NICOLAS LECA

ROUTEUR / SWITCH

EN COLLABORATION AVEC JAKUB WERLINSKI (BINÔME INFORMATIQUE)

1. Introduction

1.1. Explication du concept

Au cœur de notre infrastructure réseau, nous avons déployé un ensemble d'équipements essentiels : un routeur, un commutateur et un point d'accès. Ces trois éléments jouent un rôle central dans la gestion des communications au sein de notre réseau. Ils assurent la connectivité et le routage des données entre les divers appareils et sous-réseaux de manière efficace et sécurisée.

Dans cette configuration, nous garantissons une connectivité fiable et optimale tant pour les périphériques câblés que sans fil. Le commutateur et le routeur gèrent le trafic de manière efficace, tandis que le point d'accès offre une connectivité sans fil sécurisée. Voici les détails des adresses et des mots de passe associés à chaque équipement :

Elément	Type	Adresse	Mot de passe
Routeur	PfSense	10.0.0.1/29	Azerty13!
Commutateur	Netgear GS108Ev3.	10.0.0.2/29	Azerty13!
Point d’accès	D-Link DAP-1360	192.10.10.250/24	Azerty13!

1.2. Les dispositifs

1.2.1. Routeur (PfSense)

Notre routeur est une solution **PfSense**, un pare-feu réseau polyvalent qui offre une gamme de fonctionnalités avancées. Il assure une protection contre les menaces, facilite les connexions VPN sécurisées et simplifie la gestion du réseau pour les petites et moyennes entreprises.

1.2.2. Commutateur (Netgear GS108Ev3)

Notre commutateur, un **Netgear GS108Ev3**, se distingue par son interface graphique conviviale facilitant la configuration et la gestion du réseau. Il prend en charge les VLAN pour une segmentation efficace du réseau, et ses huit ports Gigabit garantissent des connexions rapides et fiables pour nos appareils.

1.2.3. Point d'accès (D-Link DAP-1360)

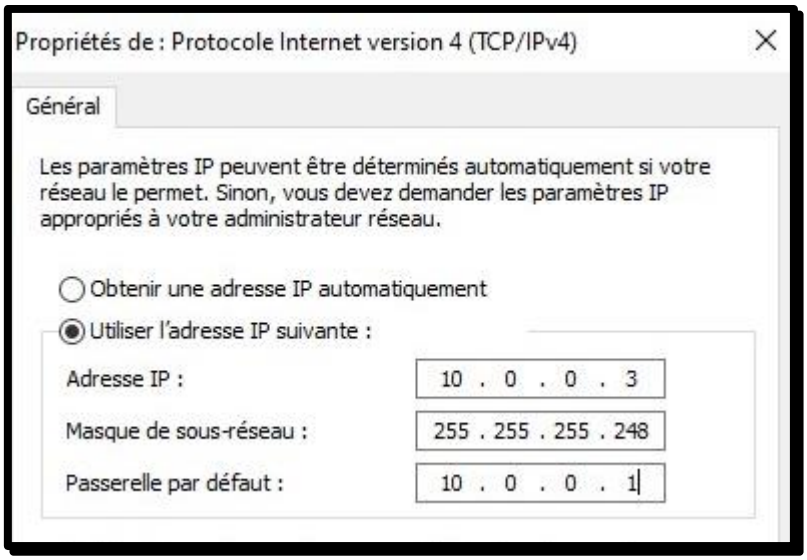
Enfin, notre point d'accès sans fil **D-Link DAP-1360** offre une connectivité rapide et sécurisée. Avec ses fonctionnalités avancées et sa facilité d'installation, il étend la portée de notre réseau sans fil et améliore la connectivité pour les utilisateurs.

