Maîtrise de la Sécurité Réseau :

Guide Pratique pour le Déploiement et l'Utilisation de pfSense

Réalisé par :

Khalid AMATOCH

Table of Contents

Chapitre 1- La mise en place d'un pare-feu pfSense pour la sécurité LAN

1.1 Présentation des outils utilisés

Afin de réaliser notre projet nous avons utilisé deux plateformes (GNS3 et VMWAR) le premier c'est pour dessiner l'architecture et réaliser les interconnexions, le deuxième est utilisé pour mettre en place les machines virtuelles et les configurer.

1.1.1 GNS3

Graphical Network Simulator-3 (abrégé en GNS3) est un émulateur de logiciel de réseau, Il permet la combinaison de dispositifs virtuels et réels, utilisés pour simuler des réseaux complexes. Initialement développé pour utiliser le logiciel d'émulation Dynamips pour simuler Cisco IOS, il est open source.

Dynamips peut émuler le matériel des plates-formes de routage de la série Cisco en démarrant directement une image logicielle Cisco IOS réelle dans l'émulateur.

Figure 1: Logo GNS3

1.1.2 VMware Workstation

VMware Workstation est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.

VMware Workstation prend en charge le pontage des cartes réseau hôte existantes et le partage de disques durs physiques et de périphériques USB avec une machine virtuelle. Il peut simuler des lecteurs de disque ; un fichier image ISO peut être monté en tant que lecteur de disque optique virtuel et les lecteurs de disque dur virtuels sont implémentés en tant que fichiers .vmdk .

Figure 2: Logo VMware Workstation:

1.2 Présentation du lab

Pour ce chapitre, j'ai choisi d'ajouter plusieurs concepts utilisés au sein d'une infrastructure d'organisation réelle, en commençant par la mise en œuvre d'une architecture réseau de base composée d'un commutateur de couche 3 et de quelques VLAN, en assurant la sécurité à l'aide de pfSense et en centralisant le système avec le l'aide du serveur Windows.

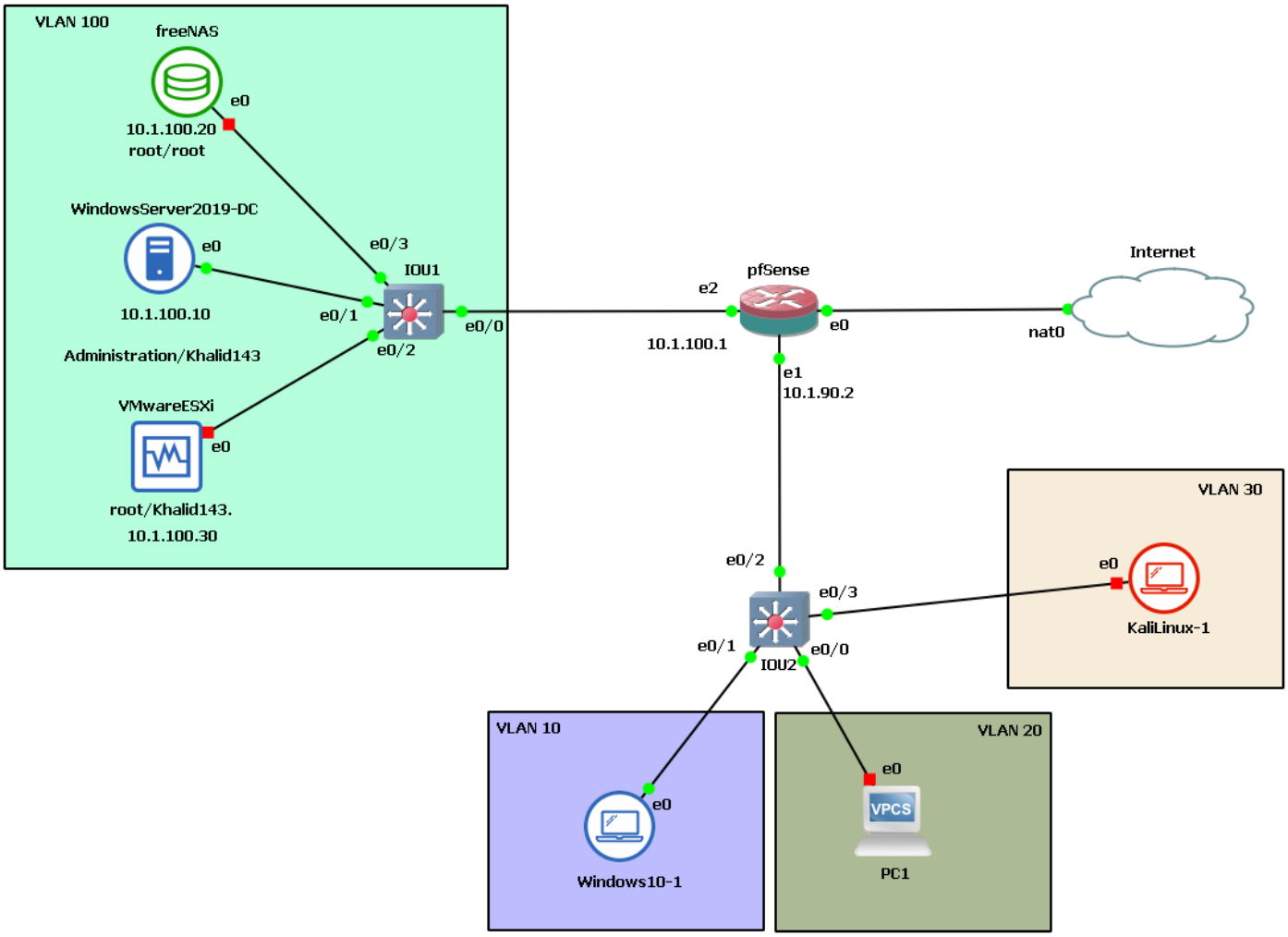

Figure 3: Architecture de réseau simple dans GNS3

1.3 Pfsense

Le projet pfSense est une distribution personnalisée open source gratuite de FreeBSD conçue pour être utilisée comme pare-feu et routeur entièrement gérée par une interface Web facile à utiliser. Cette interface Web est connue sous le nom de configurateur GUI basé sur le Web, ou WebGUI en abrégé. En plus d'être une plate-forme de pare-feu et de routage puissante et flexible, le logiciel pfSense comprend une longue liste de fonctionnalités connexes. Le système de packages pfSense permet une évolutivité supplémentaire sans ajouter de gonflement et de vulnérabilités de sécurité potentielles à la distribution de base.

1.3.1 pfSense fonctionnalités

pfSense est principalement utilisé comme routeur et logiciel de pare-feu, et généralement configuré comme serveur DHCP, serveur DNS, point d'accès WiFi, serveur VPN, tous fonctionnant sur le même périphérique matériel. pfSense permet également l'installation de packages open source tiers tels que Snort ou Squid via un gestionnaire de packages intégré, ce qui en fait le choix par défaut de nombreux administrateurs réseau.

pfSense peut être configuré comme un pare-feu de filtrage de paquets avec état, un routeur LAN ou WAN, une appliance VPN, un serveur DHCP, un serveur DNS ou pour d'autres applications et à des fins spéciales. Fonctionnalités de sécurité pfSense de nouvelle génération disponibles :

- Pare-feu de filtrage de paquets avec état ou routeur pur
- Politique de routage par passerelle et par règle pour plusieurs WAN, basculement, équilibrage de charge
- Pare-feu de couche 2 transparent
- Prise en charge d'Ipv6, NAT, BGP
- Portail captif avec filtrage MAC, prise en charge RADIUS, etc.
- VPN : Ipsec, OpenVPN, site à site, site à client, site à cloud et cloud à cloud, assistant de connexion cloud pour aamazon AWS
- Client DNS dynamique
- Fonctions serveur et relais DHCP
- Serveur PPPoE
- Fonctionnalités de création de rapports et de surveillance avec des informations en temps réel
- Packages optionnels complémentaires tels que snort ou suricata pour IDS/IPS et la surveillance de la sécurité du réseau, Squid pour une diffusion de contenu optimisée et SquidGuard pour l'anti-spam/anti-[hameçonnage et le filtrage d'URL
- Et bien d'autres disponibles !

1.3.2 Pourquoi utiliser pfSense et non l'un des routeurs standard?

Un routeur standard n'est pas fiable, a des fonctionnalités limitées en raison du verrouillage du fabricant et présente potentiellement de multiples vulnérabilités logicielles. Les fabricants des routeurs de base n'ont aucune incitation à corriger les bogues logiciels, les problèmes de performances ou même les graves failles de sécurité. Une fois le routeur vendu, le fabricant n'a aucune raison de continuer à dépenser de l'argent pour le développement et la sécurité.

Les systèmes d'exploitation Open Source tels que pfSense sont régulièrement mis à jour et sont connus pour corriger rapidement les problèmes de sécurité. pfSense vous donne le contrôle de votre réseau.

Différence entre pfSense Community Edition et pfSense Plus

pfSense CE

- Open source
- convient uniquement aux architectures amd64
- pfSense CE ne dispose d'aucun canal de support officiel que vous pouvez acheter auprès de Netgate.
- pfSense CE est libre d'utilisation à des fins personnelles ou commerciales sur votre propre matériel tant que vous conservez le fichier de licence intact et que vous suivez les autres règles de licence Apache 2.0.
- pfSense CE continuera son format de gestion des versions et ne suivra pas un calendrier de publication prédéfini.

pfSense Plus

- Propretaire
- adapté aux architectures amd64 et ARM
- Netgate est livré avec pfSense Plus.
- pfSense Plus nécessite un abonnement auprès de Netgate et n'est gratuit que pour une utilisation à domicile ou en laboratoire.
- pfSense Plus suivra la convention de numérotation des versions "année.mois" et aura des versions prévues trois fois par an.
- Plus est basé sur CE.
- Prise en charge des plates-formes de fournisseur de services cloud (CSP) (AWS, Azure)

1.3.3 Implémentation de pfSense

Nous pouvons télécharger pfSense Community Edition à partir du site Web officiel à l'adresse pfsense.org après avoir choisi le bon modèle d'architecture et le programme d'installation.

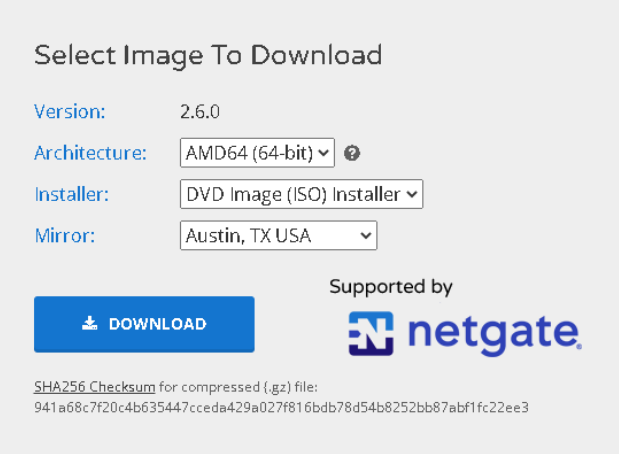

Figure 4: Page de téléchargement de pfSense

L'installation est simple, créant une nouvelle machine virtuelle dans VMware, puis ajustant la bonne configuration matérielle pour qu'elle fonctionne.

L'installation réelle de pfSense consiste à choisir la sélection de la carte de touches. L'étape de partitionnement sélectionne le système de fichiers pour le disque cible du pare-feu (qui comprend également le type de pool/disques. Dans notre cas, ZFS prend en charge plusieurs disques de différentes manières pour la redondance et/ou la capacité supplémentaire) .

1.3.4 Affectation des interfaces

Si le pare-feu ne peut pas déterminer automatiquement la disposition de l'interface réseau, il présentera une invite d'affectation d'interface comme dans la figure Écran d'affectation d'interface. C'est là que les cartes réseau installées dans le pare-feu se voient attribuer leurs rôles d'interfaces WAN, LAN et facultatives (OPT1, OPT2 … OPTn).

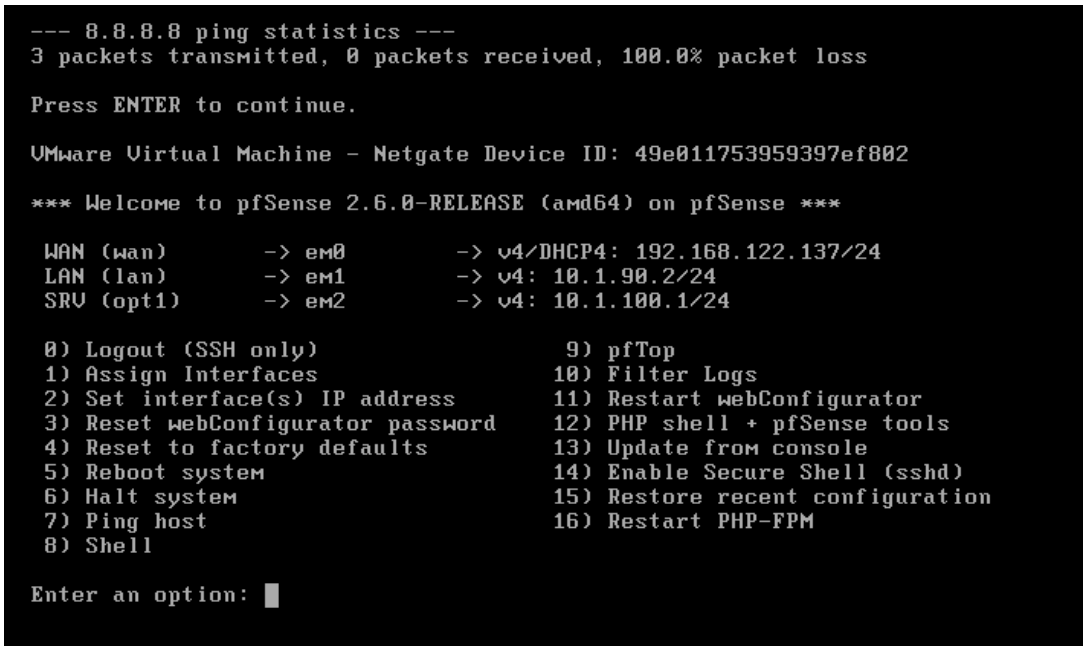

Figure 5: L'affectation de l'interface dépend de notre architecture réseau

Dans mon cas, em0 est affecté en tant qu'interface WAN, qui obtient son adresse IP du NAT en utilisant le protocole DHCP, tandis que em1 et em2 sont configurés manuellement.

1.3.5 Création d'alias vers les VLAN

Les alias définissent un groupe de ports, d'hôtes ou de réseaux en les utilisant, ce qui se traduit par des ensembles de règles beaucoup plus courts, auto-documentés et plus gérables.

Dans notre cas, je crée des alias vers les VLAN afin que le paquet soit transféré vers le réseau interne.

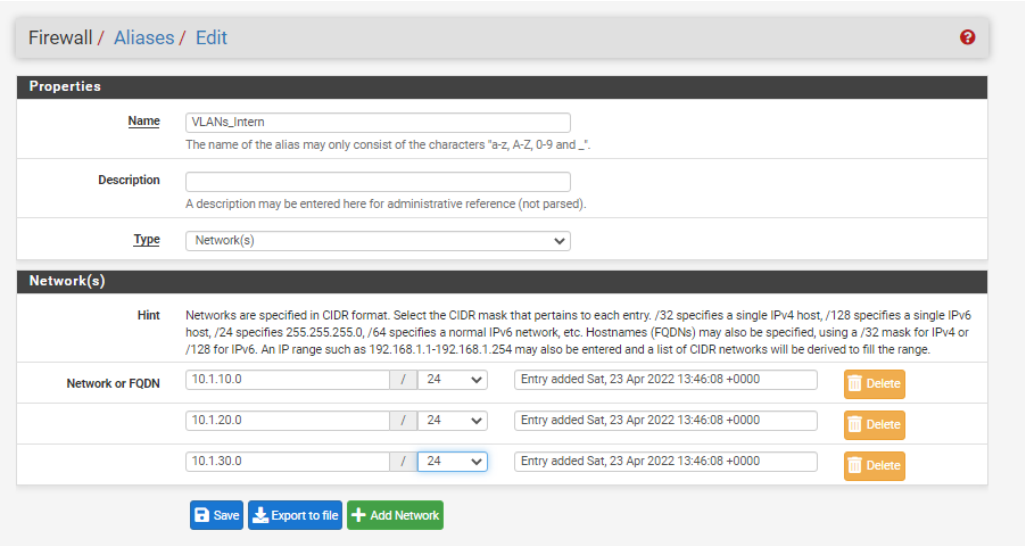

Figure 6: Création d'alias vers les VLAN

Après avoir configuré notre alias, nous devons créer une route statique pour aider pfSense à savoir où acheminer le trafic en ce qui concerne les VLAN internes. Pour que cela se produise, nous devons d'abord produire une nouvelle passerelle par défaut où pfSense enverra les paquets pour atteindre le réseau que nous avons défini dans notre alias (dans notre cas, c'est le commutateur).

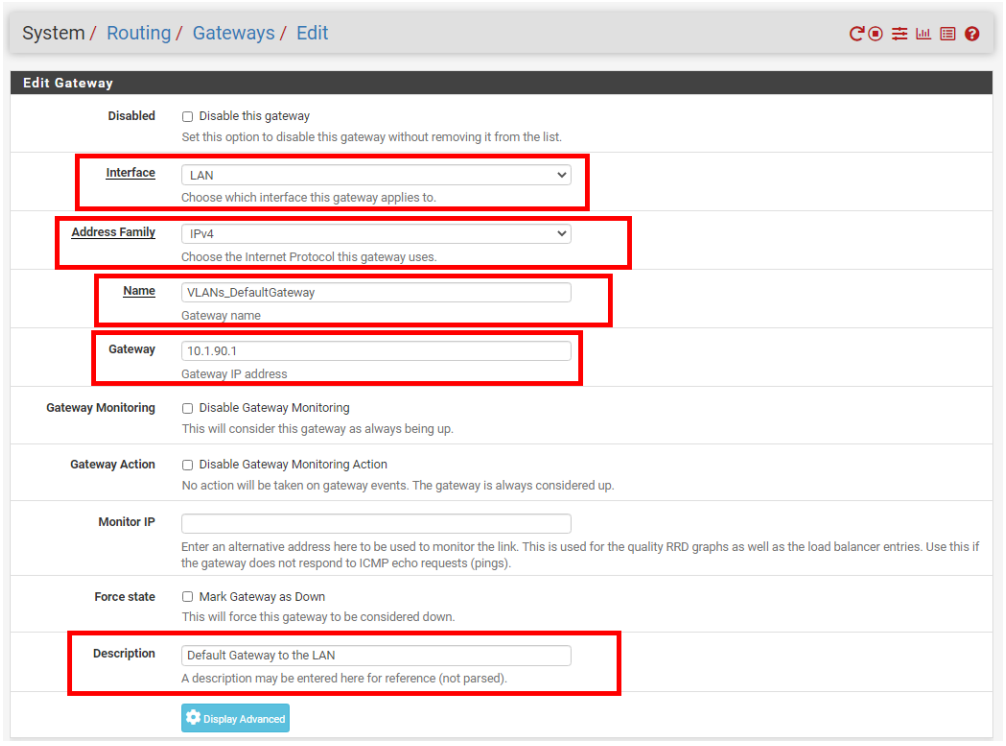

Figure 7: Creation d'une nouvelle passerelle par défaut

Après avoir créé avec succès la nouvelle passerelle par défaut, nous devrions maintenant pouvoir ajouter une route statique au LAN.

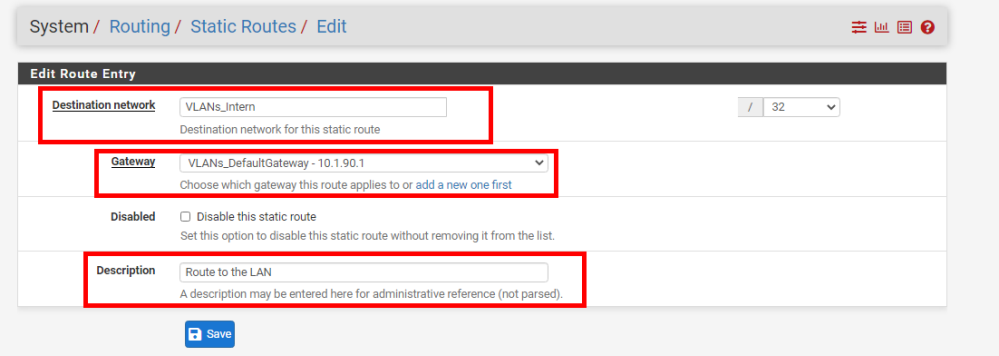

Figure 8: l'ajout d'une route statique

1.3.5.1 Vérification de la connectivité de notre hôte Windows

Avant d'aller plus loin dans nos tests, nous devons créer une règle permettant aux VLAN d'accéder au réseau extérieur.

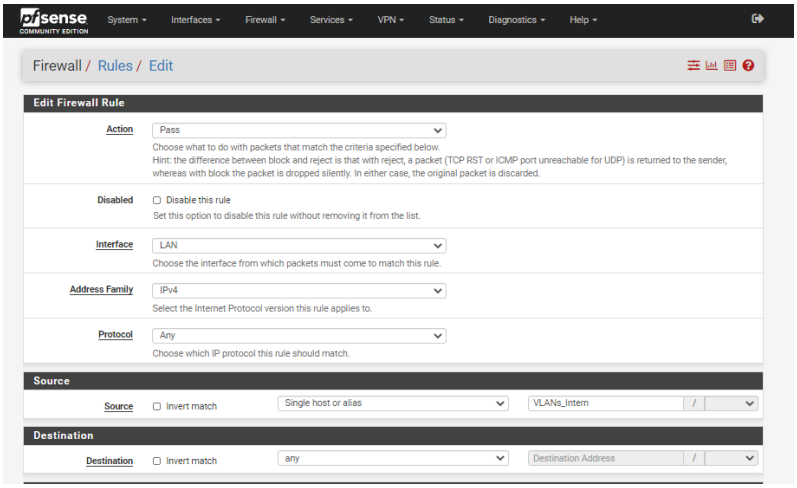

Figure 9: Creation d'une règle

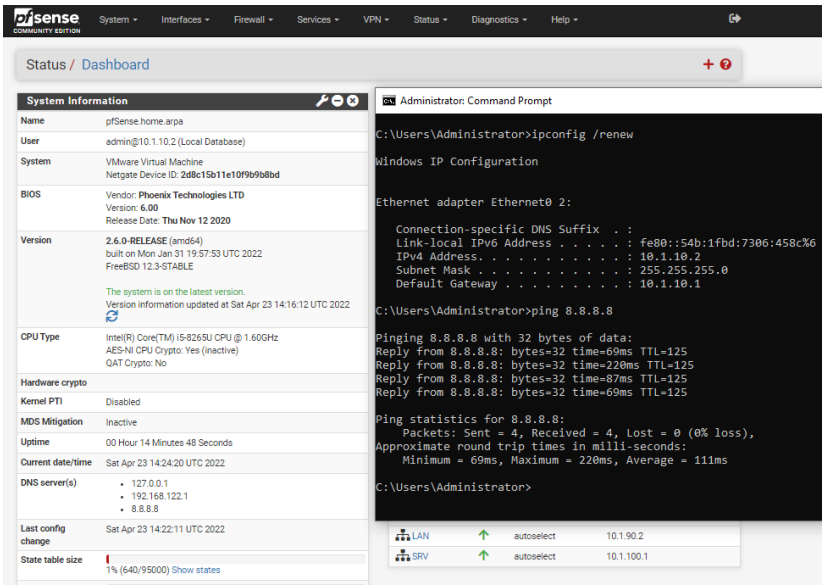

Figure 10: Test de la connectivité depuis Windows hote.

