

# **Travail Pratique Sur La Sécurité Des Infrastructures Réseaux : Cas De Pfsense**



**Sommaire:**

Listes des figures.....	2
1. Prise en charge pfsense .....	3
1.1. Présentation de pfSense .....	3
1.2. Fonctionnalités Clés de pfSense .....	3
1.3. Structure de PfSense .....	4
1.4. Avantages d'utiliser PfSense.....	4
1.5. Configuration matérielle minimale .....	5
1.6. Installation de pfsense.....	5
1.7. Architecture réseau de simulation.....	9
2. Configuration de Pfsense .....	11
2.1. Configuration du portail captif.....	11
2.2. Configuration des règles du pare-feu.....	12
2.3. Suppression des publicité, annonces, pop-up avec pfblockerNG .....	13
2.4. Filtrage des sites web avec proxy Squid et Squid Guard.....	17
2.5. Configuration d'un système de prévention des intrusions avec Snort.....	22
2.6. Configuration d'un VPN site-to-site .....	27

## Listes des figures

Figure 1 : Marketplace de GNS3.....	6
Figure 2: téléchargement de l'appliance de pfsense .....	6
Figure 3: téléchargement de l'image de pfsense .....	7
Figure 4 : Importation de pfsense dans GNS3 .....	7
Figure 5 : Importation de pfsense dans GNS3 .....	8
Figure 6: Importation réussi de pfsense dans GNS3 .....	8
Figure 7 : Architecture du réseau .....	9
Figure 8 : Interface de de connexion Web de pfsense.....	10
Figure 9: Tableau de bord de pfsense .....	10
Figure 10:Résultat final : portail captif.....	12
Figure 11 : Ensemble des règles configurées sur notre pare-feu.....	13
Figure 12 : Configuration du DNS Resolver .....	14
Figure 13 : Installation du package .....	15
Figure 14 : Listes de Blocage personnalisées .....	16
Figure 15 : Test du fonctionnement de pfblockerNG.....	17
Figure 16 : configuration générale du proxy .....	18
Figure 17 : Configuration du proxy transparent HTTP.....	18
Figure 18 : Création du certificat de d'autorité .....	19
Figure 19 : Configuration du proxy transparent HTTPS .....	20
Figure 20 : Configuration de la liste noire.....	20
Figure 21: Choix des listes à bloquer .....	21
Figure 22: Activation de SquidGuard.....	21
Figure 23 : Résultat du test : blocage du site web de Facebook.....	22
Figure 24 : credential pour activer snort .....	23
Figure 25: récupération des règles snort.....	24
Figure 26: Choix de la frequence des mises a jour .....	24
Figure 27: Mise à jour des règles .....	25
Figure 28 ; Configuration de l'interface .....	26
Figure 29: Choix de la politique IPS .....	26
Figure 30 : Test de fonctionnement de Snort .....	27
Figure 31: Phase 1 du VPN IPsec.....	29
Figure 32: Ajout de la phase 2.....	30
Figure 33: Phase 2 du VPN IPsec.....	30
Figure 34: Configuration des règles firewall pour IPsec .....	31
Figure 35: Connexion VPN site-to-site établie.....	32

## 1. Prise en charge pfsense

### 1.1. Présentation de pfSense

PfSense est un système d'exploitation open source basé sur FreeBSD, conçu pour être utilisé comme pare-feu, routeur et passerelle de sécurité pour les réseaux informatiques. À l'origine un fork de m0n0wall, il utilise le pare-feu à états **Packet Filter** ainsi que les fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Que ce soit pour protéger un petit réseau domestique ou pour mettre en place une solution de sécurité avancée pour une grande entreprise, pfSense offre une solution complète et évolutive pour répondre aux besoins en matière de sécurité réseau.

### 1.2. Fonctionnalités Clés de pfSense

En tant que pare-feu, pfSense offre ainsi un ensemble de fonctionnalités essentielles :

- ❖ **Firewall** : pfSense agit comme un pare-feu en inspectant et en filtrant le trafic réseau en fonction de règles définies par l'administrateur. Cela permet de bloquer les accès non autorisés et de protéger le réseau contre les attaques.
- ❖ **NAT (Network Address Translation)** : pfSense utilise NAT pour traduire les adresses IP internes en adresses publiques lors de la communication avec des réseaux externes. Cela offre ainsi une couche de sécurité supplémentaire en masquant les adresses IP internes.
- ❖ **VPN (Virtual Private Network)** : pfSense prend en charge les VPN. Ce qui permet aux utilisateurs de créer des connexions sécurisées et cryptées entre différents réseaux ou appareils distants. Cela pour garantir ainsi la confidentialité et la sécurité des données lors de leur transfert sur Internet.
- ❖ **Gestion de la Bande Passante** : pfSense permet de contrôler et de limiter la bande passante disponible pour certaines applications ou utilisateurs. Ce qui permet ainsi d'optimiser les performances du réseau et d'éviter la congestion.
- ❖ **Surveillance du Trafic** : pfSense offre des outils de surveillance du trafic réseau qui permettent aux administrateurs de surveiller l'utilisation de la bande passante, d'identifier les goulots d'étranglement et de détecter les activités suspectes sur le réseau.

### 1.3. Structure de PfSense

PfSense est basé sur le système d'exploitation FreeBSD et est conçu pour fonctionner comme un pare-feu et un routeur de sécurité réseau. Voici une vue d'ensemble de la structure de pfSense :

- ❖ **Noyau FreeBSD** : pfSense repose sur le noyau FreeBSD, un système d'exploitation open source connu pour sa stabilité, sa sécurité et ses performances élevées. FreeBSD fournit la base sur laquelle pfSense est construit.
- ❖ **Interface Web** : pfSense dispose d'une interface web conviviale qui permet aux utilisateurs de configurer et gérer le pare-feu et le routeur réseau à l'aide d'un navigateur web. L'interface web offre une gamme complète de fonctionnalités pour personnaliser les paramètres de sécurité et de réseau.
- ❖ **Modules de sécurité** : pfSense intègre une variété de modules de sécurité avancés, tels que le filtrage des paquets, la détection d'intrusion, la protection contre les attaques par déni de service, les VPN, les règles de pare-feu personnalisées, etc. Ces modules permettent de renforcer la sécurité du réseau et de protéger les données contre les menaces en ligne.
- ❖ **Extensions** : pfSense prend en charge les extensions tierces qui peuvent être installées pour étendre les fonctionnalités du système. Ces extensions peuvent inclure des plugins pour la surveillance du trafic, la gestion des VPN, la journalisation avancée, etc.

### 1.4. Avantages d'utiliser PfSense

Il existe de nombreux avantages à utiliser pfSense comme solution de pare-feu et de routeur de sécurité réseau. Voici quelques-uns des principaux avantages de pfSense :

- ❖ **Sécurité avancée** : pfSense offre une large gamme de fonctionnalités de sécurité avancées, telles que le filtrage des paquets, la détection d'intrusion, la protection contre les attaques par déni de service, la création de réseaux privés virtuels (VPN) et bien plus encore. Cela permet de protéger efficacement les réseaux contre les menaces en ligne.
- ❖ **Interface conviviale** : pfSense dispose d'une interface web conviviale qui rend la configuration et la gestion du pare-feu et du routeur réseau très simples et intuitives. Cela permet aux utilisateurs de gérer leur réseau sans avoir besoin de compétences techniques avancées.

- ❖ **Communauté active** : pfSense bénéficie d'une communauté active qui propose un support technique, des mises à jour régulières et des extensions pour étendre les fonctionnalités du système. Cela garantit que pfSense reste à jour et offre un support fiable aux utilisateurs.
- ❖ **Stabilité et fiabilité** : pfSense est connu pour sa stabilité et sa fiabilité, ce qui en fait une solution sûre pour sécuriser les réseaux informatiques. Il peut fonctionner de manière fiable pendant de longues périodes sans nécessiter de redémarrage fréquent.

## 1.5. Configuration matérielle minimale

La configuration matérielle minimale pour installer le logiciel pfsense est la suite :

- ✓ Un CPU 64-bit amd64 (x86-64) ;
- ✓ 1GB RAM ;
- ✓ 8GB disque dur (SSD ou HDD) ;
- ✓ 02 ou plusieurs carte réseau.

## 1.6. Installation de pfsense

### ➤ Option de téléchargement 1

Pour l'installation de pfsense, nous devons nous rendre sur le site officiel du constructeur avec le lien suivant : [Download pfSense Community Edition](#), sélectionner le produit qui correspond à notre architecture matérielle et suivre la procédure d'installation. Dans notre cas, cela pourrait être :

- ✓ **Installation** : AMD ISO64 /Virtual machine
- ✓ **Quantité** : 1

Après avoir télécharger Pfsense, nous pouvons le virtualiser sur l'hyperviseur de notre choix : **VMware Workstation**, **VirtualBox** ...

### ➤ Option de téléchargement 2

Cette option de téléchargement est familière pour les utilisateurs de GNS3 pour simuler leur architecture réseau. L'idée principale étant de d'installer pfsense dans la GNS3 VM, mais nous pouvons aussi utiliser la même image dans les plateformes de virtualisation. La procédure de téléchargement et d'installation est la suivante, il important de noter que ce n'est pas la seule méthode d'installation mais la plus simple pour les débutants :

- ✓ Nous devons nous rendre sur la marketplace de GNS3 et télécharger l'appliance de pfsense. Le lien vers la marketplace de GNS3 est [Appliances | Marketplace | GNS3](#), une fois sur le site, nous devons effectuer une recherche avec le mot clé *pfsense*. La figure suivante illustre cela :

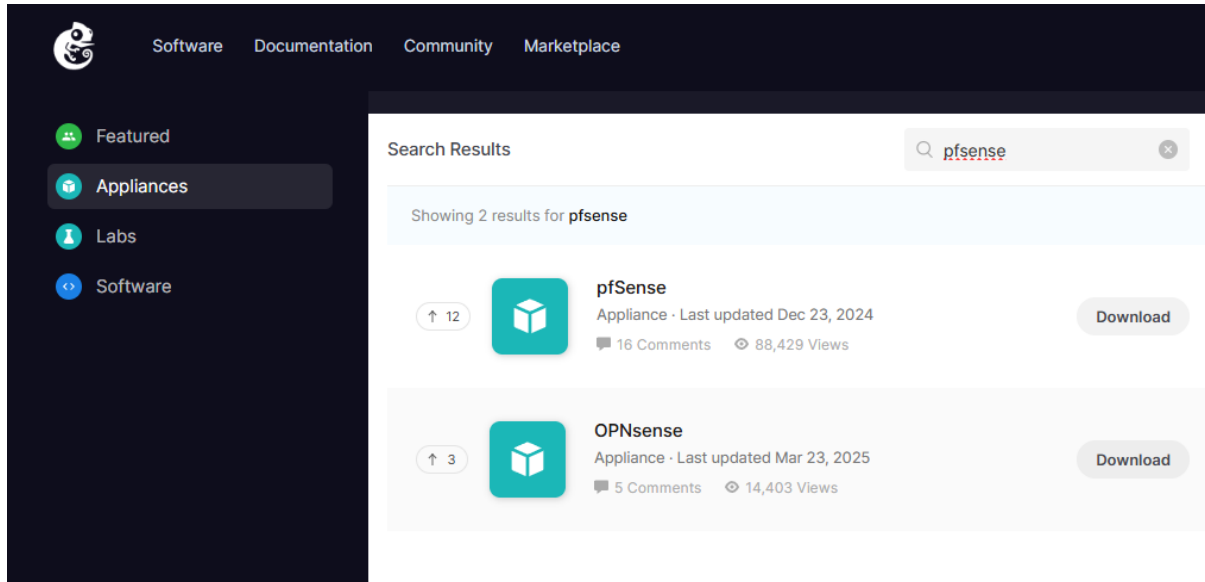


Figure 1 : Marketplace de GNS3

- ✓ Nous pouvons cliquer sur **download** pour télécharger *l'appliance de pfsense*, pour télécharger l'image de pfsense, il faut aller au fond de la page pour télécharger la version de pfsense qui nous convient.

