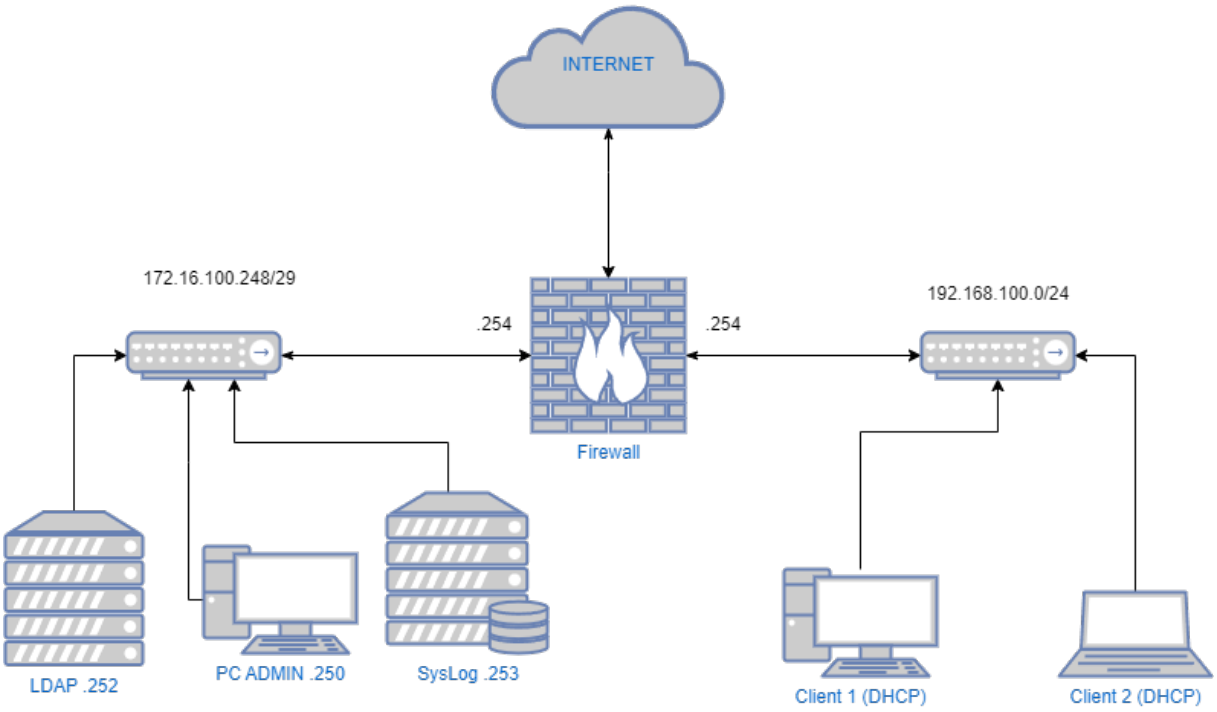
Objectif de cette mission : Dans le cadre du réseau de la M2L, proposer un système d'authentification sécurisé par portail captif afin de gérer l'accès à internet.

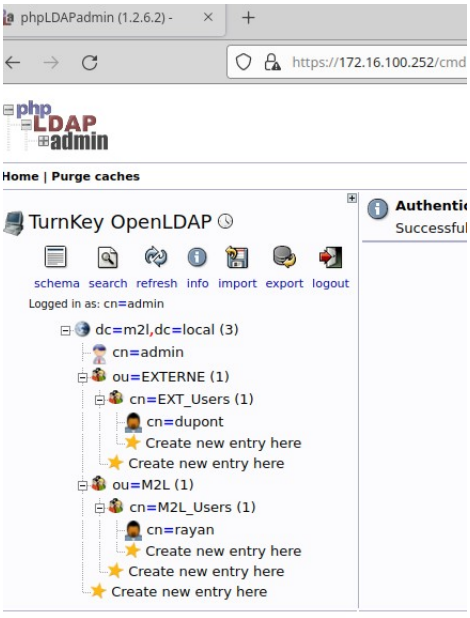
Voici le schéma du réseau utilisé dans cette mission :



