MAO Pauline **Année 2022/2023**
OUDAR Nicolas
SIO1 SISR

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.

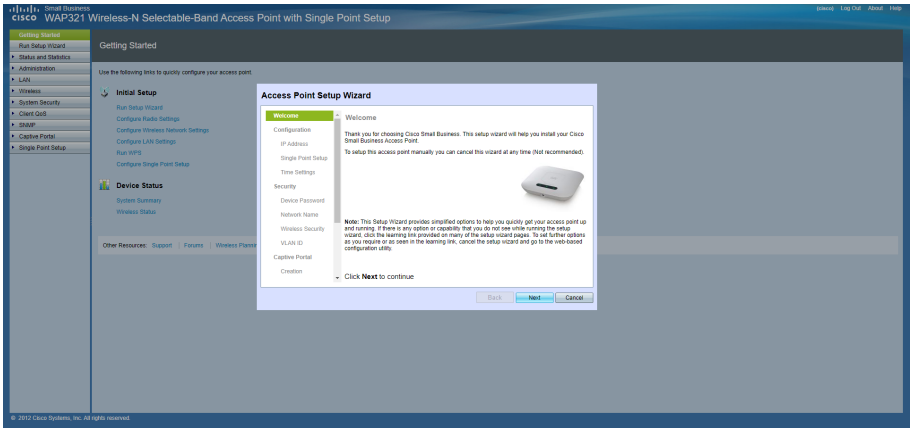
> Mise en place de la borne :

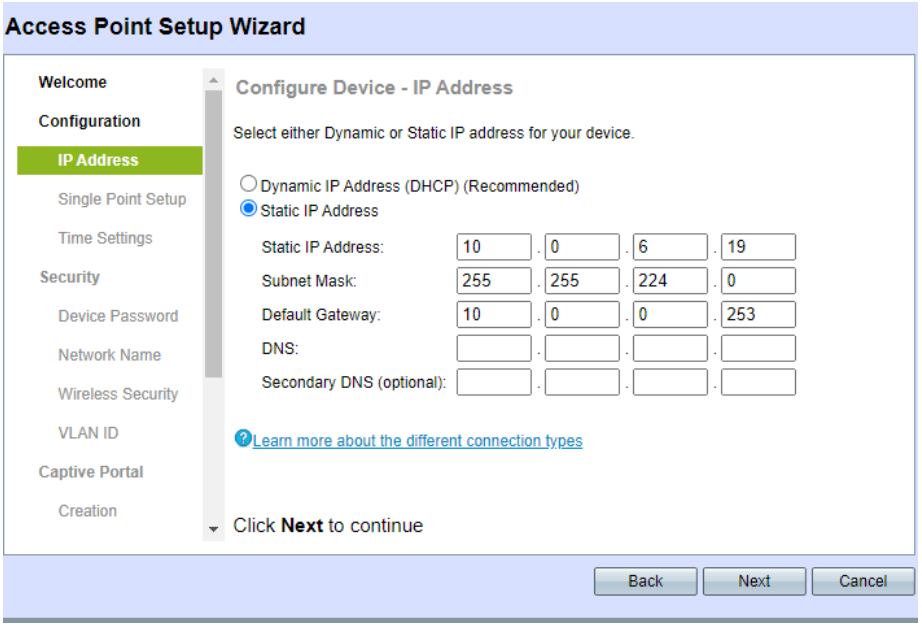
Nous allons prendre une **borne Cisco WAP321** dont l'alimentation de la borne est en PoE (soit **Power over Ethernet** est un équipement ne nécessitant pas beaucoup de volts et assure l'alimentation électrique et l'échange de paquets de données IP sur un même câble), avec deux câbles RJ45 (autrement 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 :