2. Mise en place

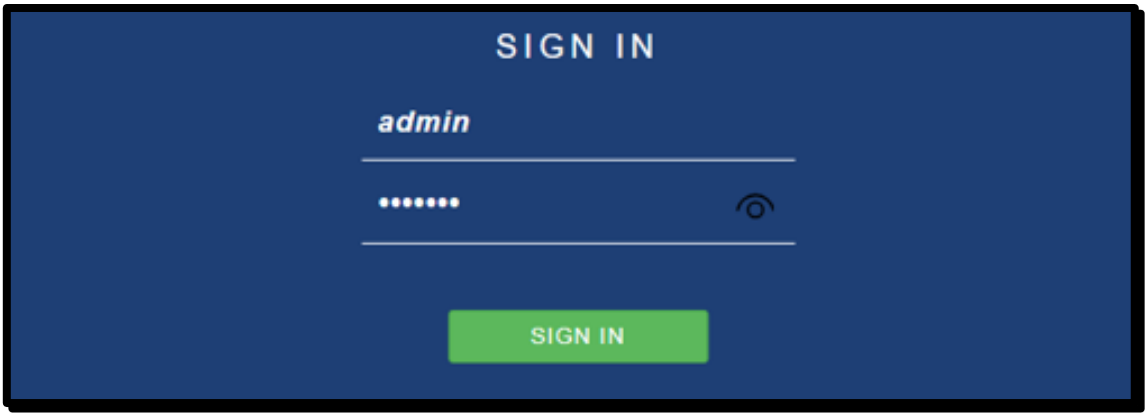
2.1. PfSense

2.1.1. Configuration Basique

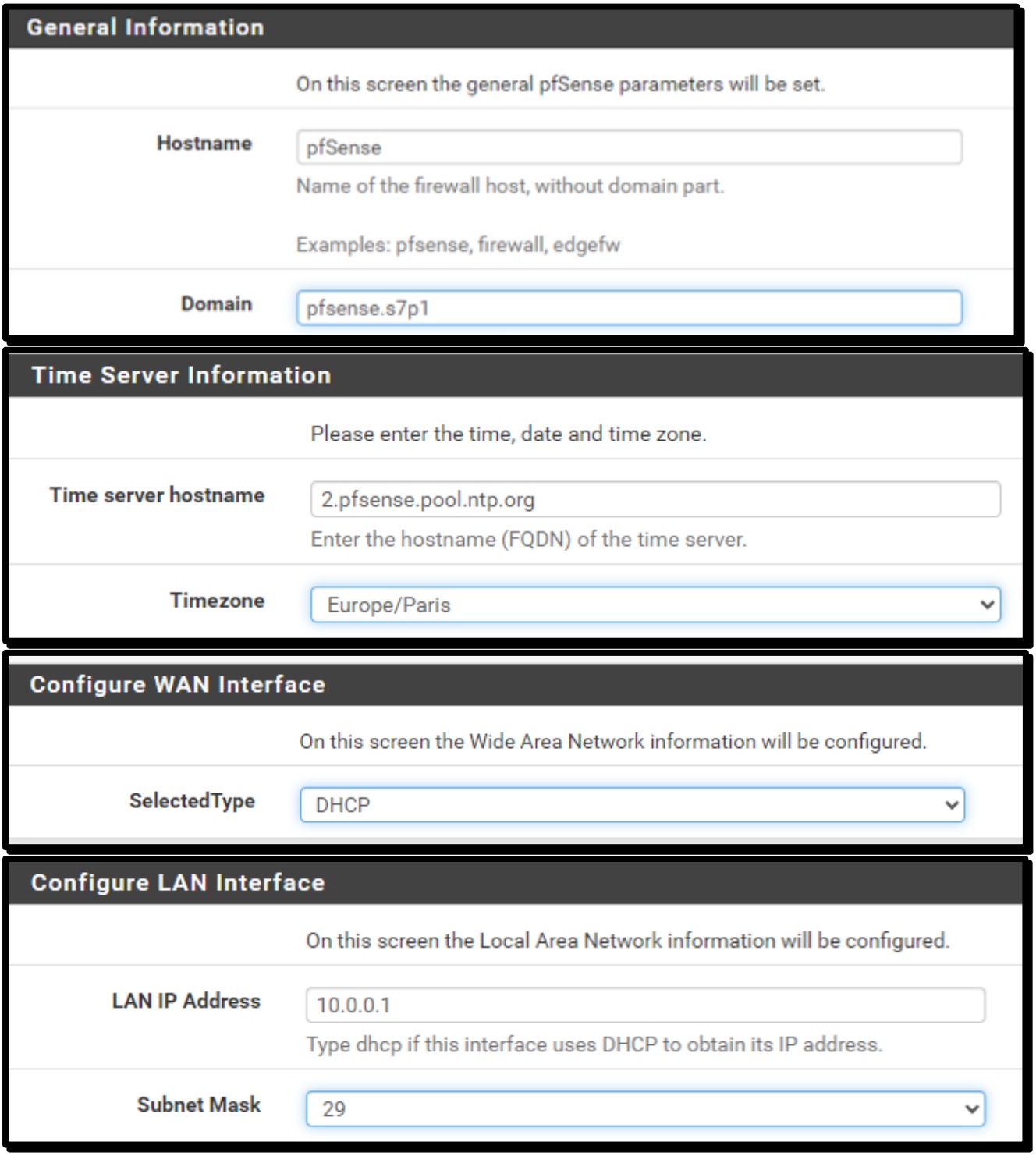
1. Après avoir installé pfSense, nous accédons à son interface web via l'adresse LAN (10.0.0.1) et les paramètres par défaut (admin/pfSense).



