FIREWALL PFSENSE

BTS – SIO 2 / SISR

Clément Paccard

22/01/2024

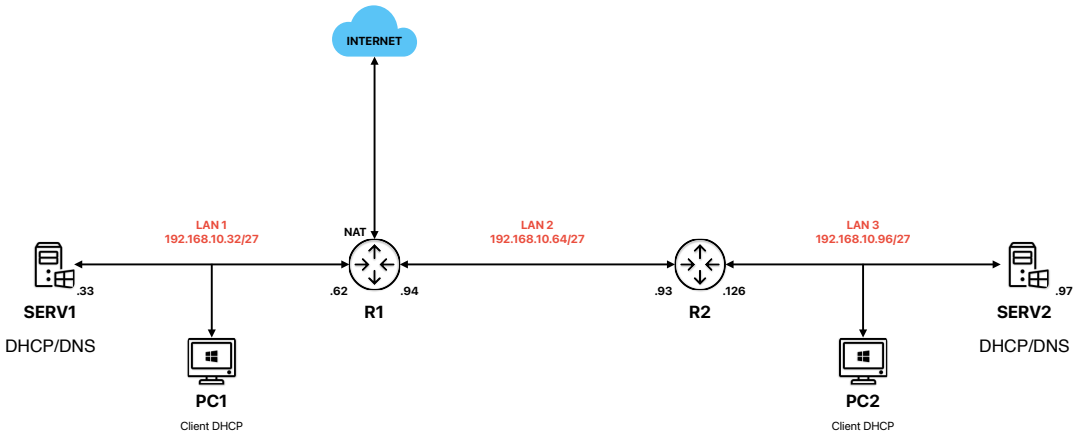
TABLE DES MATIERES

FIREWALL
PFSENSE

INTRODUCTION

Cette procédure montre comment installer et paramétrer un Pare-feu PFsense.

Précédemment nous avions configurer deux Routeur sur Windows serveur, un serveur DHCP avec basculement et un serveur DNS pour que les PC de différents réseaux puissent communiquer entre eux et avec internet en recevant une configuration IP complète et puissent résoudre les noms.



Le pare-feu, ou Firewall, joue un rôle crucial dans la sécurité des réseaux informatiques. Il agit comme une barrière protectrice en contrôlant et en filtrant le trafic réseau, autorisant ainsi uniquement les communications autorisées tout en bloquant les activités non autorisées. L'implémentation d'un pare-feu est essentielle pour renforcer la sécurité d'un réseau en surveillant le flux de données entrant et sortant.

PFsense, une solution open-source de pare-feu et de routeur, offre une virtualisation pratique pour mettre en œuvre des politiques de sécurité avancées. Cette solution permet de définir des règles de filtrage du trafic, de gérer l'accès aux ressources réseau, et de protéger les systèmes contre les menaces potentielles.

Le fonctionnement d'un pare-feu repose sur des règles configurées par l'administrateur réseau. Ces règles déterminent quels types de trafic sont autorisés ou bloqués, en fonction de critères tels que l'adresse IP source, l'adresse IP de destination, le port, etc. PFsense offre une interface conviviale pour la configuration de ces règles, facilitant ainsi la gestion des politiques de sécurité.

Dans notre cas, le pare-feu PFsense sera déployé en tant que machine virtuelle, assurant ainsi la protection du réseau. Des règles spécifiques seront définies pour contrôler le trafic entrant et sortant, renforçant ainsi la sécurité globale de l'environnement réseau.

L'adresse IP respective de chaque instance PFsense sera configurée, et des règles spécifiques seront établies pour garantir une protection efficace contre les menaces potentielles. La virtualisation de PFsense offre une solution agile et évolutive pour répondre aux besoins changeants de sécurité réseau.

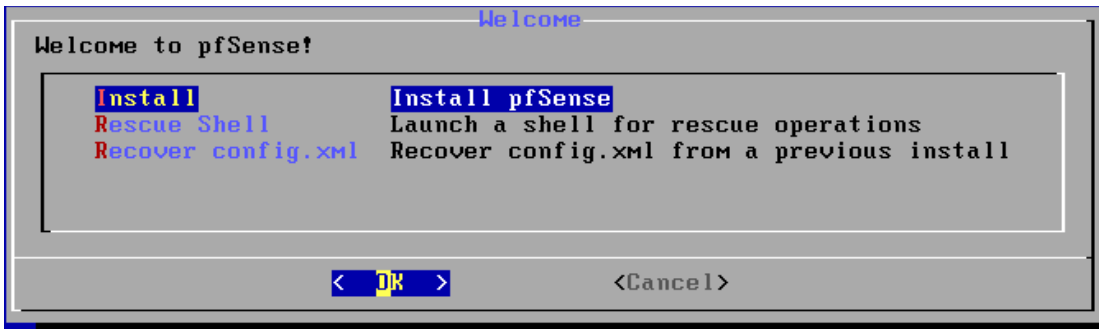
Nous allons créer également 3 LAN supplémentaires :