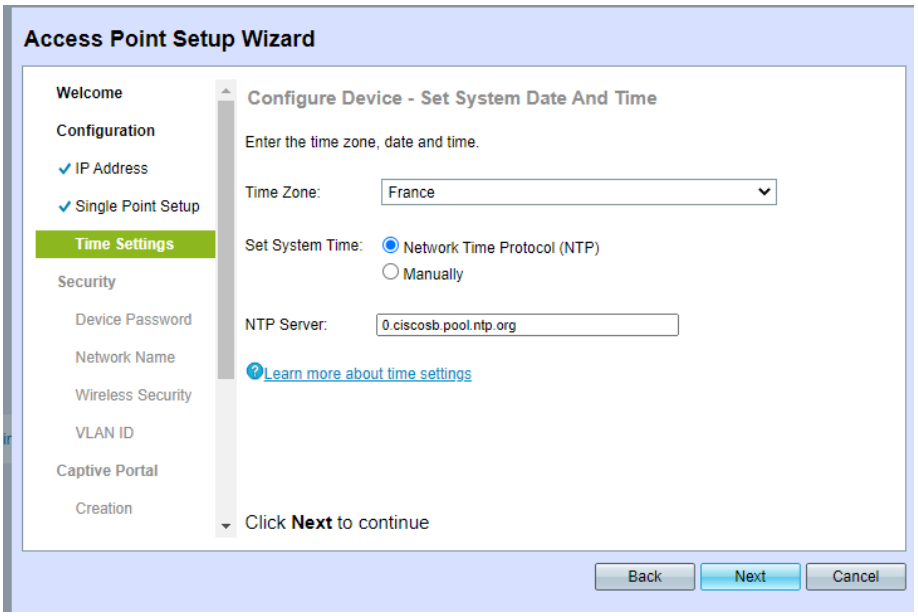
À partir de l'adresse IP par défaut de la borne (192.168.1.245) attribuée par le professeur (mais également trouvable dans la documentation de la borne), on peut accéder à la configuration de la borne en tapant l'adresse sur un navigateur.

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 :

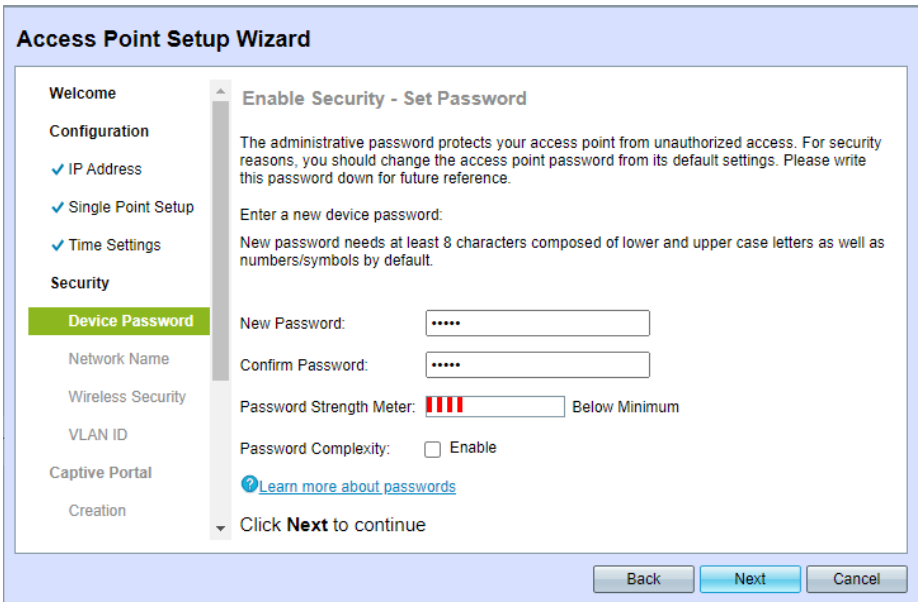




Ensuite on met en place le serveur NTP = Network Time Protocol (qui n'est pas obligatoire mais c'est mieux de le mettre) qui permet de mettre à jour automatiquement l'horloge de la borne, sur un réseau informatique.

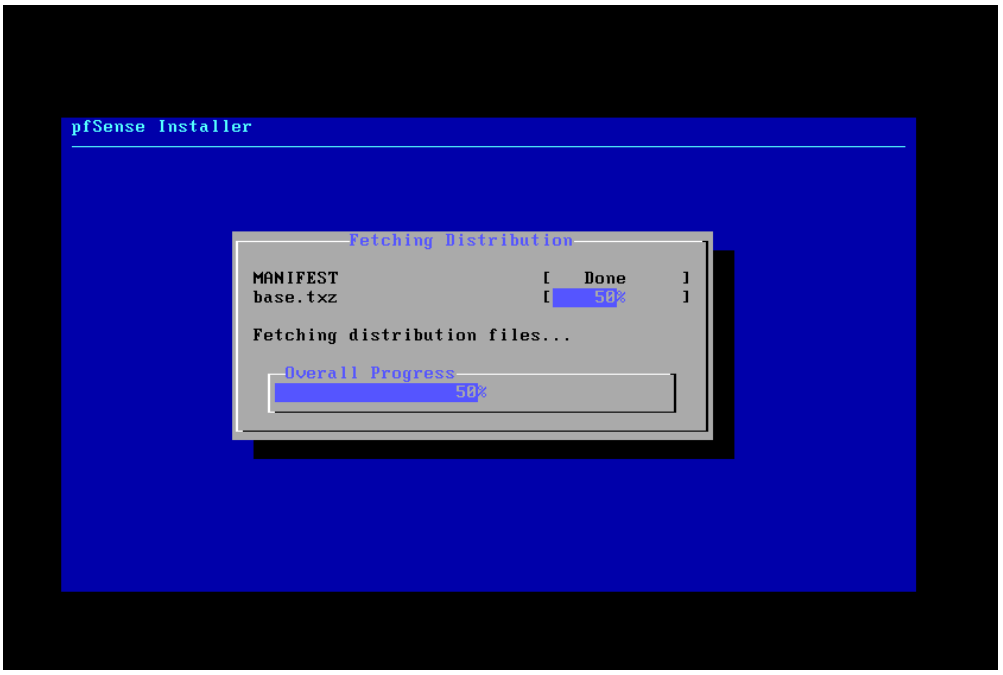


Ensuite on écrit le mot de passe d'administrateur.