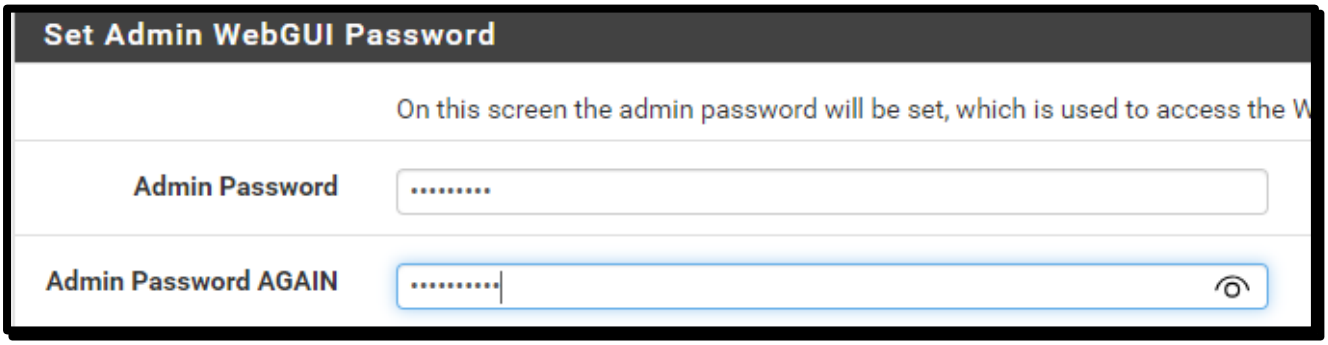
2. Après l'installation de pfSense, nous y accédons via l'interface web en utilisant l'adresse LAN (10.0.0.1) et les paramètres par défaut (admin/pfSense).



3. Dans l'interface, nous passons par le wizard de la configuration basique pour introduire les détails tels que le nom d'hôte, le domaine et le fuseau horaire.