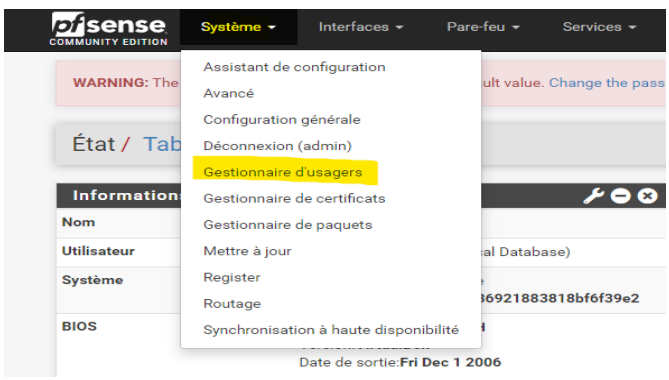
Ce compte rendu s'appuiera sur les Annexes 1 et 2 qui détaillerons l'installation des services LDAP (Annexe 1) et SysLog (Annexe 2).

Pour l'installation du serveur LDAP, se référer à l'annexe 1.

Configuration du serveur LDAP :



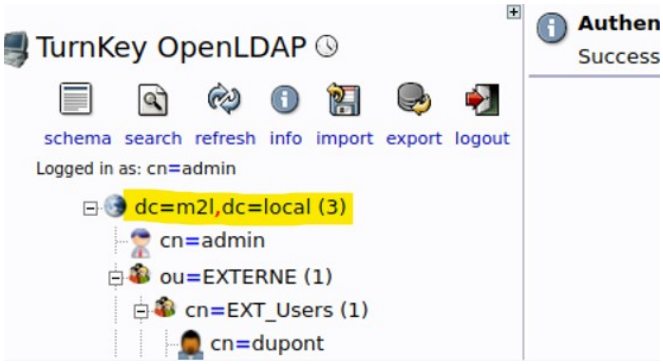
Une fois la configuration du serveur LDAP ainsi que la création d'utilisateurs effectuée, nous allons ajouter ce serveur en tant que base d'utilisateurs sur le pfSense dans « Système », « Gestionnaire d'usagers » puis « Serveur d'authentification ».



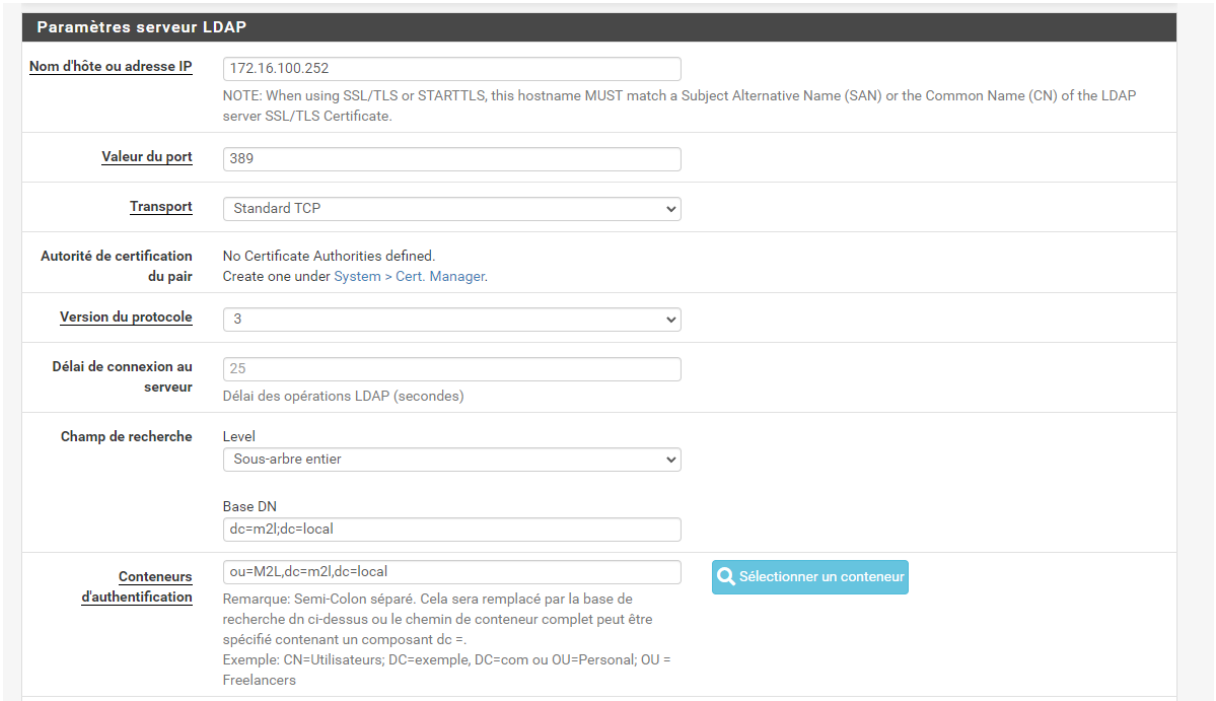
Après avoir cliqué sur « ajouter », nous renseignons les informations du serveur LDAP :