> Création du portail captif & configuration des utilisateurs :

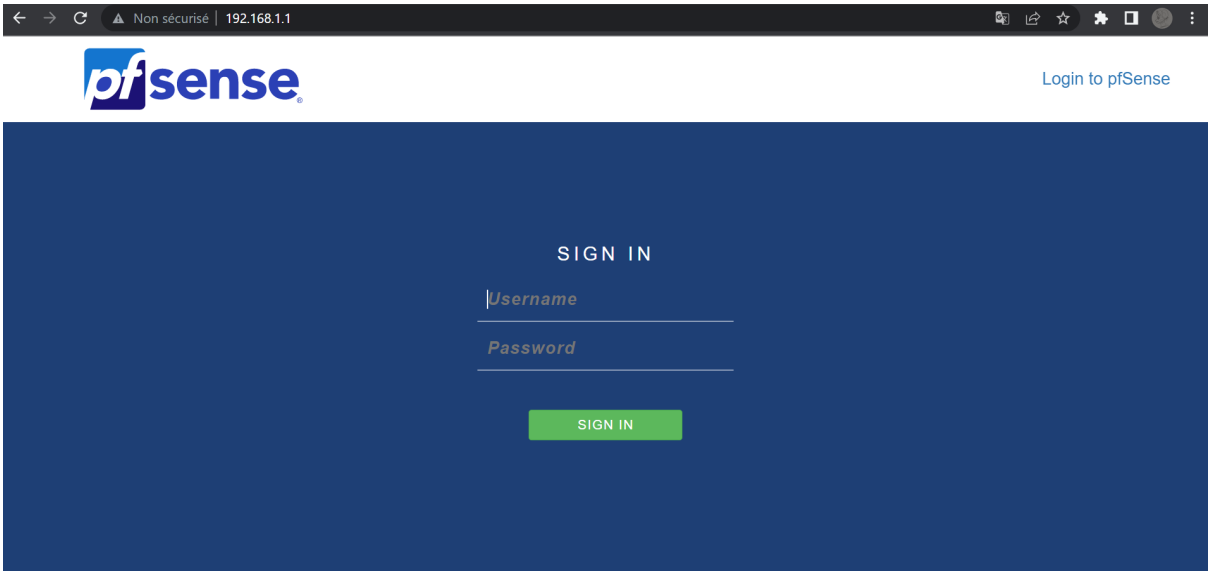
On souhaite que des utilisateurs s'authentifient via un portail captif pour accéder au WiFi. Pour cela, on va utiliser Pfsense (étant donné qu'il est utilisé pour le réseau EGNOM-BYOD…) sur une machine virtuelle (sous VMWare car c'est l'hyperviseur de préférence pour nous). Sur le site officiel de Pfsense, 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 :

