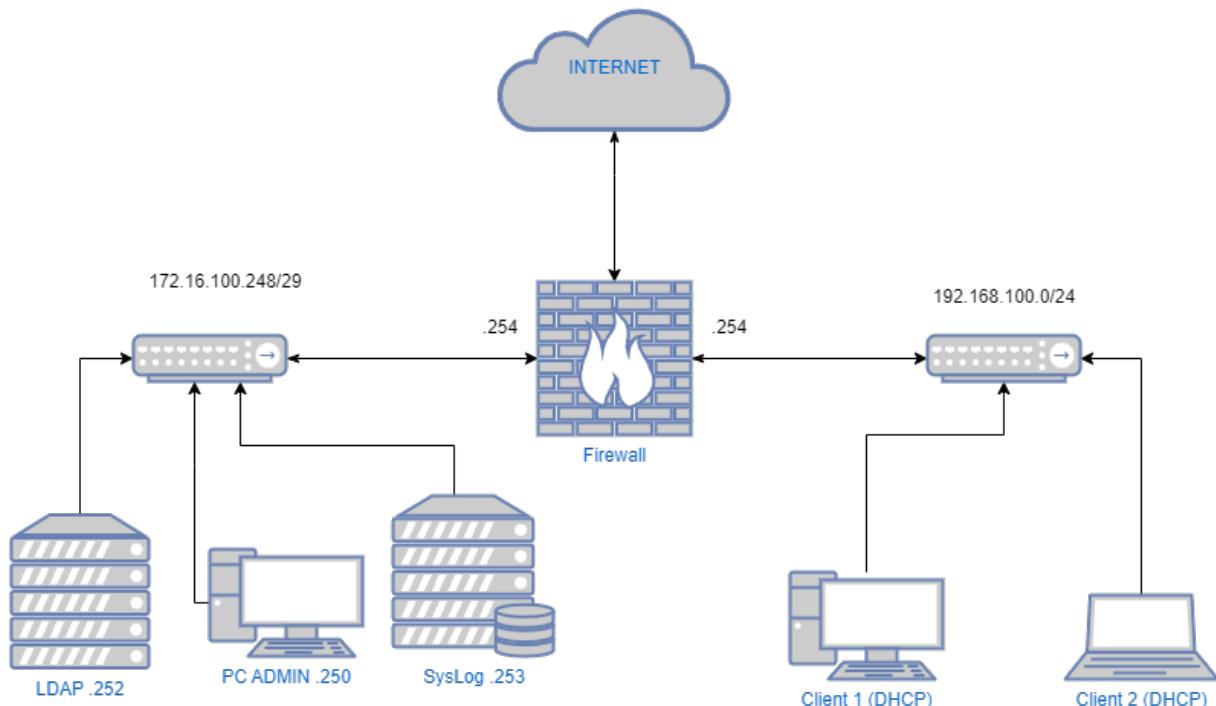


Objectif de cette mission : Dans le cadre du réseau de la M2L, proposer un système d'authentification sécurisé par portail captif afin de gérer l'accès à internet.

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'authentification », 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).

Services / Portail Captif / M2L_CAPTIF / Configuration

Configuration MACs Adresses IP autorisées Nom d'hôte permis Coupons High Availability Gestionnaire de fichiers

Configuration du portail captif

Activer Activer le Portail Captif

Description Une description peut être saisie ici à des fins de référence administrative (non analysée).

Interfaces WAN M2L_ADMIN M2L_INT Sélectionner l'interface/les interfaces pour activer le portail captif.

Nom maximal de connexions simultanées 100 Limite le nombre de connexions simultanées au serveur HTTP (S) du portail captif. Cela ne définit pas le nombre d'utilisateurs qui peuvent être connectés au portail captif, mais plutôt combien de connexions une seule adresse IP peut établir sur le serveur Web du portail.

Durée d'inactivité (minutes) 5 Les clients seront déconnectés après ce délai. Ils peuvent se connecter à nouveau immédiatement. Laissez ce champ vide pour aucun idle timeout.

Hard timeout (Minutes) 10 Les clients seront déconnectés après ce délai, indépendamment de l'activité. Ils peuvent se connecter à nouveau immédiatement. Laissez ce champ vide pour aucun hard timeout (ceci n'est pas recommandé à moins qu'un idle timeout est configuré).

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.

Authentification

Méthode d'authentification Use an Authentication backend Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Serveur d'authentification LDAP M2L Local Database You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.