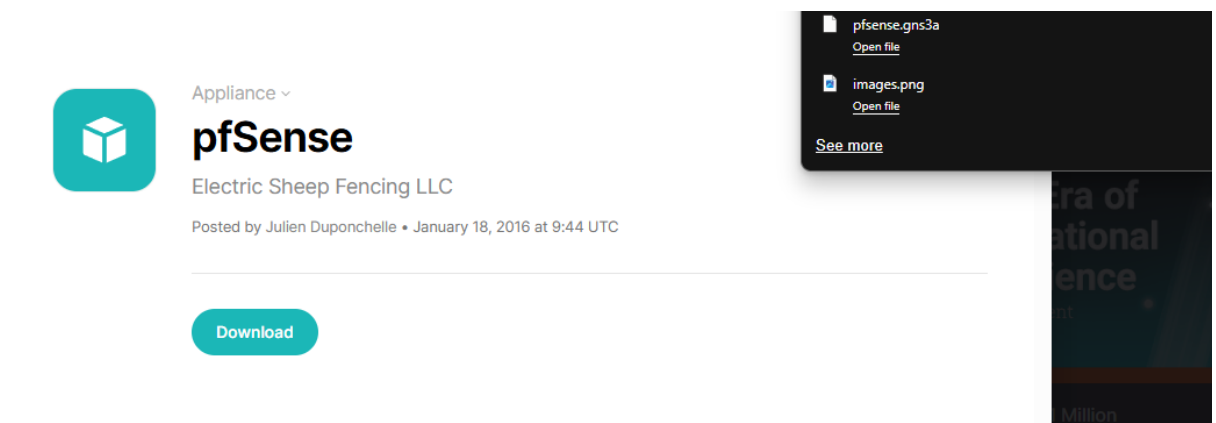


Figure 2: téléchargement de l'appliance de pfsense

### Versions Supported

pfSense 2.7.2			
File	MD5	Size	
empty100G.qcow2	1e6409a4523ada212dea2ebc50e50a65	0 MB	<a href="#">Download</a>
pfSense-CE-2.7.2-RELEASE-amd64.iso	50c3e723d68ec74d038041a34fa846f8	875 MB	<a href="#">Download</a>

pfSense 2.7.0			
File	MD5	Size	
empty100G.qcow2	1e6409a4523ada212dea2ebc50e50a65	0 MB	<a href="#">Download</a>
pfSense-CE-2.7.0-RELEASE-amd64.iso	cb0b72ca864d06682265de5e5a72a1fb	765 MB	<a href="#">Download</a>

pfSense 2.6.0			
File	MD5	Size	
empty100G.qcow2	1e6409a4523ada212dea2ebc50e50a65	0 MB	<a href="#">Download</a>
pfSense-CE-2.6.0-RELEASE-amd64.iso	5ca6d4cb89977022d2e76c9158eeeb67	767 MB	<a href="#">Download</a>

Figure 3: téléchargement de l'image de pfsense

- ✓ Lorsque cela est fait, nous allons dans GNS3 pour import notre pare-feu pfsense. L'appliance que nous venons de télécharger est un modèle (guide) pour faciliter l'installation de pfsense. Pour cela, nous devons nous rendre dans l'onglet **Fichier** puis cliquer sur **import appliance** :

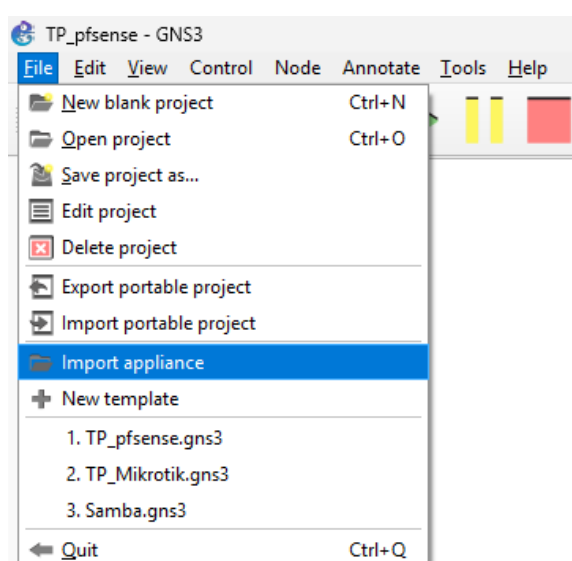


Figure 4 : Importation de pfsense dans GNS3



- ✓ Ensuite nous parcourrons notre ordinateur pour sélectionner notre appliance pfsense, la page s'ouvre nous demandant de faire tourner l'appliance sur notre serveur GNS3 VM, nous validons cette option. La page suivante s'ouvre, nous devons charger le fichier pfsense qui correspond à notre version, celui que nous avons téléchargé.

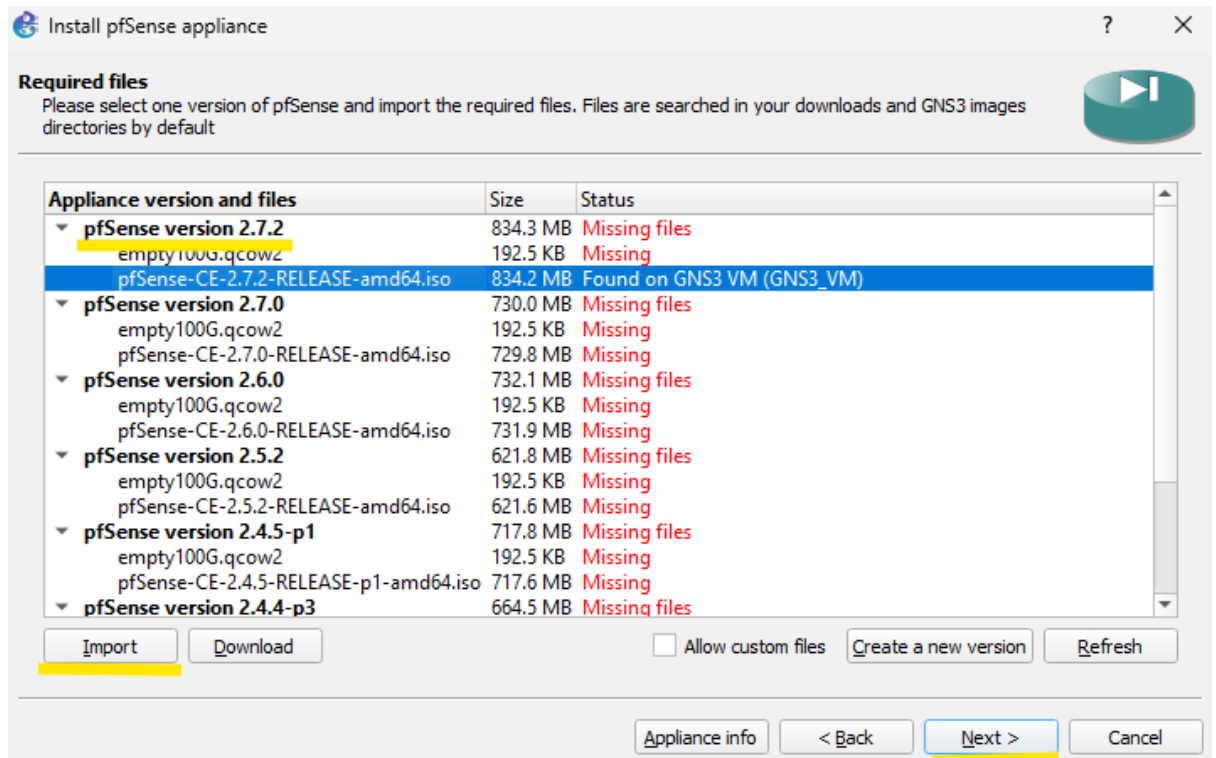


Figure 5 : Importation de pfsense dans GNS3

- ✓ Après que le processus d'importation soit terminé, pfsense apparait dans la catégorie des firewalls comme dans la figure ci-dessous :

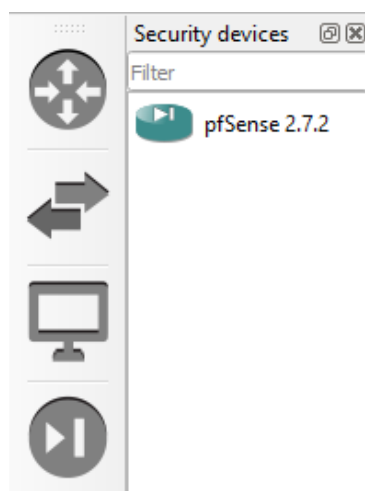


Figure 6: Importation réussie de pfsense dans GNS3

## 1.7. Architecture réseau de simulation

La figure 7 présente l'architecture du réseau que nous avons utilisé pour mettre en évidence les principales fonctionnalités de pfsense.

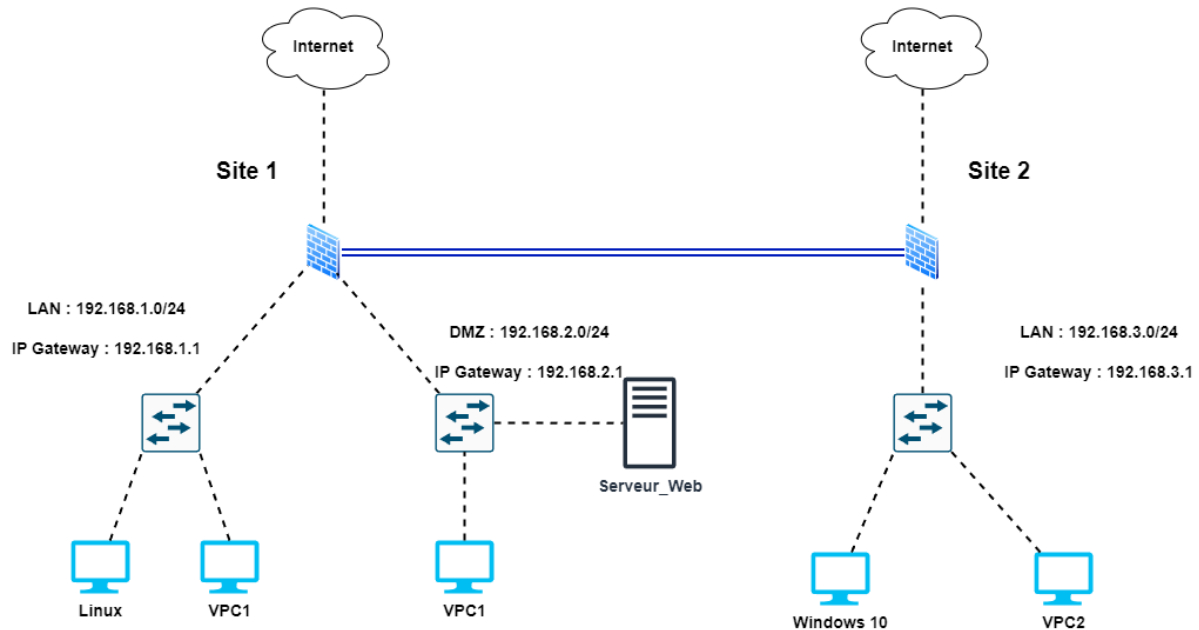


Figure 7 : Architecture du réseau

Une fois pfsense installé, nous pouvons lire à l'écran les adresses des interfaces WAN et LAN. Pour accéder à l'interface web de pfsense, nous devons saisir l'adresse de l'interface LAN de pfsense dans le navigateur d'un ordinateur du réseau LAN, car l'une des pratiques de sécurité consiste à interdire l'accès à pfsense en utilisant l'interface WAN. Ensuite nous obtenons la page de *la figure 8* dans laquelle nous devons saisir les identifiants par défaut, nom d'utilisateur : **admin** et mot de passe : **pfsense**.

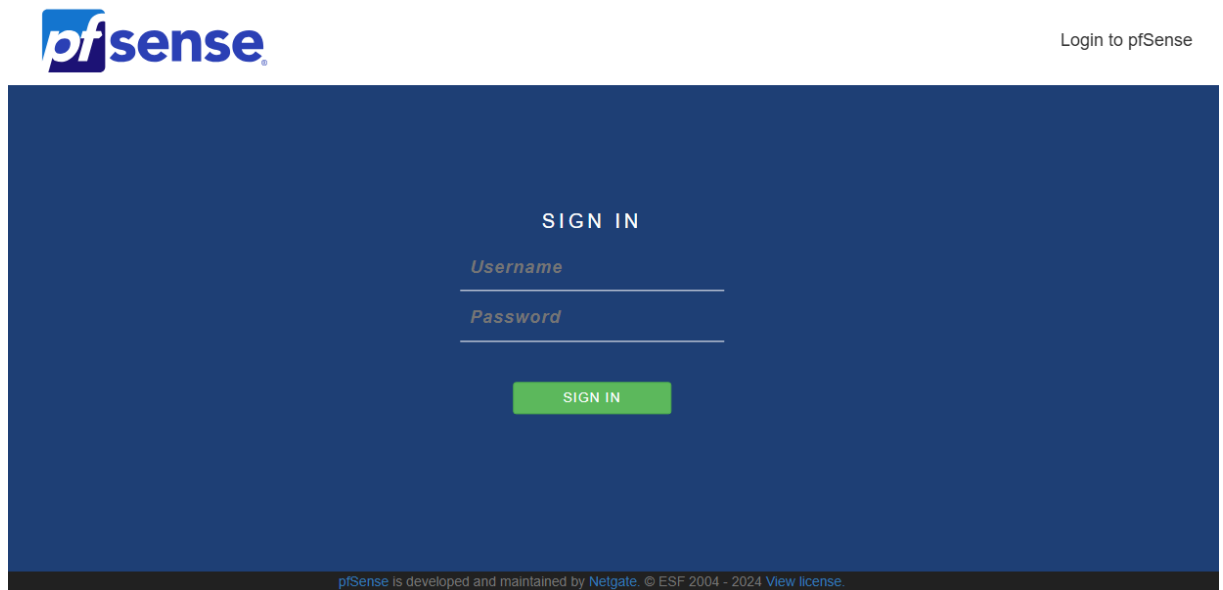


Figure 8 : Interface de de connexion Web de pfsense

Après une connexion réussie, nous obtenons le tableau de bord de pfsense qui est représenté à la *figure 9*.