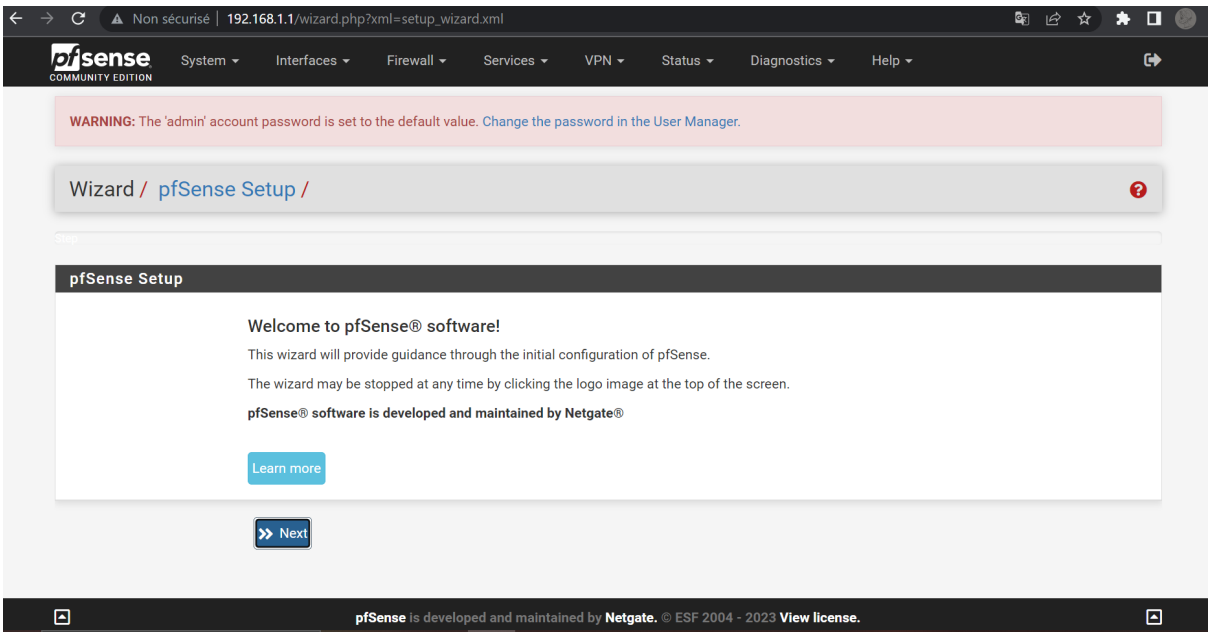


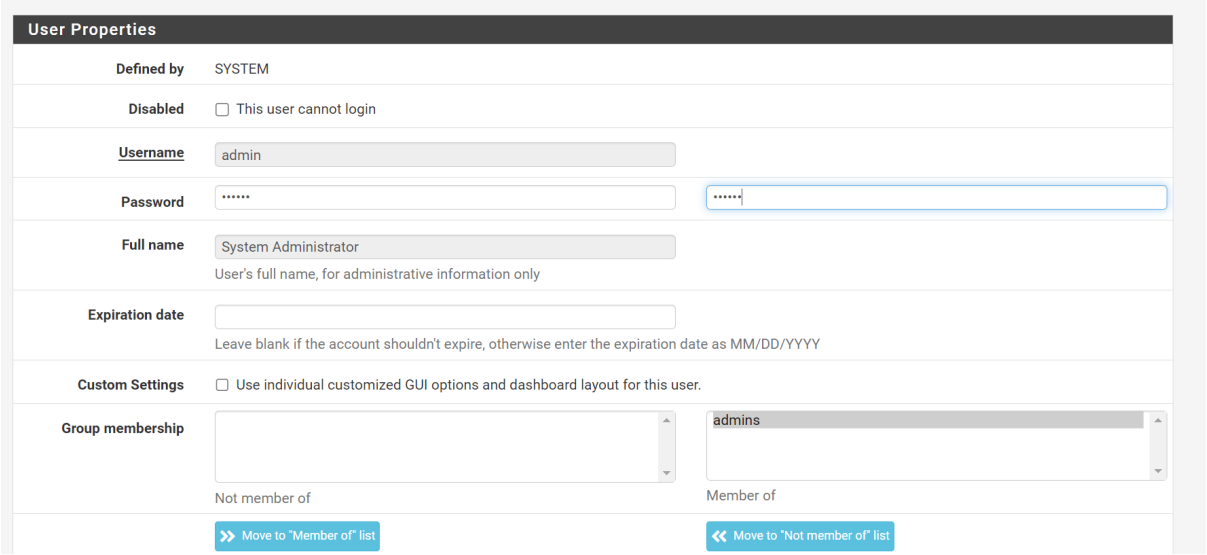
Après le bootage de Pfsense, il est possible de configurer le LAN, WAN et le reste des options proposées sur la capture d'écran en tapant un nombre entre 0 à 16.

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

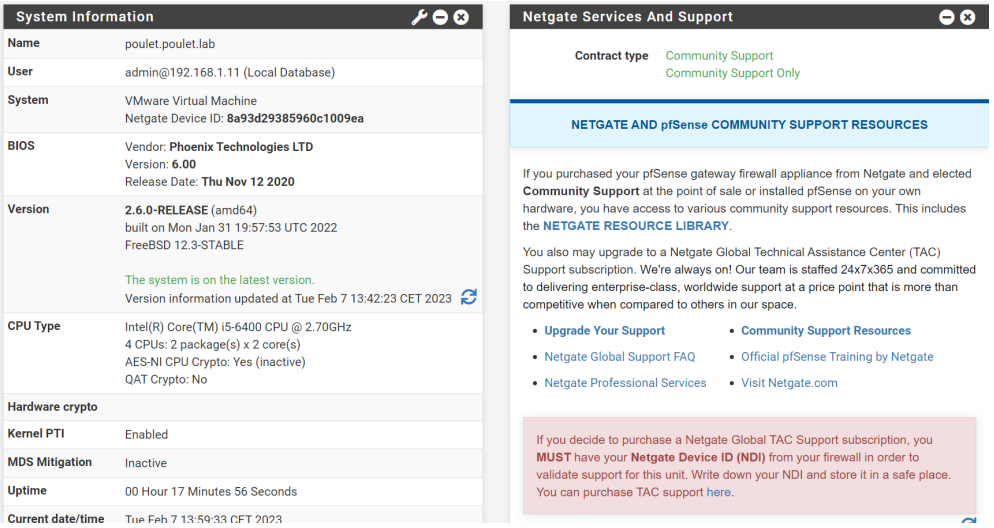
Après avoir configuré les paramètres du portail captif, on se connecte avec notre WiFi et on inscrit notre IP de DNS sur un navigateur (par exemple Google Chrome pour nous). Le portail captif de Pfsense apparaît, demandant de s'authentifier. On va se connecter sur le compte administrateur pour créer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