- *LAN 0 : 192.168.10.0/27*
- *DMZ : 172.16.0.0/12*
- *WIFI : 10.0.0.0/8*

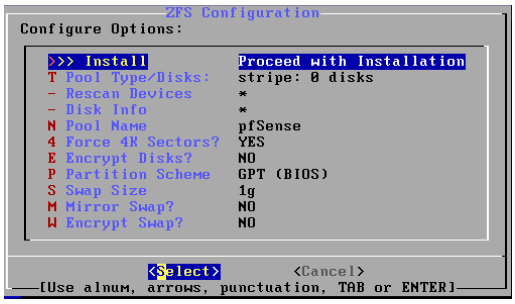
1-INSTALLER PFSENSE

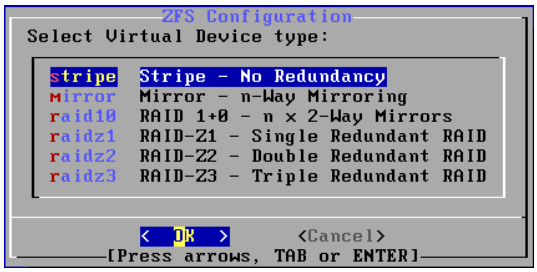
Pour commencer il faut créer une nouvelle machine virtuelle avec l'ISO de PFsense. En démarrant la VM nous avons quelques menus à passer et/ou configurer :

Sélectionner Install avec les flèches puis appuyer sur entrer (Ok)

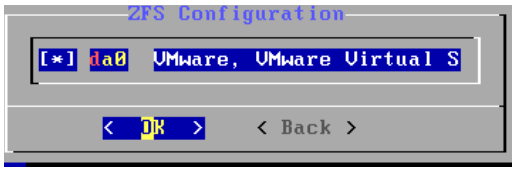


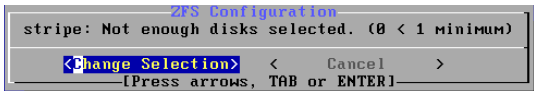
Sélectionner Install avec les flèches puis appuyer sur entrer (Ok) puis sélectionner stripe avec les flèches puis appuyer sur entrer (Ok)



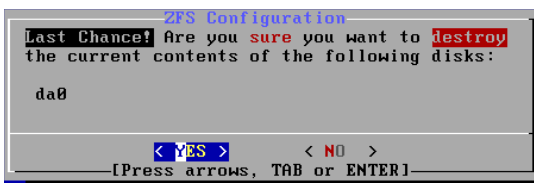


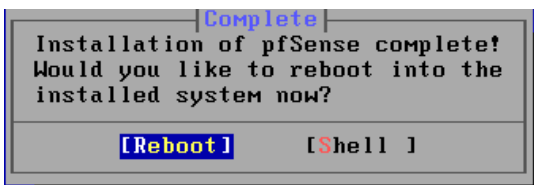
Ne pas oublier de cocher la case [ ] à l'aide de la barre d'espace puis enter et enter encore.





Ici on confirme avec enter puis une fois PF installé on redémarre.



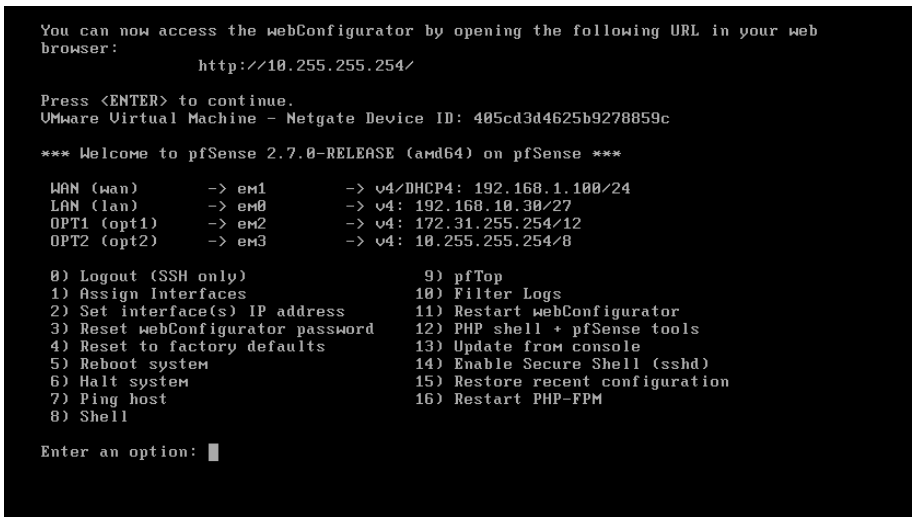


2-CONFIGURER PFSENSE

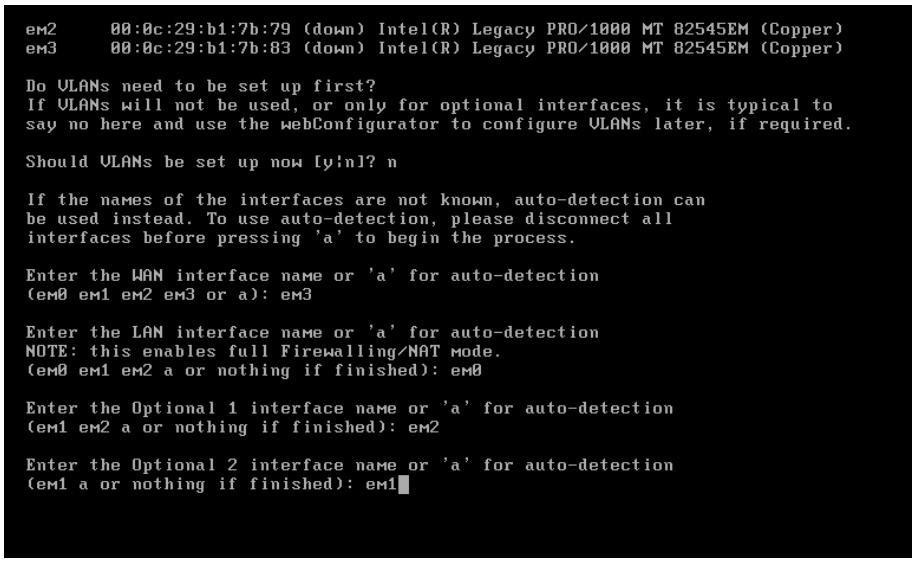
Nous allons commencer par configurer les interfaces avec leurs IP respectives.