Dans « Base DN » nous saisissons le nom absolu de la racine du serveur LDAP

que l'on retrouve ici :



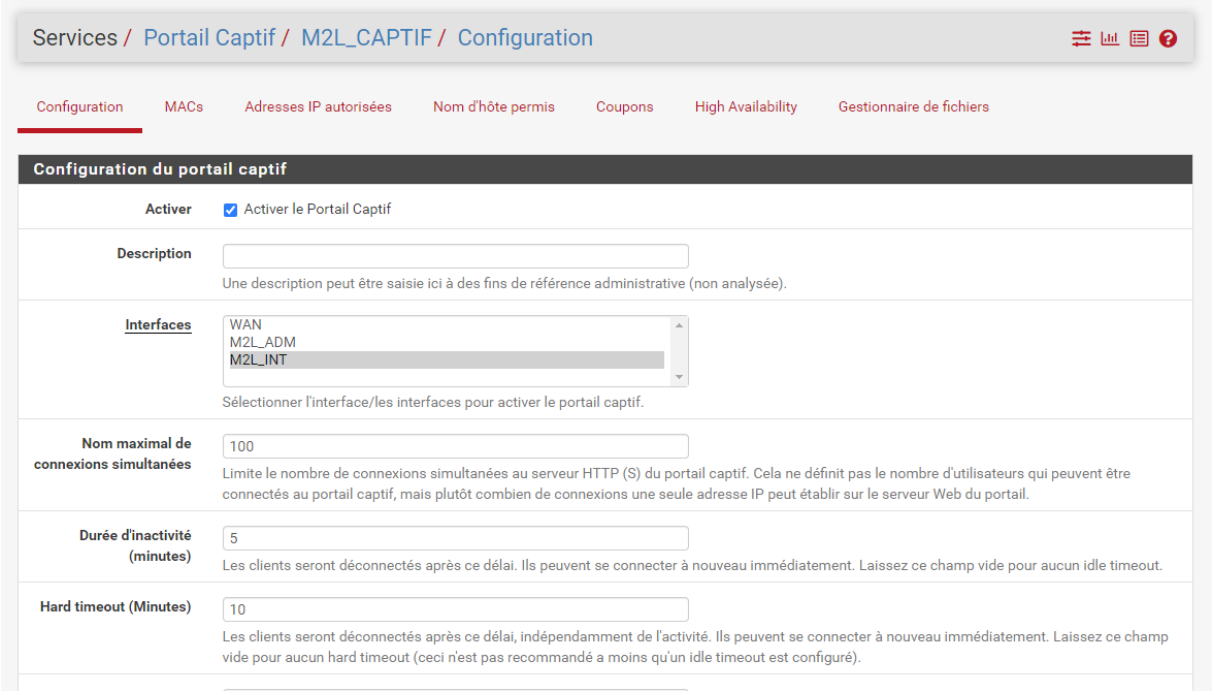
Dans « Conteneurs d'authenfication », nous pouvons saisir le DN de la base puis cliquer sur « Sélectionner un conteneur » pour choisir l'OU, ou alors nous pouvons directement taper le DN de l'OU que l'on retrouve ici :



Après avoir enregistrer les informations d'authentifications, il faut activer le portail captif. Pour ce faire, allez sur « Service », « Portail captif » puis « Ajouter ».