System Information			
Name	pfSense.home.arpa		
User	admin@192.168.126.1 (Local Database)		
System	VMware Virtual Machine Netgate Device ID: abc037c9049fcf7f606a		
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020		
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT  The system is on the latest version. Version information updated at Mon Jun 17 13:30:13 UTC 2024		
CPU Type	Intel(R) Celeron(R) CPU B830 @ 1.80GHz AES-NI CPU Crypto: No QAT Crypto: No		
Hardware crypto	Inactive		

Netgate Services And Support			
Disks			
Mount	Used	Size	Usage
> /	976M	16G	6% of 16G (zfs)
Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.126.128
LAN	↑	1000baseT <full-duplex>	192.168.1.1

Figure 9: Tableau de bord de pfsense

## 2. Configuration de Pfsense

### 2.1. Configuration du portail captif

Un **portail captif** est une solution de contrôle d'accès réseau qui oblige les utilisateurs à s'authentifier ou à accepter des conditions d'utilisation avant d'accéder à un réseau. Les portails captifs permettent aux administrateurs de définir des politiques de contrôle d'accès pour limiter l'accès au réseau en fonction de critères tels que l'heure de la journée, la bande passante disponible, le type d'appareil, etc. Cela permet de garantir une utilisation sécurisée et efficace du réseau.

Nous avons développé un portail captif personnalisé avec le logo de l'entreprise pour restreindre le nombre de personnes qui ont accès à internet. La procédure de création du portail captif est la suivante :

- **Création d'une zone** : Tout d'abord, nous devons accéder au menu **Services** de pfSense et sélectionner l'option **Portail Captif**. Sur la page qui s'affiche, nous ajoutons une nouvelle zone et cliquons sur le bouton Enregistrer et continuer.
- **Choix de l'interface** : Il est question ici, de choisir l'interface sur laquelle nous souhaitons configurer le portail captif. Nous l'avons configuré sur le LAN ;
- **Personnalisation de page de connexion** : Nous avons chargé le logo de l'entreprise et une image des meilleurs étudiants comme image de fond ;
- **Configuration de l'authentification** : Nous avons décidé d'utiliser une base de données local pour l'authentification des utilisateurs ;
- **Création d'un utilisateur** : Nous allons à présent, créer la liste des utilisateurs autorisés à utiliser le portail captif. Pour cela, nous accédons au menu **Système** et sélectionnons l'option **gestionnaire d'utilisateur**, puis nous cliquons sur **Ajouter**. Sur l'écran de création utilisateur, nous effectuons la configuration suivante : Nom d'utilisateur : *Lion*, Mot de passe : *admin*, Nom complet : *Lion-security*, Date d'expiration : 1 mai 2025
- **Attribution du privilège de connexion au portail captif** : Maintenant, nous devons modifier les autorisations du nouveau compte utilisateur. Pour cela, nous cliquons sur le crayon dans la colonne **Actions**. Sur les propriétés du compte utilisateur, nous allons dans la zone Privilèges effectifs et cliquons sur le bouton Ajouter. Puis sur la zone de privilège utilisateur, nous ajoutons le privilège : **Connexion Portail Captif**. Nous cliquons sur le bouton Enregistrer pour terminer la configuration.

Après avoir effectué toutes les étapes ci-dessus, l'interface de connexion de notre portail captif est la suivante :

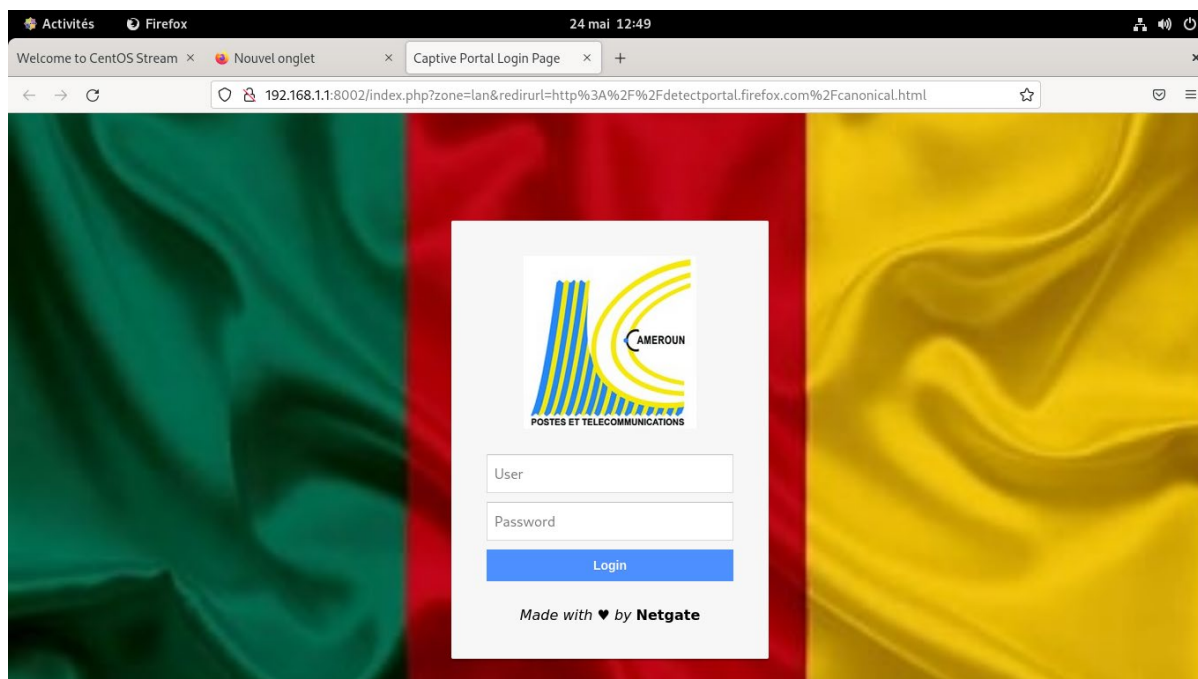


Figure 10: Résultat final : portail captif

## 2.2. Configuration des règles du pare-feu

La configuration d'un pare-feu fait référence aux règles et aux paramètres qui dictent la manière dont un pare-feu doit traiter le trafic réseau entrant et sortant. Ces paramètres de configuration déterminent quelles connexions sont autorisées et lesquelles sont bloquées, ce qui constitue la base de tout réseau sécurisé.

Il est très important de préciser que l'ordre des règles est critique pour leur bonne application. Les ensembles de règles sont évalués sur la base de la première correspondance. Cela signifie que la lecture de l'ensemble de règles d'une interface s'effectue de haut en bas, la première règle qui correspond sera celle utilisée par le pare-feu. La vérification s'arrête après avoir trouvé la correspondance, puis le pare-feu effectue l'action spécifiée par cette règle.

- **Configuration d'une règle :** Pour cela, nous allons dans le menu Firewall/ Rule, ensuite nous cliquons sur **Add** pour ajouter une nouvelle règle de filtrage ;
- **Configuration des adresses :** Nous configurons ensuite les adresses ainsi que les numéros de ports. Puis nous cliquons sur **save** et enfin **Apply Changes** pour prendre en compte la modification du pare-feu.

- **Configurations d'une exception :** Nous avons créé une règle qui autorise l'accès SSH uniquement à l'administrateur du réseau LAN, nous avons suivi le même processus mais sur l'option source nous avons choisi IP adresse
- **Visualisation de l'ensemble des règles :** En suivant le même principe que précédemment, nous avons établi les règles suivantes :
  - Interdiction d'accéder à l'interface web de pfsense depuis de le WAN pour plus de sécurité ;
  - Seul les protocole http et HTTPS permettant la navigation sur internet sont autorisés en plus de SSH.














Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 0/2 KiB	IPv4+6 *	*	*	WAN subnets	*	*	none		Allow all ipv4+ipv6 via pfSsh.php	
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	 0/0 B	IPv4 TCP	192.168.1.101	*	LAN address	22 (SSH)	*	none			
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	LAN address	22 (SSH)	*	none			
<input type="checkbox"/>	 0/0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4	
<input type="checkbox"/>	 1/44 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 11 : Ensemble des règles configurées sur notre pare-feu

## 2.3. Suppression des publicité, annonces, pop-up avec pfblockerNG

Les publicités, quel que soit leur format et le site sur lequel elles se trouvent, peuvent **cacher des arnaques ou des virus potentiels**. Les ignorer permet d'éviter ce type de souci.

Pour masquer ces publicités, qui gênent d'ailleurs souvent la navigation sur nos sites web, nous avons décidé d'associer à pfsense un bloqueur de publicités efficace, nommé pfBlockerNG.

**PfBlockerNG** offre des fonctionnalités de protection de la vie privée et de traçage avec filtrage Web permettant d'améliorer la confidentialité, de contrôler les accès, de supprimer les publicités et de bloquer l'accès aux sites publicitaires.

- **Résolveur DNS :** La première étape consiste à activer le résolveur **DNS** sur le pare-feu pfSense. Pour ce faire, nous allons dans le menu *services / DNS Resolver*. La plupart des champs sont laissés tels quels. Voici les valeurs que nous avons choisi chez nous.

- **Enable** est coché, forcément ;

- **Listen Port** est laissé par défaut (53) ;
- **Network Interfaces** est à *All* parce qu'on trouve pratique que tout le monde puisse l'utiliser ;
- **Outgoing Network Interfaces** est à *WAN* puisque c'est cette interface que le DNS Resolver enverra les requêtes.

**General DNS Resolver Options**

Enable ☒ Enable DNS resolver

**Listen Port**   
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

**Enable SSL/TLS Service** ☐ Respond to incoming SSL/TLS queries from local clients  
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

**SSL/TLS Certificate**   
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

**SSL/TLS Listen Port**   
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

**Network Interfaces**   
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

**Outgoing Network Interfaces**   
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

Figure 12 : Configuration du DNS Resolver

- **Installation du package :** Ce paquet n'étant installé par défaut, nous devons d'abord l'installer avant de l'utiliser. Pour cela, nous allons dans le menu *System / Package Manager*, puis nous cliquons sur *Available Packages* et nous saisissons le nom du package dans la barre de recherche et enfin nous cliquons sur le bouton *+Install*,

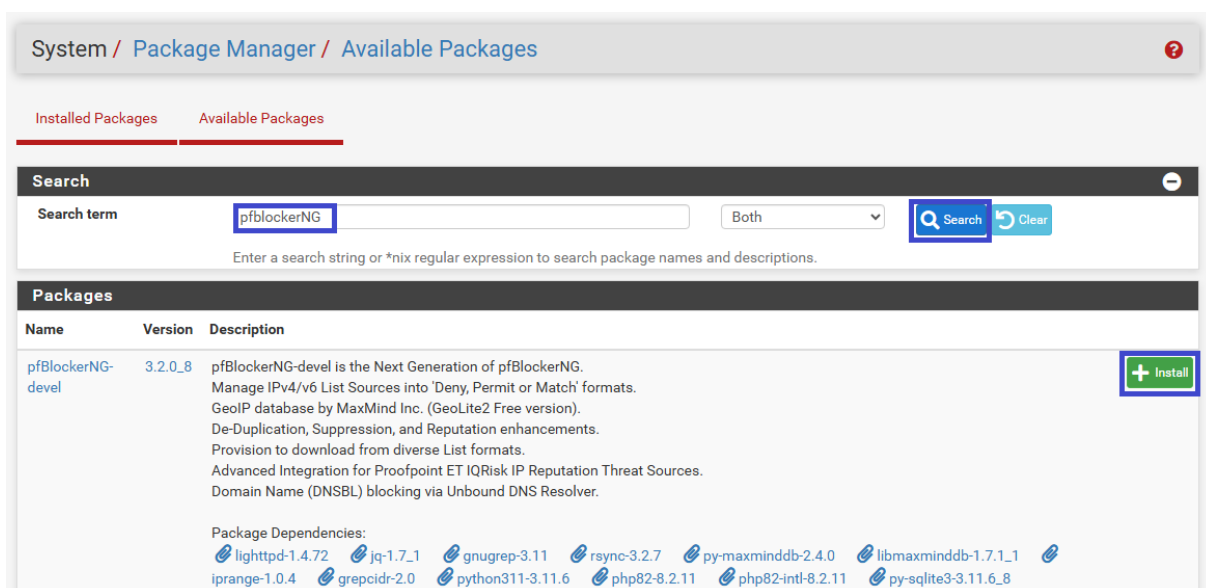


Figure 13 : Installation du package

- **Configuration du DNSBL :** Nous configurons les DNSBL. Cette fois, c'est via le menu *Firewall / pfBlockerNG* puis l'onglet *DNSBL* ;
- **DNSBL Easy List :** Nous passons à la récupération des listes de domaines à bloquer en commençant par celles préconfigurées. Toujours dans le menu de pfBlockerNG, nous cliquons sur l'onglet *DNSBL EasyList* :
  - **DNS GROUP NAME** et **Description** n'ont pour vocation que de nous permettre de les retrouver dans la configuration. On a donc mis *EasyList* dans les deux,
  - **EasyList Feeds**, l'état est à *ON*, nous avons ajouté deux (*EasyList w/o Elements* et *EasyPrivacy*), le header n'est que pour s'y retrouver (on y a mis *easy* et *privacy*),
- **Configuration des mises à jour :** Pour la configuration de leur contenu et leur mise à jour. Nous avons choisi 2 heures comme fréquence de mise à jour ;
- **Listes de blocage personnalisées :** Pour être plus complet, nous avons rajouté d'autres listes de domaines avec l'onglet *DNSBL Feeds*. Nous nous retrouvons avec plusieurs listes configurées :