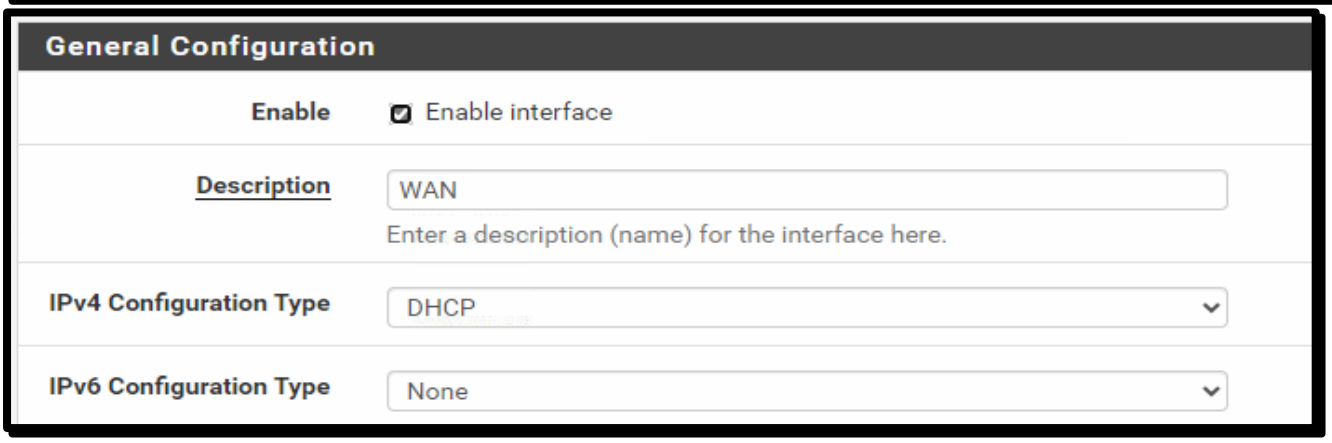


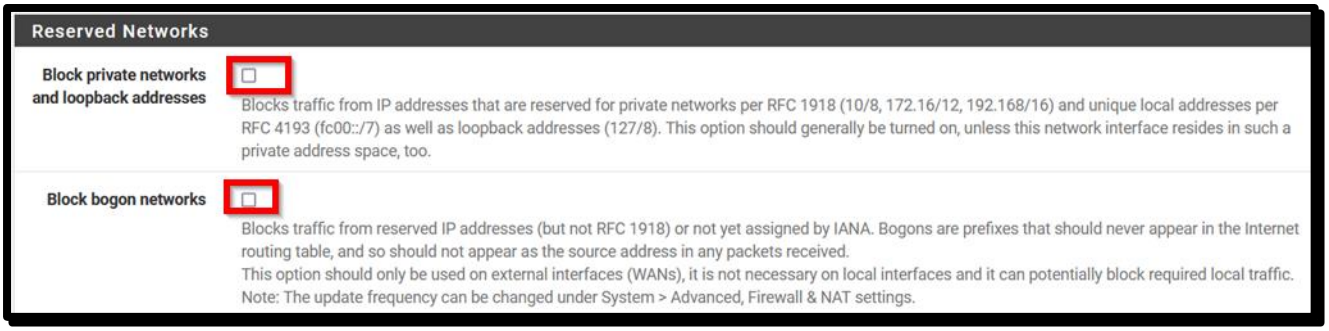
4. Nous personnalisons également le mot de passe (Azerty13!). La configuration basique de pfSense est alors complète.