1.3.6 Attribuer une nouvelle Interface à la zone Serveur

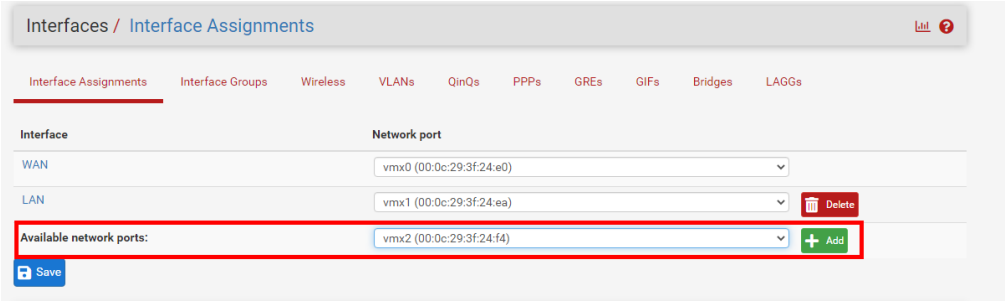

Figure 11: Attribution d'une nouvelle Interface DMZ

L'interface nouvellement attribuée sera affichée dans la liste. La nouvelle interface aura un nom par défaut attribué par le pare-feu tel que OPT1 ou OPT2, le nombre augmentant en fonction de son ordre d'attribution. Les deux premières interfaces portent par défaut les noms WAN et LAN, mais elles peuvent être renommées. Ces noms OPTx apparaissent sous le menu Interfaces, comme Interfaces > OPT1. La sélection de l'option de menu pour l'interface ouvrira la page de configuration de cette interface.

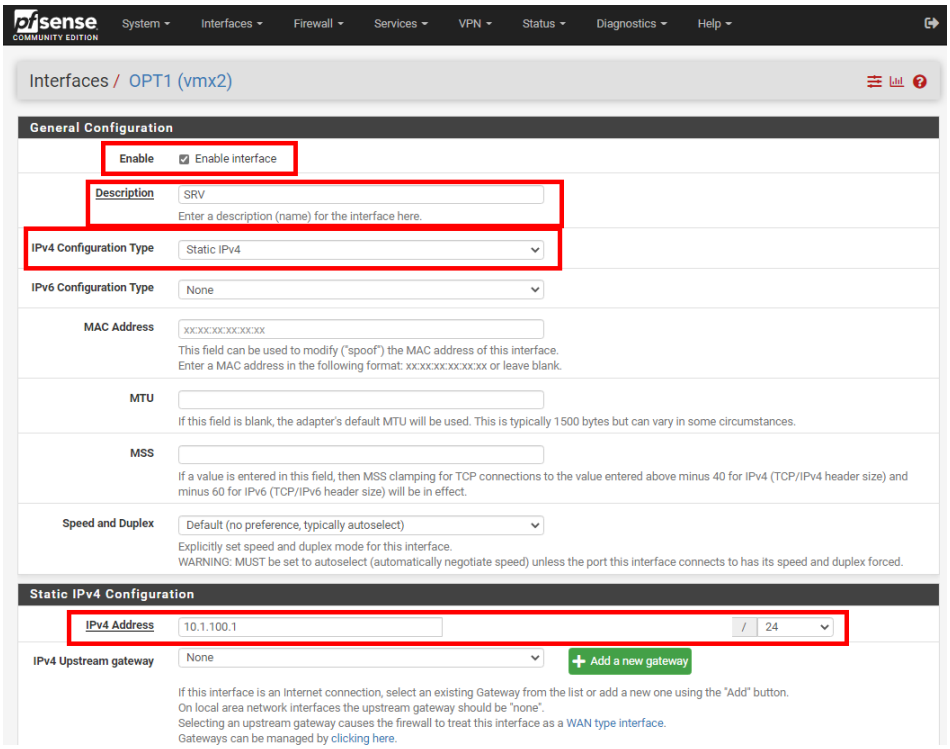

Figure 12: Activation et attribution d'une adresse IP pour l'interface nouvellement attribuée

1.3.7 Configuration DHCP

En ce qui concerne la zone serveur, je voulais dans ce cas avoir un DHCP configuré sur pfSense pour résoudre automatiquement les adresses IP des hôtes, pour ce faire.

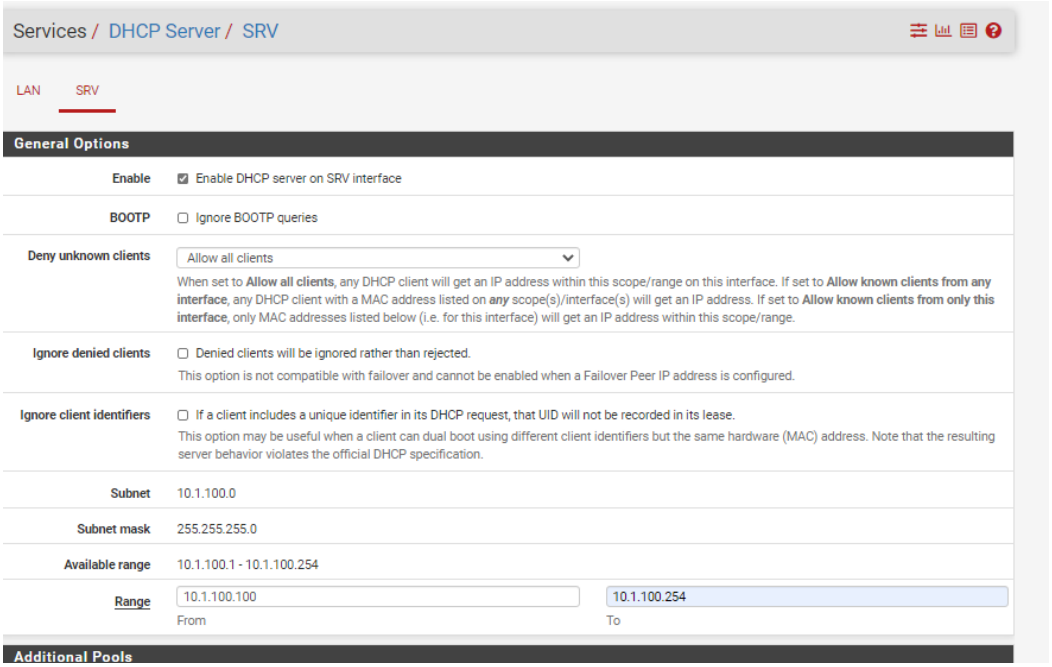

Figure 13: Configuration DHCP dans la DMZ.

Comme nous l'avons fait précédemment, nous devons créer une règle pour la zone SRV, afin qu'elle puisse accéder à Internet.

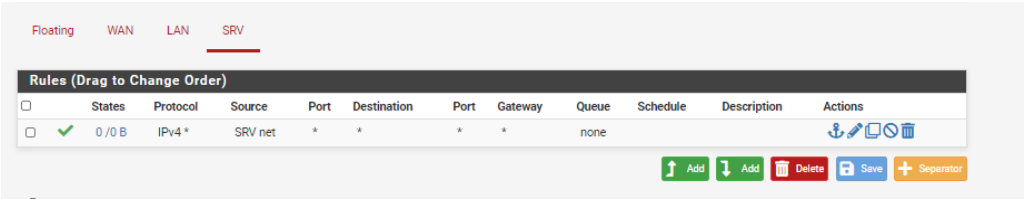

Figure 14: Création d'une règle DMZ

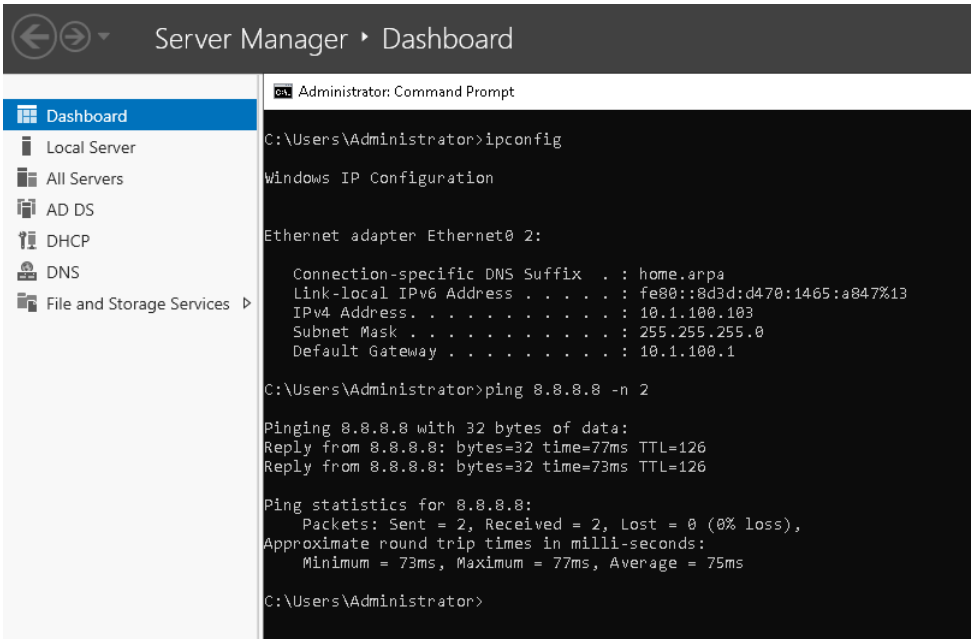

Figure 15: Test de la connectivité depuis Windows serveur.

1.4 Sécurité des aspects

1.4.1 VLAN de gestion et ACL

- Le principal avantage de l'utilisation d'un VLAN de gestion est l'amélioration de la sécurité du réseau. Lorsque tout le trafic de gestion se trouve sur un VLAN distinct, il est beaucoup plus difficile pour les utilisateurs non autorisés d'apporter des modifications à votre réseau ou de surveiller le trafic réseau.
- Minimisez l'impact d'une tempête de diffusion sur d'autres VLAN en vous donnant un chemin séparé pour accéder à votre réseau.

1.4.1.1 Implémentation des ACLs sur le commutateur:

Désactivation de l'accès à la configuration du commutateur à partir des VLAN (et seul le VLAN 10 peut accéder en tant que VLAN de gestion).

1.4.1.2 Autoriser l'accès au pare-feu uniquement au VLAN de gestion

Afin de limiter le seul accès à partir d'un VLAN spécifique, nous devons désactiver la règle anti-verrouillage, qui permet l'accès à la gestion depuis n'importe quelle machine sur le LAN et empêche la configuration des règles de pare-feu de manière à verrouiller l'utilisateur hors de l'interface Web.

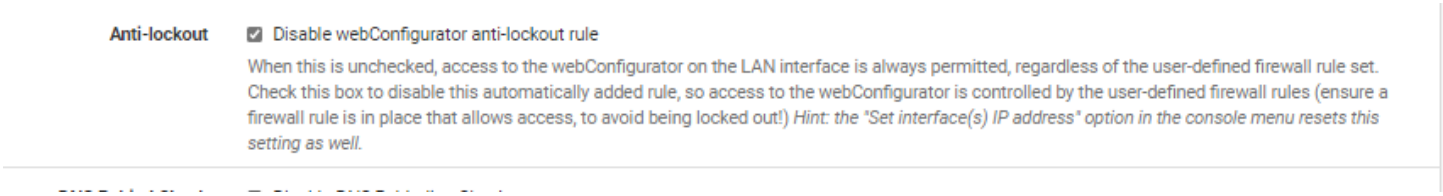

Figure 16: Désactivation de la règle de verrouillage de webConfiguration

Ensuite, nous devrions ajouter une règle uniquement au VLAN de gestion.

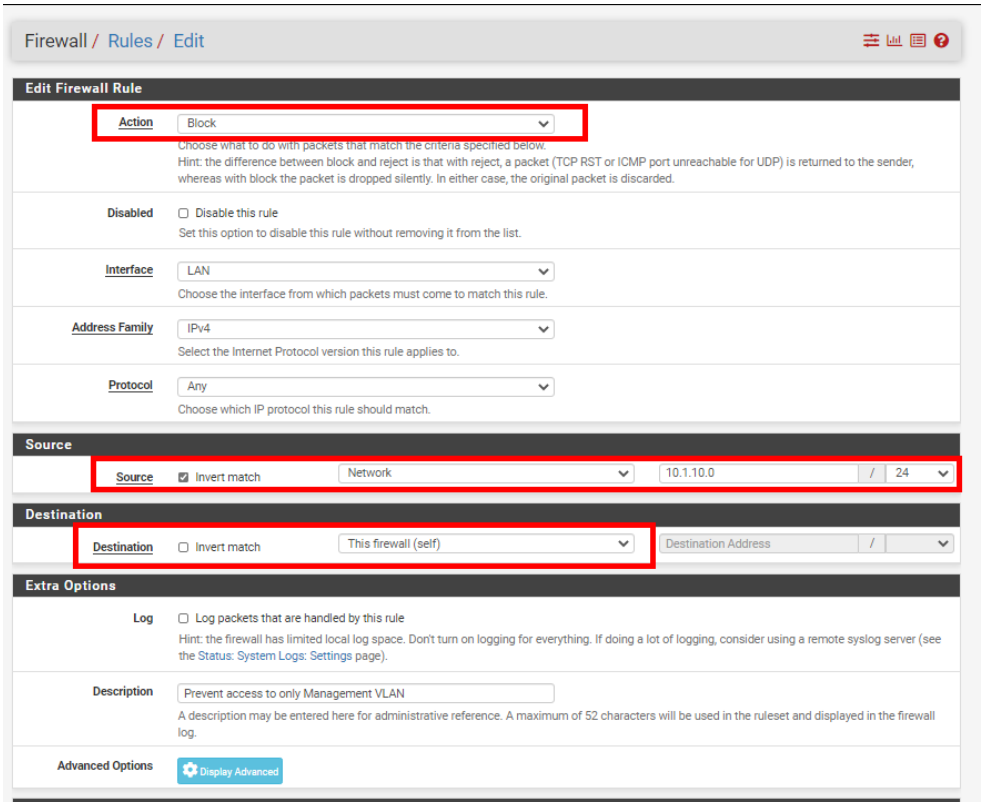

Figure 17: Ajout d'une règle à la gestion des VLAN

1.5 Système de package pfSense

pfSense offre un large éventail de fonctionnalités. Il est également possible d'ajouter des fonctionnalités supplémentaires en installant des packages. Ces forfaits peuvent offrir des services supplémentaires ou des informations statistiques avancées. Ces packages sont intégrés dans pfSense. Cela signifie qu'ils sont généralement utilisés via l'interface graphique Web pfSense.

De plus, la liste des packages disponibles est maintenue et vérifiée par Netgate pour s'assurer que les packages proposés sont correctement mis à jour et maintenus.

1.5.1 pfBlockerNG

pfBlockerNG est un excellent package gratuit et open source développé pour le logiciel pfSense® qui fournit le blocage des publicités et du contenu malveillant, ainsi que des capacités de blocage géographique.

En installant pfBlockerNG, vous pouvez non seulement bloquer les publicités, mais également le suivi Web, les logiciels malveillants et les rançongiciels. Lorsque vous utilisez pfBlockerNG, vous gagnez en sécurité et en confidentialité. Il le fera pour l'ensemble de votre réseau en utilisant une fonctionnalité connue sous le nom de DNSBL (abréviation de Domain Name System-based Blackhole List).

1.5.1.1 Caractéristiques du pfBlockerNG

- Blocage IP.
- Blocage DNS.
- Filtrage du trafic entrant/sortant.
- Routage basé sur des règles.
- Blocage DNS malveillant et limitation des publicités.
- Filtrage des spams.
- Listes blanches.
- Recherche sécurisée Installation.

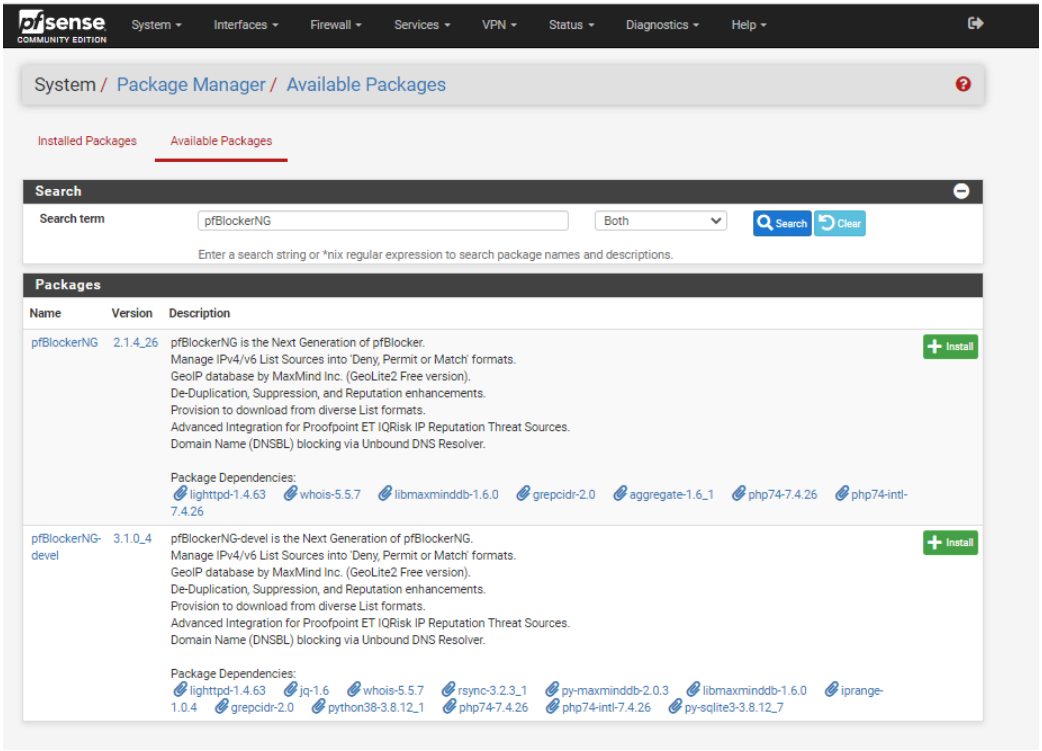

Figure 18: Paquet pfBlockerNG

1.5.1.2 Blocage de l'accès à Facebook

Afin de bloquer l'accès aux services Facebook, nous devons d'abord rechercher son ASN, qui représente un ensemble de préfixes IP routables sur Internet appartenant à un réseau ou à un ensemble de réseaux qui sont tous gérés, contrôlés et supervisés par un seul entité ou organisation, pour résoudre le problème d'avoir une pléthore d'adresses IP.

Tout d'abord, j'ai envoyé un ping à Facebook, puis j'ai recherché son ASN en utilisant les services asn.cymru.com.

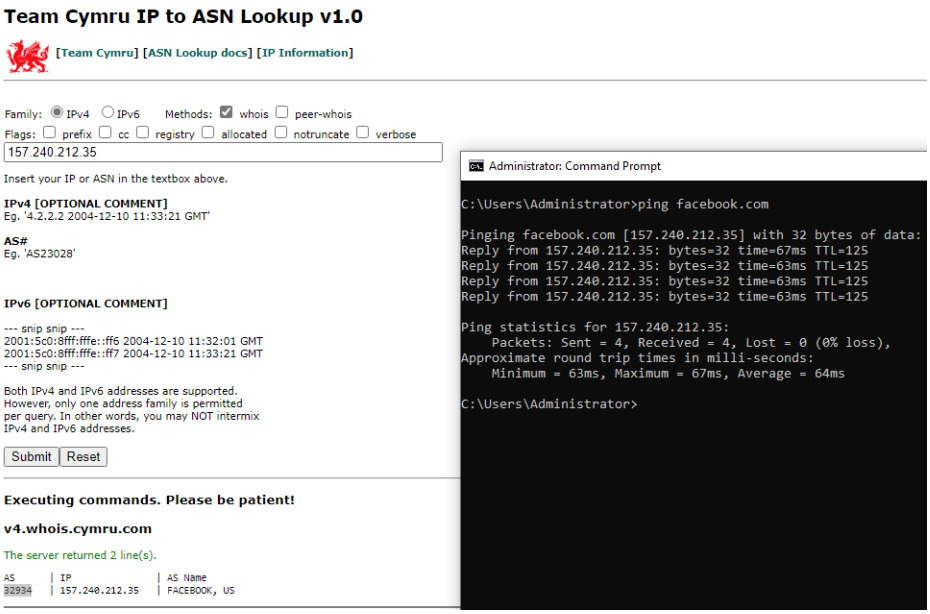

Figure 19: Rechercher l'ASN de Facebook

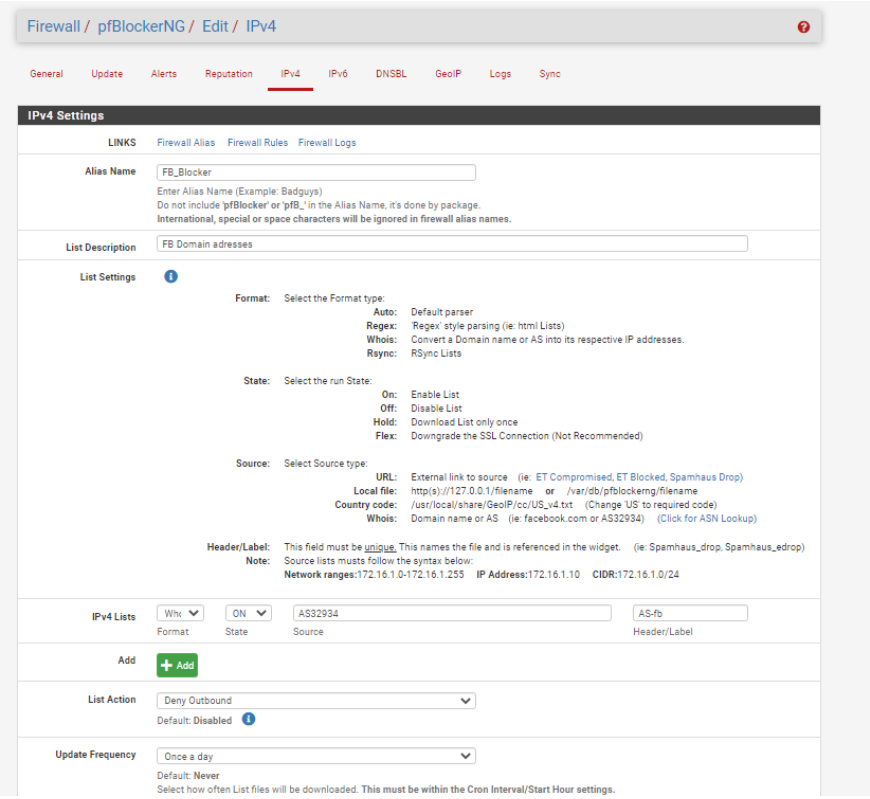

Figure 20: Ajout de l'ASN de Facebook au pfBlockerNG

Dans l'image ci-dessus, nous avons demandé à notre pfBlockerng de bloquer en fonction du numéro ASN, et nous avons défini l'action sur le trafic sortant, nous devons maintenant mettre à jour les paramètres pour confirmer les modifications.