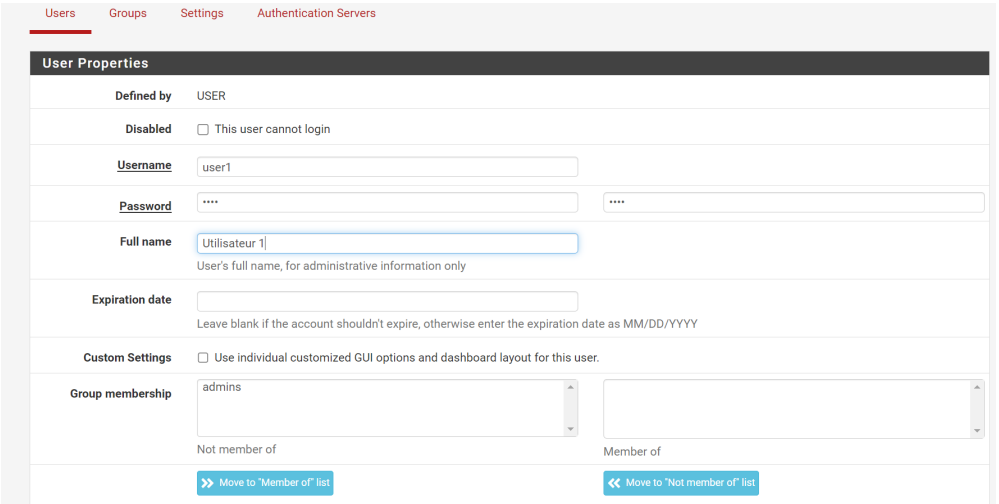




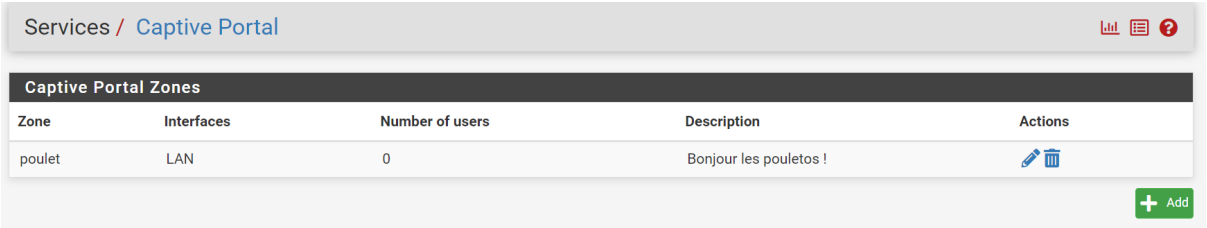
Après la configuration du setup, on accède à la page d'accueil qui indique les informations du système à savoir le nom de notre DNS, le système qui "maintient la connexion" et la vitesse du WiFi (ainsi que d'autres informations).