- *WAN : DHCP*
- *LAN 0 : 192.168.10.30*
- *DMZ : 172.16.255.254*
- *WIFI : 10.255.255.254*

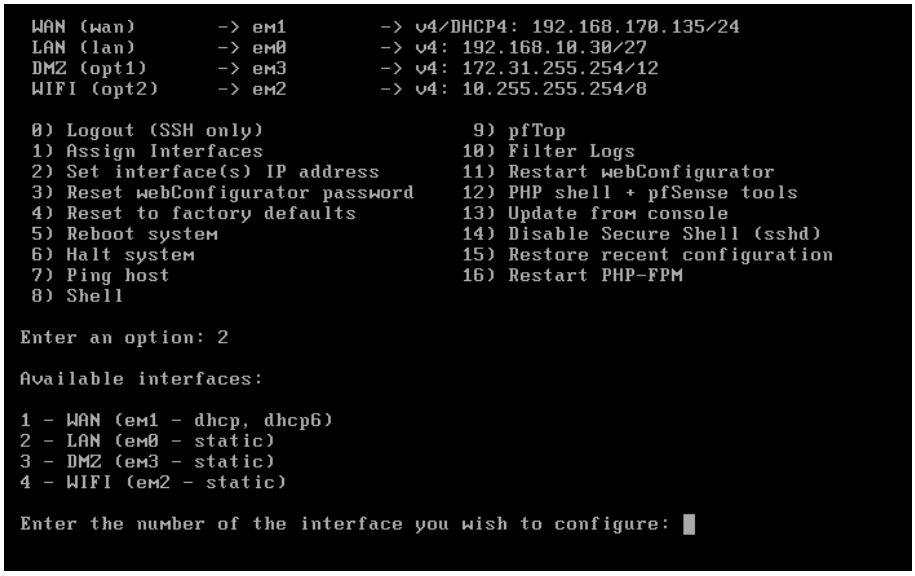
Pour ce faire il faut aller dans le menu 1 de PFsense :



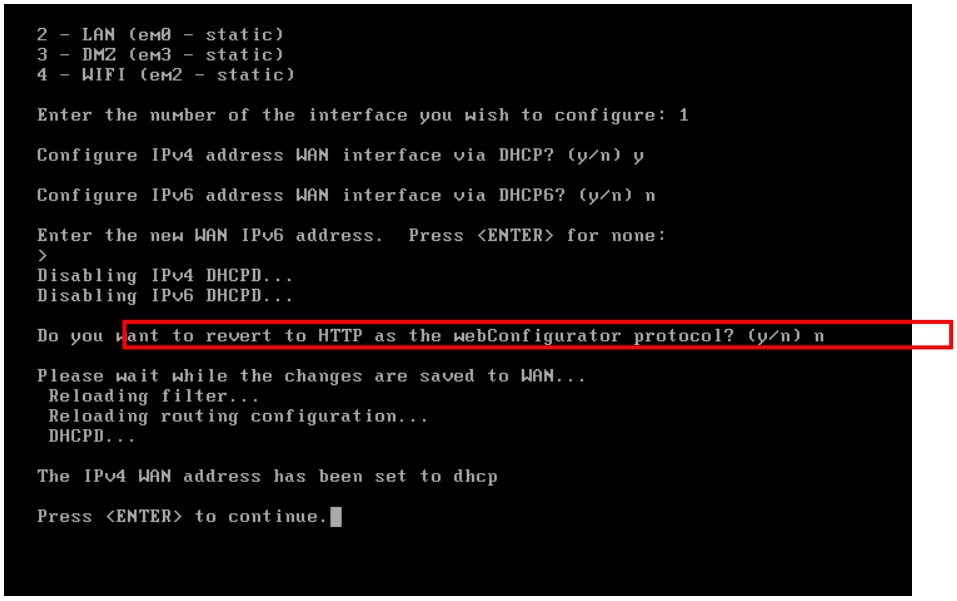
Ici on attribue le nom des interfaces (em0, em1…) grâce à leur adresse MAC.



Ensuite dans le menu 2 on peut attribuer les IP des interfaces avec leur nom.



En premier on choisit DHCP ou non sur IPv4/IPv6, si on choisit de ne pas être en DHCP on renseigne ensuite l'IP et masque de l'interface.