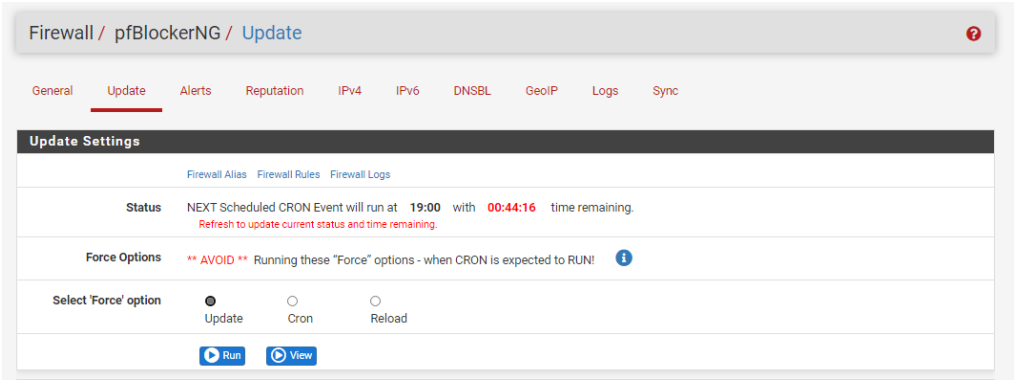

Figure 21: Redémarrage du service pour la synchronisation avec la configuration

En vérifiant les journaux, nous remarquerons que pfBlockerNG est allé chercher toutes les adresses IP liées au numéro AS que nous avons donné auparavant. Il a été ajouté avec succès 212 adresses IP à la liste des adresses IP refusées.

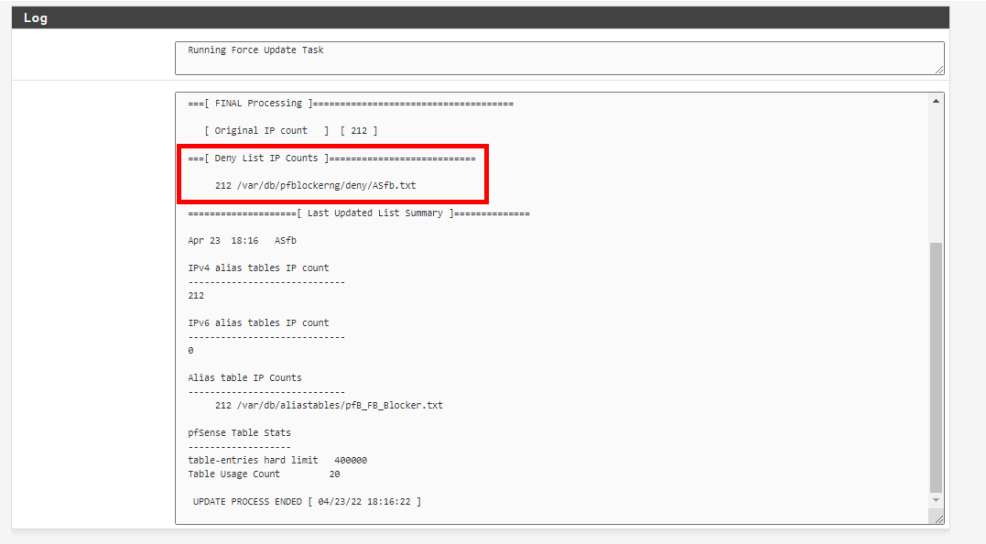

Figure 22: Recherches IP de l'ASN

Si nous survolons la section des règles, nous remarquons que les règles que nous avons définies sur le pfBlockerNG se sont automatiquement ajoutées aux règles gérées par le pare-feu. Après avoir vérifié l'accès à l'aide de notre hote Windows, nous ne pouvons plus y accéder.

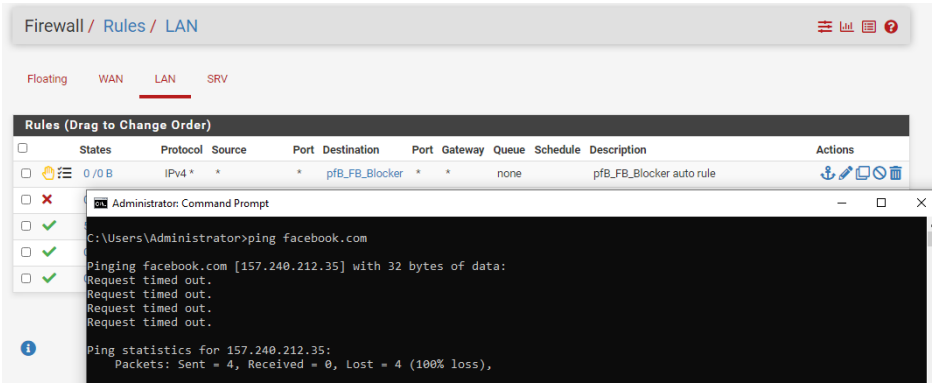

Figure 23: Vérification du blocage de Facebook

1.6 Qu'est-ce que l'IDS et l'IPS ?

La détection d'intrusion est le processus de surveillance des événements se produisant sur votre réseau et d'analyse de ceux-ci pour détecter des signes d'incidents, de violations ou de menaces imminentes possibles pour vos politiques de sécurité.

La prévention des intrusions est le processus de détection des intrusions, puis d'arrêt des incidents détectés. Ces mesures de sécurité sont disponibles sous forme de systèmes de détection d'intrusion (IDS) et de systèmes de prévention d'intrusion (IPS), qui font partie de votre réseau pour détecter et arrêter les incidents potentiels.

Un réseau d'entreprise typique possède plusieurs points d'accès à d'autres réseaux, publics et privés. L'enjeu est de maintenir la sécurité de ces réseaux tout en les gardant ouverts à leurs clients. Actuellement, les attaques sont

si sophistiquées qu'elles peuvent contrecarrer les meilleurs systèmes de sécurité, en particulier ceux qui fonctionnent encore en supposant que les réseaux peuvent être sécurisés par cryptage ou pare-feu. Malheureusement, ces technologies ne suffisent pas à elles seules à contrer les attaques d'aujourd'hui.

1.6.1 Que pouvez-vous faire avec IDS/IPS ?

Les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) surveillent en permanence votre réseau, identifient les incidents possibles et consignent des informations à leur sujet, stoppent les incidents et les signalent aux administrateurs de sécurité. De plus, certains réseaux utilisent IDS/IPS pour identifier les problèmes avec les politiques de sécurité et dissuader les individus de violer les politiques de sécurité. IDS/IPS sont devenus un complément nécessaire à l'infrastructure de sécurité de la plupart des organisations, précisément parce qu'ils peuvent arrêter les attaquants pendant qu'ils collectent des informations sur votre réseau.

1.6.2 Comment fonctionnent les IDS/IPS ?

Les trois méthodologies de détection IDS sont généralement utilisées pour détecter les incidents.

- La détection basée sur les signatures compare les signatures aux événements observés pour identifier les incidents possibles. Il s'agit de la méthode de détection la plus simple car elle compare uniquement l'unité d'activité actuelle (telle qu'un paquet ou une entrée de journal, à une liste de signatures) à l'aide d'opérations de comparaison de chaînes.
- La détection basée sur les anomalies compare les définitions de ce qui est considéré comme une activité normale avec les événements observés afin d'identifier les écarts significatifs. Cette méthode de détection peut être très efficace pour repérer des menaces jusque-là inconnues.
- L'analyse de protocole avec état compare des profils prédéterminés de définitions généralement acceptées pour une activité de protocole bénigne pour chaque état de protocole avec des événements observés afin d'identifier les écarts.

1.6.3 Pourquoi IDS et IPS sont essentiels pour la cybersécurité

Les équipes de sécurité sont confrontées à une menace croissante de violation de données et d'amendes de conformité tout en continuant à lutter avec les limites budgétaires et la politique de l'entreprise. La technologie IDS/IPS couvre des tâches spécifiques et importantes d'une stratégie de cybersécurité :

- **Automatisation** : les systèmes IDS/IPS sont largement autonomes, ce qui en fait des candidats idéaux pour une utilisation dans la pile de sécurité actuelle. IPS offre la tranquillité d'esprit que le réseau est protégé contre les menaces connues avec des besoins en ressources limités.
- **Conformité** : une partie de la conformité nécessite souvent de prouver que vous avez investi dans des technologies et des systèmes pour protéger les données. La mise en œuvre d'une solution IDS/IPS coche une case sur la feuille de conformité et répond à un certain nombre de contrôles de sécurité CIS. Plus important encore, les données d'audit constituent un élément précieux des enquêtes de conformité.

- **Application des politiques** : IDS/IPS sont configurables pour aider à appliquer les politiques de sécurité internes au niveau du réseau. Par exemple, si vous ne prenez en charge qu'un seul VPN, vous pouvez utiliser l'IPS pour bloquer un autre trafic VPN.

1.6.4 HIDS Host-based Intrusion Detection System

Un système de détection d'intrusion basé sur l'hôte (HIDS) est un système de détection d'intrusion capable de surveiller et d'analyser les composants internes d'un système informatique ainsi que les paquets réseau sur ses interfaces réseau, de la même manière qu'un système de détection d'intrusion basé sur le réseau. (NIDS) fonctionne. Il s'agissait du premier type de logiciel de détection d'intrusion à avoir été conçu, le système cible d'origine étant l'ordinateur central où l'interaction extérieure était peu fréquente.

Un IDS basé sur l'hôte est capable de surveiller tout ou partie du comportement dynamique et de l'état d'un système informatique, en fonction de sa configuration. Outre des activités telles que l'inspection dynamique des paquets réseau ciblés sur cet hôte spécifique, un HIDS peut détecter quel programme accède à quelles ressources et le découvrir.

En général, un HIDS utilise une base de données (base de données d'objets) d'objets système qu'il doit surveiller - généralement (mais pas nécessairement) des objets de système de fichiers. Un HIDS pourrait également vérifier que les régions appropriées de la mémoire n'ont pas été modifiées. Pour chaque objet en question, un HIDS se souviendra généralement de ses attributs (autorisations, taille, dates de modification) et créera une somme de contrôle quelconque (un hachage MD5, SHA1 ou similaire) pour le contenu, le cas échéant. Ces informations sont stockées dans une base de données sécurisée pour une comparaison ultérieure (base de données de somme de contrôle).

1.6.5 Snort

SNORT est un puissant système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) open source qui fournit une analyse du trafic réseau en temps réel et un enregistrement des paquets de données. SNORT utilise un langage basé sur des règles qui combine des méthodes d'inspection d'anomalies, de protocoles et de signatures pour détecter les activités potentiellement malveillantes.

À l'aide de SNORT, les administrateurs réseau peuvent détecter les attaques par déni de service (DoS) et les attaques DoS distribuées (DDoS), les attaques Common Gateway Interface (CGI), les dépassements de mémoire tampon et les analyses de ports furtifs. SNORT crée une série de règles qui définissent l'activité réseau malveillante, identifient les paquets malveillants et envoient des alertes aux utilisateurs.

SNORT est un logiciel open source gratuit qui peut être déployé par des particuliers et des organisations. Le langage de règles SNORT détermine quel trafic réseau doit être collecté et ce qui doit se passer lorsqu'il détecte des paquets malveillants. Cette signification de reniflement peut être utilisée de la même manière que les renifleurs et les systèmes de détection d'intrusion réseau pour découvrir les paquets malveillants ou comme une solution IPS réseau complète qui surveille l'activité du réseau et détecte et bloque les vecteurs d'attaque potentiels.

1.6.5.1 Quelles sont les fonctionnalités de SNORT?

Il existe diverses fonctionnalités qui rendent SNORT utile aux administrateurs réseau pour surveiller leurs systèmes et détecter les activités malveillantes. Ceux-ci inclus:

- **Moniteur de trafic en temps réel:** SNORT peut être utilisé pour surveiller le trafic entrant et sortant d'un réseau. Il surveillera le trafic en temps réel et émettra des alertes aux utilisateurs lorsqu'il découvrira des paquets ou des menaces potentiellement malveillantes sur les réseaux IP (Internet Protocol).
- **Journalisation des paquets:** SNORT active la journalisation des paquets via son mode enregistreur de paquets, ce qui signifie qu'il enregistre les paquets sur le disque. Dans ce mode, SNORT collecte chaque paquet et l'enregistre dans un répertoire hiérarchique basé sur l'adresse IP du réseau hôte.
- **Analyse du protocole**: SNORT peut effectuer une analyse de protocole, qui est un processus de détection de réseau qui capture des données dans des couches de protocole pour une analyse supplémentaire. Cela permet à l'administrateur réseau d'examiner plus en détail les paquets de données potentiellement malveillants, ce qui est crucial, par exemple, dans la spécification du protocole de pile TCP/IP (Transmission Control Protocol/IP).
- **Correspondance de contenu**: SNORT rassemble les règles par protocole, comme IP et TCP, puis par ports, puis par ceux qui ont du contenu et ceux qui n'en ont pas. Les règles qui ont du contenu utilisent un comparateur multi-modèle qui augmente les performances, en particulier lorsqu'il s'agit de protocoles tels que le protocole de transfert hypertexte (HTTP). Les règles qui n'ont pas de contenu sont toujours évaluées, ce qui affecte négativement les performances.

1.6.5.2 Quels sont les différents modes SNORT ?

Il existe trois modes différents dans lesquels SNORT peut être exécuté, qui dépendront des drapeaux utilisés dans la commande SNORT.

- **Renifleur de paquets**: Le mode renifleur de paquets de SNORT signifie que le logiciel lira les paquets IP puis les affichera à l'utilisateur sur sa console.
- **Enregistreur de paquets:** En mode enregistreur de paquets, SNORT enregistrera tous les paquets IP qui visitent le réseau. L'administrateur réseau peut alors voir qui a visité son réseau et avoir un aperçu du système d'exploitation et des protocoles qu'il utilisait.
- **NIPDS** *(Système de détection et de prévention des intrusions sur le réseau):* En mode NIPDS, SNORT n'enregistrera que les paquets considérés comme malveillants. Pour ce faire, il utilise les caractéristiques prédéfinies des paquets malveillants, qui sont définies dans ses règles. L'action entreprise par SNORT est également définie dans les règles définies par l'administrateur réseau.

1.6.5.3 Implémentation de Snort sur notre topologie

Heureusement, le projet pfSense nous permet de télécharger snort depuis son gestionnaire de packages, ce qui facilite son intégration, sa gestion et sa maintenance. Tout ce que nous avons à faire est de survoler le gestionnaire de packages et d'installer notre IDS/IPS.

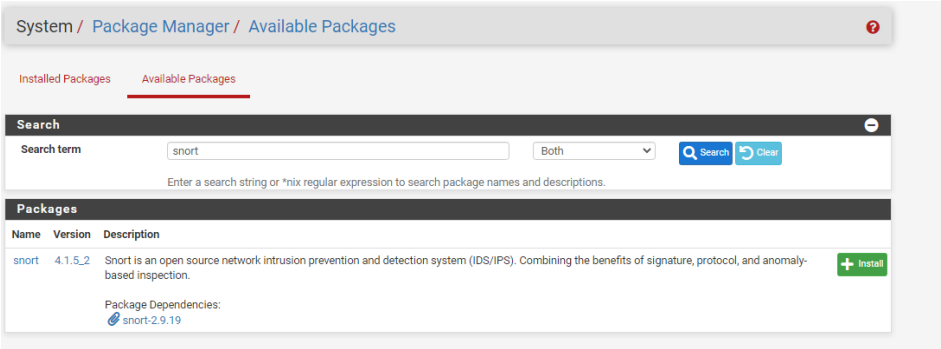

Figure 24: Le package SNORT

Plongeons maintenant dans snort (Services->Snort) et sélectionnons l'interface que nous voulons écouter et renifler.

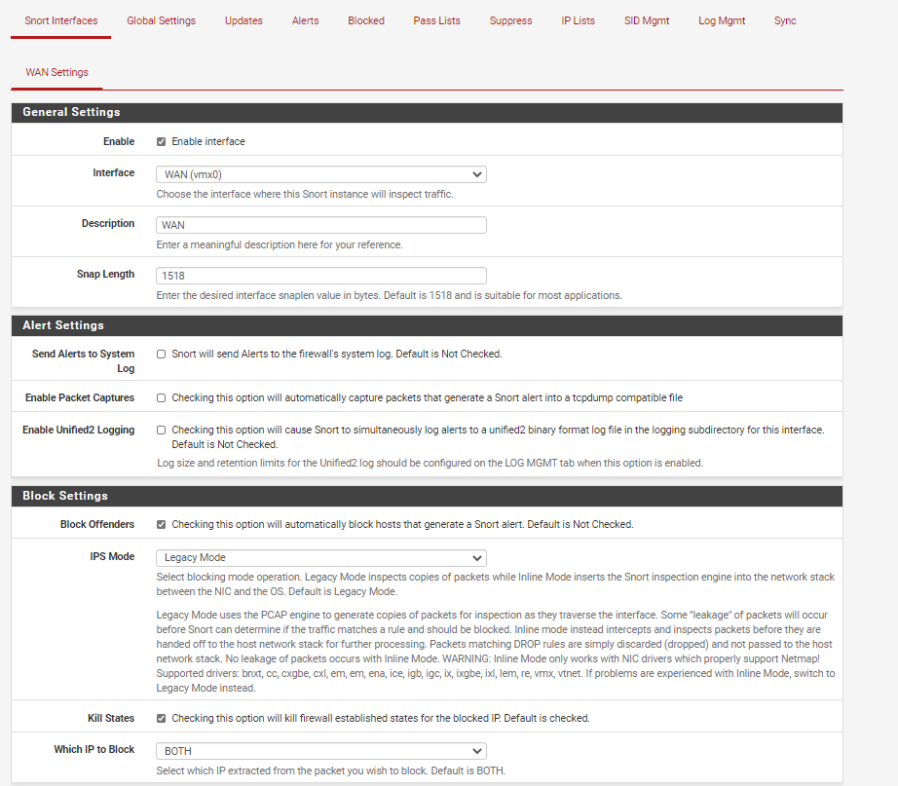

Figure 25: L"activation du service Snort

Dans les paramètres de l'interface Snort, nous avons choisi l'interface à écouter et le mode IPS, qui dans notre cas est le mode hérité, la bibliothèque pcap est utilisée pour faire une copie (clone si vous voulez) de chaque paquet à mesure qu'il arrive de la carte réseau en route vers le moteur de pare-feu pf. Nous pouvons également activer les journaux.

Snort fonctionne à l'aide de signatures de détection appelées règles. Les règles Snort peuvent être personnalisées par l'utilisateur, ou l'un des nombreux ensembles de règles pré-packagés peut être activé et téléchargé. Le package Snort offre actuellement un support pour ces règles pré-packagées :

- **Snort VRT (Vulnerability Research Team) rules**: L'ensemble de règles d'abonné Snort fait référence aux règles qui ont été développées, testées et approuvées par l'équipe de recherche et de renseignement de sécurité de Talos (Talos). L'ensemble de règles d'abonné Snort publié après le 7 mars 2005 est régi par le contrat de licence de l'ensemble de règles d'abonné Snort.
- **Snort GPLv2 Community Rules:** L'ensemble de règles de la communauté Snort est un ensemble de règles certifié GPLv2 Talos qui est distribué gratuitement sans aucune restriction de licence d'abonné Snort. Cet ensemble de règles est mis à jour quotidiennement et est un sous-ensemble de l'ensemble de règles de l'abonné.
- **Emerging Threats Open Rules:** L'ensemble de règles ETOpen est un excellent ensemble de règles anti-malware IDS/IPS qui permet aux utilisateurs soumis à des contraintes de coût d'améliorer considérablement leur détection de malware basée sur le réseau.
- **OpenAppID** Open detectors and rules for application detection: Le package OpenAppID Detectors contient les signatures d'application requises par le préprocesseur AppID et les règles de texte OpenAppID.

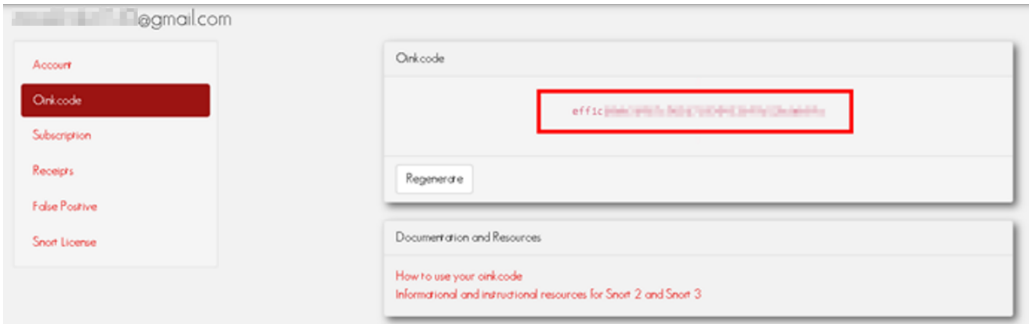

Figure 26: Clé d'abonnement gratuite de Snort

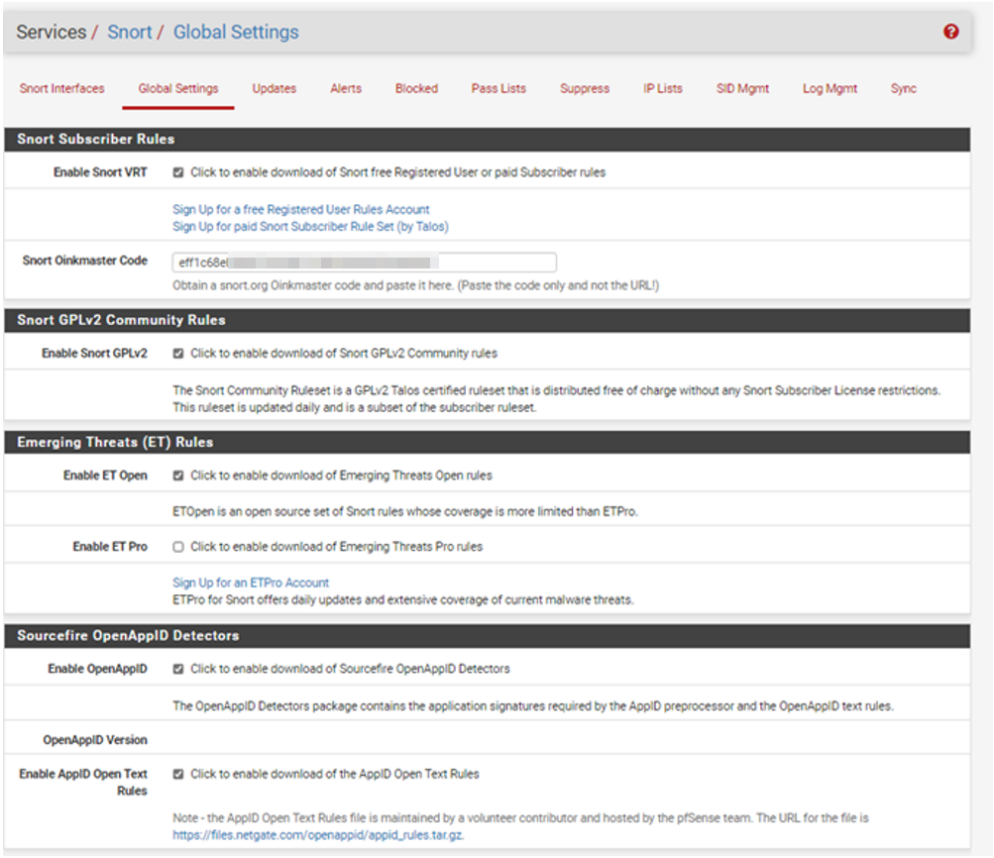

Figure 27: Les règles de Snort

L'onglet Mises à jour est utilisé pour vérifier l'état des packages de règles téléchargés et pour télécharger de nouvelles mises à jour. Le tableau affiche les packages de règles disponibles et leur état actuel (non activé, non téléchargé ou somme de contrôle et date MD5 valides).