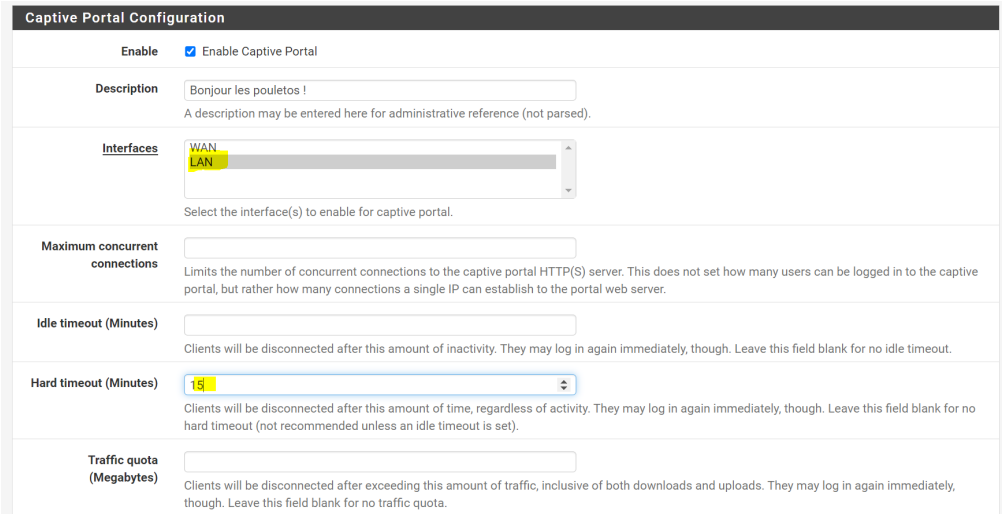


Afin de créer un utilisateur, il faut aller dans "System/User Manager/Users/Edit"

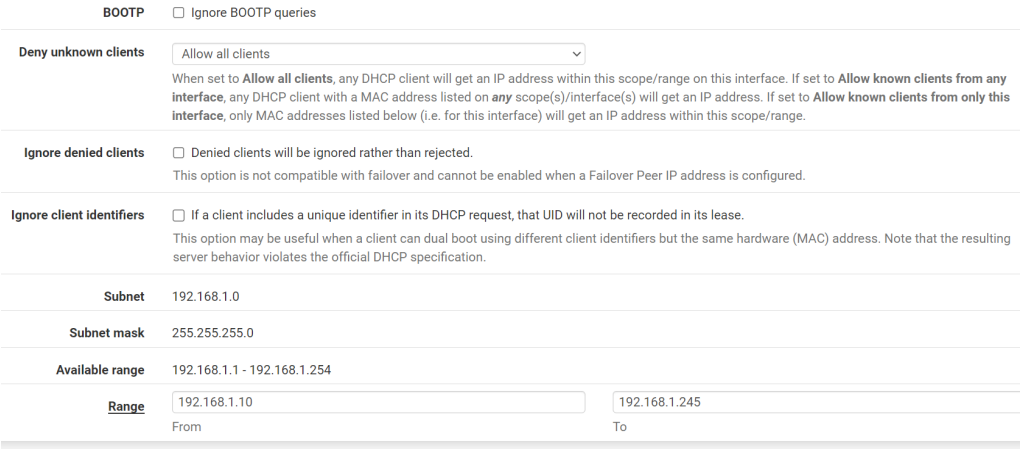


Pour le portail captif, il faut aller dans “Services/Captive Portal” puis créer une zone de portail captif et configurer.

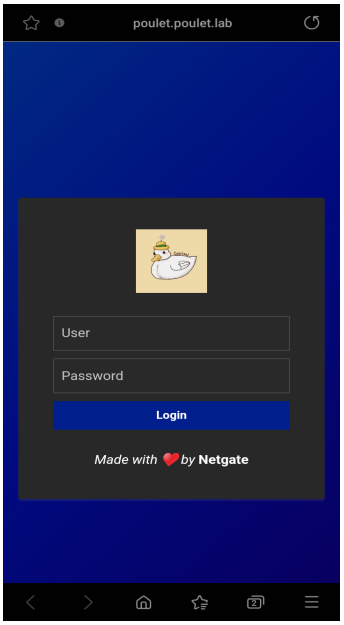




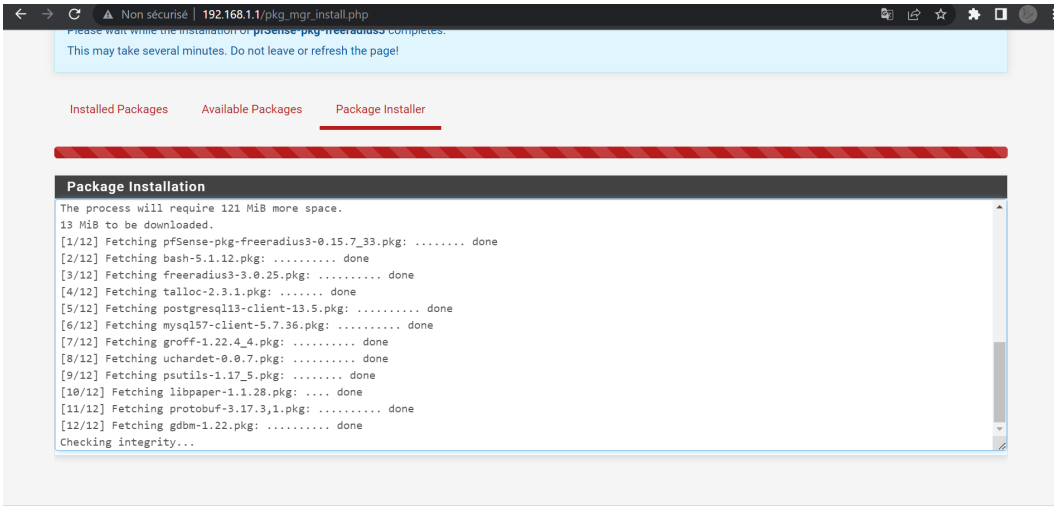
Configuration du serveur DHCP :



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 !)