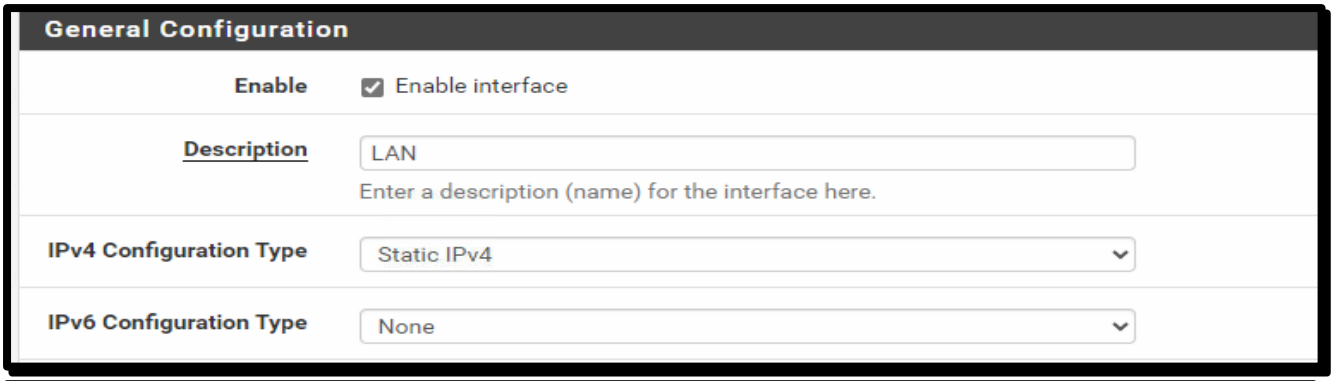
2.1.2. Configuration des cartes réseau

1. Configuration de la carte réseau WAN

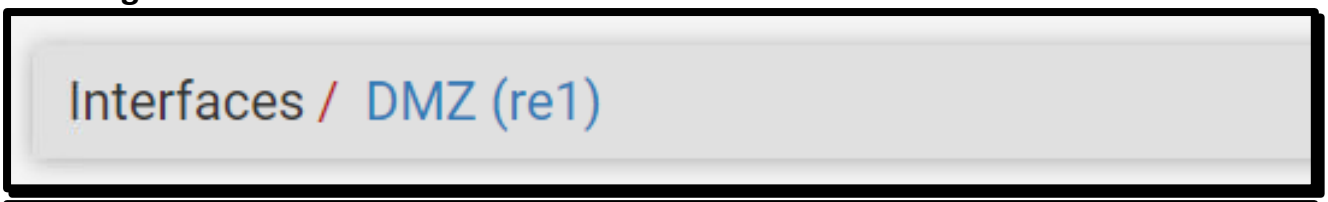


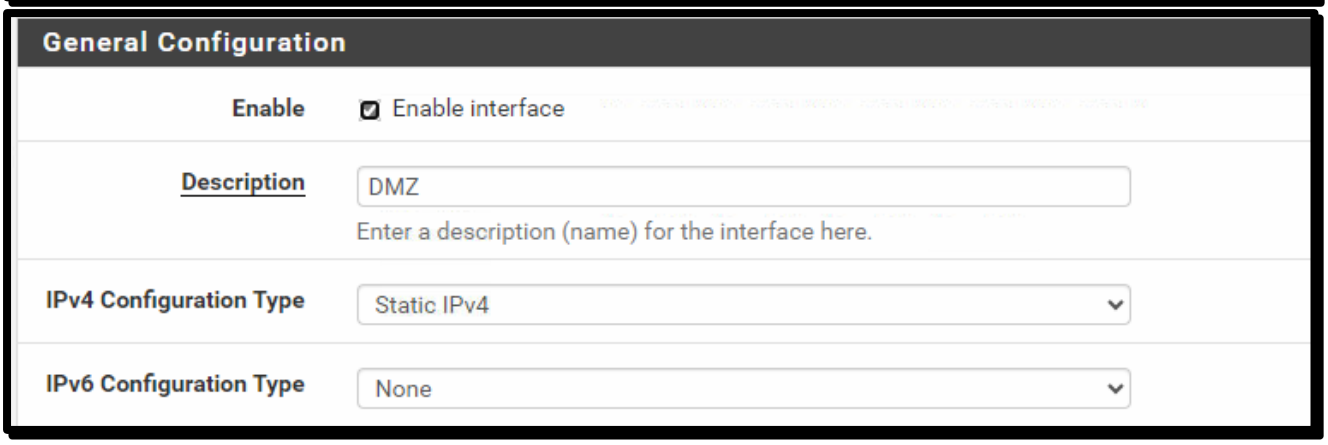


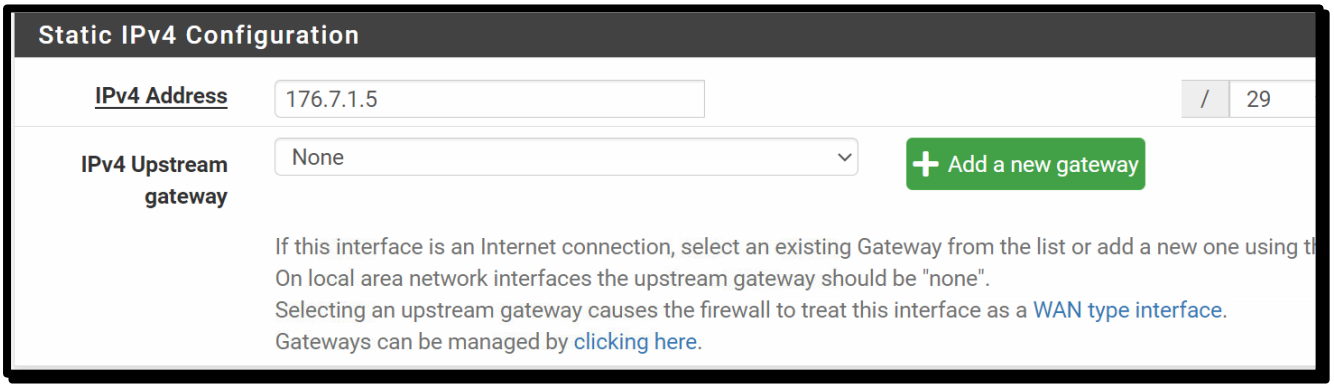