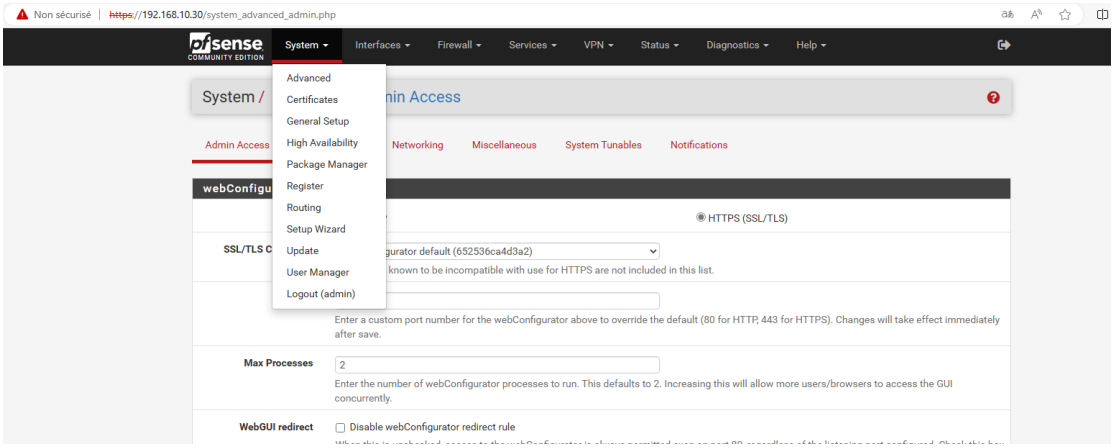
On peut ensuite on peut se connecter à l'interface web depuis le LAN 0 en renseignant l'adresse de l'interface LAN : 192.168.10.30

3- REGLAGE PFSENSE

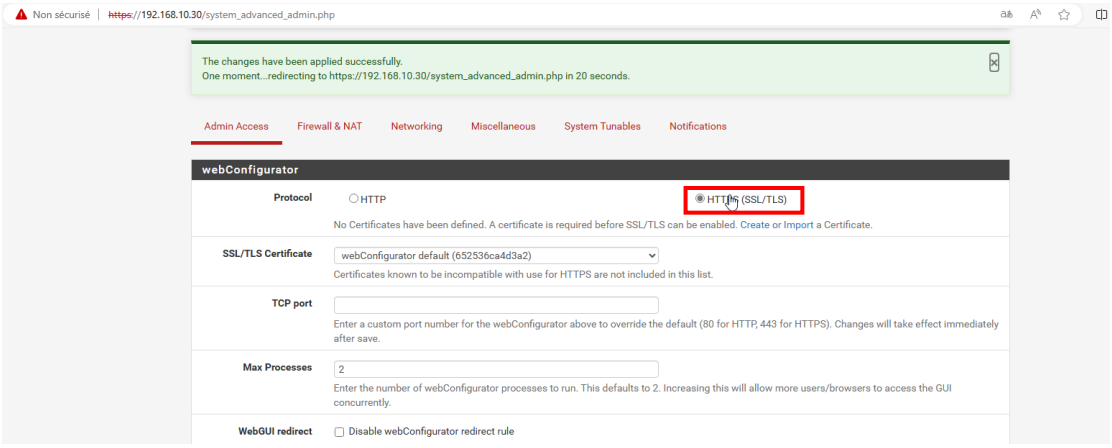
A. SSH/HTTPS

Pour commencer on va activer le SSH et l'HTTPS sur l'interface WEB.

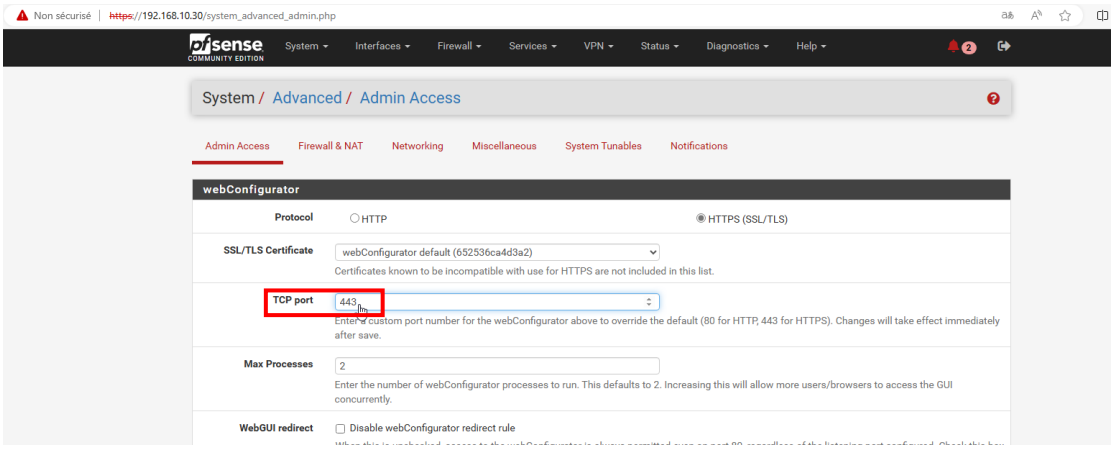
Pour ce faire aller dans System → Advenced