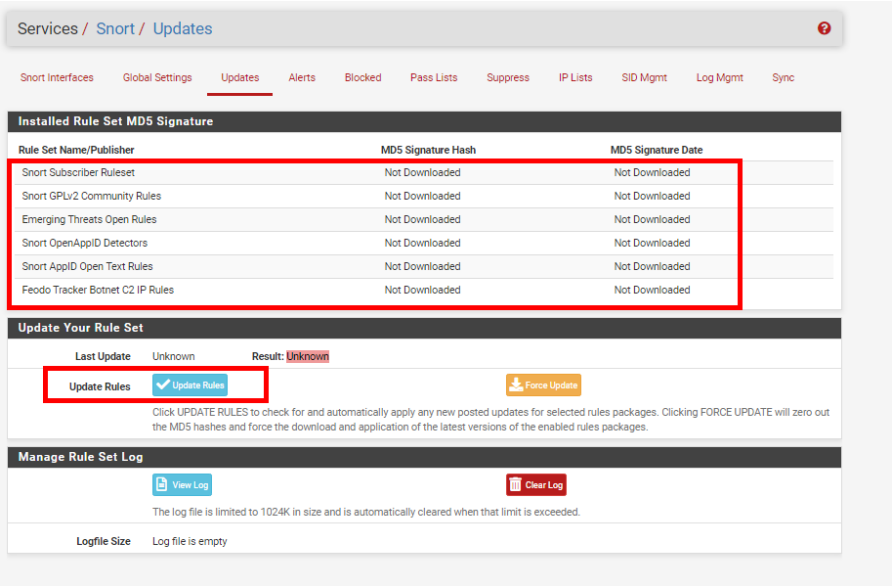

Figure 28: Synchronisation de la configuration

Après la mise à jour des règles, nous devrions exécuter Snort

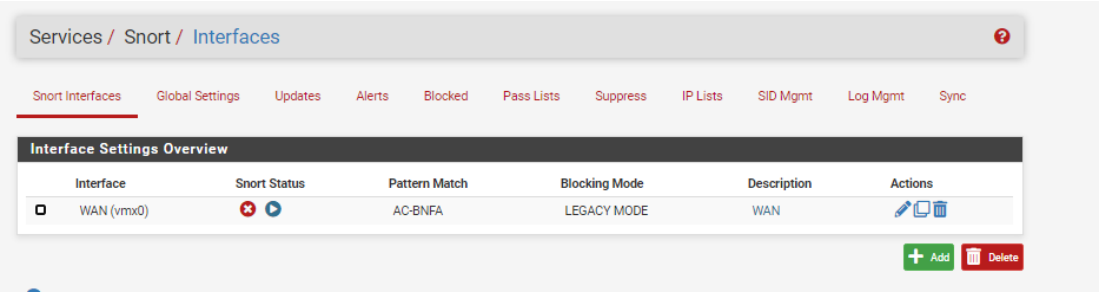

Figure 29: Exécution du service Snort

S'il y avait des faux négatifs, nous pouvons ajouter l'alerte à la liste de suppression à ignorer lors de la vérification des règles.

1.7 Configuration du service Portail Captif

Le portail captif du logiciel pfSense® oblige les utilisateurs d'une interface à s'authentifier avant d'accorder l'accès à Internet. Dans la mesure du possible, le pare-feu présente automatiquement une page Web de connexion dans laquelle l'utilisateur doit entrer des informations d'identification telles qu'un nom d'utilisateur/mot de passe, un code promotionnel ou un simple accord de clic.

Cette fonctionnalité est couramment utilisée dans l'industrie hôtelière (hôtels, restaurants, aéroports, etc.) ainsi que dans les environnements d'entreprise et même à domicile. Il est principalement utilisé pour les points d'accès sans fil ou pour une authentification supplémentaire avant d'autoriser l'accès aux réseaux internes à partir de clients sans fil.

1.7.1 Implementation

Nous devons d'abord définir une zone, les zones de portail captif définissent des portails séparés pour différents ensembles d'interfaces. Une zone peut avoir plusieurs interfaces, mais une interface ne peut être membre que d'une seule zone. Tenter d'ajouter la même interface à plusieurs zones entraînera une erreur.

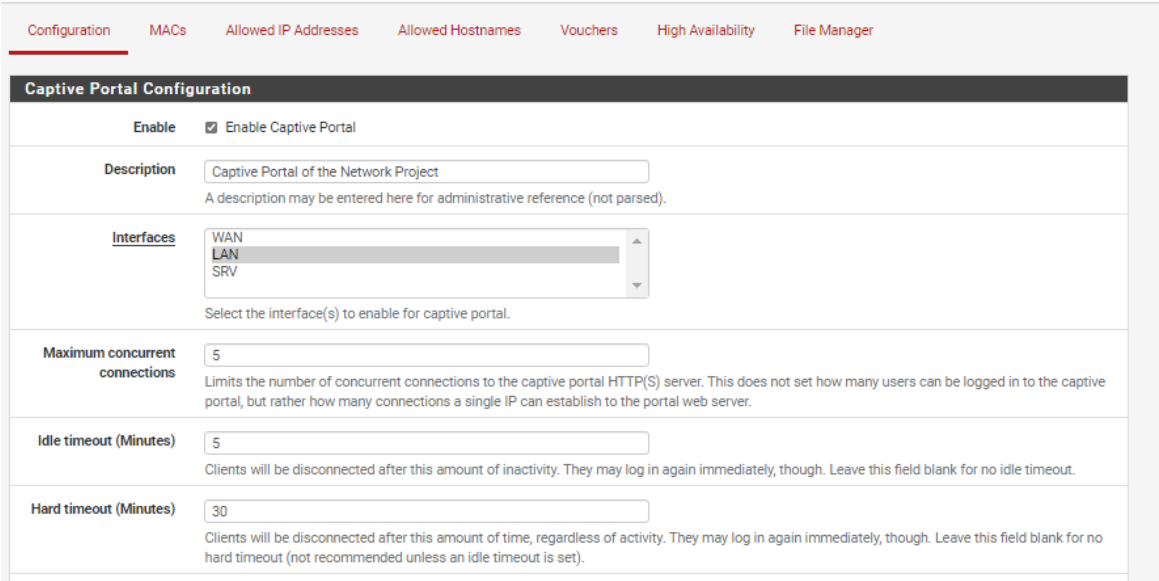

Figure 30: Activation du service Portail Captif

- **Nombre maximal de connexions simultanées** : spécifie le nombre maximal de connexions simultanées au serveur Web du portail par adresse IP.
- **Délai d'inactivité** : délai d'attente, spécifié en minutes, après lequel les utilisateurs inactifs seront déconnectés par le portail. Les utilisateurs peuvent se reconnecter immédiatement.
- **Délai d'attente dur** : un délai d'attente, spécifié en minutes, après lequel le portail déconnectera de force les utilisateurs.
- **Crédits Pass-Through :** ces crédits donnent aux appareils une période de grâce avant qu'ils ne doivent s'authentifier via le portail. Par exemple, un appareil peut se connecter 3 fois en une journée sans voir la page du portail, mais pas plus que cela et il doit se connecter.
- **Crédits d'intercommunication autorisés par adresse MAC :** le nombre de fois qu'une adresse MAC spécifique peut se connecter via le portail.
- **Connexions utilisateur simultanées :** contrôle si les utilisateurs sont autorisés ou non à se connecter plusieurs fois.
- **Restrictions de bande passante par utilisateur :** le portail captif peut également éventuellement limiter le débit des utilisateurs pour les empêcher d'utiliser trop de bande passante.

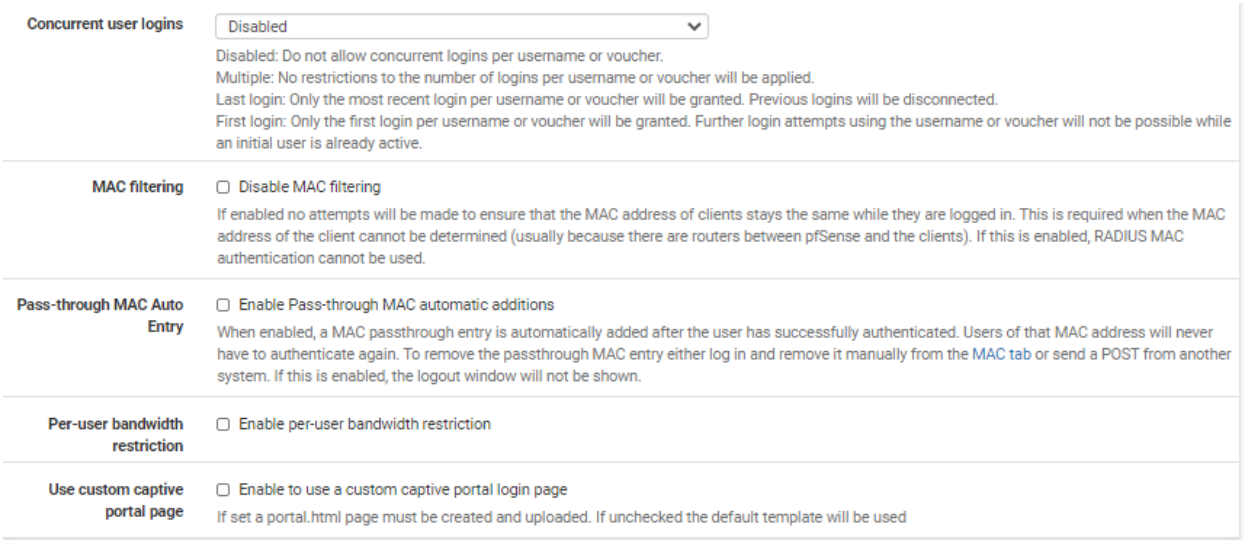

Figure 31: Paramètres de configuration du Portail Captif

1.7.2 Sécurisation du portail captif

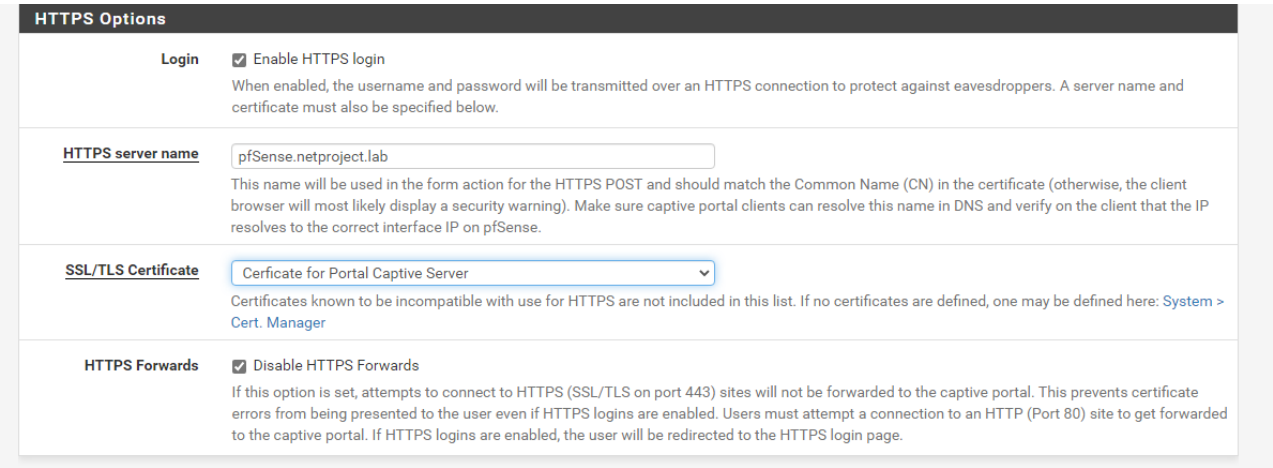

Figure 32: Sécurisation du portail captif

Lorsque la connexion HTTPS est définie, le portail écoute et accepte les requêtes HTTPS pour la page du portail. Cette option nécessite un certificat SSL/TLS. Le nom du serveur HTTPS doit correspondre au nom commun (CN) sur le certificat pour empêcher les utilisateurs de recevoir des erreurs de certificat. Nous devons également sélectionner le certificat SSL utilisé par le portail pour HTTPS.

Lorsque "Disable HTTPS Forwards" est coché, les tentatives des clients de se connecter aux sites HTTPS sur le port 443 ne sont pas redirigées vers le portail. Cela empêche les utilisateurs de recevoir des erreurs de certificat non valides. Les utilisateurs doivent tenter une connexion à un site HTTP, qui sera ensuite redirigé vers le portail.

Les autorités de certification aident à sécuriser Internet pour les organisations et les utilisateurs. L'objectif principal d'une autorité de certification est de vérifier l'authenticité et la fiabilité d'un site Web, d'un domaine et

d'une organisation afin que les utilisateurs sachent exactement avec qui ils communiquent en ligne et si cette entité peut faire confiance à leurs données.

En ayant un certificat auto-signé, vous êtes effectivement seul, sans le soutien d'une autorité de certification de confiance et l'application des dernières méthodes cryptographiques nécessaires pour garantir une authentification et un cryptage appropriés des données, des appareils et des applications.

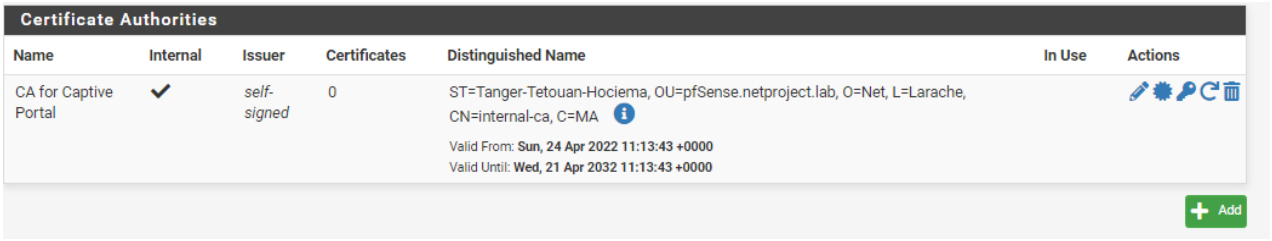

Figure 33:Création de l'autorité de certification

Après avoir créé avec succès une autorité de certification, nous pouvons maintenant créer des certificats basés sur notre autorité de certification auto-créée.

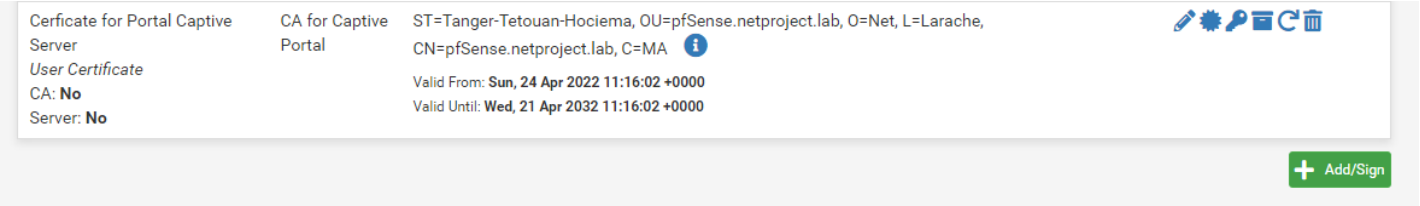

Figure 34: Création de certificat pour le service de portail captif

1.7.3 Authentification du portail captif

Cette section configure l'authentification pour le portail captif. Si l'authentification est requise pour la zone, elle peut être gérée par la base de données d'utilisateurs locale, RADIUS ou LDAP.

Dans le cas de cette topologie, j'ai choisi d'authentifier à l'aide de LDAP (Lightweight Directory Access Protocol), un protocole ouvert et multiplateforme utilisé pour l'authentification des services d'annuaire. LDAP fournit le langage de communication utilisé par les applications pour communiquer avec d'autres serveurs de services d'annuaire.

La conservation des données dans un système centralisé donne un meilleur contrôle sur l'ensemble de vos processus, quel que soit le domaine d'activité auquel ils appartiennent. Parfois, avoir différents types de documents peut poser un défi à certaines organisations car ils ne peuvent pas être traités de la même manière.

1.7.4 Création d'UO dans notre AD

Tout d'abord, nous devons créer une unité d'organisation dans notre service d'annuaire actif. Une unité d'organisation (OU) est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des

utilisateurs, des groupes et des ordinateurs. Il s'agit de la plus petite unité à laquelle un administrateur peut attribuer des paramètres de stratégie de groupe ou des autorisations de compte.

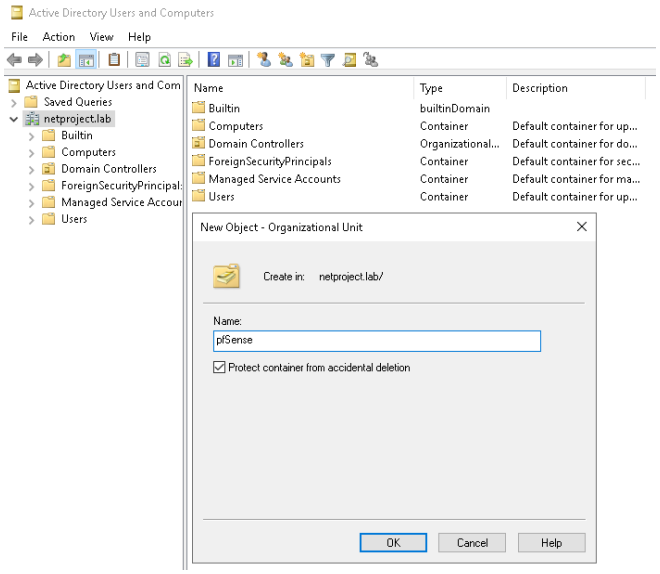

Figure 35: Création d'UO pfSense

Maintenant, je crée des utilisateurs autorisés à accéder au service de portail captif sur le pare-feu.

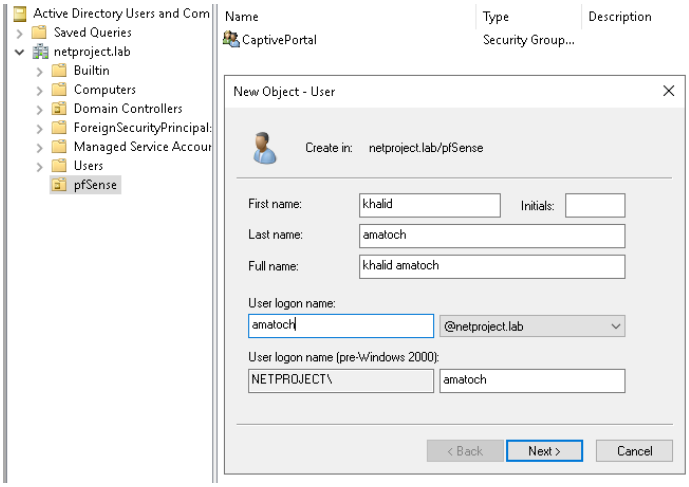

Figure 36: Création d'un nouvel utilisateur dans pfSense OU

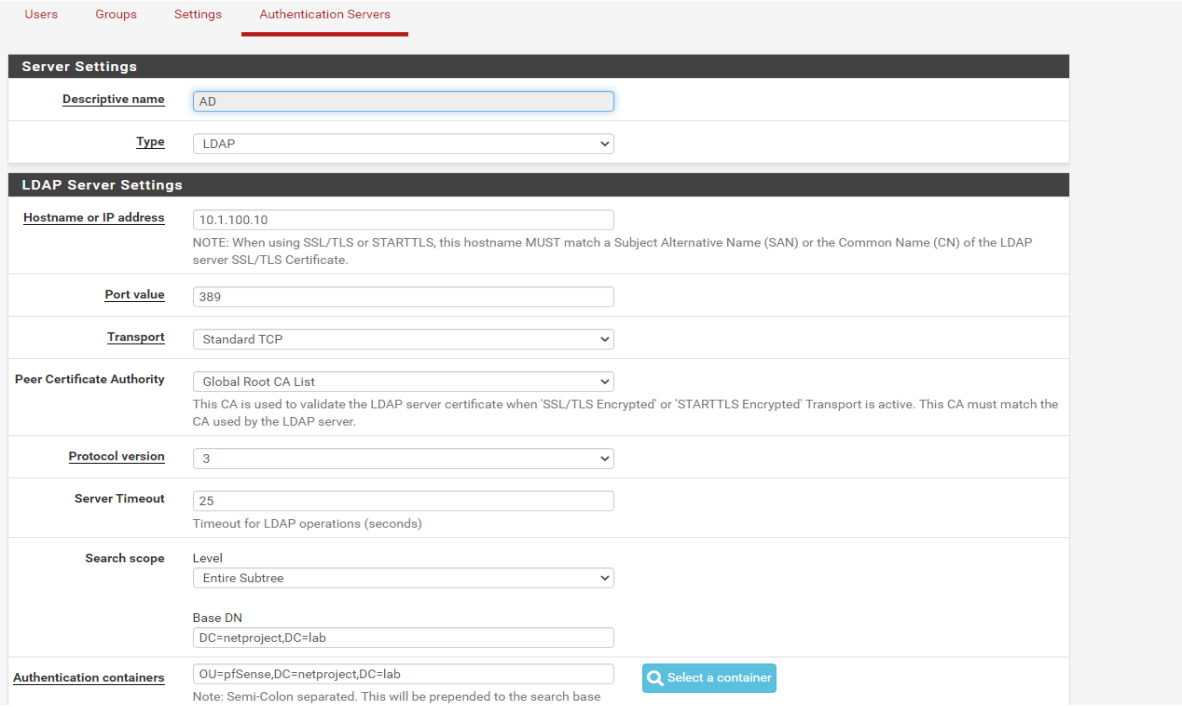

Figure 37: Synchronisation de l'authentification du portail captif avec notre Active Directory.

Maintenant, nous devons survoler les serveurs d'authentification pour ajouter notre serveur Active Directory, nous devons fournir l'adresse IP de notre serveur et le PORT utilisé, puis nous devons lui donner le nom distinctif (DN) qui a un nom unique qui identifie l'entrée à la hiérarchie respective.

Une façon de trouver le DN, nous utilisons PowerShell (PowerShell est un programme d'automatisation de tâches et de gestion de configuration de Microsoft, composé d'un shell de ligne de commande et du langage de script associé) en utilisant la commande de ligne "Get-ADUser".

```
PS C:\Users\Administrator> Get-ADUser khalid | Select-Object *


DistinguishedName  : CN=khalid,OU=pfSense,DC=netproject,DC=lab
Enabled            : True
GivenName          : khalid
Name               : khalid
ObjectClass        : user
ObjectGUID         : 489ab888-cd56-4898-8fe2-c873dff7e474
SamAccountName     : khalid
SID                : S-1-5-21-2527146709-838010375-2080984311-1112
Surname            :
UserPrincipalName  : khalid@netproject.lab
PropertyNames      : {DistinguishedName, Enabled, GivenName, Name...}
AddedProperties    : {}
RemovedProperties  : {}
ModifiedProperties : {}
PropertyCount      : 10
```

Figure 38: Recherche du nom distinctif.

