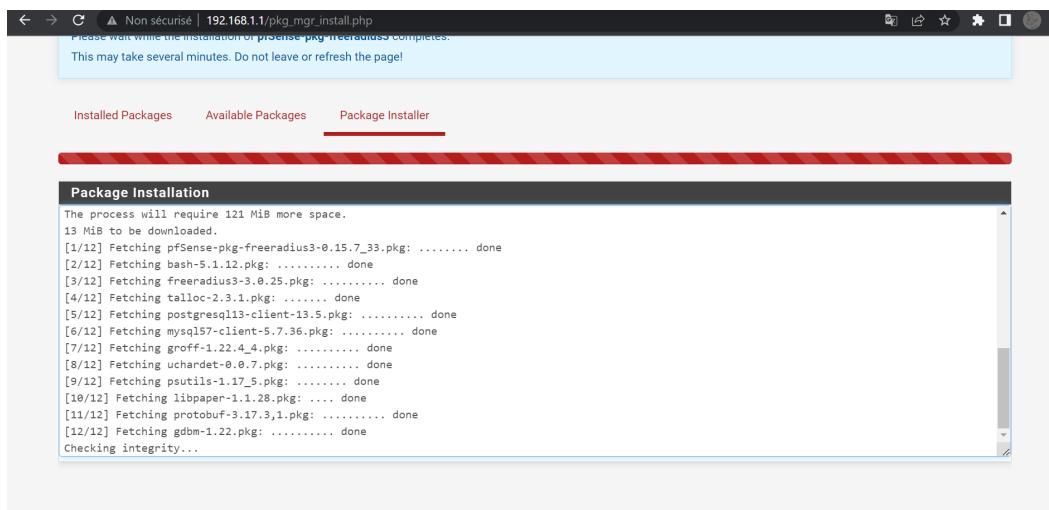
Range: 192.168.1.10 To 192.168.1.245

From:

Quand on se connecte sur le WiFi via mobile, la redirection sur le portail captif apparaît bien sur le navigateur (avec un petit logo pseudopouletmaiscanard !)



Dans System → Package Manager, nous prenons le paquet “Free Radius” qui permet d'avoir une base de données qui stockera les utilisateurs et qui mettra un time-out concernant leur authentification sur le réseau public.



On installe également le paquet “Squid Proxy” pour gérer le filtrage d'url web et bloquer l'accès aux utilisateurs à certains sites comme Youtube ou Twitter.

## Filtrage web :

Destination domains that will be accessible to the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Blacklist** youtube.com twitter.com lifeheberg.com

Destination domains that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Configuration de l'heure**

Date d'expiration	<input type="text"/>
Entrez la date à laquelle ce compte doit expirer. Format requis : Mmm jj aaaa (par exemple, 01 janvier 2012)	
Expiration de la session	<input type="text"/>
Saisissez le temps dont dispose cet utilisateur avant de se reconnecter (en secondes).	
Heures de connexion possibles	<input type="text"/>
Saisissez l'heure à laquelle cet utilisateur doit avoir accès. "Toujours" si aucune heure n'est saisie. Cliquez sur Infos pour plus de détails. <span style="color: blue;">i</span>	
Quantité de temps	<input type="text" value="15"/>
Entrez la durée pour ce nom d'utilisateur (en minutes).	
Période de temps	<input type="text" value="Pour toujours"/>
Sélectionnez la période de temps après laquelle le 'Amount of Time' est réinitialisé.	

Ensute on a été dans la configuration de NAS/client dans le service FreeRadius.  
Et on a entré l'adresse IP du client et le mot de passe du client.

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

**General Configuration**

<b>Client IP Address</b>	<input type="text" value="192.168.1.245"/>
Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).	
<b>Client IP Version</b>	<input type="text" value="IPv4"/>
<b>Client Shortname</b>	<input type="text" value="wap321"/>
Enter a short name for the client. This is generally the hostname of the NAS.	
<b>Client Shared Secret</b>	<input type="text" value="....."/>
Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. <b>Warning:</b> Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\").	

**Miscellaneous Configuration**

<b>Client Protocol</b>	<input type="text" value="UDP"/>
Enter the protocol the client uses (Default: UDP)	

## > Partie juridique :

### Condition d'utilisation lors de la création d'un compte

Avant de créer un compte, il est utile d'être en accord avec les conditions d'utilisation du service afin de préciser les différentes règles, donc ce que l'utilisateur peut et ne peut pas faire lorsqu'il se connecte sur le WiFi de l'entreprise, cela concerne tout autant les salariés que d'autres parties prenantes qui l'utilisent.