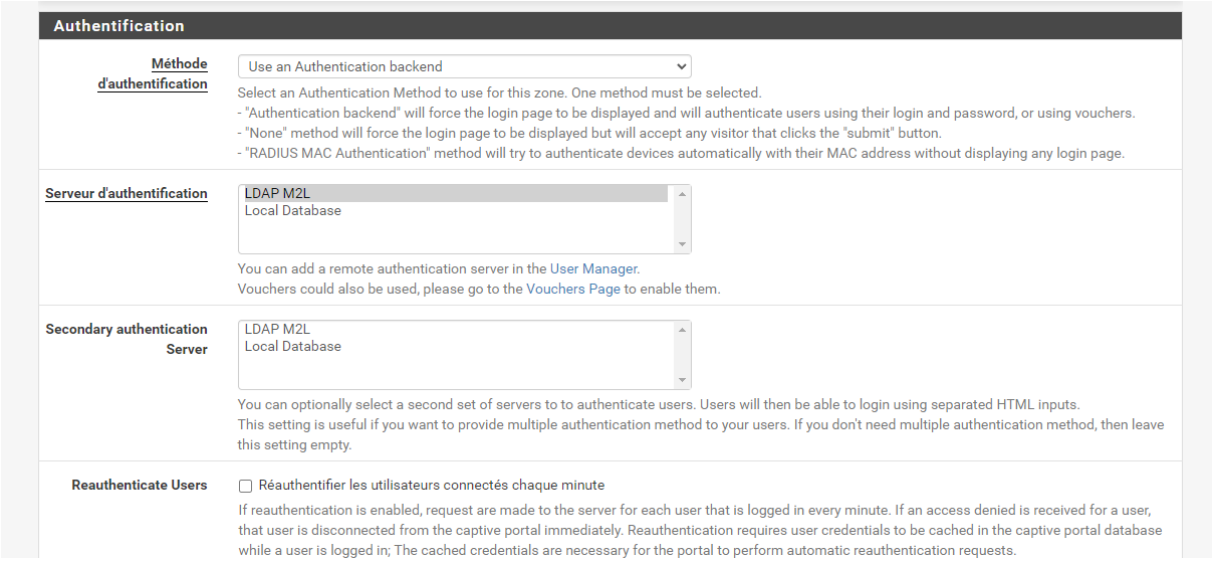
Ici, nous allons configurer les paramètres du portail captif comme l'interface pour laquelle il faut authentifier la connexion WEB, le nombre de connexions en simultanés, le timetout, ...

Ici, nous activons le portail sur l'interface interne du réseau M2L (là où nous aurons les machines clientes de la M2L).



Dans la section « Authentification », nous sélectionnons le serveur LDAP précédemment configuré.

Nous pouvons également proposer un second serveur d'authentification (local ou distant) si besoin.