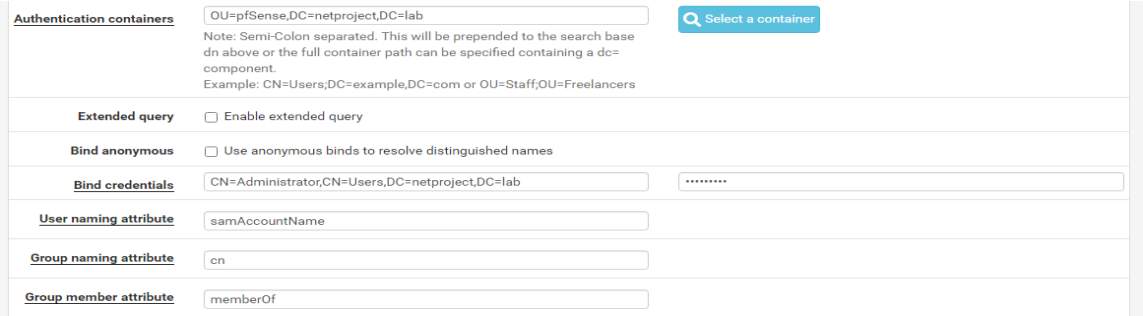

Figure 39: Synchronisation du portail captif à l'aide de LDAP

1.7.5 Test de la connectivité à AD

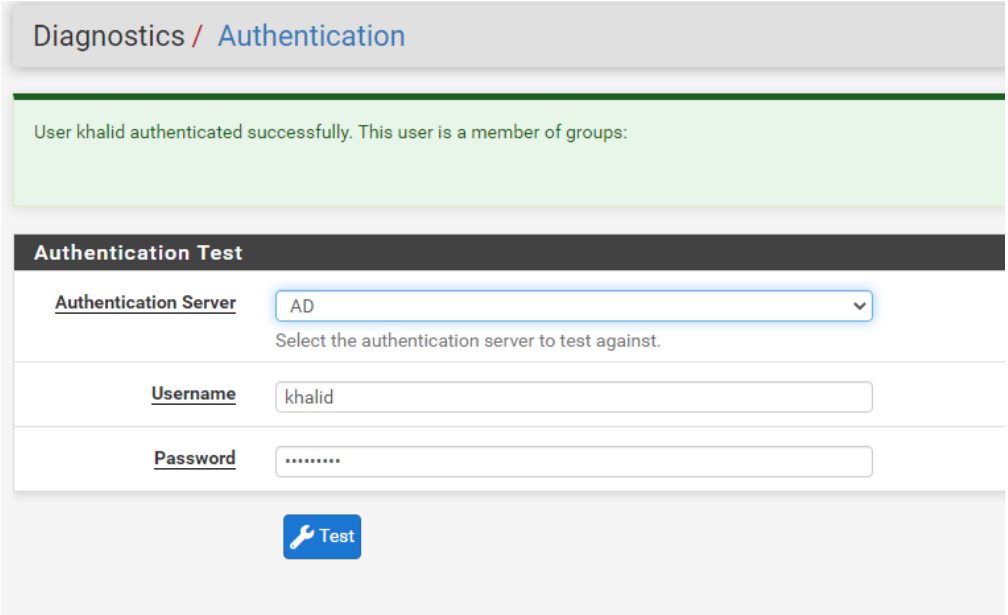

Figure 40: Test de la connectivité à AD

L'une des caractéristiques d'avoir pfSense, nous permettant de diagnostiquer et de tester la connectivité aux serveurs que nous avons ajoutés à notre configuration. En fournissant le nom d'utilisateur et le mot de passe que nous avons ajoutés à l'unité d'organisation pfSense, nous avons réussi à établir la connectivité avec notre serveur AD.

1.7.6 Captive Portal Authentification

Figure 41: Page d'authentification du portail captif.

Nous pouvons nous authentifier avec succès à l'aide de nos services AD en utilisant LDAP.

1.8 Qu'est-ce qu'un serveur proxy?

Un serveur proxy agit comme une passerelle entre l'utilisateur et Internet. Il s'agit d'un serveur intermédiaire séparant les utilisateurs finaux des sites Web qu'ils naviguent. Les serveurs proxy offrent différents niveaux de fonctionnalité, de sécurité et de confidentialité en fonction de la politique de l'entreprise.

1.8.1 Comment fonctionne un serveur proxy?

Lorsque vous envoyez une requête Web, votre requête est d'abord transmise au serveur proxy. Le serveur proxy effectue ensuite votre demande Web en votre nom, recueille la réponse du serveur Web, la stocke puis transmet les données de la page Web afin que les utilisateurs finaux puissent voir la page dans leurs navigateurs.

Lorsque le serveur proxy transmet vos requêtes Web, il peut apporter des modifications aux données envoyées par les utilisateurs finaux tout en leur obtenant les informations qu'ils s'attendent à voir. Un serveur proxy peut modifier l'adresse IP, de sorte que le serveur Web ne sait pas exactement d'où provient la demande.

1.8.2 Pourquoi devrions-nous utiliser un serveur proxy?

Il existe plusieurs raisons pour lesquelles les organisations et les individus utilisent un serveur proxy. Dans notre cas:

- **Pour contrôler l'utilisation d'Internet par les employés** : les organisations mettent en place des serveurs proxy pour contrôler et surveiller la façon dont leurs employés utilisent Internet. Ils peuvent également

surveiller et enregistrer toutes les requêtes Web. Ainsi, même s'ils ne bloquent pas le site, ils savent combien de temps vous passez à cyberloafer.

- **Économies de bande passante et vitesses améliorées** : les serveurs proxy peuvent mettre en cache (enregistrer une copie du site Web localement) des sites Web populaires. Ainsi, lorsque vous demandez un site Web, le serveur proxy vérifie s'il dispose de la copie la plus récente du site, puis vous envoyer la copie enregistrée.
- **Avantages en matière de confidentialité :** les particuliers et les organisations utilisent des serveurs proxy pour naviguer sur Internet de manière plus privée
- **Sécurité améliorée :** les serveurs proxy offrent des avantages en matière de sécurité en plus des avantages en matière de confidentialité.

De plus, les organisations peuvent coupler leur serveur proxy avec un réseau privé virtuel (VPN), de sorte que les utilisateurs distants accèdent toujours à Internet via le proxy de l'entreprise. Un VPN est une connexion directe au réseau de l'entreprise que les entreprises fournissent aux utilisateurs externes ou distants.

1.8.3 Types de serveurs proxy

Tous les serveurs proxy ne fonctionnent pas de la même manière. Il est important de comprendre exactement quelle fonctionnalité.

- **Proxy transparent** Un proxy transparent indique aux sites Web qu'il s'agit d'un serveur proxy et qu'il transmettra toujours votre adresse IP, vous identifiant au serveur Web.
- **proxy anonyme** Un proxy anonyme s'identifiera en tant que proxy, mais il ne transmettra pas votre adresse IP au site Web - cela aide à prévenir le vol d'identité et à garder vos habitudes de navigation privées
- **Proxy déformant** Un serveur proxy déformant transmet une fausse adresse IP pour vous tout en s'identifiant en tant que proxy.
- **Proxy à haut anonymat** Les serveurs proxy à haut anonymat changent périodiquement l'adresse IP qu'ils présentent au serveur Web, ce qui rend très difficile le suivi de quel trafic appartient à qui. Les proxys à anonymat élevé, comme le réseau TOR, constituent le moyen le plus privé et le plus sûr de lire Internet.

1.8.4 Squid

Squid est un proxy de mise en cache dans les packages pfSense pour le Web prenant en charge HTTP, HTTPS, FTP, etc. Il réduit la bande passante et améliore les temps de réponse en mettant en cache et en réutilisant les pages Web fréquemment demandées. Squid dispose de contrôles d'accès étendus et constitue un excellent accélérateur de serveur.

1.8.4.1 *Installation du service Squid sur pfSense*

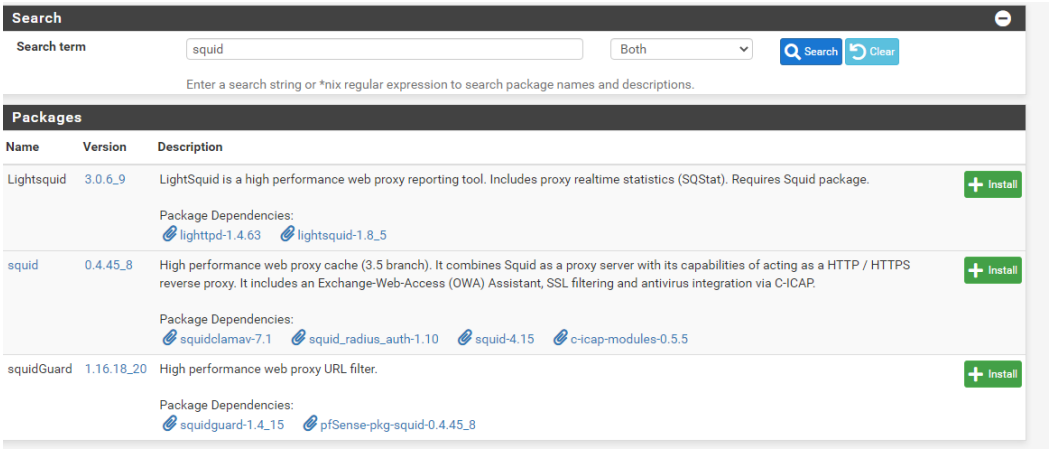

Figure 42: Package de Squid

- **Squid** est un proxy de mise en cache pour HTTP et d'autres protocoles.
  - Peut accélérer l'accès en mettant en cache localement les sites/objets couramment chargés.
  - Peut économiser de la bande passante en réduisant les téléchargements multiples en double.
  - Permet d'autres actions sur le trafic Web (contrôle d'accès, rapports).

- **SquidGuard** est utilisé pour le contrôle d'accès basé sur le domaine ou l'URL demandé par un client.
  - Des décisions peuvent être prises pour autoriser ou refuser l'accès en fonction du client et/ou destination.
  - Les sites bloqués peuvent être redirigés vers une page d'erreur dans la plupart des cas.
  - Listes personnalisées de sites ou listes noires prédéfinies provenant d'autres sources.
- **Lightsquid** est utilisé pour signaler l'historique d'accès au Web.
  - Analyse le journal d'accès au calmar, note qui est allé où, combien de bande passante ils ont utilisé.
  - A des rapports pour une utilisation quotidienne, une utilisation mensuelle, etc.

1.8.4.2 *Configuration de SQUID dans pfSense*

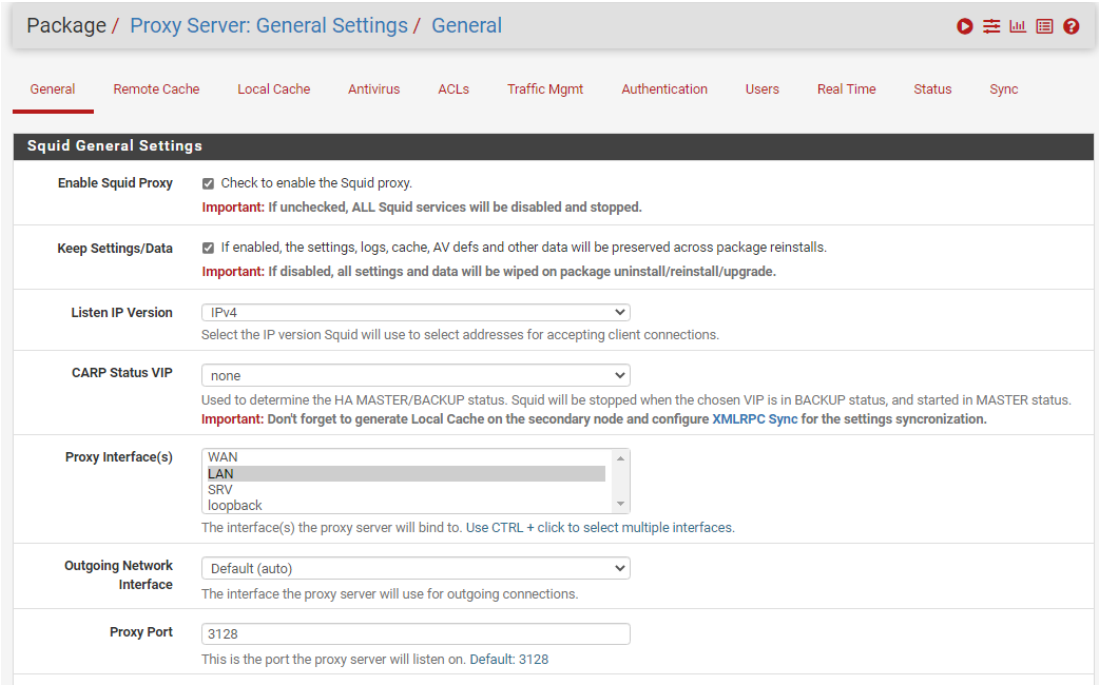

Figure 43: L'activation de Squid sur l'interface LAN

Nous devrions activer le proxy, choisir l'interface à laquelle nous voulons que le serveur se lie, puis choisir le port et la CARP pour la haute disponibilité, au cas où nous aurions le statut master/backup.

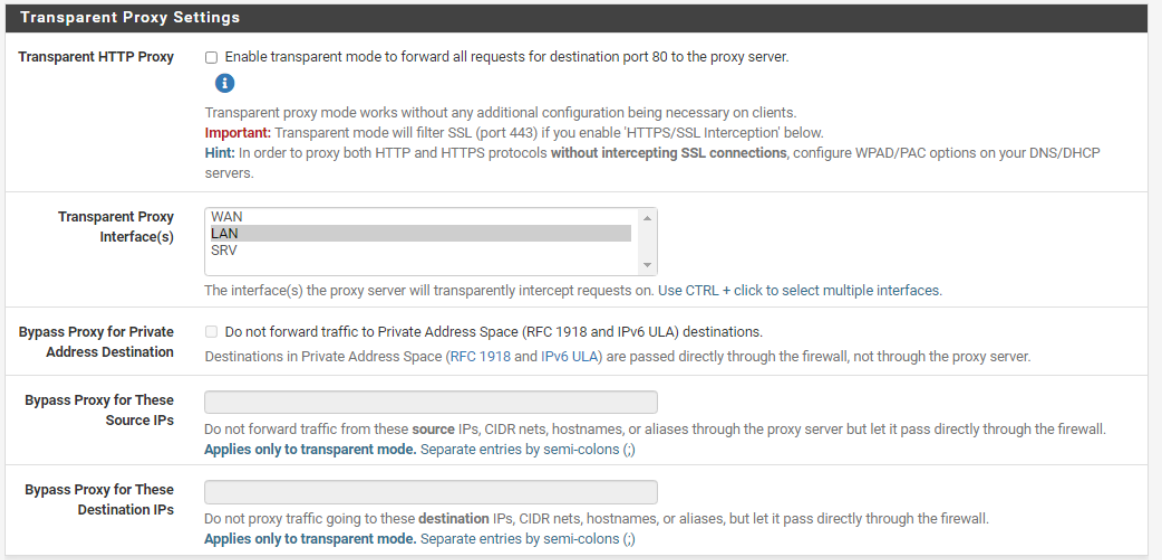

Figure 44: Paramètres proxy transparents

Comme nous l'avons expliqué précédemment, un proxy transparent fonctionne sans qu'aucune configuration supplémentaire ne soit nécessaire pour les clients, cela signifie qu'il redirige tous les trafics via le serveur.

Dans notre cas, je l'ai désactivé car nous ne pouvons pas définir l'authentification si un proxy transparent est activé.

1.8.4.3 Configuration du stockage local

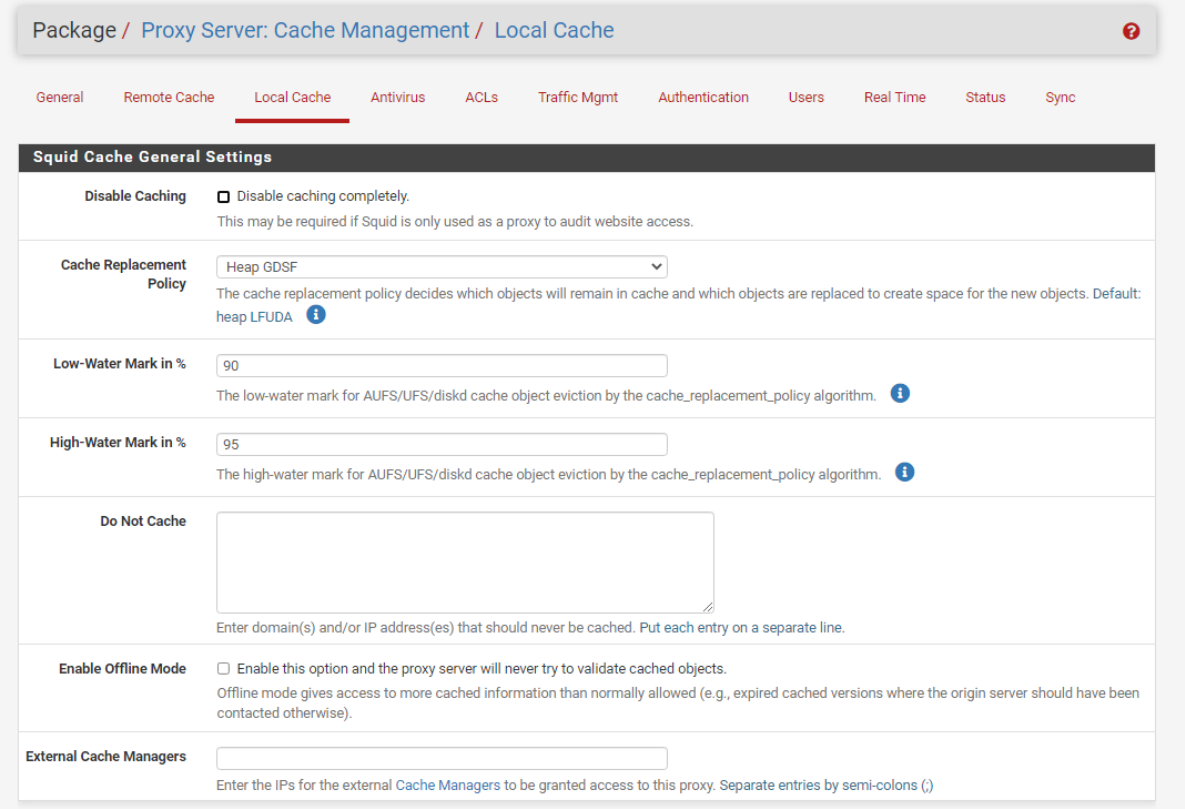

Figure 45: Configuration du stockage local

Le cache local est l'endroit que le serveur proxy utilisera pour stocker les pages, plus tard, nous pouvons définir comme paramètres, le type de cache, qu'il soit stocké sur le disque dur ou sur le RAM, le mécanisme de stockage et les tailles d'objet à stocker.

Figure 46: Configuration du navigateur pour passer par le proxy

1.8.4.4 Paramétrage de l'authentification avec Active Directory

L'idée derrière cette partie est que seuls les utilisateurs stockés dans l'unité d'organisation pfSense sont autorisés à accéder à Internet via le proxy.

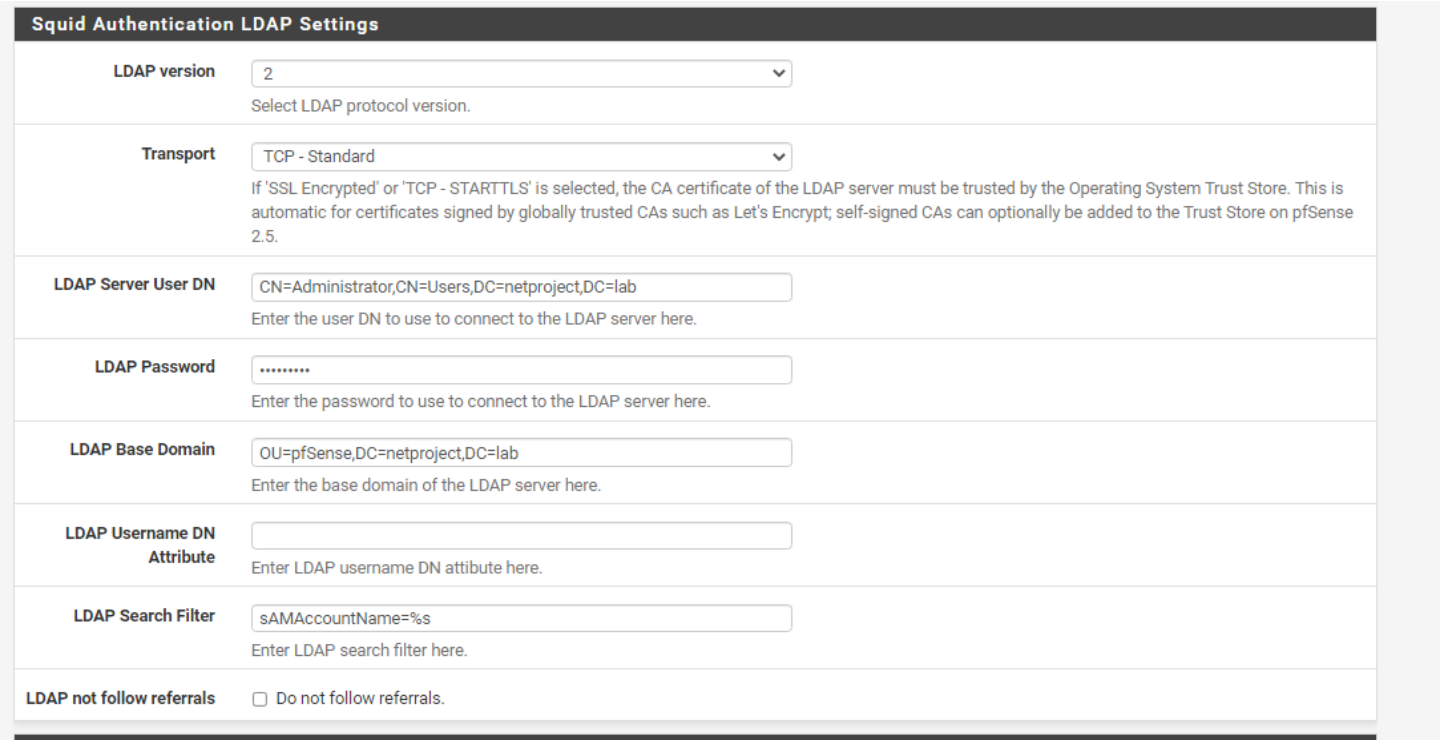

Figure 47: Squid, Paramétrage de l'authentification avec Active Directory

Remarque : J'ai essayé d'implémenter le portail captif avec un proxy, mais cela ne fonctionne pas, a déclaré l'un des modérateurs.