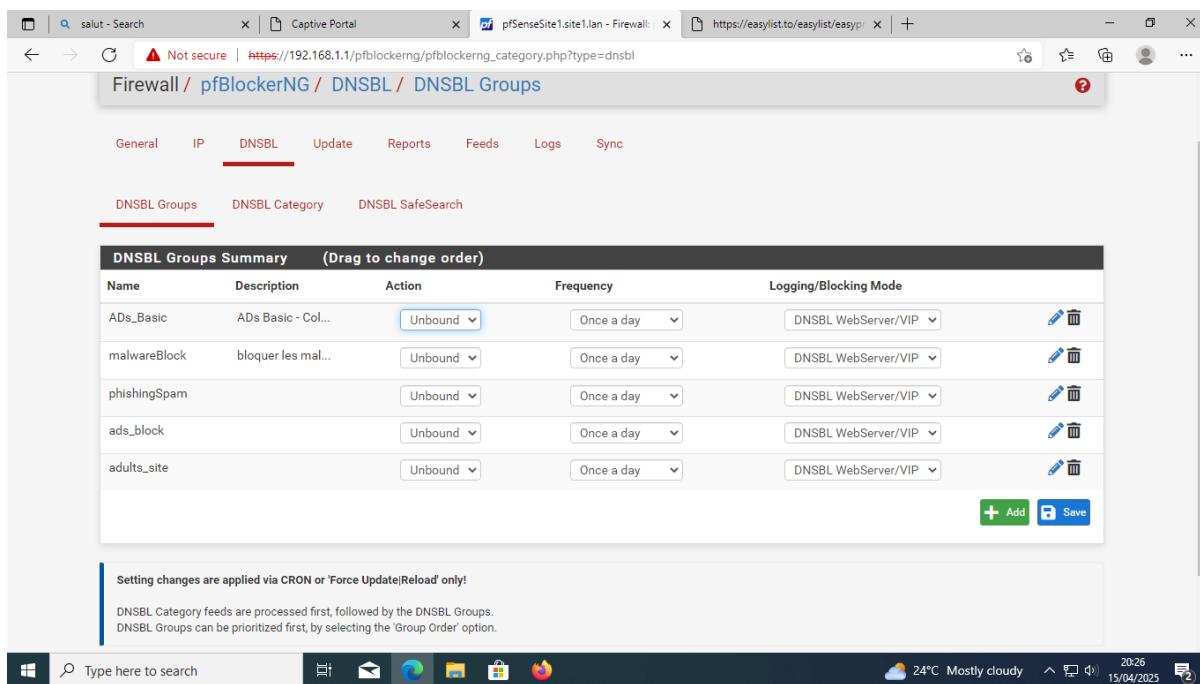


Figure 14 : Listes de Blocage personnalisées

- **Mise à jour manuelle :** Plutôt qu'attendre la prochaine exécution automatique, nous allons nous assurer que la configuration est valide et bien en place. C'est via le menu *Firewall / pfBlockerNG* puis onglet *Update*.
- **Test de fonctionnement :** Pour nous assurer que le filtrage DNSBL fonctionne, nous avons essayé de nous connecter à un domaine de publicité connu : *ads.google.com*. Lorsque nous saisissons cela dans notre navigateur, la page de blocage DNSBL s'affiche.

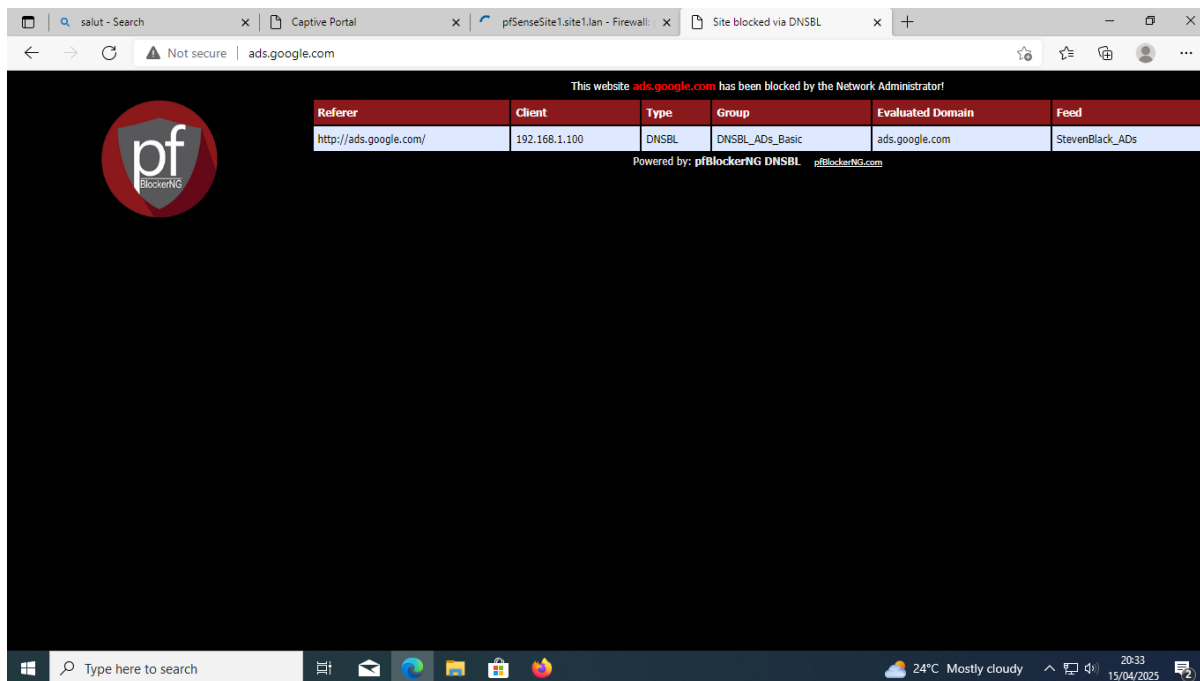


Figure 15 : Test du fonctionnement de pfblockerNG

## 2.4. Filtrage des sites web avec proxy Squid et Squid Guard

Afin d'améliorer les performances du réseau, nous avons décidé de restreindre l'accès à certaines catégories de sites web tel que les jeux, les contenus pour adulte ainsi que les sites de streaming vidéo. Pour cela, nous avons utilisé le package Squid Guard.

Un serveur proxy, appelé également serveur mandataire, est un serveur qui jouera le rôle d'intermédiaire entre un client et un serveur distant. Le serveur proxy va pouvoir réaliser plusieurs actions :

- **Filtrage**, ce qui va permettre de bloquer certains sites ou certaines catégories de sites.
- **Cache**, ce qui va permettre de mettre en cache les requêtes (exemple : page web) afin de les retourner plus rapidement aux postes de travail.
- **Journalisation**, toutes les requêtes reçues de la part des clients (postes de travail) seront stockées dans des journaux (*logs*).
- **Anonymat**, puisque votre poste de travail se cache derrière le proxy, le serveur Web verra seulement le proxy.

Le package Squid n'étant pas installé par défaut, nous devons d'abord l'installer.

- **Configuration de la cache** : La configuration de Squid s'effectue via le menu **Services/Squid proxy server**. Afin de pouvoir activer Squid, Nous configurons la cache locale. Pour cela, nous cliquons sur l'onglet "**Local Cache**". Le champs qui attire notre est : **Hard Disk Cache Size** : par défaut sur "100" pour 100 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Nous avons augmenté cette valeur à **1024 Mo** pour avoir 1 Go de cache.
- **Configuration générale du proxy** : Nous cliquons sur l'onglet **General pour configurer le proxy**. Nous observons de nombreux champs. Mais nous n'avons modifié que quelques-uns :
  - **Enable Squid Proxy** : nous cochons la case pour activer Squid sur le pare-feu ;
  - **Listen IP Version** : Nous sélectionnons les versions IPv4 et IPv6 ;
  - **Proxy interface(s)** : Nous sélectionnons l'interface sur laquelle nous souhaitons activer le proxy qui est l'interface **LAN** ;
  - **Proxy Port** : nous laissons le port par défaut, à savoir 3128 ;
  - **Allow Users on interface** : nous cochons cette case pour autoriser implicitement les utilisateurs connectés sur le réseau "LAN" à utiliser le proxy ;

**Squid General Settings**

<b>Enable Squid Proxy</b>	<input checked="" type="checkbox"/> Check to enable the Squid proxy. <b>Important:</b> If unchecked, ALL Squid services will be disabled and stopped.
<b>Keep Settings/Data</b>	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. <b>Important:</b> If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
<b>Listen IP Version</b>	<div style="border: 1px solid #ccc; padding: 2px;">IPv4+IPv6</div> <small>Select the IP version Squid will use to select addresses for accepting client connections.</small>
<b>CARP Status VIP</b>	<div style="border: 1px solid #ccc; padding: 2px;">none</div> <small>Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.  <b>Important:</b> Don't forget to generate Local Cache on the secondary node and configure <a href="#">XMLRPC Sync</a> for the settings synchronization.</small>
<b>Proxy Interface(s)</b>	<div style="border: 1px solid #ccc; padding: 2px;">         10.10.10.1 (pfb DNSBL - DO NOT EDIT)          WAN  <b>LAN</b>          loopback       </div> <small>The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.</small>
<b>Outgoing Network Interface</b>	<div style="border: 1px solid #ccc; padding: 2px;">Default (auto)</div> <small>The interface the proxy server will use for outgoing connections.</small>
<b>Proxy Port</b>	<div style="border: 1px solid #ccc; padding: 2px;">3128</div> <small>This is the port the proxy server will listen on. Default: 3128</small>
<b>ICP Port</b>	<div style="border: 1px solid #ccc; padding: 2px;"></div> <small>This is the port the proxy server will send and receive ICP queries to and from neighbor caches.          Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.</small>
<b>Allow Users on Interface</b>	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

Figure 16 : configuration générale du proxy

- **Configuration du proxy transparent HTTP** : Plus bas toujours sur l'onglet **General** nous cochons l'option "**Transparent HTTP Proxy**" pour activer le mode proxy transparent pour le protocole HTTP.

**Transparent Proxy Settings**

<b>Transparent HTTP Proxy</b>	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server. <div style="background-color: #007bff; color: white; border-radius: 50%; width: 15px; height: 15px; margin: 5px 0; display: flex; align-items: center; justify-content: center;">i</div> <small>Transparent proxy mode works without any additional configuration being necessary on clients.  <b>Important:</b> Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.  <b>Hint:</b> In order to proxy both HTTP and HTTPS protocols <b>without intercepting SSL connections</b>, configure WPAD/PAC options on your DNS/DHCP servers.</small>
<b>Transparent Proxy Interface(s)</b>	<div style="border: 1px solid #ccc; padding: 2px;">         10.10.10.1 (pfb DNSBL - DO NOT EDIT)          WAN  <b>LAN</b> </div> <small>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</small>
<b>Bypass Proxy for Private Address Destination</b>	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. <small>Destinations in Private Address Space (<a href="#">RFC 1918</a> and <a href="#">IPv6 ULA</a>) are passed directly through the firewall, not through the proxy server.</small>
<b>Bypass Proxy for These Source IPs</b>	<div style="border: 1px solid #ccc; padding: 2px;"></div> <small>Do not forward traffic from these <b>source</b> IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.  <b>Applies only to transparent mode.</b> Separate entries by semi-colons (;)</small>
<b>Bypass Proxy for These Destination IPs</b>	<div style="border: 1px solid #ccc; padding: 2px;"></div> <small>Do not proxy traffic going to these <b>destination</b> IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.  <b>Applies only to transparent mode.</b> Separate entries by semi-colons (;)</small>

Figure 17 : Configuration du proxy transparent HTTP

➤ **Configuration de la journalisation** : Nous allons à présent configurer la journalisation dans le but de connaître qui fait quoi sur internet

- **Enable Access Logging** : nous cochons l'option pour activer les journaux ;
- **Rotate Logs** : ce champ définit pendant combien de jours nous souhaitons conserver les logs. Nous avons sélectionné 30 jours

Nous allons permettre à notre proxy transparent de filtrer le protocole HTTPS. Nous allons faire du **SSL Inspection** car un flux HTTPS est chiffré, le proxy ne peut pas seulement regarder les trames passer. En effet, pour chaque connexion, il doit déchiffrer le flux, l'inspecter puis le chiffrer à nouveau afin de l'acheminer.

➤ **Création du certificat d'autorité** : Nous devons créer une autorité de certification sur notre pare-feu PfSense. Pour cela, nous rendons dans le menu "**System/Certificate**". Ensuite nous cliquons sur "**Add**" et nous renseignons les différents champs :

The screenshot shows the 'Internal Certificate Authority' configuration page in pfSense. The browser address bar shows 'https://192.168.1.1/system\_camanager.php?act=new'. The form contains the following fields and values:

- Key type**: RSA
- Key length**: 2048 (with a note: 'The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.')
- Digest Algorithm**: sha256 (with a note: 'The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.')
- Lifetime (days)**: 3650
- Common Name**: internal-ca
- Country Code**: CM (with a note: 'The following certificate authority subject components are optional and may be left blank.')
- State or Province**: Cameroon
- City**: Ouést
- Organization**: lion-security
- Organizational Unit**: Network security

A 'Save' button is located at the bottom left of the form.