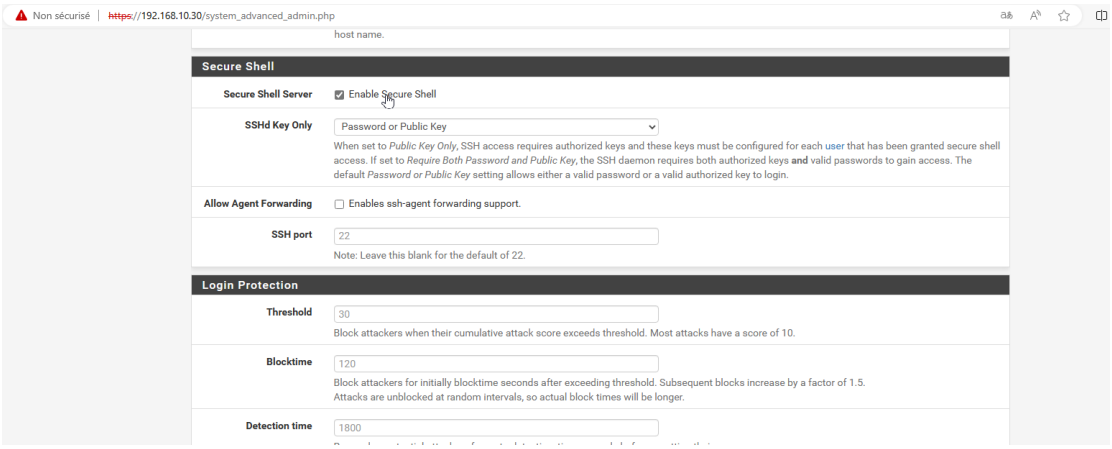
Cocher HTTPS (SSL/TLS)



Renseigner le port TCP 443



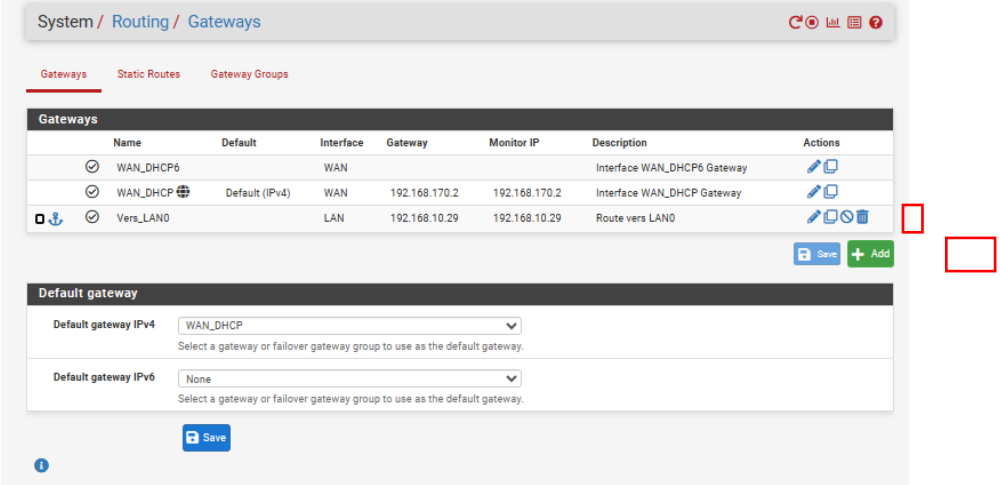
Puis dans la rubrique Secure Shell cocher Enable Secure Shell



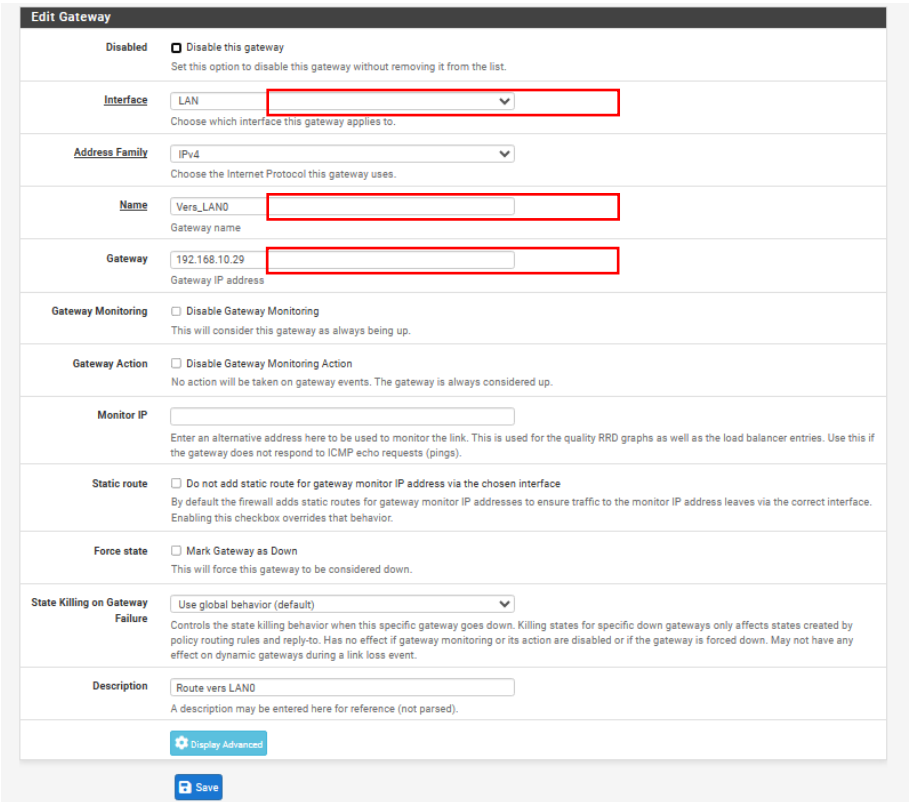
B. AJOUTER UNE PASSERELLE

Il faut ajouter la passerelle R1 (192.168.10.29) pour que le routage puisse se faire par la suite.