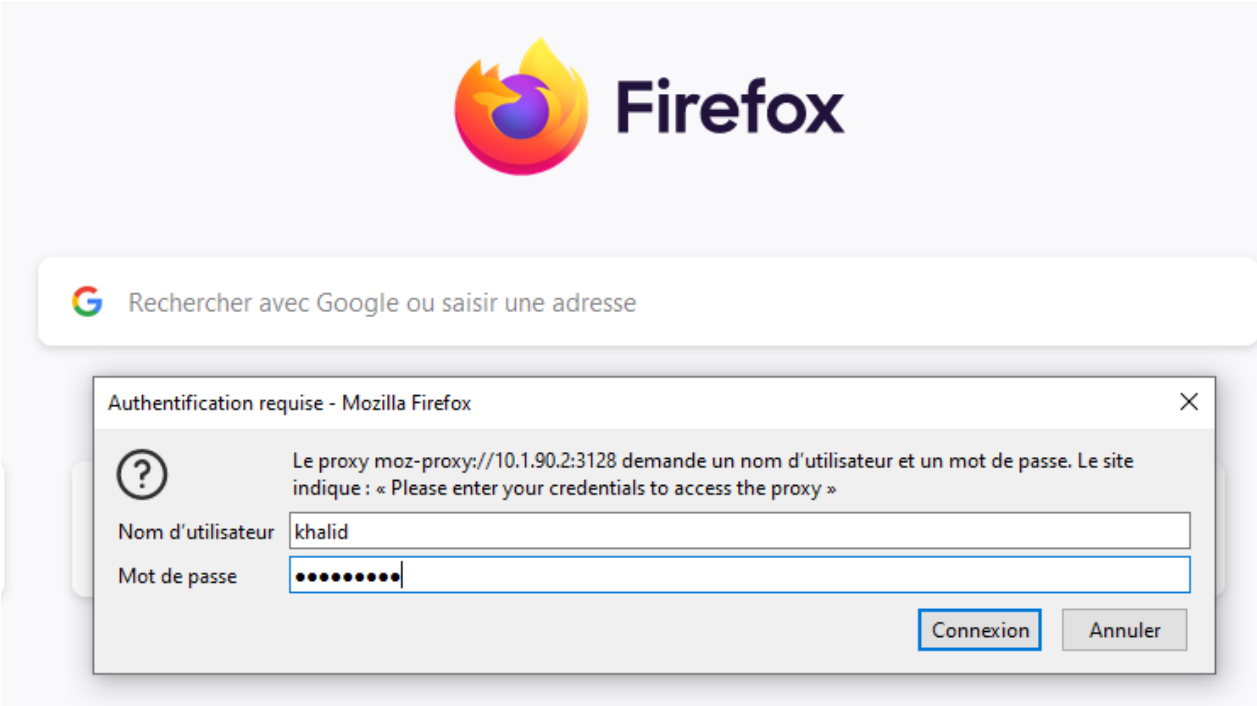

Figure 48: Fenêtre contextuelle d'authentification Squid

1.8.4.5 Intégration antivirus ClamAV

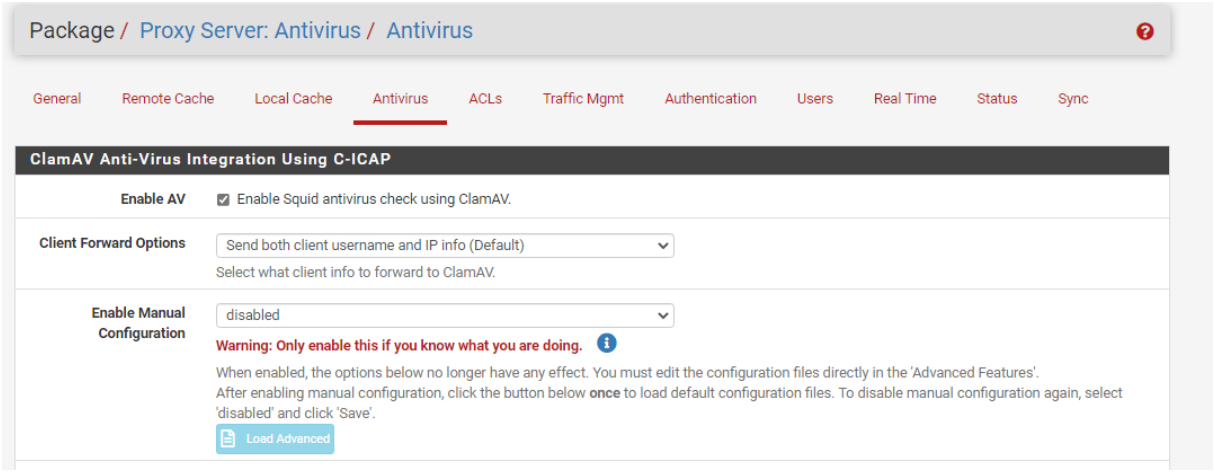

Figure 49: L'Intégration antivirus ClamAV

Nous devrions lancer le service.

Figure 50: Démarrage du service clamAV

1.8.5 Configuration de SquidGuard

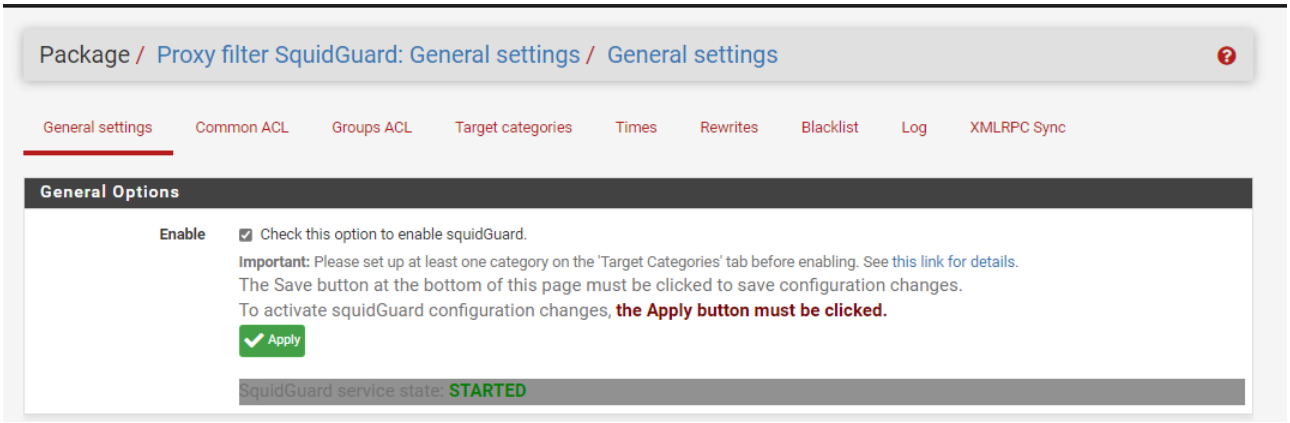

Figure 51: L'activation du service SquidGuard

SquidGuard est un logiciel de redirection d'URL, qui peut être utilisé pour contrôler le contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit comme un plug-in pour Squid et utilise des listes noires pour définir les sites pour lesquels l'accès est redirigé.

Nous pouvons télécharger des listes noires prêtes et modérées sur Internet, ce sont des listes noires prêtes à être utilisées et elles filtrent les sites Web par catégories.

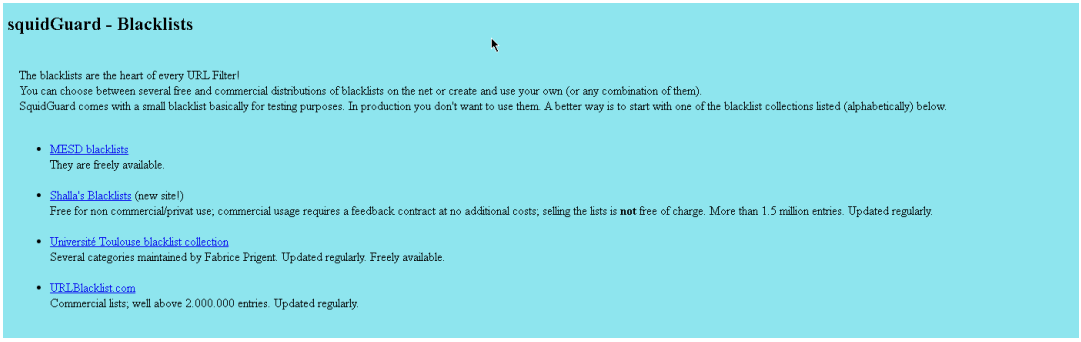

Figure 52: Listes noires recommandées par SquidGuard

Voici la liste noire recommandée recommandée par Netgate. (http://www.squidguard.org/blacklists.html)

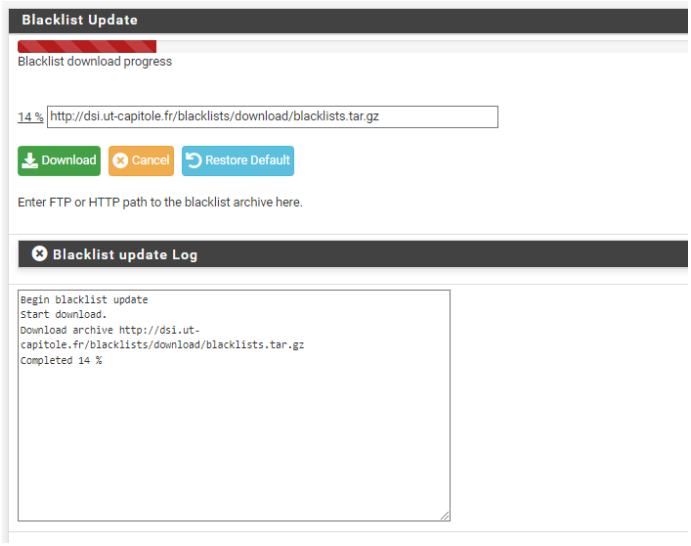

Figure 53: Téléchargement d'une liste noire

Pour mon cas j'utilise une liste noire modérée par l'université de Toulouse.

(http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz)

1.8.5.1 Mise en place d'horaire

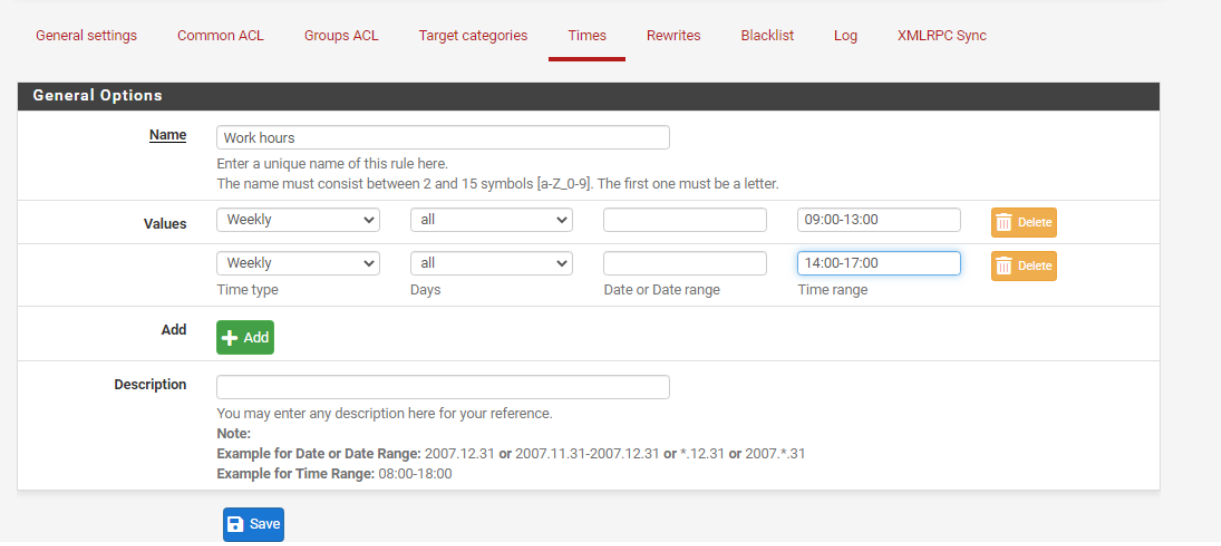

Figure 54: Mise en place d'un horaire

Les horaires aident à effectuer des tâches à des moments précis, dans mon cas, je couperai les sites Web de médias sociaux des utilisateurs aux heures de travail.

1.8.5.2 ACL

Créer une ACL, qui empêche les utilisateurs d'accéder aux médias sociaux pendant les heures de travail

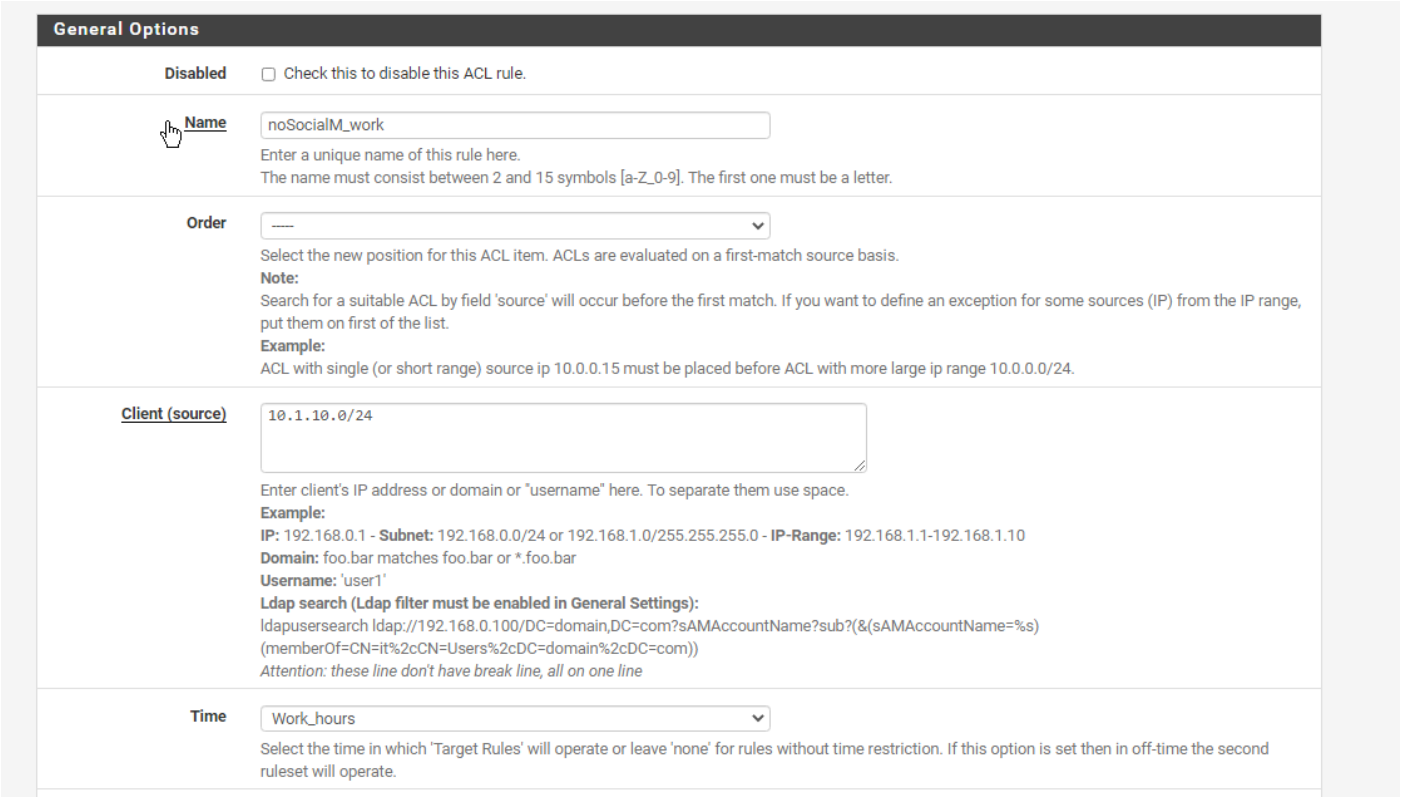

Figure 55: Création d'une nouvelle liste d'accès dans squidguard

Voici les catégories que nous avons téléchargées de la collection Toulouse

Figure 56: Blocage des réseaux sociaux

J'ai refusé l'accès aux médias sociaux.

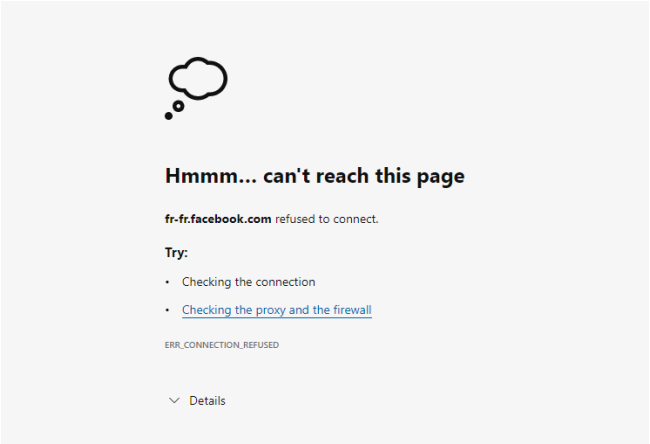

Figure 57: Test de la connectivité aux sites Web de médias sociaux

Comme vous pouvez le voir, nous ne pouvons pas accéder à Facebook.com

1.8.6 Configuration de lightSquid

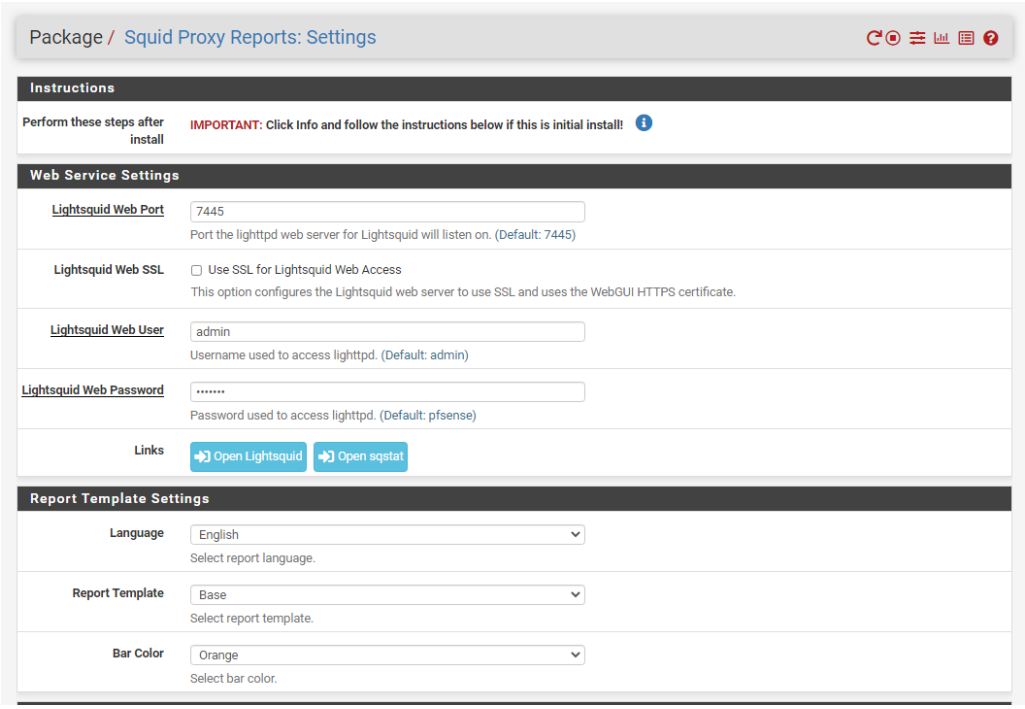

Figure 58: Configuration de lightSquid

lightSquid a un serveur Web en son sein, nous devons maintenant définir le port auquel nous voulons accéder au Web afin de voir les détails de ce service, et nous demande également si nous le voulons sécurisé (HTTPS) et nous devons fournir le nom d'utilisateur et le mot de passe, avec le type de vue (Simple pour voir les noms d'utilisateur et les adresses IP utilisées).

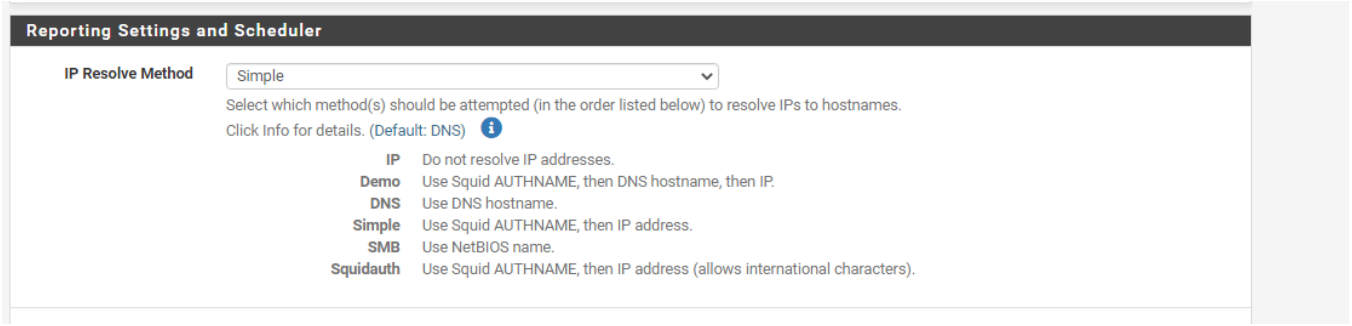

Figure 59: Format de résolution

Squid user access report

User: khalid (?)
Group: ?
Date: 02 May 2022

Total			4.0 M		
#	Accessed site	Connect	Bytes	Cumulative	%
1	tesla-cdn.thron.com:443	11	1.9 M	1.9 M	47.2%
2	www.pj.ma	52	640 059	2.5 M	15.4%
3	www.tesla.com:443	2	435 560	2.9 M	10.5%
4	www.fpl.ac.ma:443	5	221 827	3.1 M	5.3%
5	uifserver.net	7	168 633	3.3 M	4.0%
6	static.xx.fbcdn.net:443	11	140 680	3.4 M	3.3%
7	ocsp.pki.goog	101	85 805	3.5 M	2.0%
8	detectportal.firefox.com	219	80 829	3.6 M	1.9%
9	cdn-design.tesla.com:443	4	69 324	3.6 M	1.6%
10	www.columbia.edu	3	63 478	3.7 M	1.5%
11	glossaire.infowebmaster.fr	6	45 833	3.7 M	1.1%
12	pagead2.googlesyndication.com	1	40 794	3.8 M	0.9%
13	ajax.googleapis.com	1	34 499	3.8 M	0.8%
14	platform.twitter.com	3	31 724	3.8 M	0.7%
15	ocsp.digicert.com	31	27 314	3.9 M	0.6%
16	yt3.ggpht.com:443	5	21 810	3.9 M	0.5%
17	scontent.frba3-2.fna.fbcdn.net:443	3	19 458	3.9 M	0.4%
18	www.google.com	3	11 656	3.9 M	0.2%
19	ocsp.sca1b.amazontrust.com	9	9 929	3.9 M	0.2%
20	blog.infowebmaster.fr	2	6 207	3.9 M	0.1%
21	ocsp.godaddy.com	2	4 781	3.9 M	0.1%
22	pub.menara.ma	1	4 668	3.9 M	0.1%
23	www.google.com:443	18	4 286	3.9 M	0.1%
24	push.services.mozilla.com:443	6	3 976	3.9 M	0.0%
25	r3.o.lencr.org	3	2 974	3.9 M	0.0%
26	ocsp.sectigo.com	2	2 083	3.9 M	0.0%
27	ocsp.globalsign.com	1	1 993	3.9 M	0.0%
28	status.geotrust.com	2	1 852	3.9 M	0.0%
29	www.infowebmaster.fr	2	1 292	4.0 M	0.0%
30	partner.googleadservices.com	1	1 086	4.0 M	0.0%
31	info.cern.ch	1	994	4.0 M	0.0%

Figure 60: Les journaux de l'utilisateur Khalid.

1.8.6.1 Scripts WPAD

Le protocole WPAD (Web Proxy Auto-Discovery) est une méthode utilisée par les clients pour localiser l'URL d'un fichier de configuration à l'aide des méthodes de découverte DHCP et/ou DNS. Une fois la détection et le téléchargement du fichier de configuration terminés, il peut être exécuté pour déterminer le proxy pour une URL spécifiée.

dans mon cas : WPAD indique à un navigateur Web quel proxy Internet utiliser lorsqu'un utilisateur sur un réseau demande une page Web. Plus précisément, WPAD indique au navigateur où aller pour accéder à un WPAD. dat qui fournit ensuite les détails du réseau au navigateur Web. Le protocole WPAD permet à un administrateur de domaine de pointer vers un WPAD. Lorsque nous activons WPAD, le navigateur obtient automatiquement la configuration du proxy, nous n'avons pas besoin de les insérer manuellement.

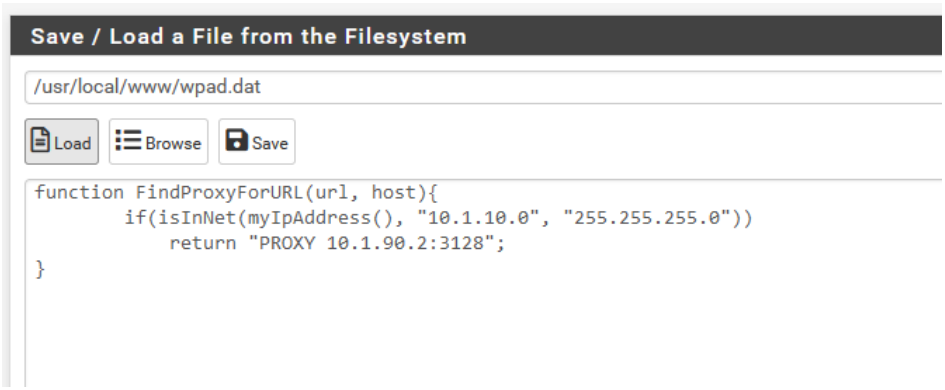

Figure 61: Script WPA]D

Si mon adresse IP dans la plage de 10.1.10.0/24 signifie utiliser un proxy.