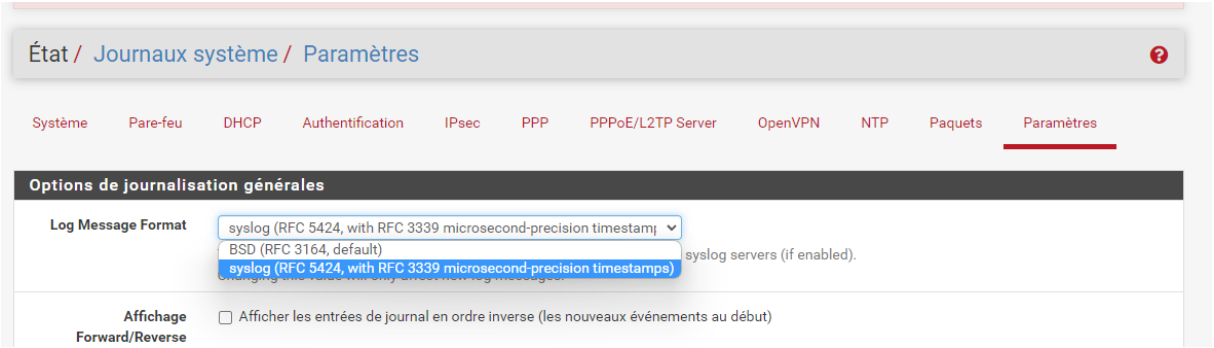


Configuration du syslog

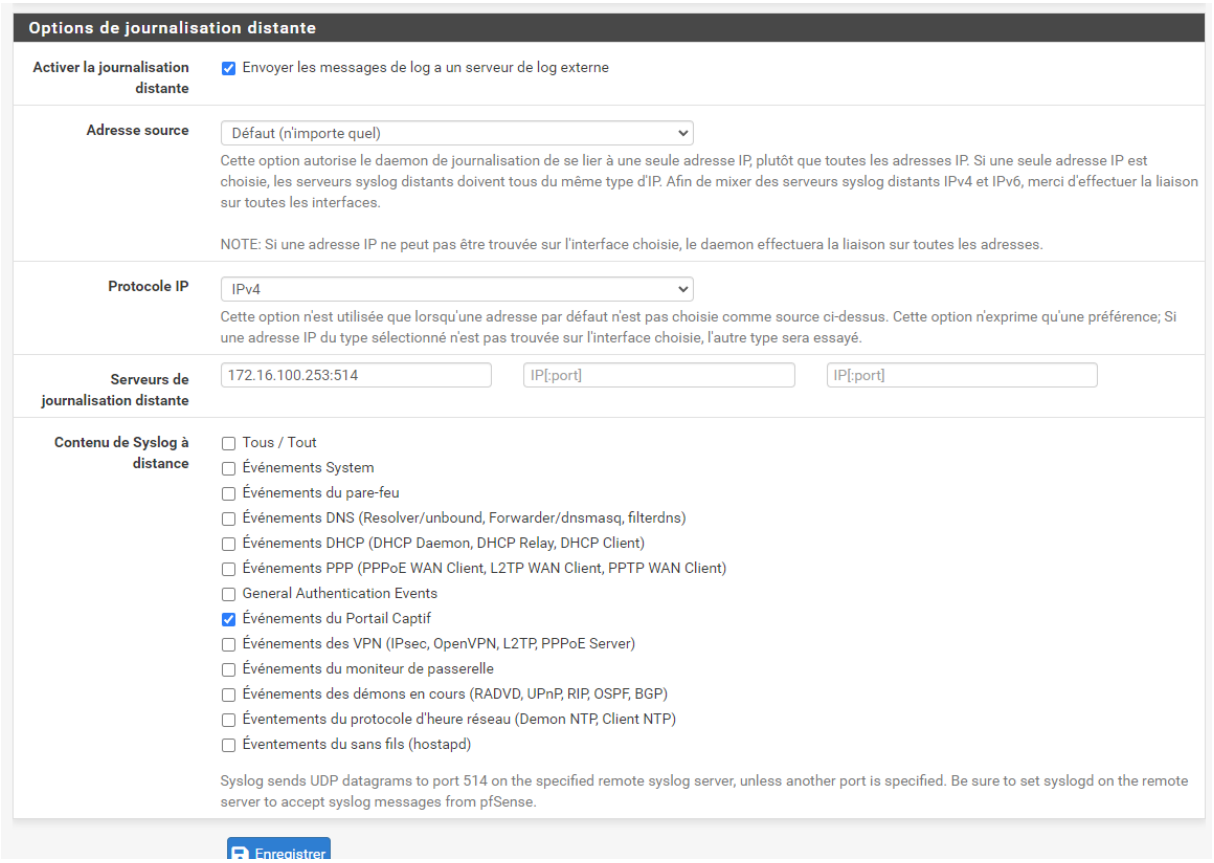
Maintenant que le portail captif est en place, il faut configurer pfSense de sorte à ce qu'il remonte les logs de connexions au serveur Syslog précédemment installé (Voir annexe 2).

Dans pfSense, aller dans « Etat », « Journaux système » puis « Paramètres ».

Préciser ici le format « Syslog RFC5424 » pour l'envoie des journaux.