Aller dans System/Routing/Gateways puis cliquer sur Add si elle n'existe pas, ou modifier (le crayon) si elle existe déjà.



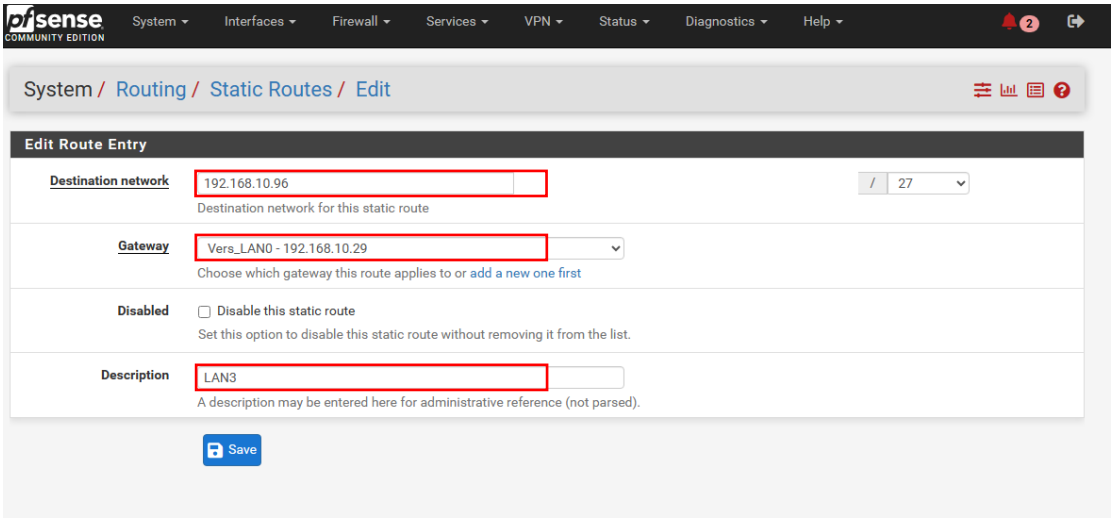
Puis ici on renseigne les informations, l'interface concernée, le nom et l'IP de la passerelle.



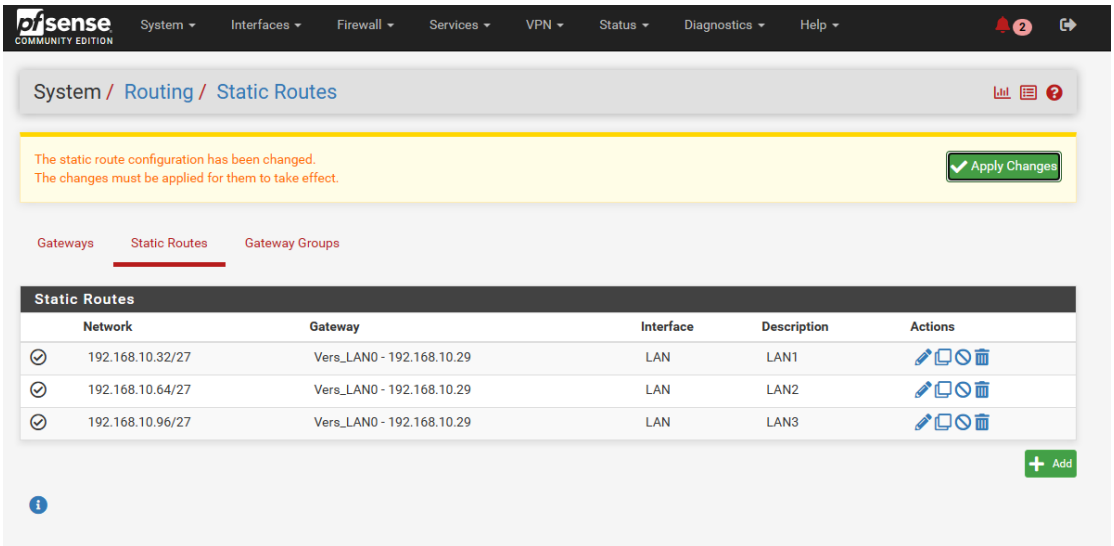
C. AJOUTER UNE ROUTE

Ici nous allons ajouter des routes pour renseigner le chemin vers les LAN1/LAN2/LAN3. Pour ce faire aller dans System/Routing/Static Routes et ajouter ici les trois routes en cliquant sur Add.

On renseigne l'adresse réseau de destination, la passerelle à utiliser (ici R2 configuré précédemment) et la description



Il ne faut pas oublier de confirmer avec Apply Changes.