1.9 Implémentation du serveur VPN

1.9.1 Problématique

À un moment donné, l'entreprise doit se développer et fournir plus d'assistance et de services aux clients situés dans différentes zones en dehors de la succursale (différents pays). Pour cette raison, la société a décidé qu'une autre succursale serait mieux adaptée pour répondre aux demandes du nouveau site.

Cependant, une préoccupation est de savoir comment les employés du nouveau site distant accéderont aux ressources du bâtiment principal de votre pays d'origine.

Il existe quelques solutions à ce problème. Une méthode consiste à répliquer l'infrastructure informatique de la succursale d'origine dans la nouvelle succursale distante, mais cela sera un peu coûteux car la nouvelle succursale ne nécessite que quelques employés et il n'est pas nécessaire d'avoir une équipe informatique dédiée.

Donc, Comment mettre en place une solution alternative sans avoir à payer les frais de connexion WAN et sans répliquer le site ?

1.9.2 Hypothèse

Une autre solution consiste à créer un réseau privé virtuel (VPN) entre les deux bureaux. Un VPN crée un tunnel crypté entre deux appareils ou plus sur un réseau non sécurisé tel qu'Internet. Cela signifie que tout le trafic envoyé via le tunnel VPN sera crypté et gardé confidentiel vis-à-vis des pirates sur un réseau ou sur Internet.

Voici les avantages de l'utilisation d'un VPN :

- L'utilisation d'un VPN vous fera économiser de l'argent car il est gratuit.
- Les VPN assurent la sécurité de tout votre trafic envoyé à travers le tunnel VPN.
- Un VPN prend en charge l'évolutivité, afin que davantage de sites distants et d'utilisateurs puissent se connecter au réseau d'entreprise en toute sécurité

1.9.3 Quels types de VPN existe-t-il?

Il existe de nombreux types de VPN différents, mais vous devez certainement être familiarisé avec les trois types principaux:

1.9.3.1 VPN de site à site

Un VPN de site à site est essentiellement un réseau privé conçu pour masquer les intranets privés et permettre aux utilisateurs de ces réseaux sécurisés d'accéder aux ressources des autres.

Un VPN de site à site est utile si vous avez plusieurs sites dans votre entreprise, chacun avec son propre réseau local (LAN) connecté au WAN (Wide Area Network). Les VPN de site à site sont également utiles si vous disposez de deux intranets distincts entre lesquels vous souhaitez envoyer des fichiers sans que les utilisateurs d'un intranet n'accèdent explicitement à l'autre.

Chaque emplacement nécessitera un concentrateur VPN pour établir et terminer le tunnel VPN. Un concentrateur VPN est un routeur ou un pare-feu capable d'établir une connexion VPN entre lui-même et un client VPN ou un autre concentrateur VPN.

1.9.3.2 VPN client-serveur

La connexion via un client VPN peut être imaginée comme si vous connectiez votre PC domestique à l'entreprise avec un câble d'extension. Les employés peuvent se connecter au réseau de l'entreprise depuis leur bureau à domicile via la connexion sécurisée et agir comme s'ils étaient assis au bureau. Cependant, un client VPN doit d'abord être installé et configuré sur l'ordinateur.

L'administrateur du pare-feu peut configurer le VPN d'accès à distance pour les utilisateurs dans l'un des modes suivants :

- Tunnel complet

En mode Full Tunnel, tout le trafic qui doit sortir sur Internet à partir du PC du client sera envoyé via le tunnel VPN au concentrateur VPN, où il sera envoyé sur Internet. Tout le trafic retour reprendra le même chemin vers le PC du client.

- Tunnel divisé

En mode Split-Tunnel, seul le trafic avec le réseau d'entreprise comme destination sera crypté et envoyé à travers le tunnel VPN. Le trafic qui a Internet comme destination ne sera pas envoyé via le tunnel VPN mais plutôt directement sur Internet à partir du PC de l'utilisateur. Ce mode crée moins de surcharge sur le tunnel VPN et réduit la consommation de CPU et de RAM sur le concentrateur VPN.

1.9.3.3 VPN sans client.

Avec un VPN sans client, il n'est pas nécessaire d'installer un client VPN sur la machine de l'utilisateur. Cependant, la connexion est cryptée et sécurisée entre le navigateur Web d'un client à l'aide du cryptage SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) sur HTTPS. Le trafic entre le navigateur Web et le concentrateur VPN est crypté ; tout autre trafic ne l'est pas.

1.9.4 Protocoles VPN

Tous les VPN n'ont pas été créés égaux. Selon son protocole VPN, il peut avoir des vitesses, des capacités ou même des vulnérabilités de sécurité et de confidentialité différentes. Il existe différents types de VPN.

	Avantages	Inconvénients
OpenVPN	• Open source, ce qui signifie qu'il est transparent. • Polyvalence. Il peut être utilisé avec un ensemble de protocoles de cryptage et de trafic différents. • Sécurité. Il peut exécuter presque n'importe quel protocole de cryptage.	• Configuration complexe.
IPSec/IKEv2	• Stability, IKEv2 ensures a VPN connection as you move between internet connections. • Sécurité. IKEv2 fonctionne avec l'algorithme de cryptage le plus avancé. • La vitesse. Il prend peu de bande passante lorsqu'il est actif.	• Compatibilité limitée. IKEv2 n'est pas compatible avec trop de systèmes.
Wireguard*	• Gratuit et Open Source. • Moderne et extrêmement rapide.	• Incomplet.
SSTP	• Secure. Supports the AES-256 encryption protocol. • Contourner les pare-feux.	• Propriété de Microsoft.
L2TP/IPSec	• Largement disponible.	• Potentiellement compromis par la NSA. • Lent. • A des difficultés avec les pare-feux.

PPTP	• Rapide et hautement compatible.	• Craqué par la NSA et bloqué par les pare-feux.

1.9.5 Implémentation de VPN dans notre topologie

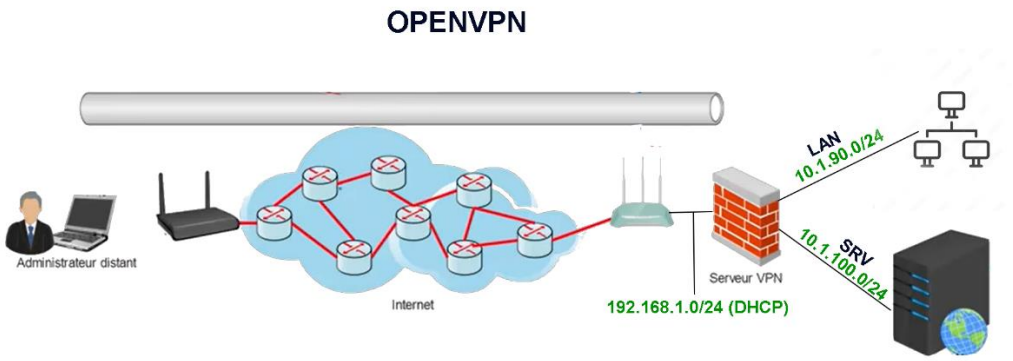

Figure 62: Implémentation de VPN

Problèmes que j'ai rencontrés lors de la mise en œuvre du VPN

L'adresse IP du routeur change, ce qui signifie que nous ne pouvons pas obtenir une adresse IP statique que nous pouvons connecter depuis l'extérieur du site, afin de résoudre ce problème, nous devons acheter une adresse IP statique auprès du FAI, ce qui est si cher , comme alternative, j'ai utilisé une technologie DynDNS, qui consiste à mettre à jour les enregistrements DNS traditionnels sans modification manuelle et à permettre des mises à jour légères et immédiates souvent à l'aide d'un client mis à jour.

Avec l'aide du mécanisme de transfert de port (mappage de port), j'ai pu rediriger une demande de communication de l'adresse WAN pfSense et du numéro de port de la combinaison VPN vers le routeur pendant que les paquets traversent la passerelle.

No-Ip est un service DDNS gratuit, qui permet d'accéder aux appareils à distance sans avoir besoin d'une adresse IP statique. et est implémenté dans pfSense.

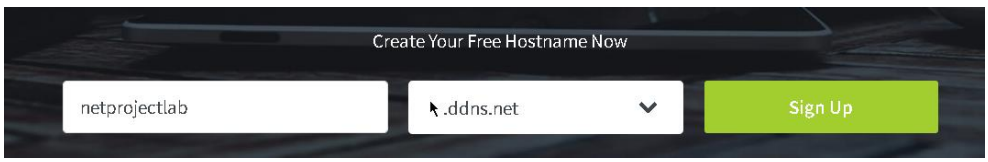

Figure 63: Enregistrement du domaine dans No-Ip

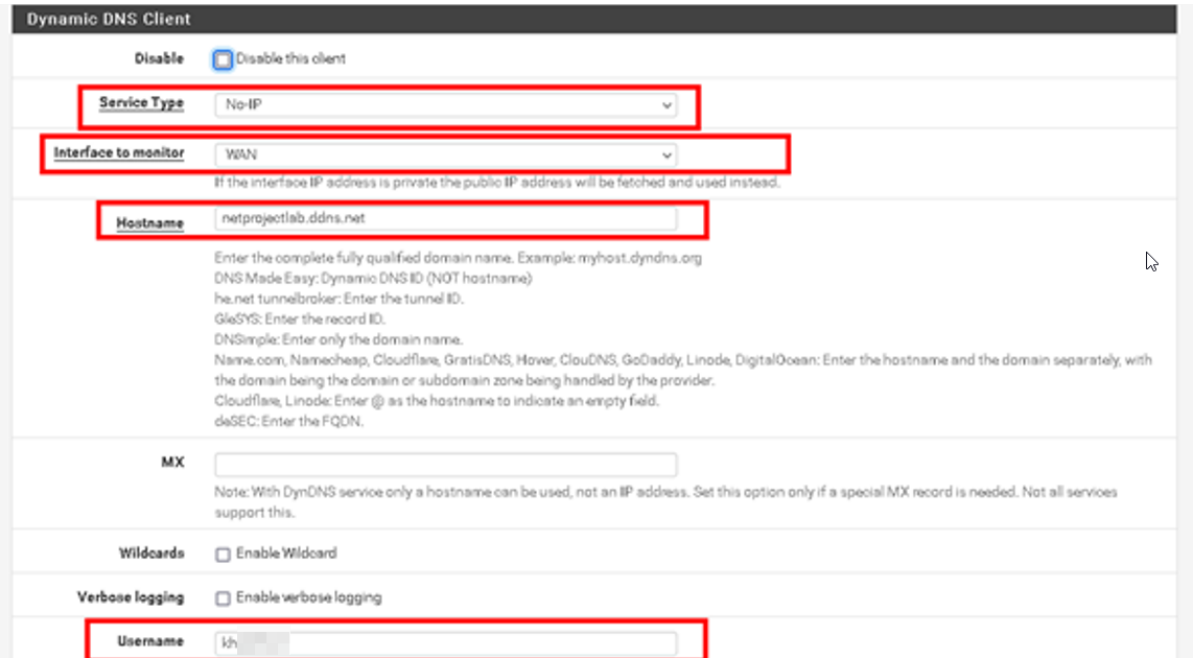

Figure 64: Configuration de DynDNS sur pfSense

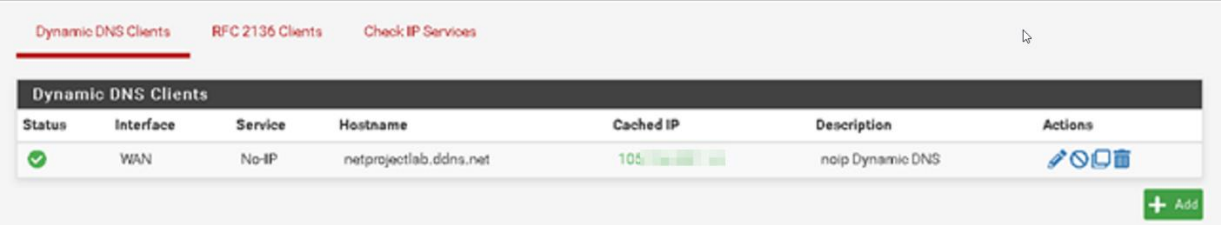

Figure 65: Vérification du dynDNS

Après avoir configuré le dynDNS sur notre pare-feu, nous pouvons vérifier avec succès sur le site Web no-IP les changements d'adresse IP.

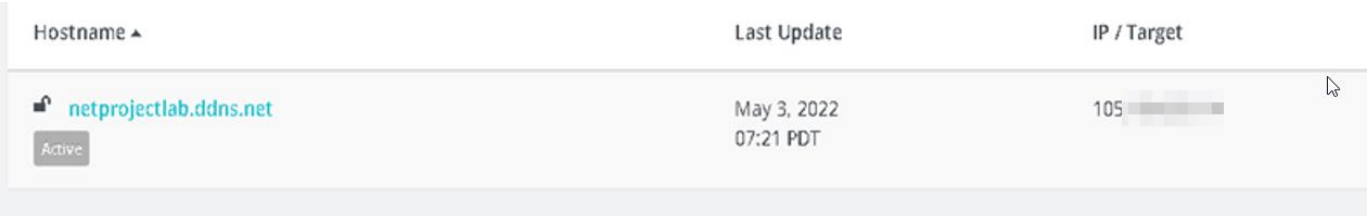

Figure 66: Vérification sur NoIP

1.9.5.1 Configuration de openVPN sur pFsense

OpenVPN prend en charge l'authentification bidirectionnelle basée sur des certificats, ce qui signifie que le client doit authentifier le certificat du serveur et le serveur doit authentifier le certificat client avant que la confiance mutuelle ne soit établie.

pour cela, nous devons créer 3 certifications :

- **L'autorité de certification** : l'entité émet des certificats numériques.

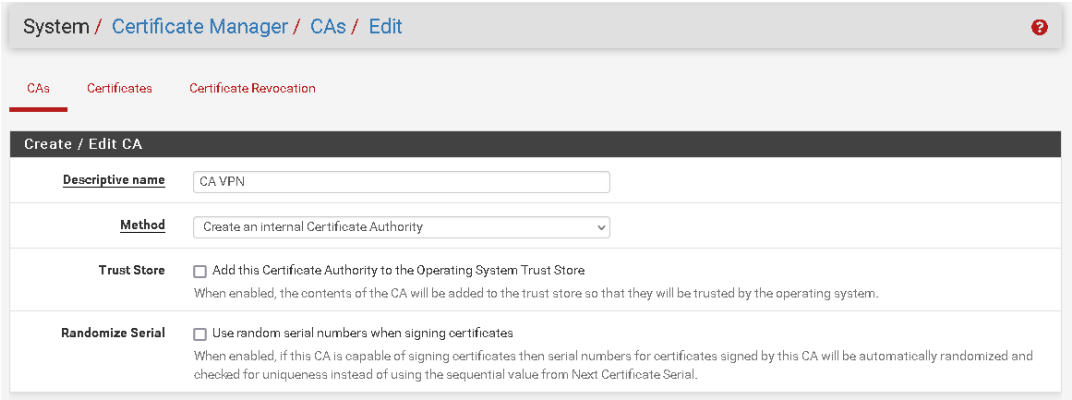

Figure 67: Création d'une autorité de certification pour VPN

- **Certificat de serveur :** utilisé pour authentifier l'identité d'un serveur.

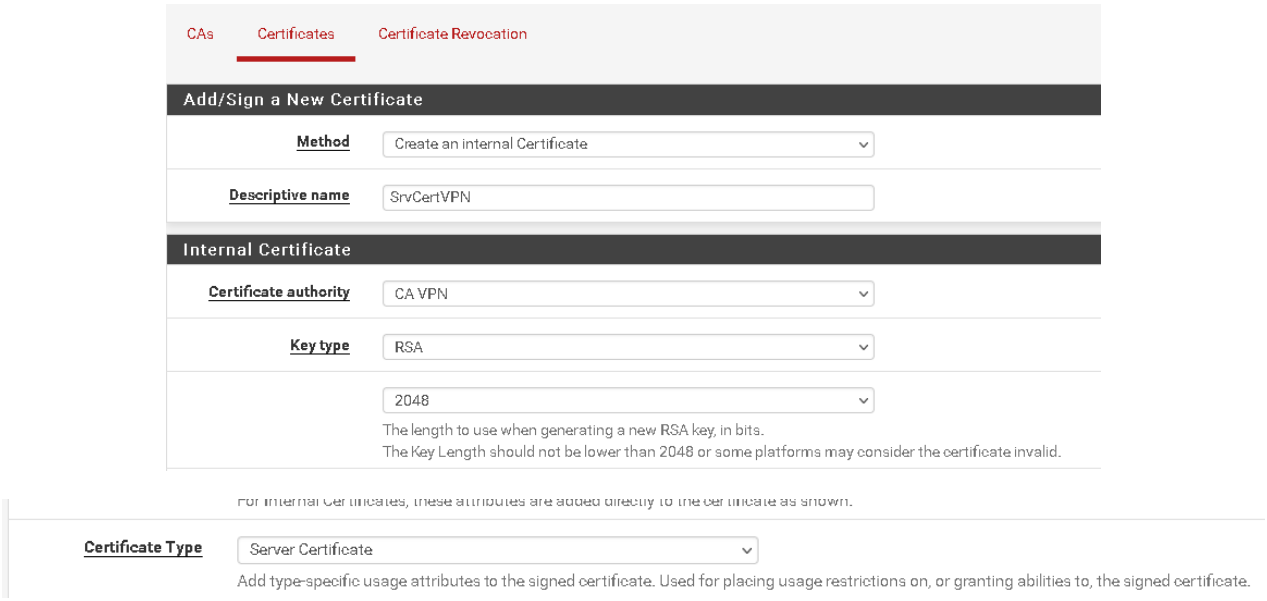

Figure 68: Création de certification de serveur pour VPN

- **Certificat client :** pour garantir au serveur qu'il communique avec un utilisateur légitime. (Validation de l'identité d'un client)

1.9.5.2 Création d'un client et l'attribuer d'un certificate

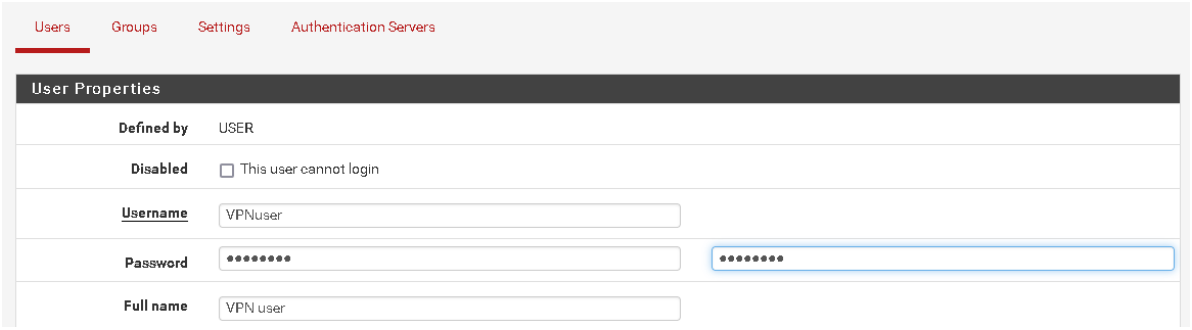

Figure 69: Création d'un nouvel utilisateur pour le service VPN

Création d'un utilisateur local autorisé à accéder au VPN via Internet.

1.9.5.2.1 Certificate:

Il est temps de créer un certificat utilisateur pour l'utilisateur que nous avons créé ci-dessus et d'affecter le certificat à cet utilisateur.

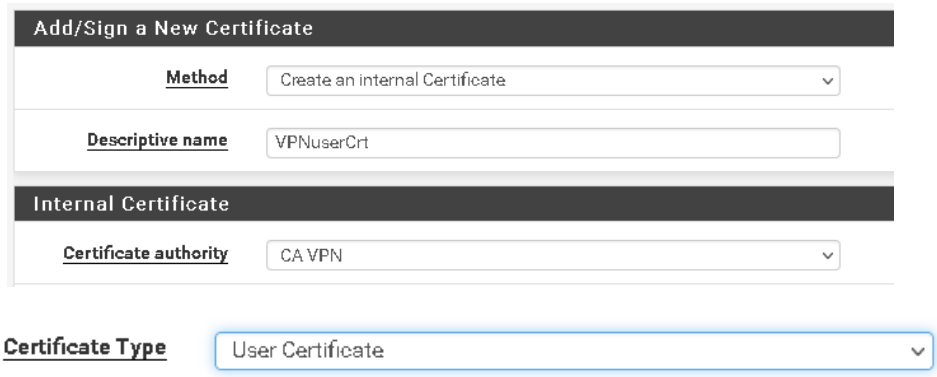

Figure 70: Création de la certification des utilisateurs

1.9.5.2.2 Affectation:

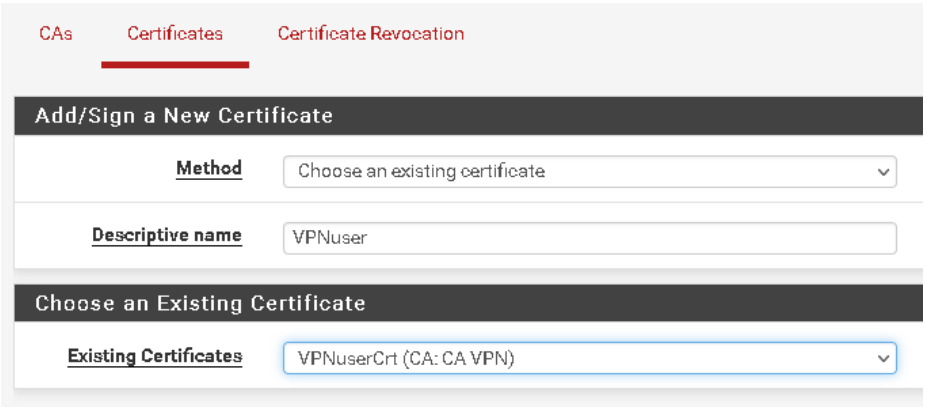

Figure 71: Affectation de la certification de l'utilisateur à l'utilisateur nouvellement créé

Pour l'exportation automatique de la configuration openVPN, nous utilisons un package nommé openVPN-client-export

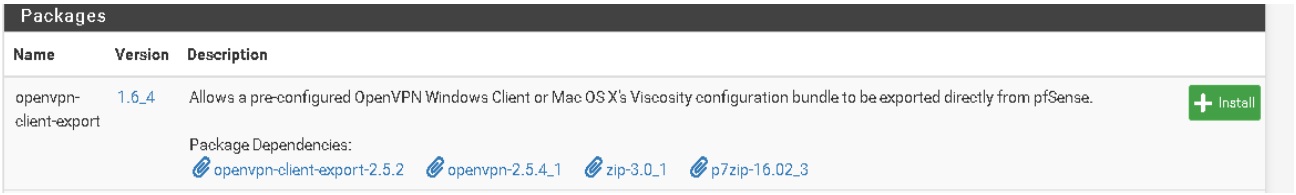

Figure 72 :openVPN-client-export package

1.9.5.3 Configuration d'openVPN

Pour cette configuration, j'utiliserai l'assistant pour m'aider.