### Description du service :

Le WiFi permet aux utilisateurs de se connecter sur un réseau public au sein des locaux de l'entreprise. Il peut naviguer et publier du contenu comme des photos, des vidéos et du texte sur les différents sites qu'il recherche et consulte.

### Les droits et les obligations de l'utilisateur :

Les utilisateurs sont limités à 15 minutes de connexion. Après le délai dépassé, ils seront automatiquement redirigés sur le portail captif et déconnectés du réseau. L'accès aux sites comme YouTube et Twitter est bloqué et toutes tentatives de contournement à cette règle mèneront à des sanctions.

### Les conditions d'utilisation d'un forum ou d'un espace de libre échange :

L'éditeur n'est pas tenu responsable en cas de propos injurieux ou de publication de contenu contrefaisant les droits de propriété intellectuelle d'un tiers. Il est interdit à tout utilisateur de poster les informations confidentielles de l'entreprise auquel cas des sanctions seront appliquées par l'entreprise et/ou le tribunal.

### Les modalités de règlement des litiges :

En cas de litige, l'utilisateur doit avoir le choix entre le tribunal de son domicile ou le tribunal du lieu de la société éditrice du site.

Les CGU doivent également être affichés sur le portail captif pour que les utilisateurs soient au courant des conditions et de ce qu'ils sont autorisés à faire sur ce service. Pour cela, on se dirige dans les configurations du portail captif sur Pfsense et on inscrit la description dans "Terms and conditions".

Ensuite sur un appareil comme un smartphone, on se connecte sur le portail captif et lorsqu'on appuie et coche sur les termes et les conditions, on voit la description en dessous.

**Captive Portal Login Page**

Display custom logo  Enable to use a custom uploaded logo image

Logo Image  Aucun fichier choisi

Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.\* The image can be of any image type: .png, .jpg, .svg **This image will not be stored in the config.** The default logo will be used if no custom logo is selected.

Display custom background image  Enable to use a custom uploaded background image

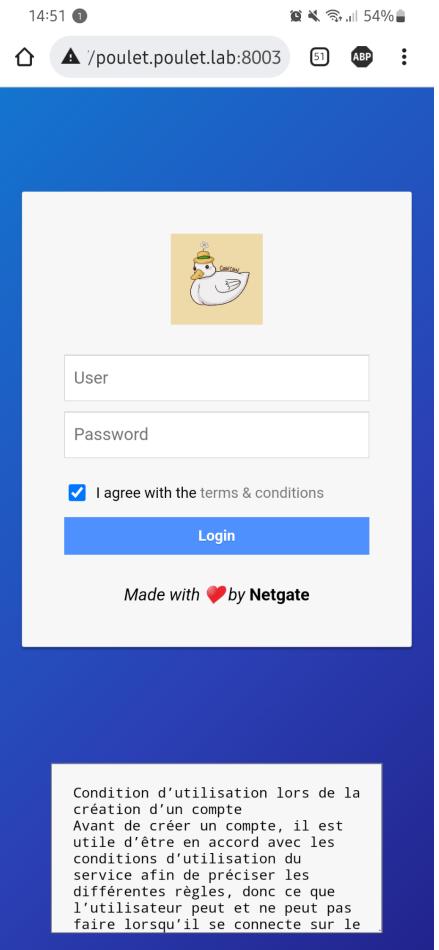
Background Image  Aucun fichier choisi

Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.\* The image will not be stored in the config. The default background image will be used if no custom background image is selected.

**Terms and Conditions**

Condition d'utilisation lors de la création d'un compte  
Avant de créer un compte, il est utile d'être en accord avec les conditions d'utilisation du service afin de préciser les différentes règles, donc ce que l'utilisateur peut et ne peut pas faire lorsqu'il se connecte sur le

Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out



## > Problèmes rencontrés :

1. Un souci avec la borne WiFi Cisco Aironet car lorsqu'on voulait changer les paramètres du WiFi avec nos propres informations, cela affichait "404 not found" et remettait sur les anciens paramètres, alors nous avons pris la borne WAP321 qui ne nécessite plus le câble console et la M&J de l'ISO Cisco (où nous avons aussi eu une mauvaise version de l'image).
2. L'ISO Pfsense devait être dézippé + mettre le fichier en .gz + il fallait mettre la VM en pont et non pas en NAT. Il fallait notamment faire attention à ne pas installer l'ISO "en live" et booter sur le disque dur.
3. Le portail captif n'est pas sécurisé et on ne peut pas se connecter avec les identifiants d'utilisateur réalisés avec le radius alors nous sommes restés en local database. Le radius est cependant utile pour surveiller l'activité d'un compte d'utilisateur.
4. La blacklist du Squid Proxy (une fonctionnalité de Pfsense) ne fonctionne pas, même en mettant les DNS des sites souhaités comme youtube.com ou twitter.com. (au final ça a marché un instant)
5. Le radius ne fonctionnait pas car la borne est configurée en 10.0.0.17 et le portail captif Pfsense est configuré en 192.168.1.1, ce n'est pas dans le même réseau.

## > Sources et annexes :

Documentation sur la borne Cisco WAP321 Wireless-N :

[https://www.cisco.com/c/dam/en/us/td/docs/wireless/access\\_point/csbap/wap121/administration/guide/fr\\_FR/1CSWAP121\\_321-SWUM1xx.pdf](https://www.cisco.com/c/dam/en/us/td/docs/wireless/access_point/csbap/wap121/administration/guide/fr_FR/1CSWAP121_321-SWUM1xx.pdf)

Tutoriel pour la mise à jour OS de la borne (pour l'ancienne borne utilisée...) :

<https://www.inspectmygadgets.com/converting-a-cisco-aironet-ap-to-standalone-autonomous-mode/>

### Note au cas où, pour une mise à jour de borne avec cette méthode :

Mettre à jour nous permettra de visualiser les différentes informations de la borne et de configurer des paramètres propres à nous, comme changer le nom par exemple. Avant tout, il faut un câble console relié entre le PC et la borne pour visualiser les informations qui passent dans la borne via PuTTY en Serial. Ensuite, nous installons Tftpd64 (un programme open-source créé par P. Jounin qui intègre des services de transferts de fichiers via TFTP, DHCP, DNS...) pour le téléchargement de l'ISO Cisco que nous allons déposer sous le répertoire C:\Users\Pipouette\Desktop\Cisco.

Nous pouvons alors configurer les paramètres de la borne en tapant l'IP de la borne sur le navigateur (pour la trouver, il faut taper la commande "show ip interface" sur la console de commande de PuTTY)

Comment configurer un portail captif avec PfSense :

<https://neptunet.fr/pfsense-install/>

<https://www.pc2s.fr/pfsense-installation-et-configuration/>

<https://www.pfsense.org/download/> (Pour avoir l'ISO Pfsense, prendre l'architecture AMD64 (64-bit) et choisir DVD Image (ISO) Installer)

Authentification des utilisateurs sur Pfsense :

<https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/>

<https://techexpert.tips/fr/pfsense-fr/pfsense-authentification-radius-a-laide-de-freeradius/>

Filtrage URL Web avec le paquet Squid Proxy Server:

<https://www.it-connect.fr/proxy-transparent-mise-en-place-de-squid-sur-pfsense/>

Tutoriel pour rédiger les CGU :

<https://www.francenum.gouv.fr/guides-et-conseils/developpement-commercial/site-web/rediger-des-conditions-generales-dutilisation>

<https://www.captaincontrat.com/contrats-commerciaux-cgv/cgv-cgu-cga/cgu-conditions-generales-utilisation>

**> Bloc-note (pour nous) :**

**Groupe 6 → IP : 10.0.6.17 (ou 19) Psd : 10.0.0.253**

**IP Borne Cisco WAP321 : 192.168.1.245**

**Nom du WiFi :** Poulet

**Identifiant borne Cisco :** Id : cisco / Mdp : cisco

**IP WAN : 10.0.6.254 /24**

**IP LAN/IP du portail d'authentification :** 192.168.1.1

**Plage DHCP :** 192.168.1.10 à 192.168.1.20

**Identifiant admin de Pfsense :** Id : admin / Mdp : poulet

**Identifiants créés pour l'accès au WiFi :**

Id : user1 / prof / nico

Mdp : mdp1 / prof / nico

**DNS Wifi (ne pas oublier de se connecter sur le réseau Poulet) :**

<http://poulet.poulet.lab> / <http://192.168.1.1>

**Nextcloud de la classe (où l'on se partage un peu tout) :**

<https://nextcloud.btssio.tk/s/J5pz5fefKWMHrql>