Figure 18 : Création du certificat de d'autorité

➤ **Configuration du proxy transparent HTTPS** : Ensuite, activez l'option "**Enable SSL filtering**". Pour le mode "**SSL/MITM Mode**", choisissez le mode "**Splice All**" : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le certificat de l'autorité de certification sur l'ensemble des postes clients.

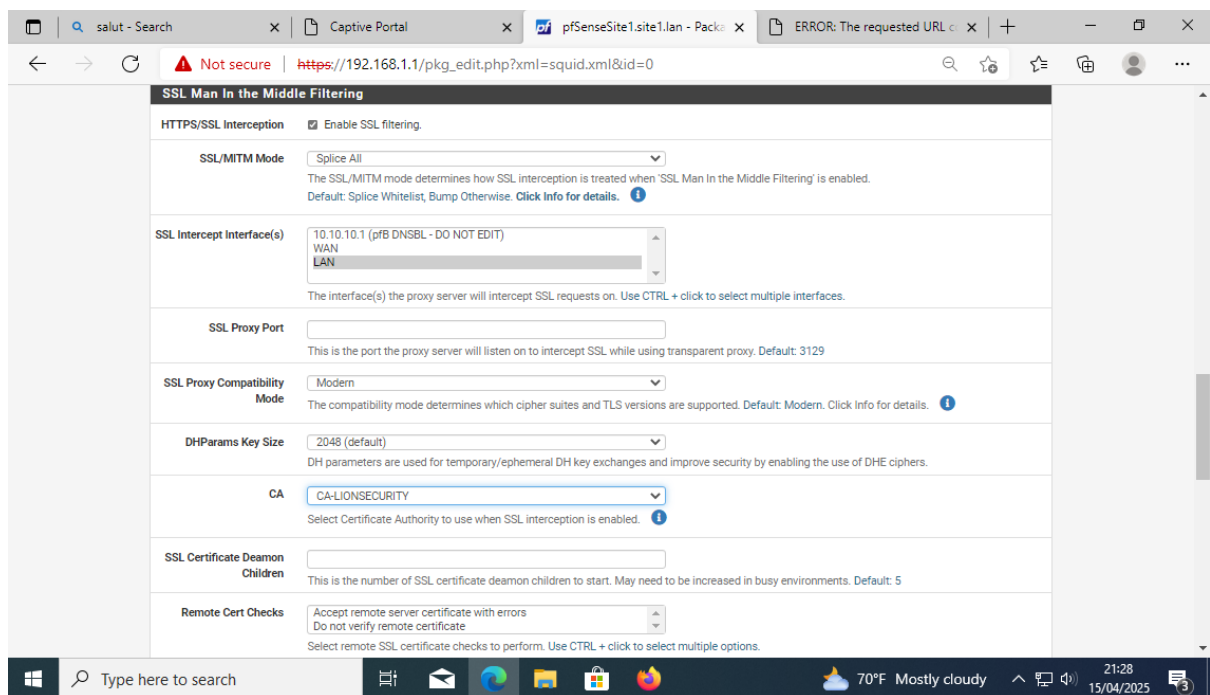


Figure 19 : Configuration du proxy transparent HTTPS

- **Configuration de la liste noire :** Au sein de la section "**Blacklist**", nous cochons l'option "**Check this option to enable blacklist**" afin d'activer l'utilisation d'une blacklist. Nous allons utiliser **la liste noire de L'Université Toulouse Capitole**, car elle est fiable et elle existe depuis plusieurs années.

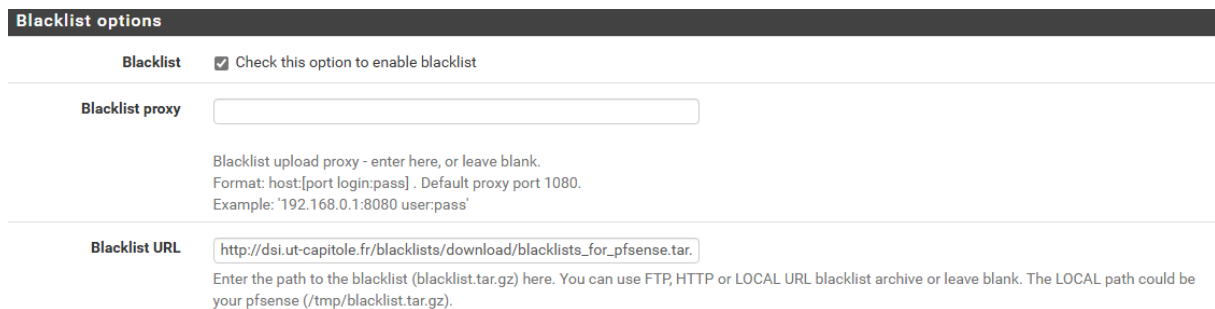


Figure 20 : Configuration de la liste noire

- **Quelques listes bloquées :** Afin d'exploiter la liste noire, nous avons créé des règles sous la forme d'ACL. Nous cliquons sur "**Common ACL**" afin de créer une règle de base et commune au sein de Squid. Au sein du champ "**Target Rules List**", nous avons la liste de toutes les catégories récupérées à partir de la blacklist toulousaine.

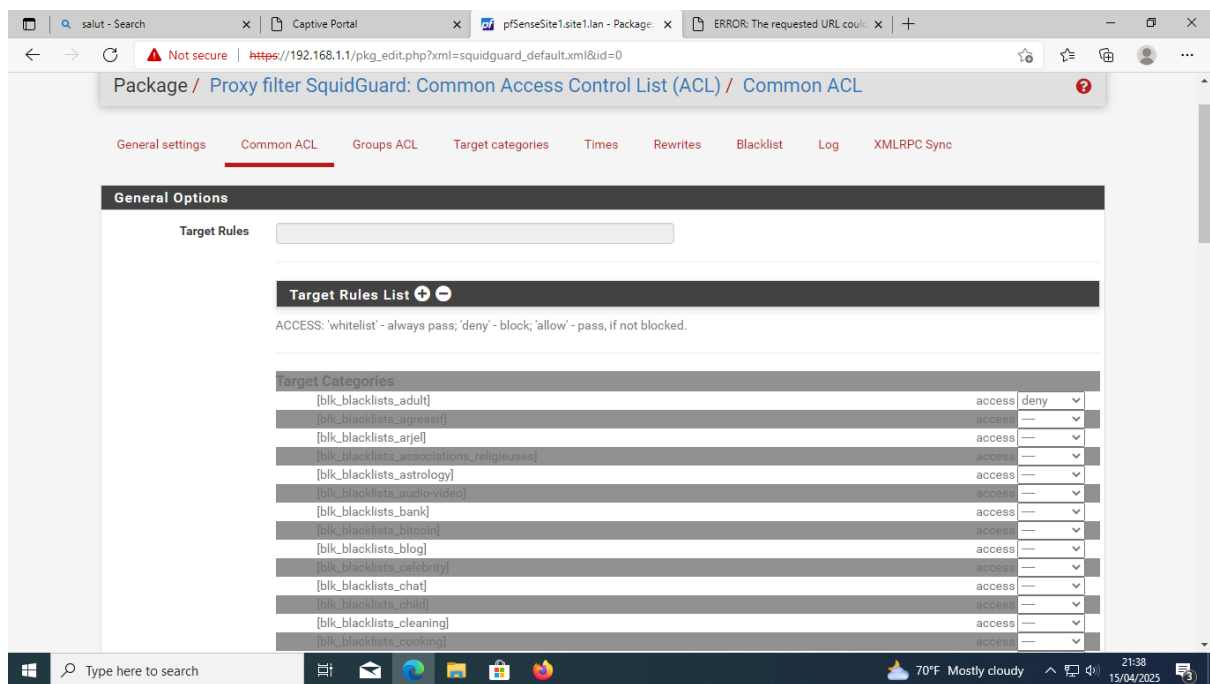


Figure 21: Choix des listes à bloquer

- **Validation des configurations :** La configuration étant prête, retournez dans "General Settings", cochez l'option "Check this option to enable SquidGuard" et cliquez sur "Apply".

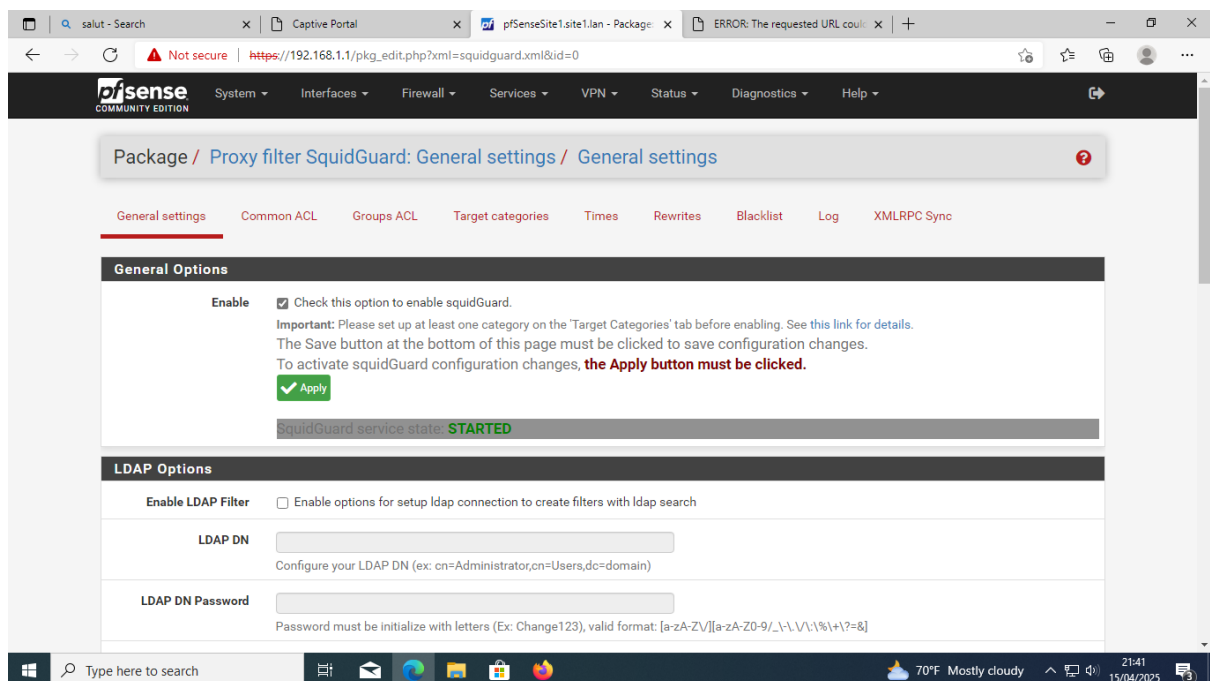


Figure 22: Activation de SquidGuard

- **Test de fonctionnement :** À partir d'un poste client, nous tentons d'accéder à un réseau social, *Facebook* par exemple nous constatons que la connexion est en erreur. En réalité,

c'est Squid Guard qui est intervenu pour bloquer la connexion à ce site, conformément à la politique de filtrage mise en place.

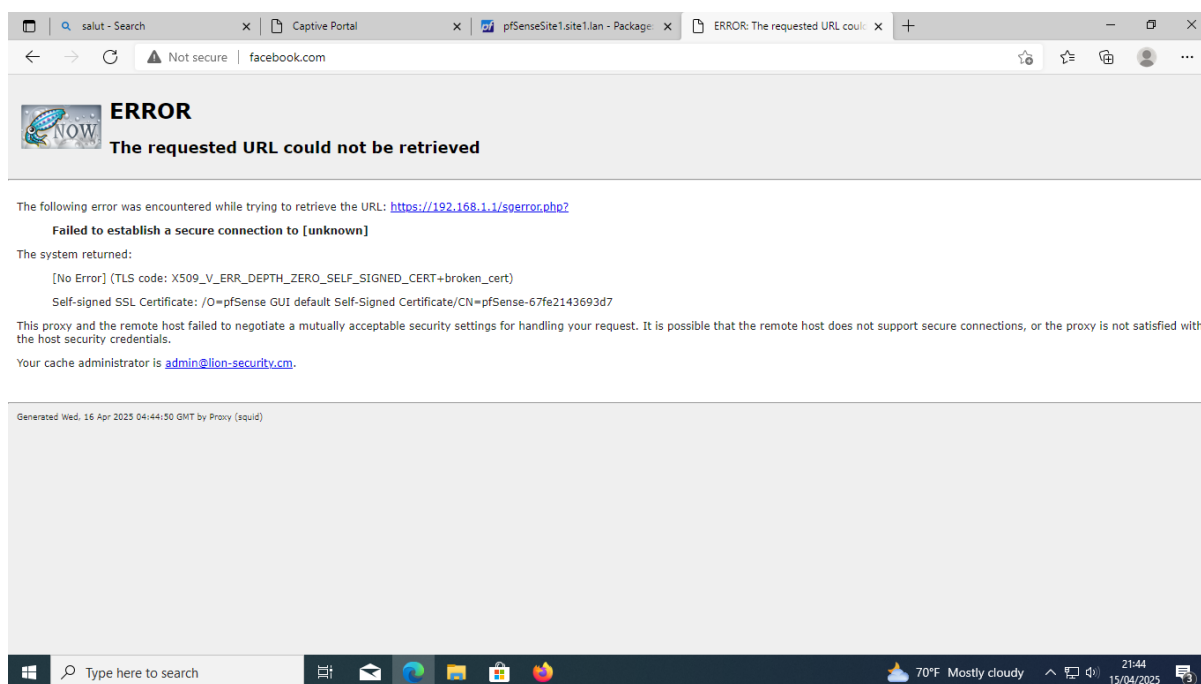


Figure 23 : Résultat du test : blocage du site web de Facebook

## **2.5. Configuration d'un système de prévention des intrusions avec Snort**

Les pirates et autres menaces sont constamment à l'affût de failles dans notre réseau. Une seule machine compromise peut mettre en danger l'ensemble de notre infrastructure. Il est crucial de détecter et de prévenir les intrusions pour protéger les réseaux contre les menaces malveillantes. C'est pour cette raison que nous avons décidé d'installer Snort.