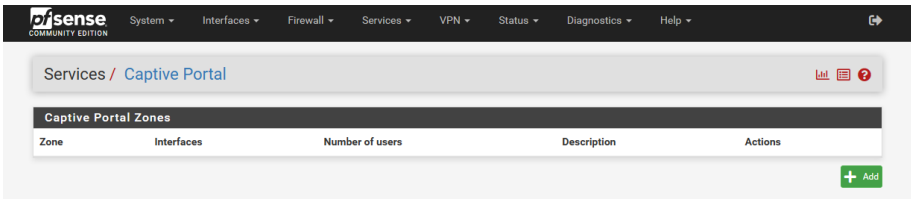


4-PORTAIL CAPTIF

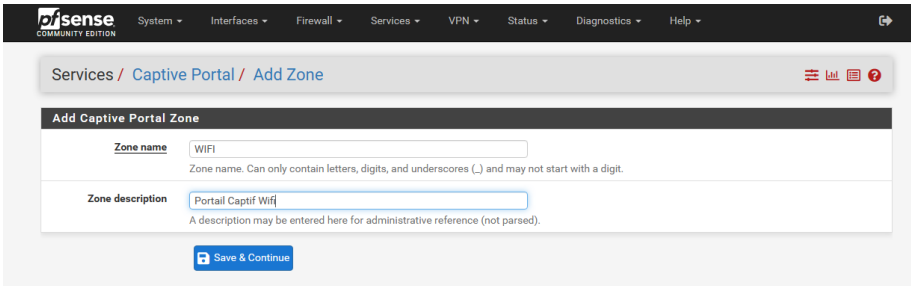
Ici l'objectif va être d'installer un portail captif sur le Pare-Feu PFsense.

Un portail captif est un système de contrôle d'accès à un réseau informatique, souvent utilisé dans les environnements publics tels que les cafés, les hôtels, les aéroports ou les entreprises. Son objectif principal est de sécuriser l'accès à Internet en obligeant les utilisateurs à passer par une page d'authentification avant d'accéder au réseau.

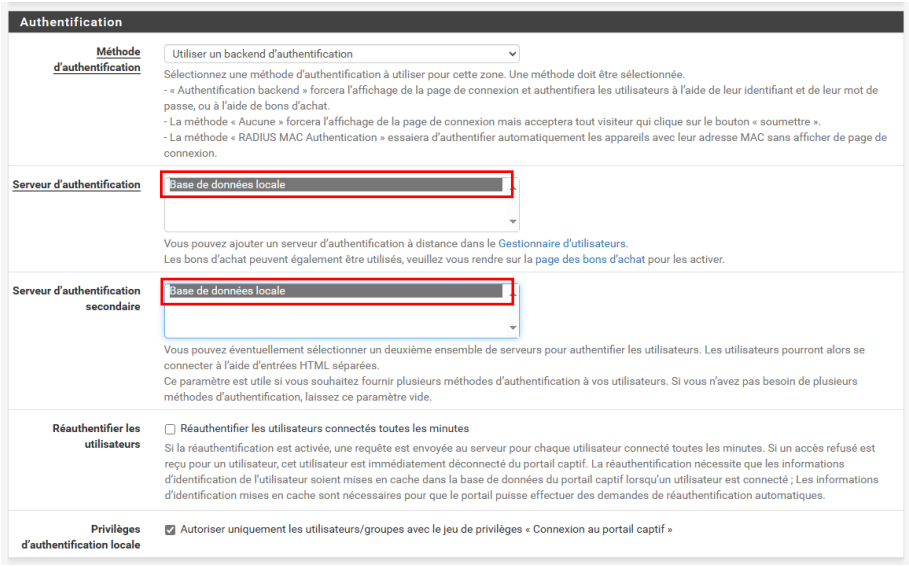
Pour le faire allez dans Services/Captive Portal et sélectionner Add



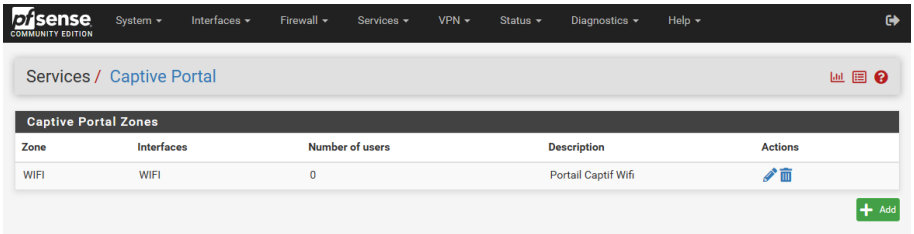
On renseigne ici le nom de la zone (du portail captif) et avec une petite description.



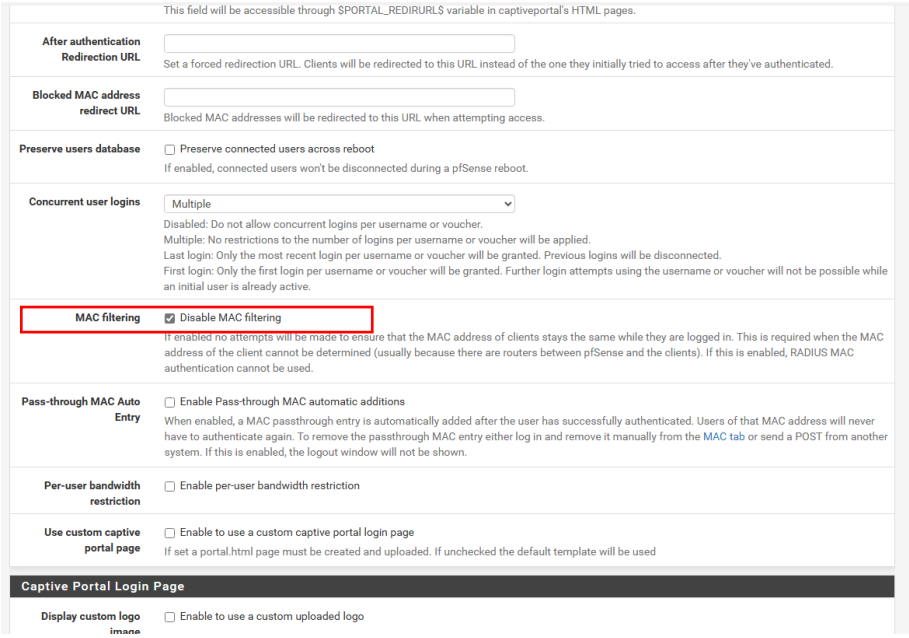
Puis dans Authentification on clique sur Base de données locale pour Serveur d'authentification et Serveur d'authentification secondaire.