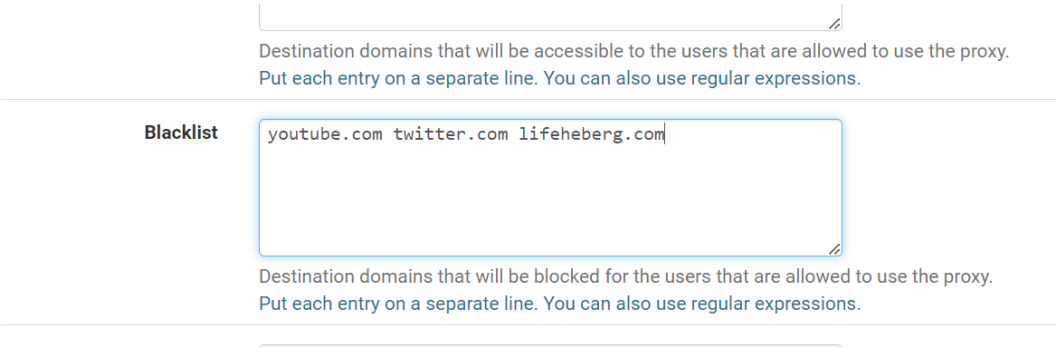


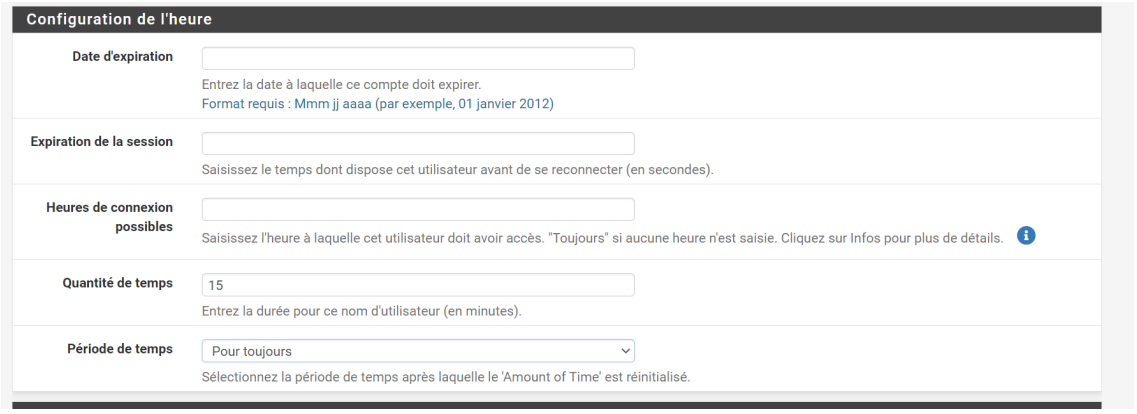
Dans System → Package Manager, nous prenons le paquet “Free Radius” qui permet d’avoir une base de données qui stockera les utilisateurs et qui mettra un time-out concernant leur authentification sur le réseau public.



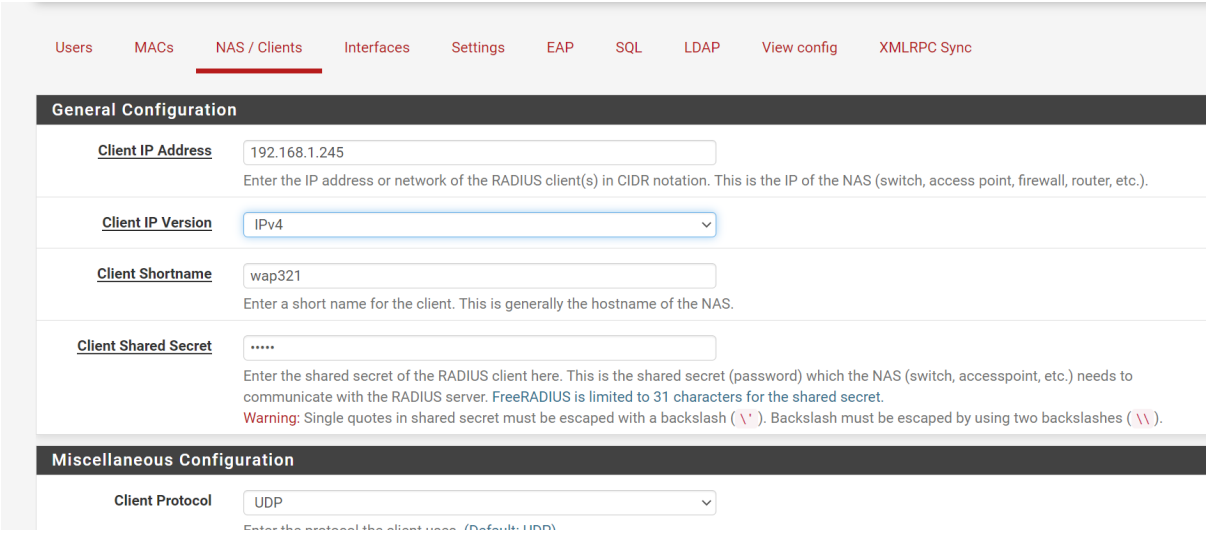
On installe également le paquet “Squid Proxy” pour gérer le filtrage d’url web et bloquer l’accès aux utilisateurs à certains sites comme Youtube ou Twitter.