2. Configuration de la carte réseau LAN



3. Configuration de la carte réseau DMZ

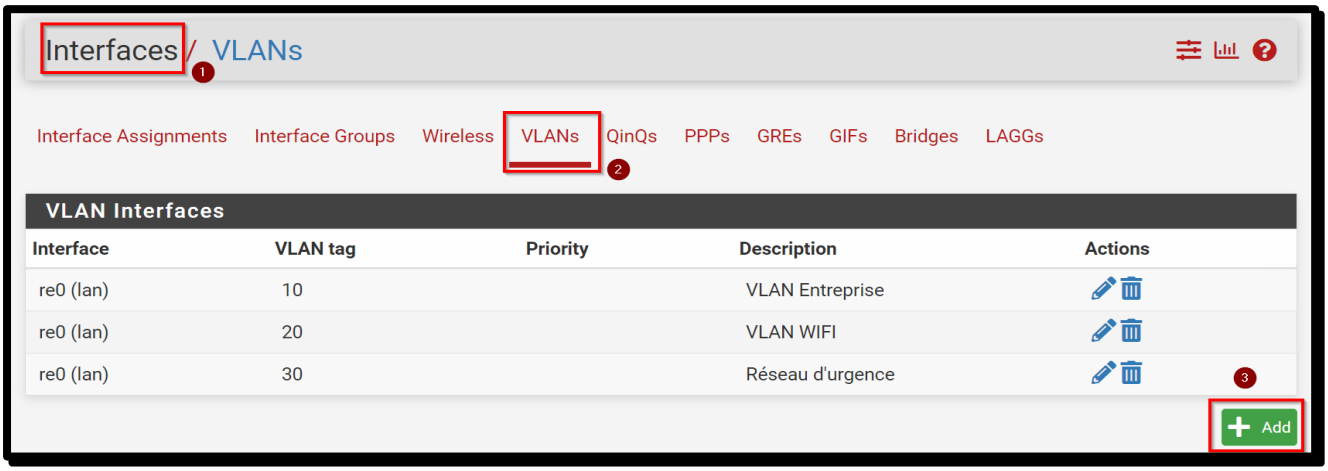




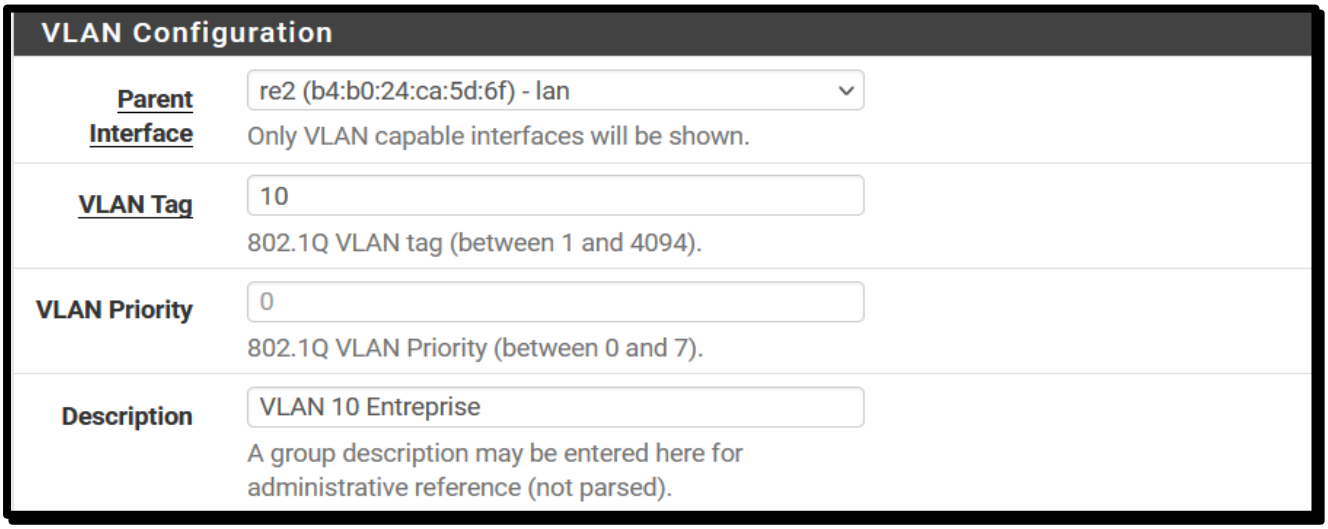


2.1.3. Configuration des VLANs sur pfSense

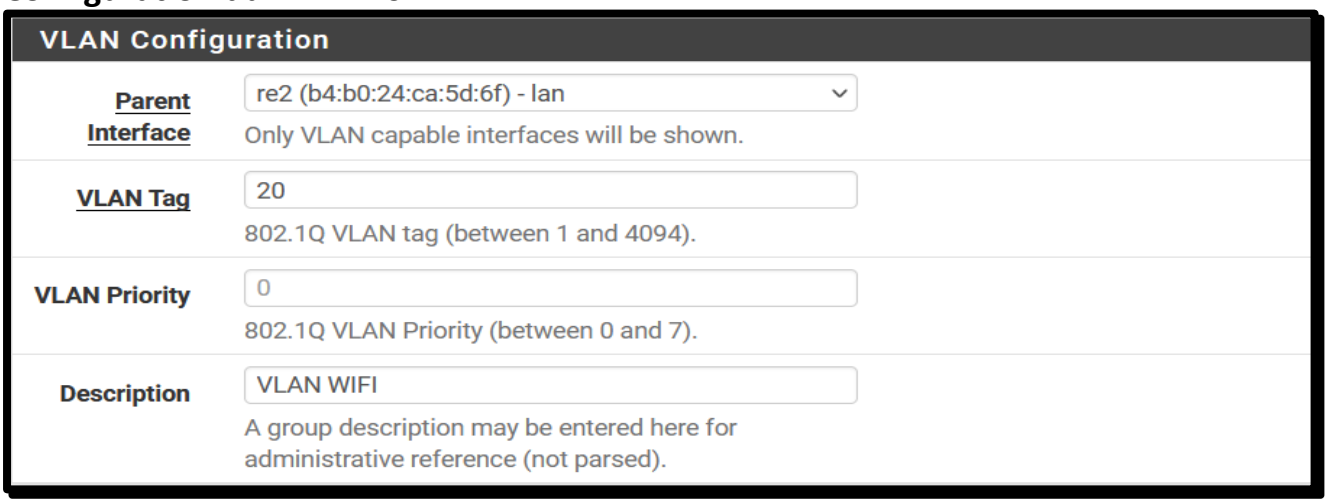