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

Snort est un logiciel open source gratuit qui peut être déployé par des individus et des organisations. Le langage de règle Snort détermine quel trafic réseau doit être collecté et ce qui doit se passer lorsqu'il détecte des paquets malveillants. Cette politique peut être utilisée de la même manière que les renifleurs et les systèmes de détection d'intrusion réseau pour détecter

les paquets malveillants ou comme une solution IPS réseau complète qui surveille l'activité réseau et détecte et bloque les vecteurs d'attaque potentiels.

Par défaut le paquet Snort n'est pas installé sur pfsense il faut donc le télécharger puis l'installer. Une fois l'installation terminée, nous nous rendons dans le menu **Services/ Snort**.

- **Création du compte :** Dans la zone **Global Settings**, nous cochons la case **Enable Snort VR**, puis pour le **Snort Oinkmaster Code**, nous nous inscrivons sur Snort en cliquant sur le premier lien, une fois cela fait nous récupérons le code sur **notre profil Snort** dans la section **OinkCode** ;

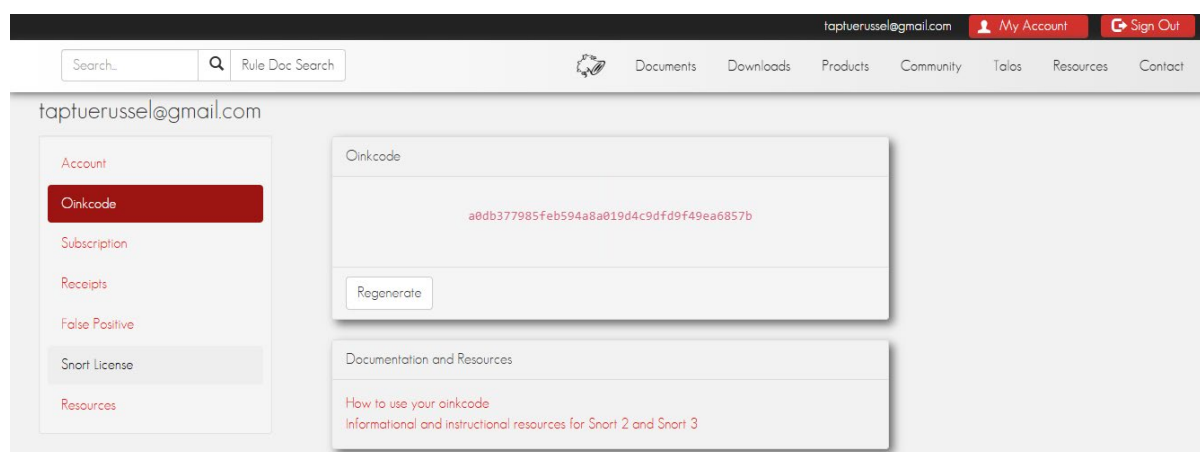


Figure 24 : credential pour activer snort

- **Récupération des règles Snort :** Nous cochons les cases **Enable ET Open** et **Enable Snort GPLv2** pour récupérer l'ensemble des règles contre les menaces malveillantes publiée par la communauté ;



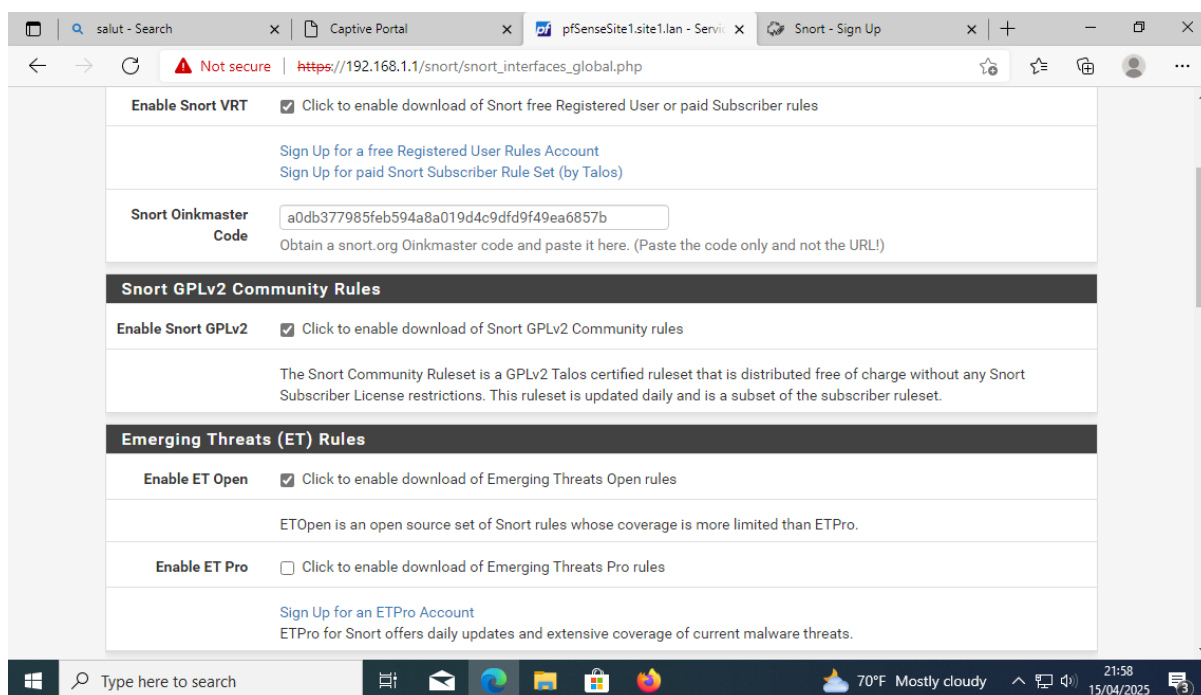


Figure 25: récupération des règles snort

- **Configurations des mises à jour :** Nous configurons ensuite la mise à jour des règles Snort pour **Update Interval** nous allons configurer pour que les règles soit mise à jour chaque jour et nous allons cochez la **Case Hide Dprecated Rules Catégories** qui permettra de supprimer les règles obsolètes ;

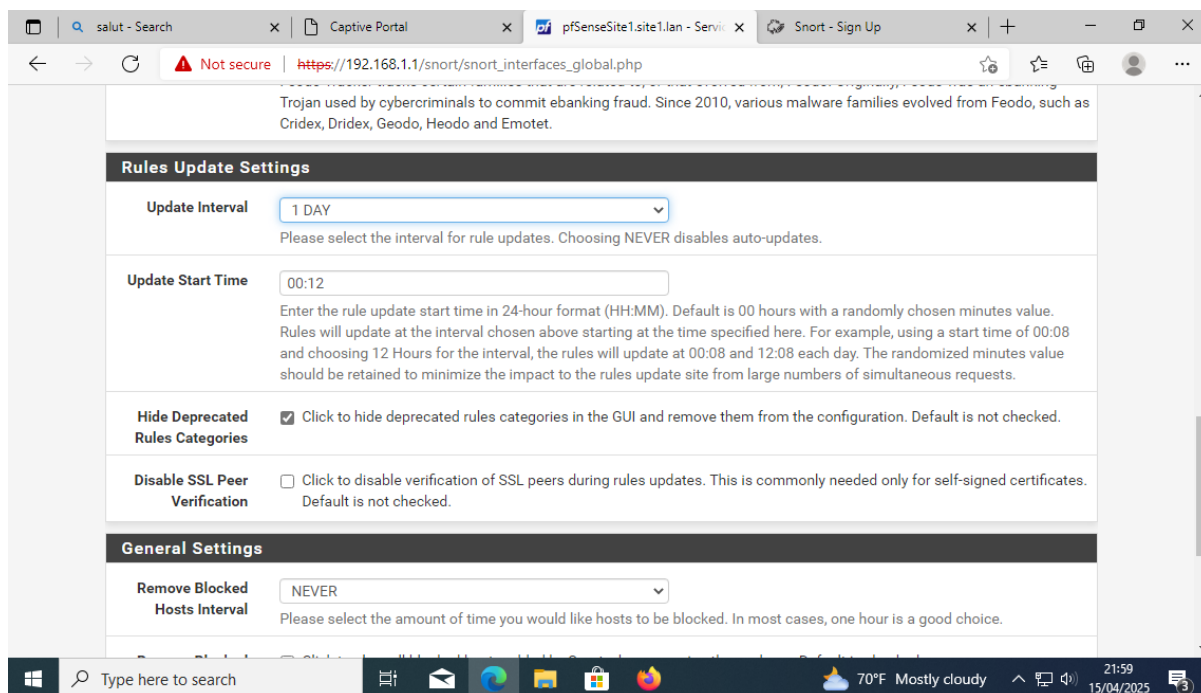


Figure 26: Choix de la frequence des mises a jour

- **Mise à jour des règles :** Pour mettre à jour les règles Snort, nous nous rendons dans l'onglet **Updates** puis nous cliquons sur **Updates Rules** :

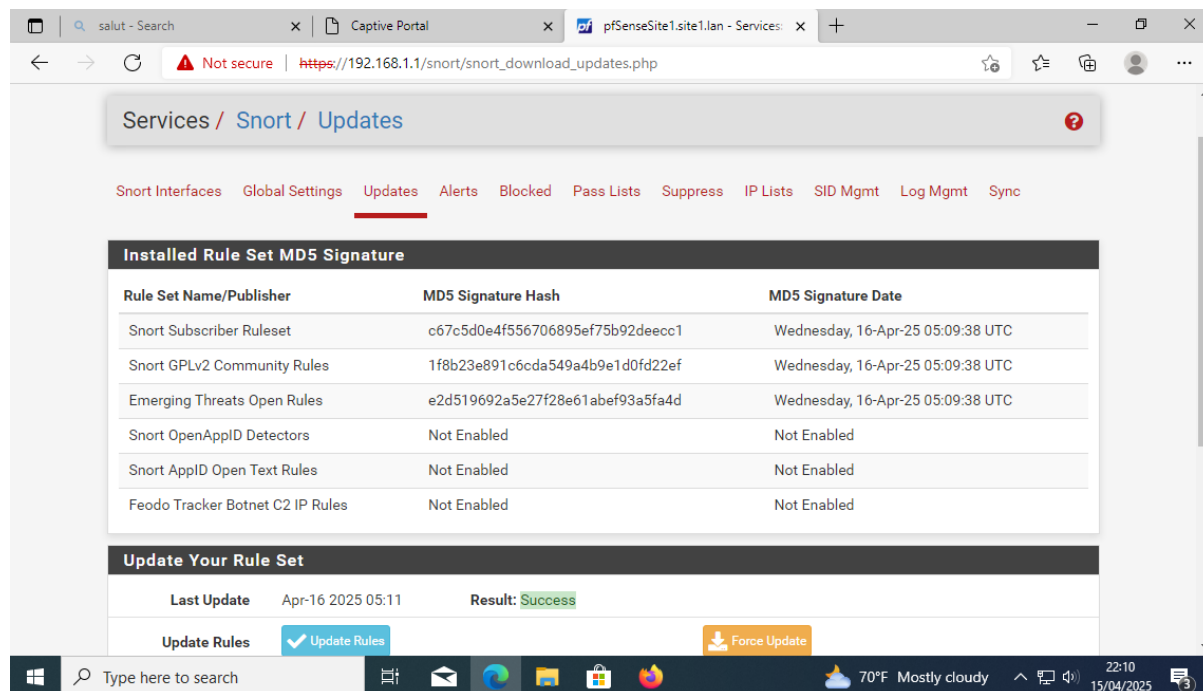


Figure 27: Mise à jour des règles

- **Configuration de l'interface :** Nous allons dans l'onglet Snort Interfaces et nous cliquons sur **Add**. Nous cochons **Enable interface**, **Send Alerts to System Log** et **Enable Packet Captures** ce dernier va permettre de créer un fichier qui sera par la suite possible d'analyser avec un logiciel comme Wireshark :