Secondary authentication Server LDAP M2L Local Database You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

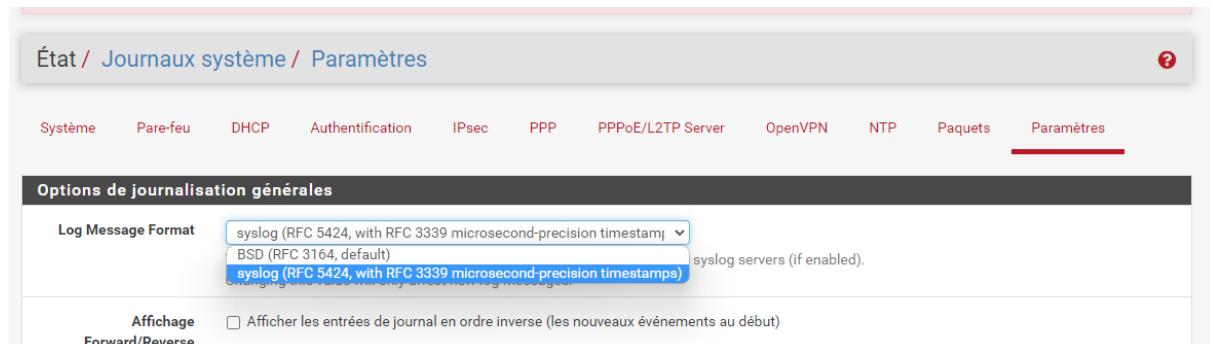
Reauthenticate Users Réauthentifier les utilisateurs connectés chaque minute If reauthentication is enabled, requests are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

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.



État / Journaux système / Paramètres

Système Pare-feu DHCP Authentification IPsec PPP PPPoE/L2TP Server OpenVPN NTP Paquets **Paramètres**

Options de journalisation générales

Log Message Format: **syslog (RFC 5424, with RFC 3339 microsecond-precision timestamp)** (selected)

Affichage: Afficher les entrées de journal en ordre inverse (les nouveaux événements au début)

Options de journalisation distante

Activer la journalisation distante: Envoyer les messages de log à un serveur de log externe

Adresse source: **Défaut (n'importe quel)**

Protocole IP: **IPv4**

Serveurs de journalisation distante: **172.16.100.253:514**

Contenu de Syslog à distance:

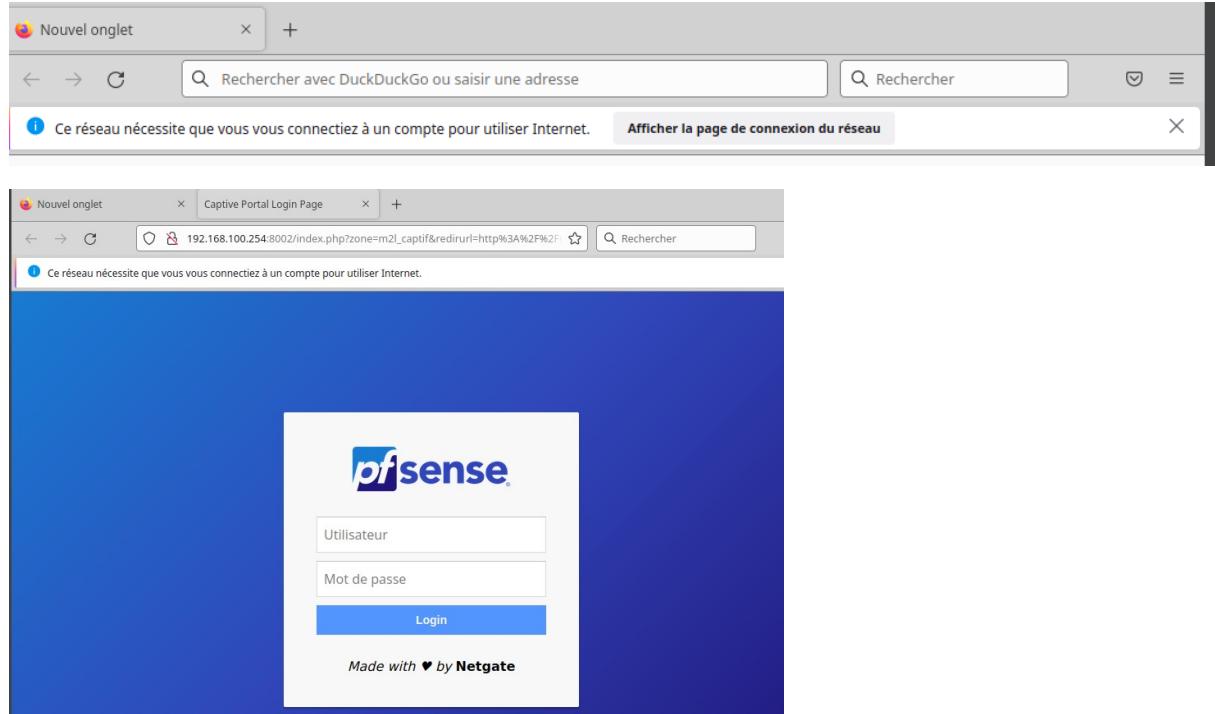
- Tous / Tout
- Événements System
- Événements du pare-feu
- Événements DNS (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- Événements DHCP (DHCP Daemon, DHCP Relay, DHCP Client)
- Événements PPP (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- General Authentication Events
- Événements du Portail Captif
- Événements des VPN (IPsec, OpenVPN, L2TP, PPPoE Server)
- Événements du moniteur de passerelle
- Événements des démons en cours (RADVD, UPnP, RIP, OSPF, BGP)
- Événements du protocole d'heure réseau (Demon NTP, Client NTP)
- Événements du sans fil (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogger on the remote server to accept syslog messages from pfSense.