Une fois ajouté on le retrouve dans la liste des portails captif et on peut modifier ses propriétés dans actions.

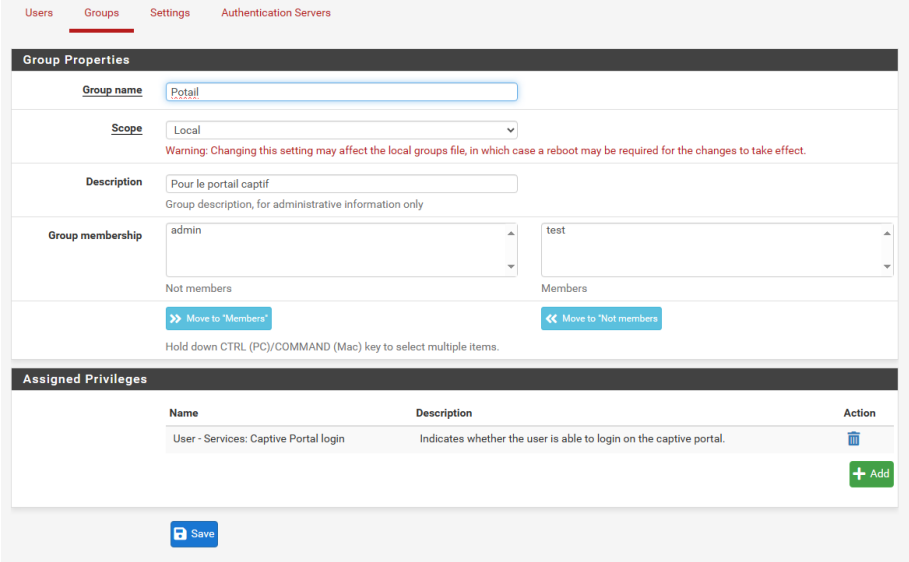


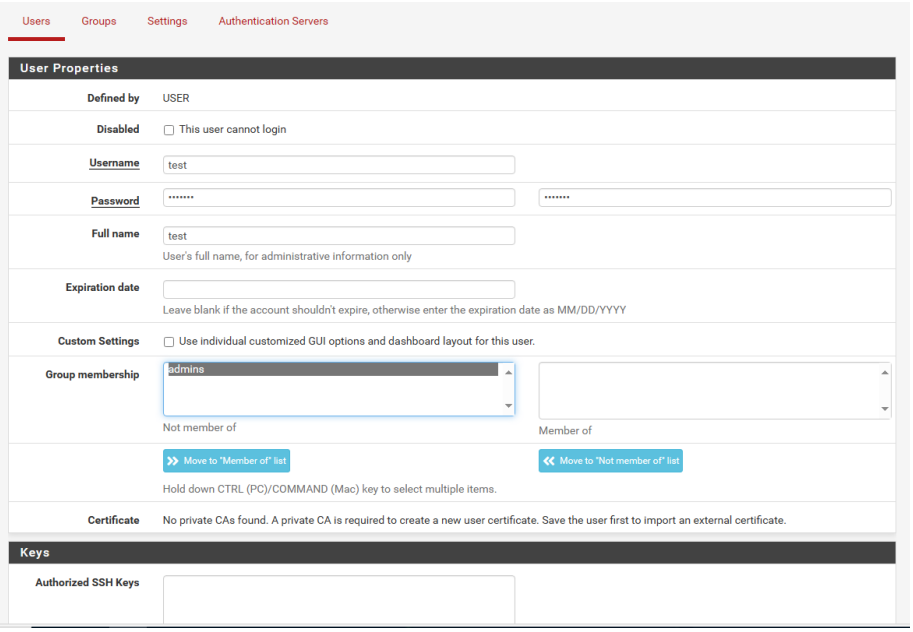
Il faut désactiver MAC filtering



Nous allons maintenant ajouter des groupes et utilisateurs qui pourront se connecter au portail captif de la zone WIFI.

Aller dans System/User Manager et puis Groups faire Add. On renseigne les informations diverses, dans les Assigned Privileges il faut ajouter le rôle User – Services : Captive Portal Login.





CONCLUSION

La mise en place de PFsense en virtualisation offre une solution de pare-feu robuste et configurable. Les étapes ci-dessus permettent de déployer PFsense, configurer les règles de filtrage, et assurer une gestion efficace de la sécurité du réseau.

Il restera quelques tests à effectuer avec un PC dans le LAN WIFI en essayant de se connecter sur le portail captif.