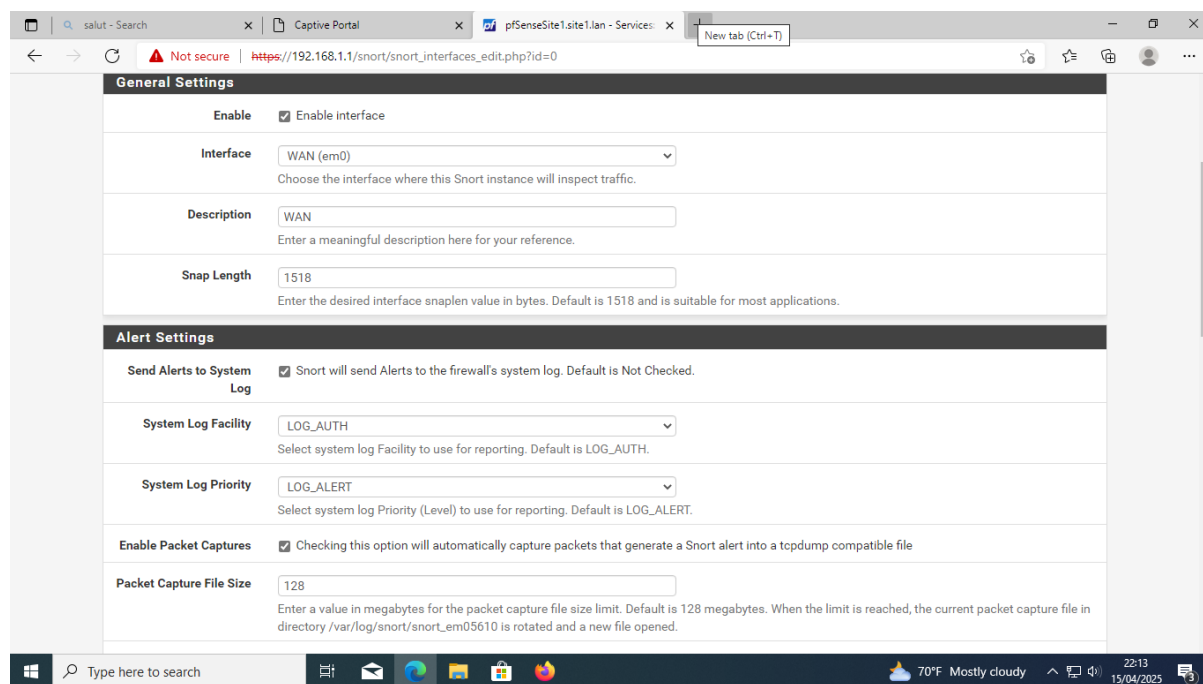


Figure 28 ; Configuration de l'interface

➤ **Configuration de la politique IPS** : Après l'ajout de l'interface WAN nous l'avons éditée pour ajouter la politique IPS. Les politiques Snort IPS sont :

- **Connectivity** : bloque la plupart des menaces majeures avec peu ou pas de faux positifs.

- **Balanced** : est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivité.

- **Security** : est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique.

- **Max-Detect** : est une stratégie créée pour tester le trafic réseau via votre appareil.

Pour notre organisation, nous avons optés pour la politique Balanced

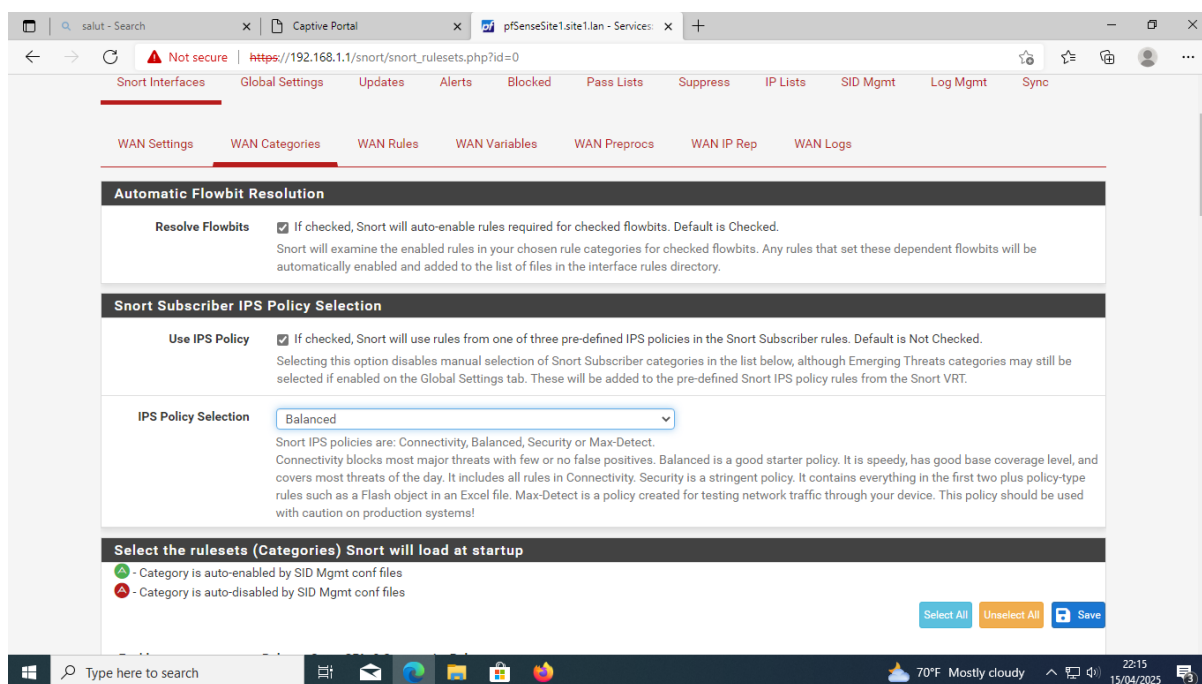


Figure 29: Choix de la politique IPS

➤ **Test de fonctionnement de Snort** : Après avoir fait un test Nmap sur notre interface WAN, nous voyons les logs remontés dans la section **Alert** de **Snort**

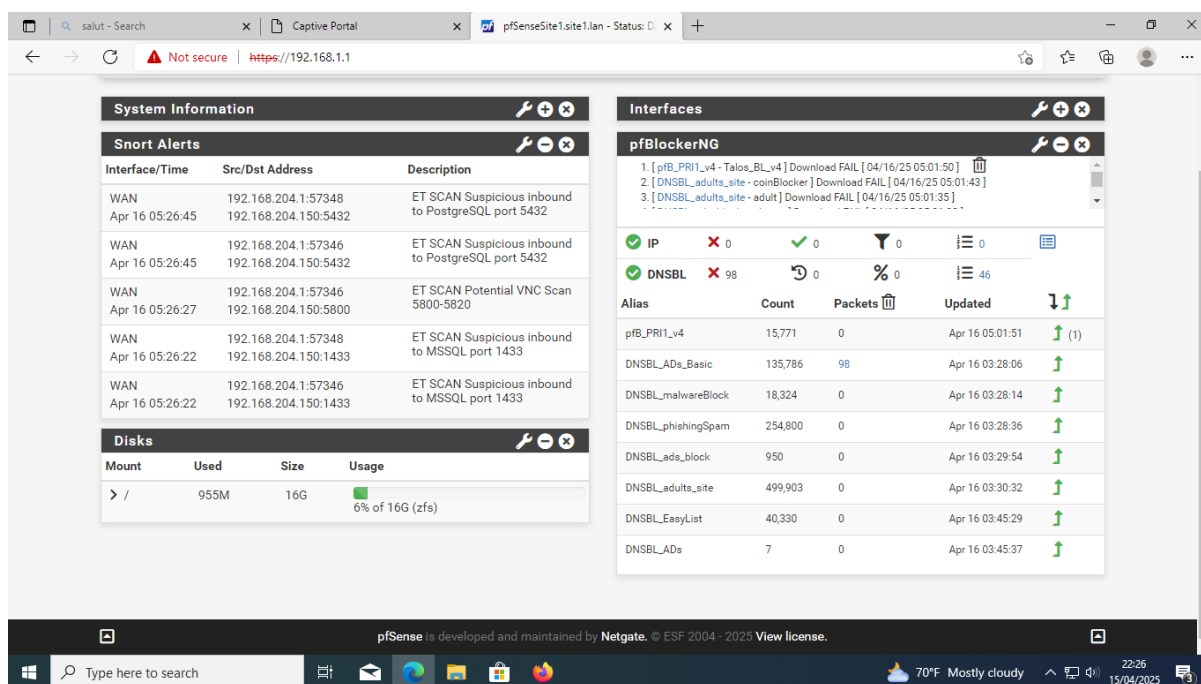


Figure 30 : Test de fonctionnement de Snort

## 2.6. Configuration d'un VPN site-to-site

VPN (Virtual Private Network) désigne une technologie qui permet de créer une connexion sécurisée et chiffrée entre un utilisateur et un réseau distant ou entre plusieurs réseaux. Il existe plusieurs types de VPN, chacun adapté à des besoins spécifiques :

### ➤ VPN personnel

- Utilisé principalement par des particuliers pour protéger leur vie privée en ligne, masquer leur adresse IP et accéder à des contenus géo-restreints.
- L'utilisateur se connecte à un serveur VPN via une application dédiée sur son appareil.

### ➤ VPN d'accès à distance (Remote Access VPN)

- Permet aux utilisateurs distants (par exemple, des employés en télétravail) d'accéder en toute sécurité aux ressources internes d'une entreprise comme s'ils étaient physiquement présents dans les locaux.
- Nécessite l'installation d'un client VPN sur l'appareil de l'utilisateur, qui s'authentifie pour établir un tunnel sécurisé avec le réseau privé.

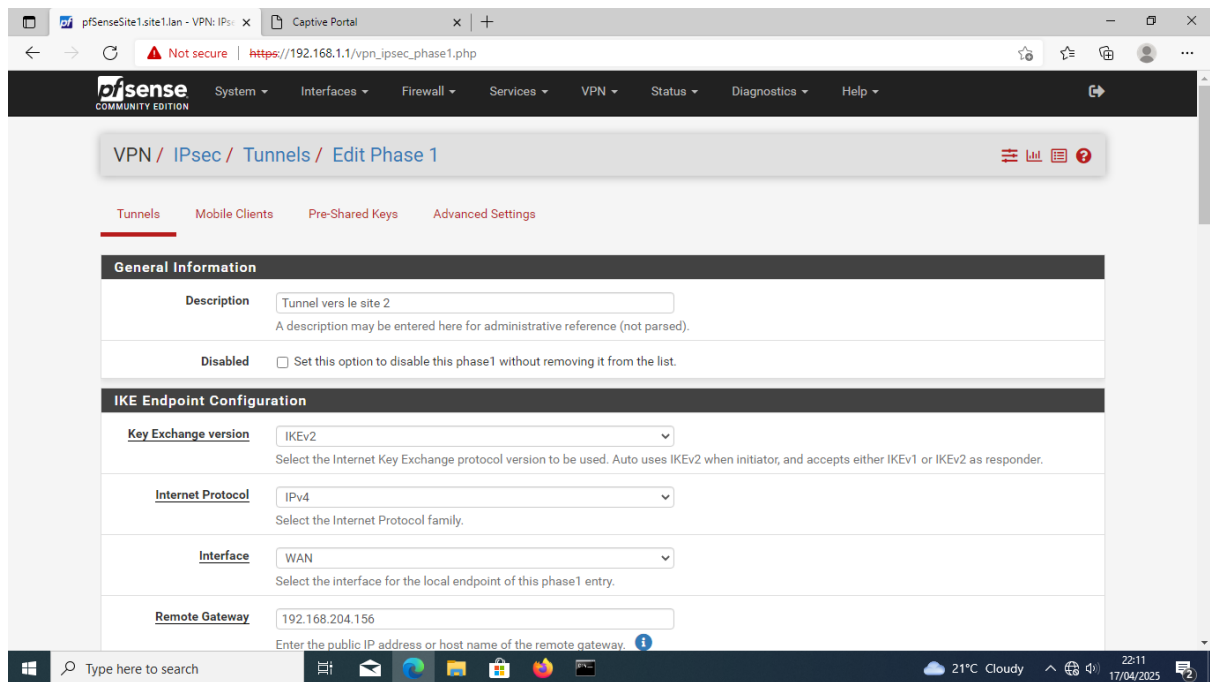
➤ **VPN site-à-site (Site-to-Site VPN)**

- Connecte plusieurs réseaux locaux (LAN) distants via Internet, souvent utilisé par des entreprises ayant plusieurs bureaux ou filiales.
- Permet la communication sécurisée entre différents sites comme s'ils faisaient partie d'un même réseau interne.