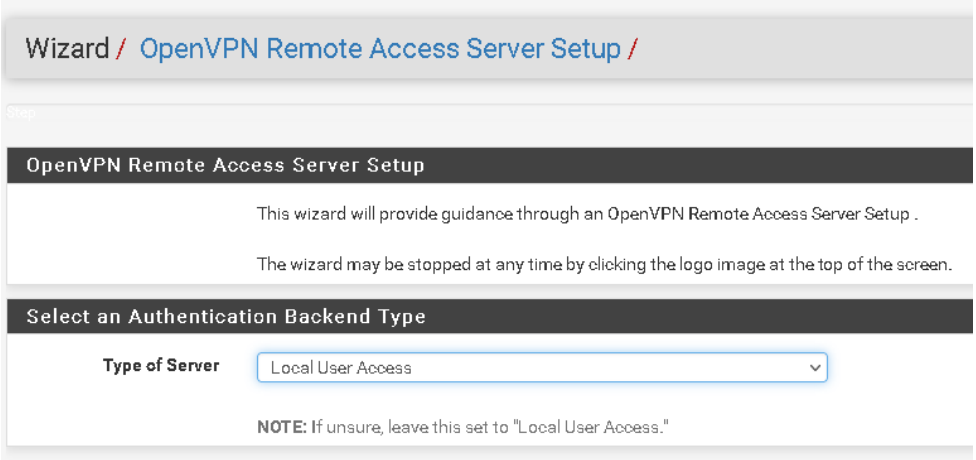

Figure 73: Assistant de configuration OpenVPN

Il a demandé comme pour le type de backend d'authentification, nous avons déjà configuré un utilisateur, donc je choisirai l'accès utilisateur local.

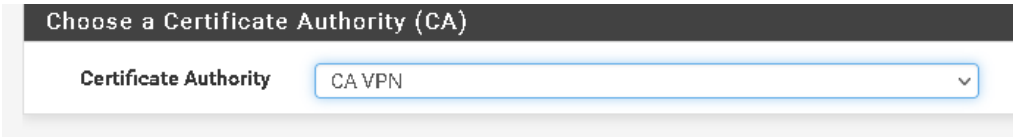

Figure 74: Sélection de l'autorité de certification

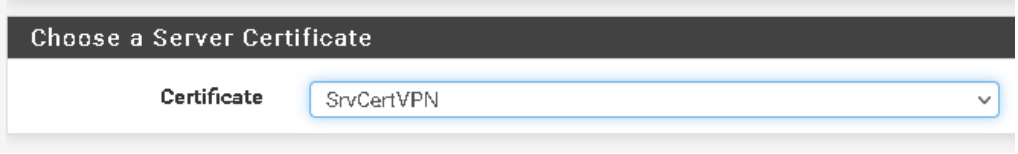

Figure 75: Sélection du certificat du serveur

Il nous demande la certification du CA et du serveur que nous avons créée auparavant.

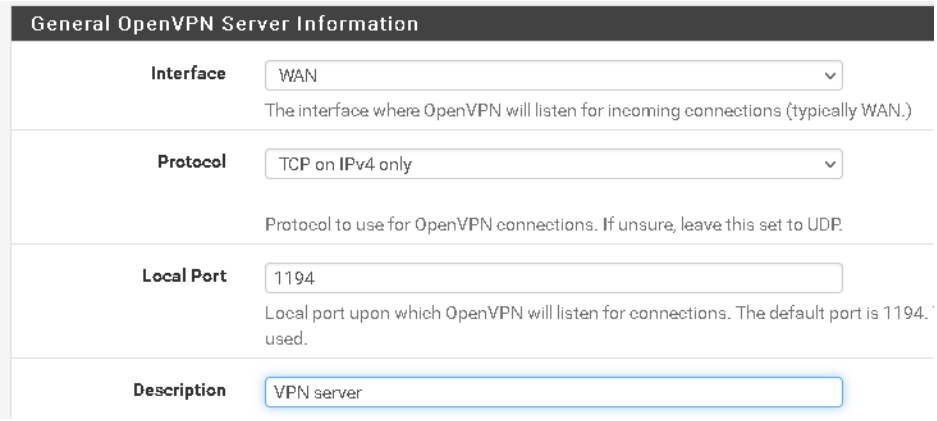

Figure 76: L'interface qui écoutera sur le service VPN

Maintenant, il nous demande sur quel port et quel protocole le serveur utilisera pour écouter.

Cela nous donne également des options d'algorithmes de cryptage parmi lesquelles choisir (j'ai choisi 128 bits pour ne pas épuiser les ressources de mon hôte)

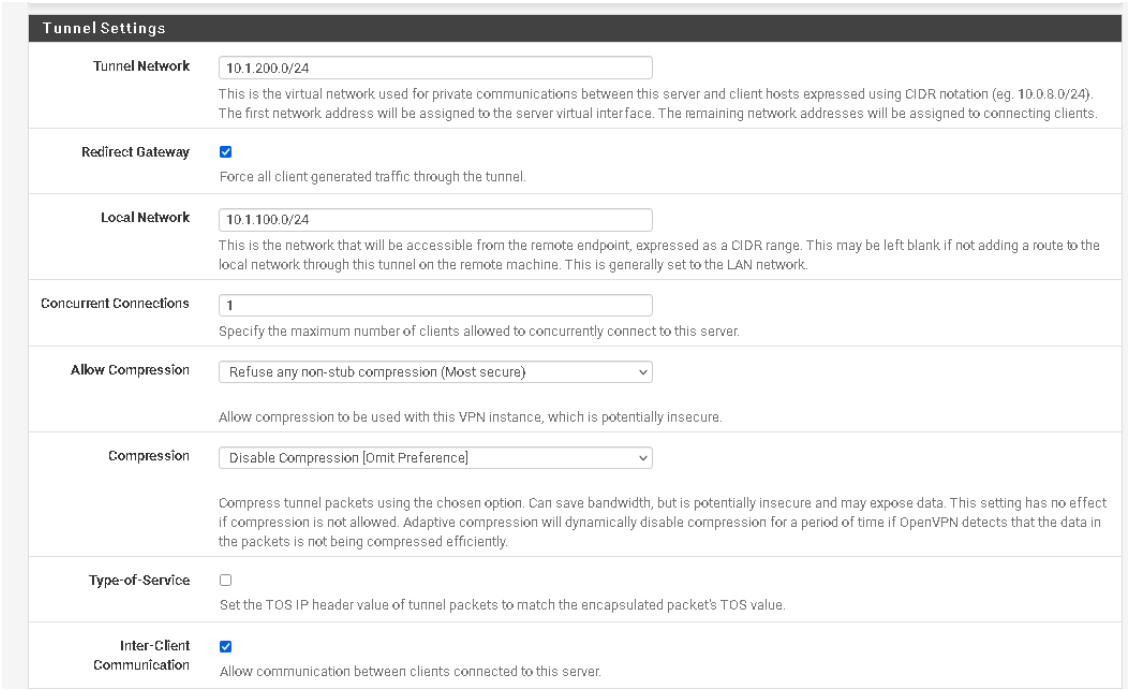

Figure 77: Paramètres du tunnel OpenVPN

Nous devons affecter un réseau au tunnel, afin que le serveur et le client puissent communiquer entre eux, et j'ai vérifié le canapé de la passerelle, automatiquement pfsense créera une carte réseau virtuelle qui pourra acheminer le trafic depuis le réseau du tunnel à notre LAN et au-delà.

Local Network: est le réseau qui sera accessible à partir du point de terminaison distant.

Concurrent Connections: spécifiez le nombre maximal de clients autorisés à se connecter simultanément à ce serveur.

Nous pouvons également définir si nous voulons compresser notre paquet pour la conservation de la bande passante et également définir si nous voulons autoriser la communication entre les clients.

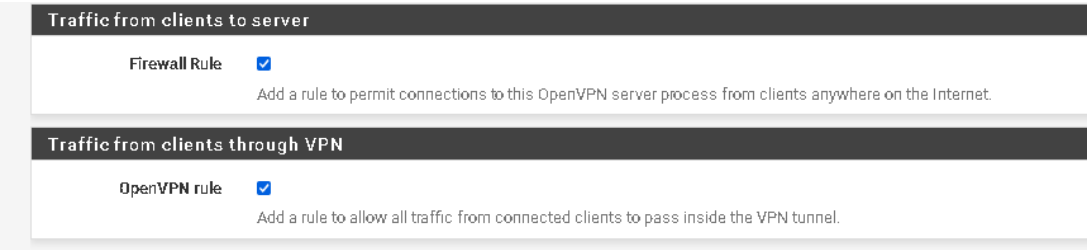

Figure 78: Création de règles OpenVPN

Nous créons une règle qui ouvre openVPN et le rend accessible depuis Internet. Et les utilisateurs autorisés à passer par le canal.

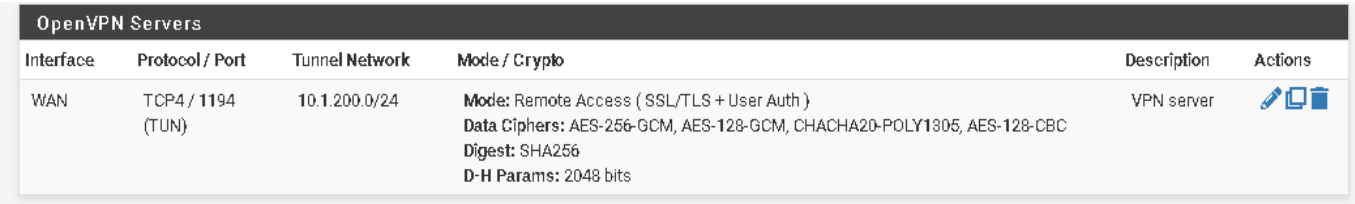

Figure 79: Vérification du service OpenVPN

1.9.6 Port-Forwarding sur TD5130 v3

Nous effectuons une redirection de port, nous pouvons donc accéder au service depuis Internet.

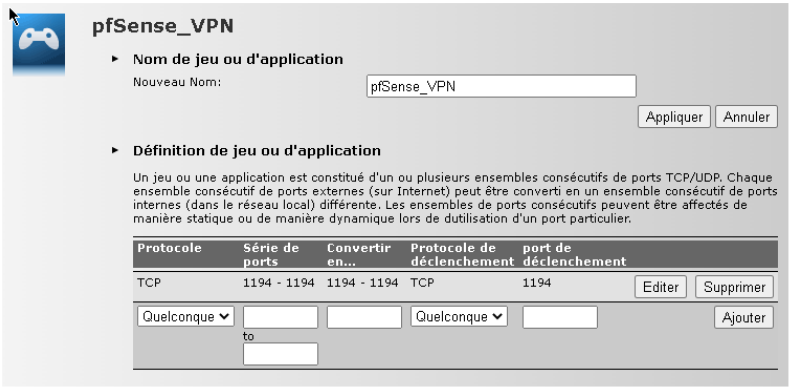

Figure 80: I.37.6 Port-Forwarding sur TD5130 v3

Nous affectons l'hôte à l'application que nous avons créée pour qu'elle soit transmise.

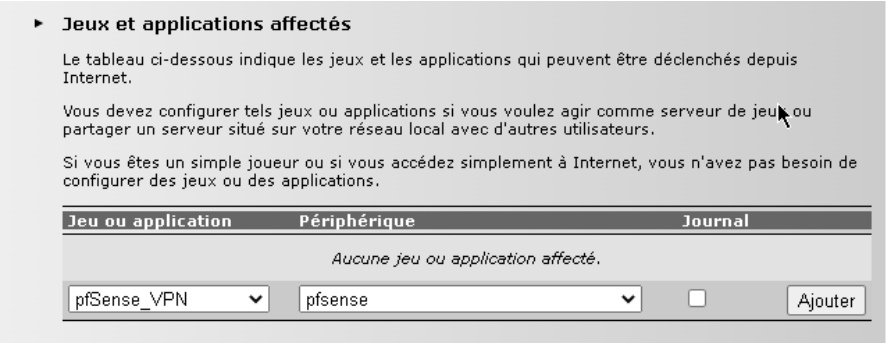

Figure 81: Affectation du port à pfSense

1.9.6.1 Verification:

J'ai utilisé le site Web (canyouseeme.org) pour vérifier si le port est ouvert.

Figure 82: Vérification du port accessible depuis Internet

1.9.7 OpenVPN client installation

Maintenant, nous devons installer le client OpenVPN sur notre hôte que nous voulons connecter à notre serveur VPN.

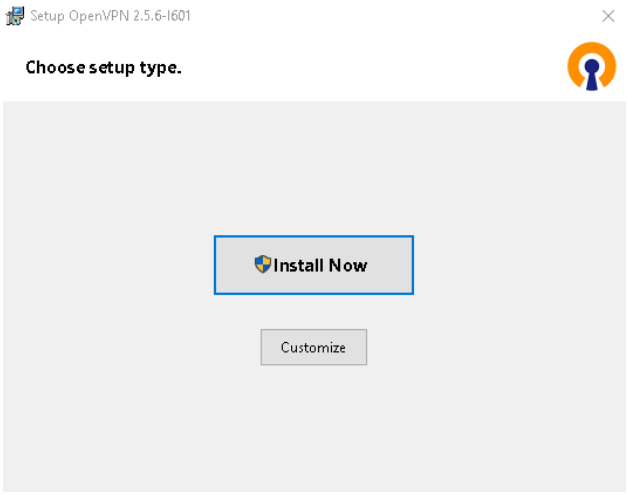

Figure 83: Installation du client OpenVPN

1.9.7.1 Exportation de la configuration depuis pfSense

Si toute la configuration est correctement configurée, nous devrions maintenant pouvoir télécharger différentes versions du client pour connecter le serveur OpenVPN.

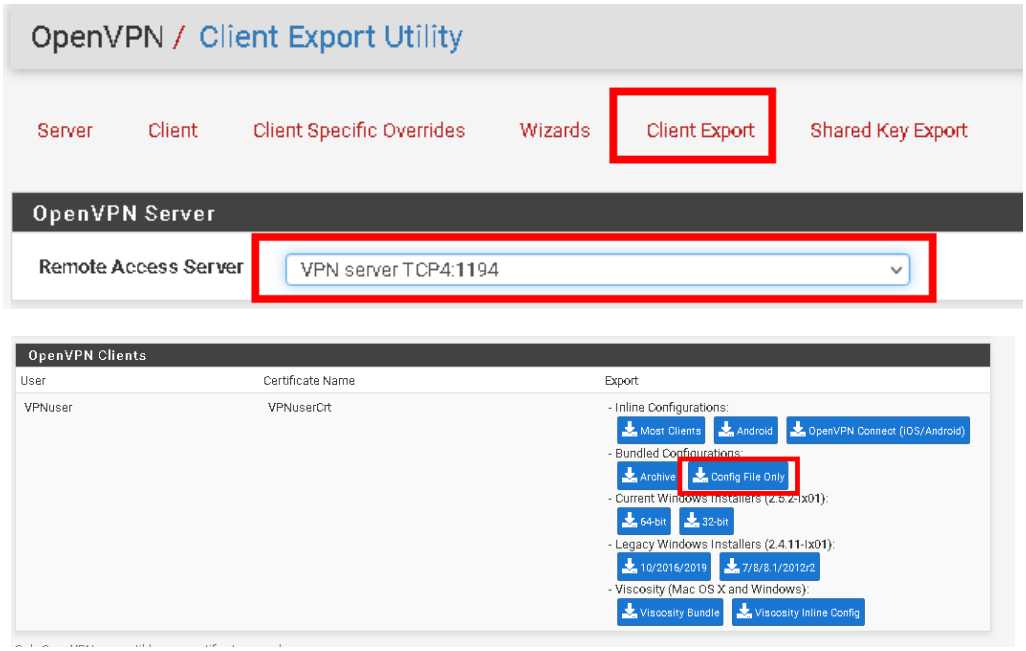

Figure 84: Exportation de la configuration client

Nous devons maintenant déplacer le fichier de configuration vers le Client (*C:\Program Files\OpenVPN\config).*

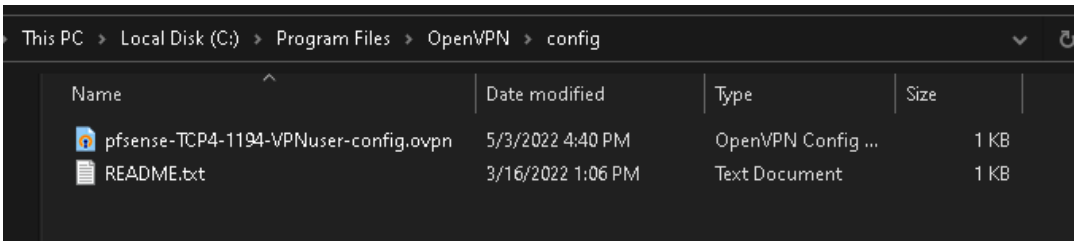

Figure 85: Déplacement de la configuration dans le dossier OpenVPN du client

Nous lançons l'interface graphique openVPN.

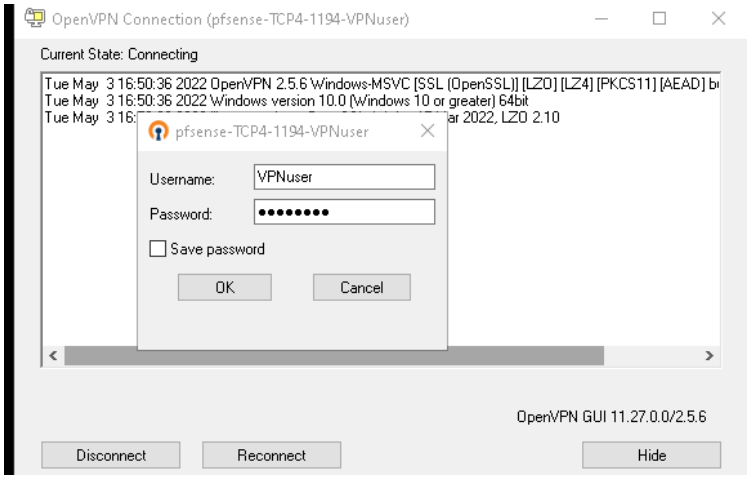

Figure 86: Lancement du client OpenVPN

Nous nous sommes connectés au VPN avec succès.

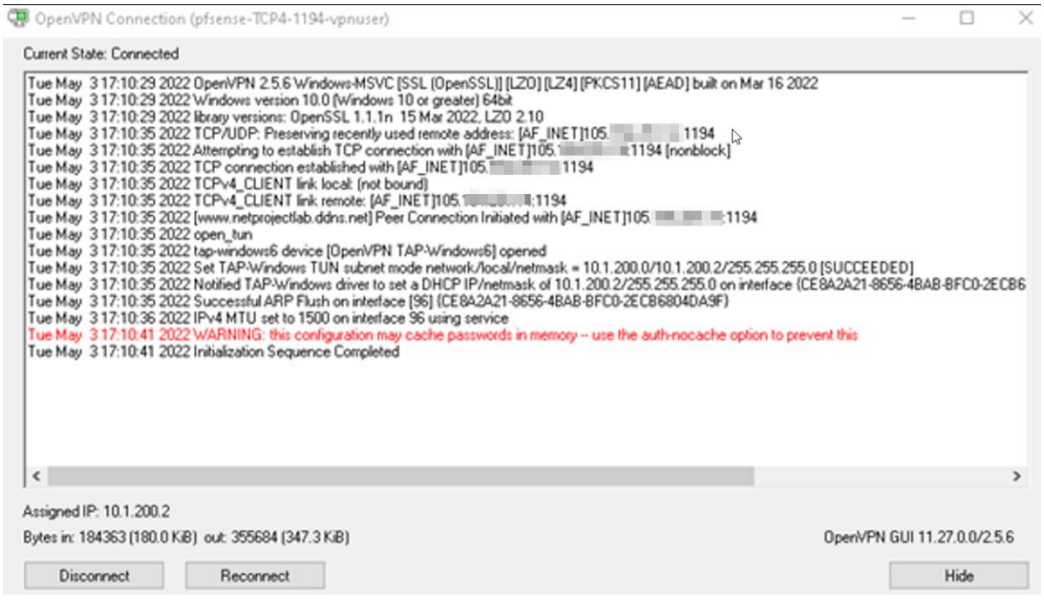

Figure 87: Connexion à votre serveur VPN

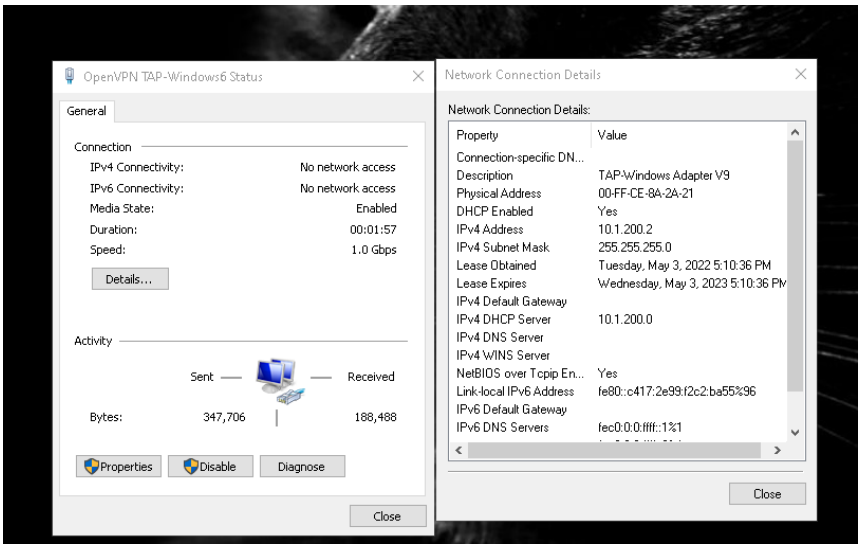

Figure 88: Résumé de l'adaptateur réseau OpenVPN

Nous avons accédé au réseau en utilisant le VPN avec succès.

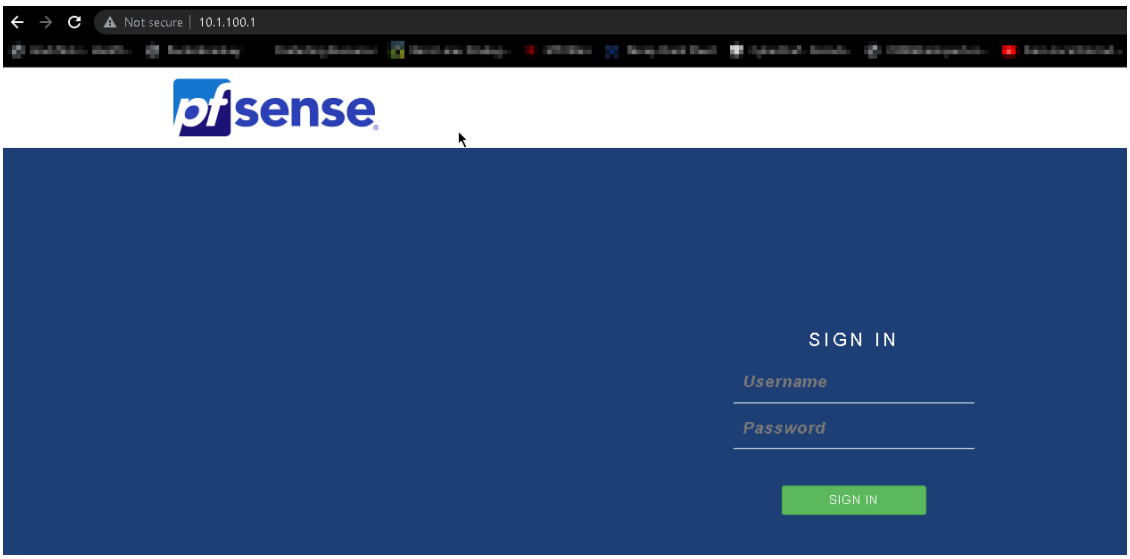

Figure 89: Vérification de la connectivité à la configuration Web pfSense

1.10 Conclusion

Dans ce chapitre, nous avons expliqué comment nous pouvons implémenter pfSense dans une topologie de réseau simple. Nous avons parlé du pfSense et de ses fonctionnalités, avec les différents services que nous pouvons obtenir de cette solution open-source. Nous avons également implémenté le portail captif, le proxy et le VPN pour la communication à partir de différentes parties.