Filtrage web :





Ensuite 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.



> 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.

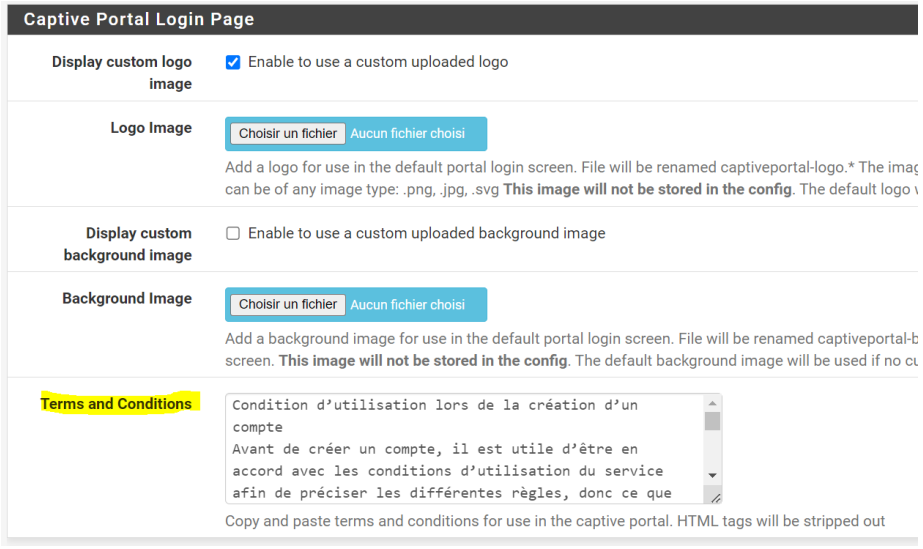
Les conditions d'utilisation d'un forum ou d'un espace de libre échange :

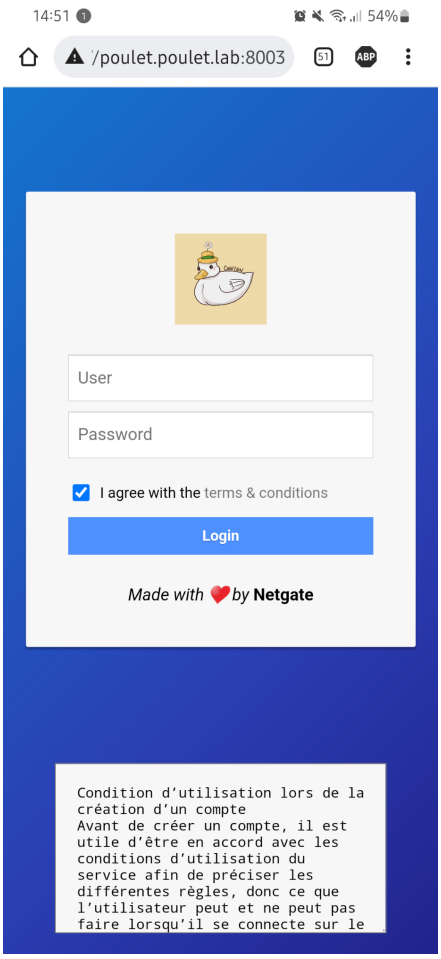
L'éditeur n'est pas tenu responsable en cas de propos injurieux ou de publication de contenu contrefaisant les droits de propriété intellectuelle d'un tiers. Il est interdit à tout utilisateur de poster les informations confidentielles de l'entreprise auquel cas des sanctions seront appliquées par l'entreprise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





> 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 MàJ 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

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