Dans le cas de notre travail pratique, nous avons opté pour un **VPN Site-to-Site** avec **IPsec**. La configuration se fait en trois étapes, sur chaque pare-feu :

✓ **Configuration de la phase 1 sur le pare-feu du site 1** : Pour cela, nous nous rendons dans l'onglet **VPN**, puis **IPsec** et nous cliquons sur **Add P1**. Nous modifions quelques champs, ceux qui nous intéressent sont les suivantes :

- **Remote Gateway** : Saisissez l'adresse IP WAN du Site 2, 192.168.204.156.
- **Description** : Tunnel vers Site 2.
- **Key Exchange version** : IKEv2 (recommandé).
- **Authentication method** : Mutual PSK.
- **Pre-Shared Key** : Saisissez une clé forte, identique sur les deux sites.
- **Encryption Algorithm** : Choisissez AES (256 bits recommandé).
- **Hash Algorithm** : SHA256.
- **DH Group** : 14 ou supérieur (2048 bits ou plus).



*Figure 31: Phase 1 du VPN IPsec*

✓ **Configuration de la Phase 2 sur le Site 1 :** Dans la section IPsec, nous cliquons sur **Show Phase 2 Entries** puis **Add P2**. Les champs qui nous intéressent sont les suivants :

- **Local Network :** Saisissez le sous-réseau local du Site 1, 192.168.1.0/24.
- **Remote Network :** Saisissez le sous-réseau local du Site 2 192.168.3.0/24.
- **Protocol :** ESP.
- **Encryption Algorithms :** AES 256 bits.
- **Hash Algorithms :** SHA256.
- **PFS key group :** 14 ou supérieur.

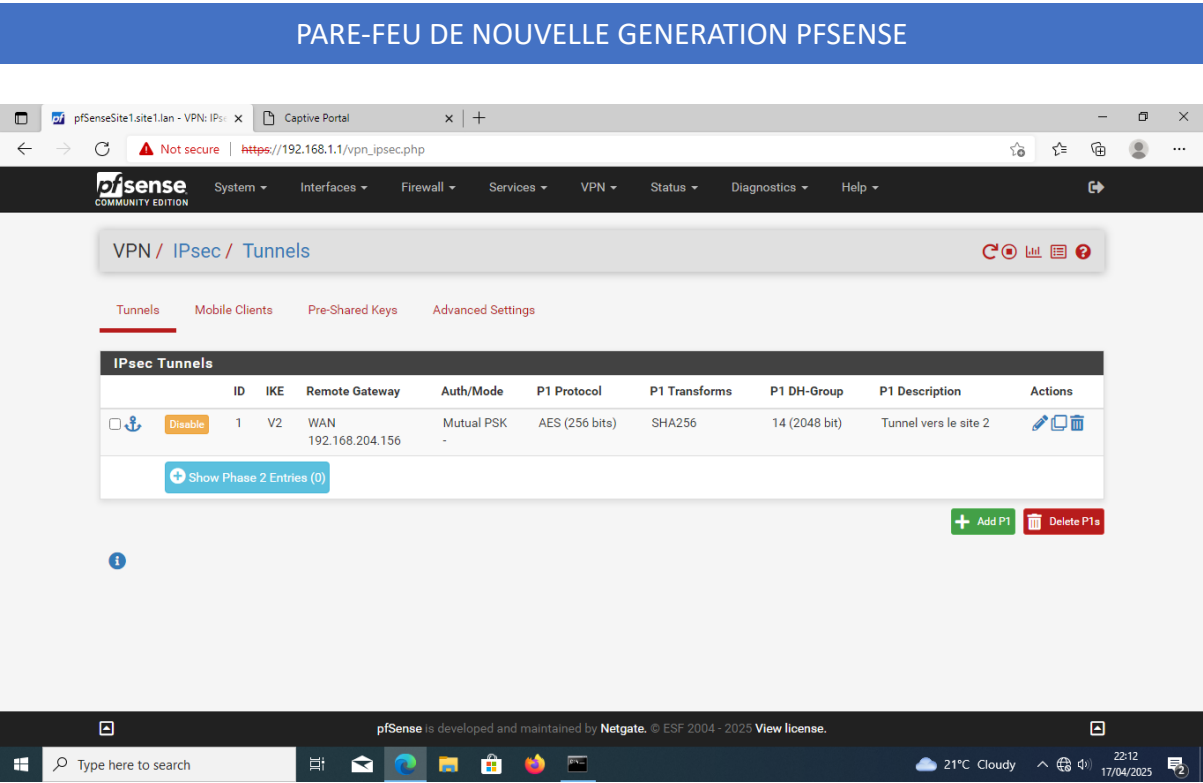


Figure 32: Ajout de la phase 2

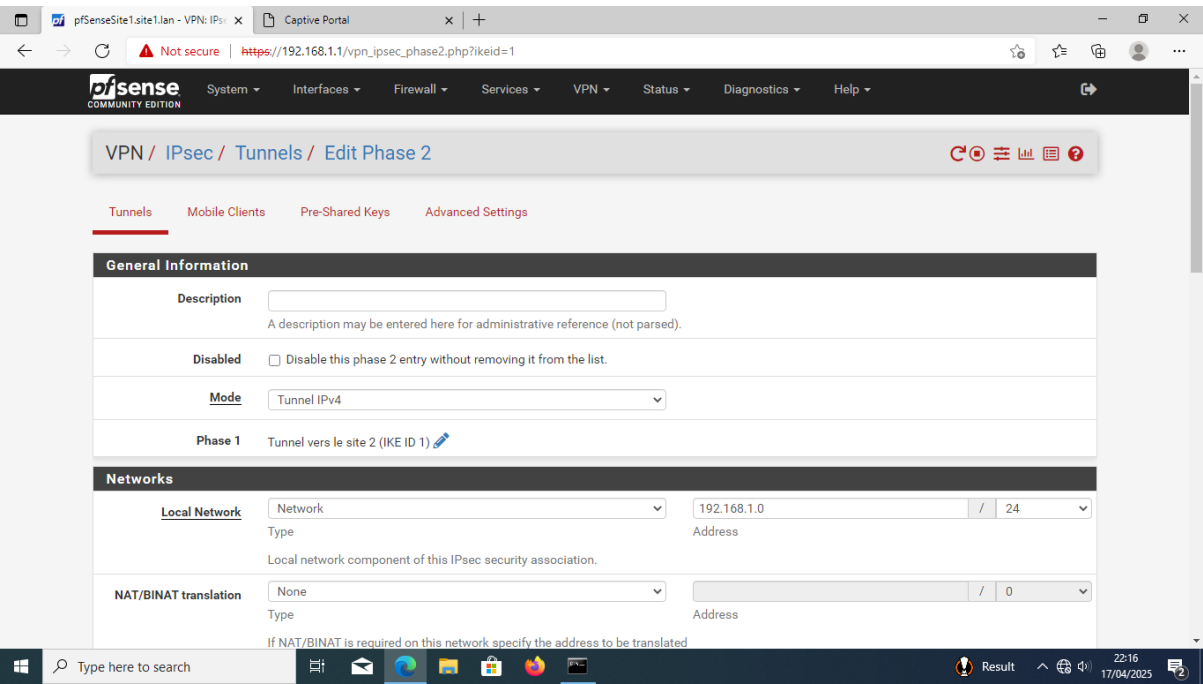
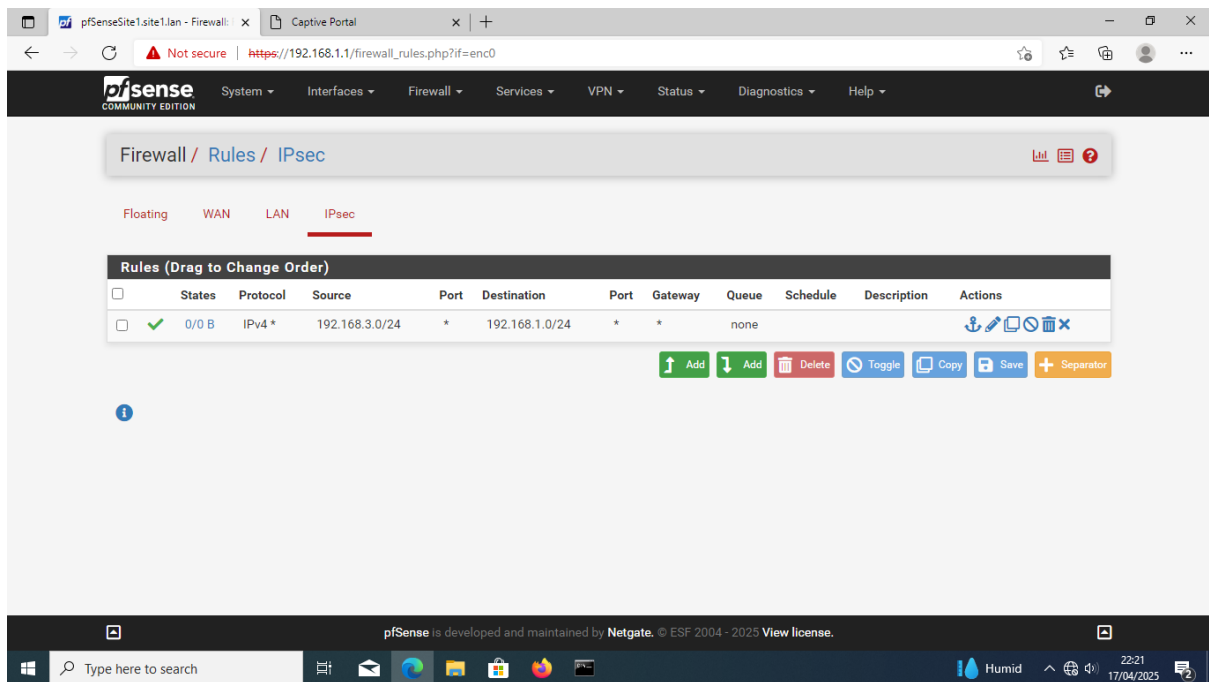


Figure 33: Phase 2 du VPN IPsec

✓ **Création de la règle de pare-feu sur le Site 1** : pour cela, nous allons dans **Firewall > Rules > IPsec**, puis nous cliquons sur **Add**.

- **Action** : Pass.
- **Protocol** : Any.
- **Source** : Réseau du site 2, 192.168.3.0/24.
- **Destination** : Réseau du site 1, 192.168.1.0/24.



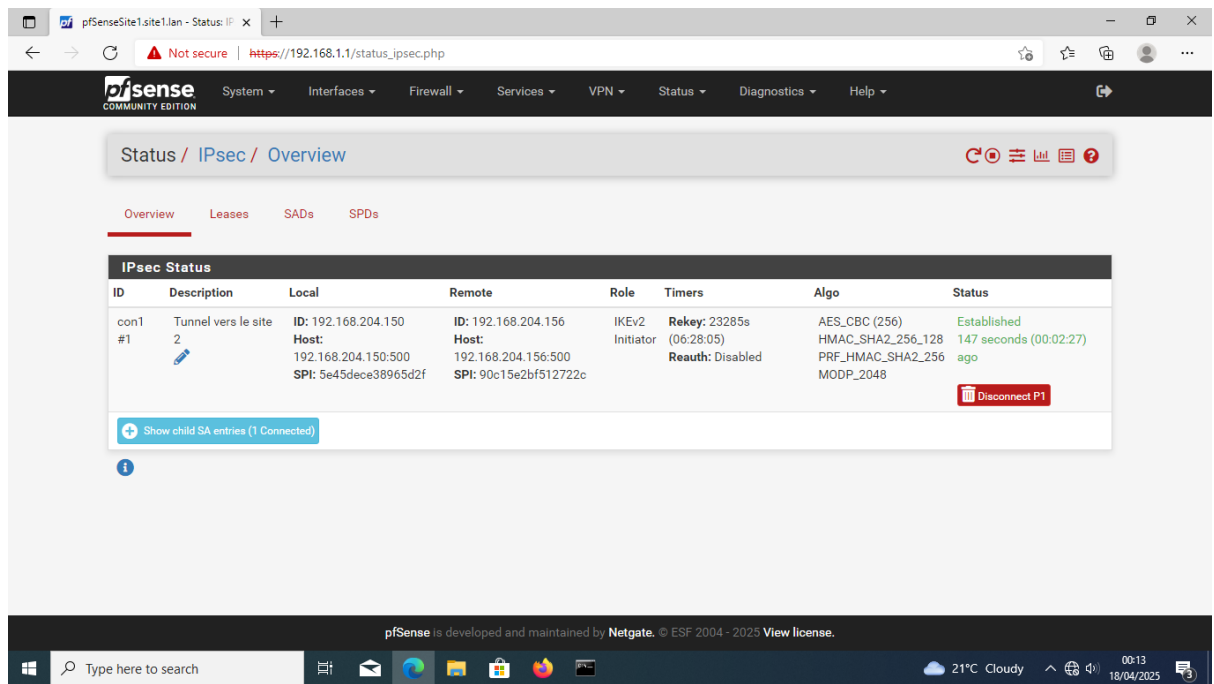
*Figure 34: Configuration des règles firewall pour IPsec*

✓ **Répétons les étapes 1 à 3 sur le Site 2** : nous devons Utiliser exactement la même Pre-Shared Key et les mêmes paramètres de chiffrement.

- **Remote Gateway**: IP WAN du Site A.
- **Local Network** : Sous-réseau local du Site B.
- **Remote Network** : Sous-réseau local du Site A.

Une fois la configuration terminée sur les deux sites, allez dans **Status > IPsec** pour vérifier que le tunnel est bien établi.





*Figure 35: Connexion VPN site-to-site établie*