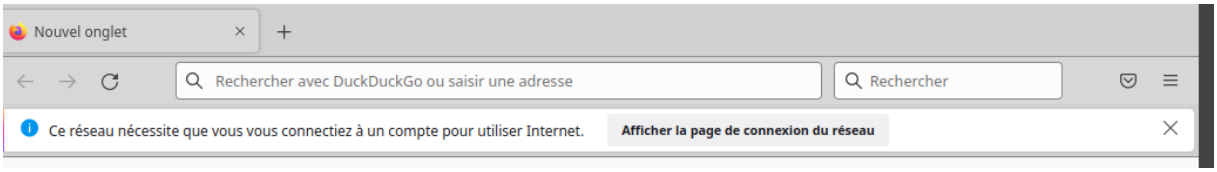


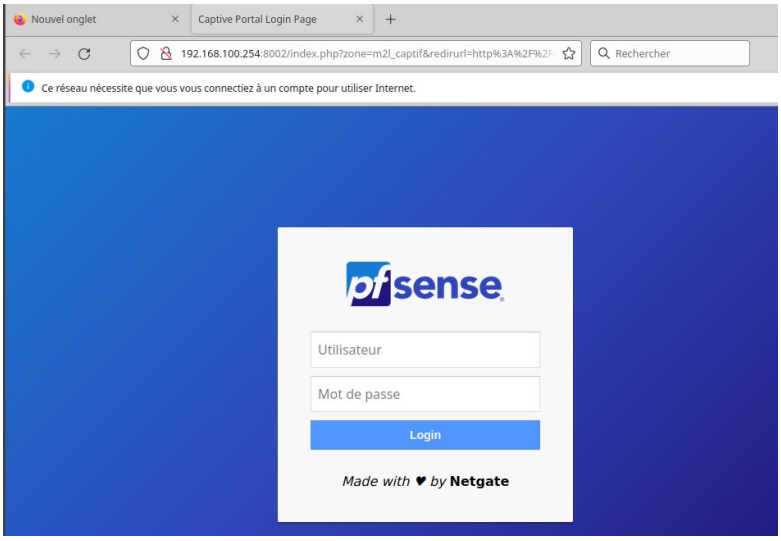
Dans les options de journalisation distantes, mettre l'@IP du serveur Syslog ainsi que le port choisi (ici le port par défaut, 514), puis sélectionner les informations à envoyer au serveur, ici nous allons sélectionner les évènements du portail captif.



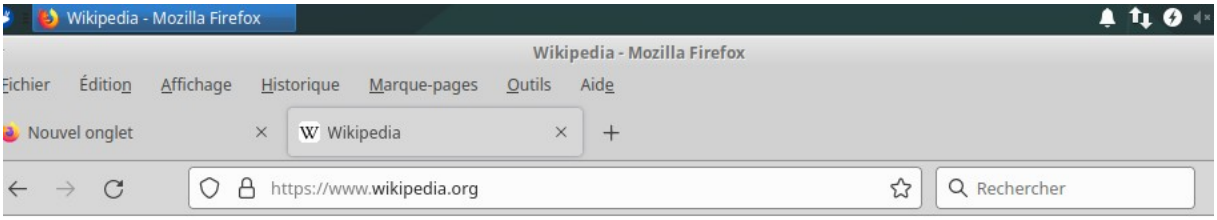
Une fois le serveur LDAP, le portail captif ainsi que l'envoie des journaux vers le serveur Syslog a bien été configuré, testons la solution en plaçant une machine sur le réseau interne (192.168.100.0/24), et tentons d'aller sur internet :

En ouvrant Firefox, ce bandeau apparait. Il nous demande de s'authentifier au portail captif :





On se connecte une première fois avec un user inscrit dans le serveur LDAP, nous arrivons à aller sur internet



Puis on se connecte avec un user non inscrit dans le LDAP, puis avec le compte admin du pfSense, le portail ne laisse pas passer.

En analysant les logs, nous pouvons voir que l'utilisateur « rayan » a été accepté (« ACCEPT ») et qu'il est resté connecté 1min avant de se déconnecter (« DISCONNECT »).

Ensuite, nous voyons les tentatives de connexion avec les user test, test2 et admin qui n'ont pas réussi à passer le firewall (« FAILURE »).