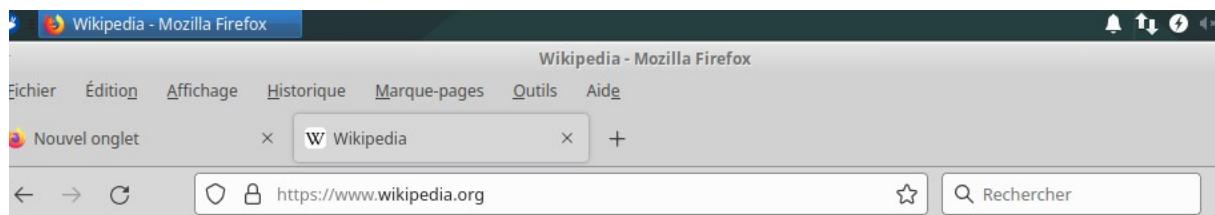
Enregistrer

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 apparaît. 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 »).

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

Recent syslog messages										
Date	Facility	Severity	Host	Syslogtag	ProcessID	Message type	Message			
Today 18:35:34	LOCAL4	INFO	pfSense.m2i.local	logportalauth[367]	0	Syslog	 Zone: m2i_captif - FAILURE: admin, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test2, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - ACCEPT: rayan, 08:00:27:63:5c:b5, 192.168.100.1
Today 18:35:31	LOCAL4	INFO	pfSense.m2i.local	logportalauth[367]	0	Syslog	 Zone: m2i_captif - FAILURE: test2, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - RECONNECT: rayan, 08:00:27:63:5c:b5, 192.168.100.1
Today 18:35:21	LOCAL4	INFO	pfSense.m2i.local	logportalauth[367]	0	Syslog	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - DISCONNECT: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - RECONFIGURING captive portal(M2L_CAPTIF).
Today 18:34:50	LOCAL4	INFO	pfSense.m2i.local	logportalauth[47901]	0	Syslog	 Zone: m2i_captif - FAILURE: test2, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - RECONFIGURING captive portal(M2L_CAPTIF).
Today 18:33:50	LOCAL4	INFO	pfSense.m2i.local	logportalauth[47901]	0	Syslog	 Zone: m2i_captif - FAILURE: test2, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - RECONFIGURING captive portal(M2L_CAPTIF).
Today 18:33:19	LOCAL4	INFO	pfSense.m2i.local	logportalauth[47332]	0	Syslog	 Zone: m2i_captif - FAILURE: test2, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: test, 08:00:27:63:5c:b5, 192.168.100.1, Invalid log ...	 Zone: m2i_captif - FAILURE: rayan, 08:00:27:63:5c:b5, 192.168.100.1	 Zone: m2i_captif - RECONFIGURING captive portal(M2L_CAPTIF).
Today 18:17:53	SYSLOG	ERR	pfSense.m2i.local	syslogd	0	Syslog	 exiting on signal 15	 Syncing firewall		
Today 18:17:53	USER	NOTICE	pfSense.m2i.local	check_reload_status[395]	0	Syslog	 Syncing firewall			