1. Nous configurons les interfaces réseaux virtuels dans **Interfaces** -> **Assignements** -> **VLANs**. Nous créons les **VLANs 10**, **20** et **30**.



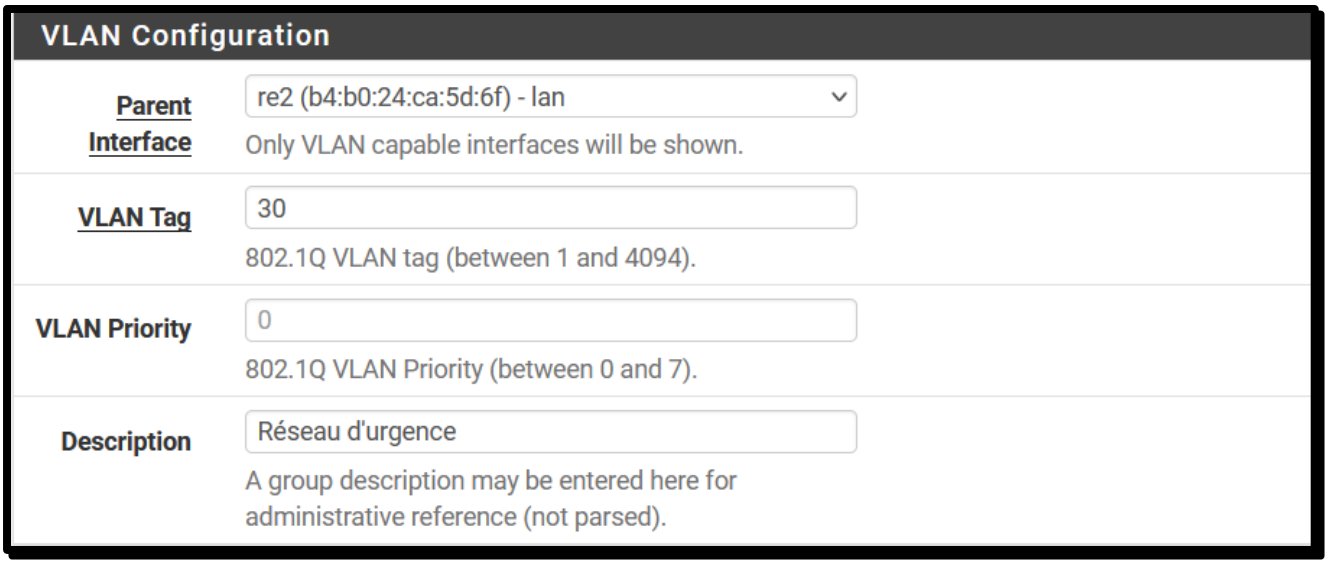
Configuration du VLAN 10 :



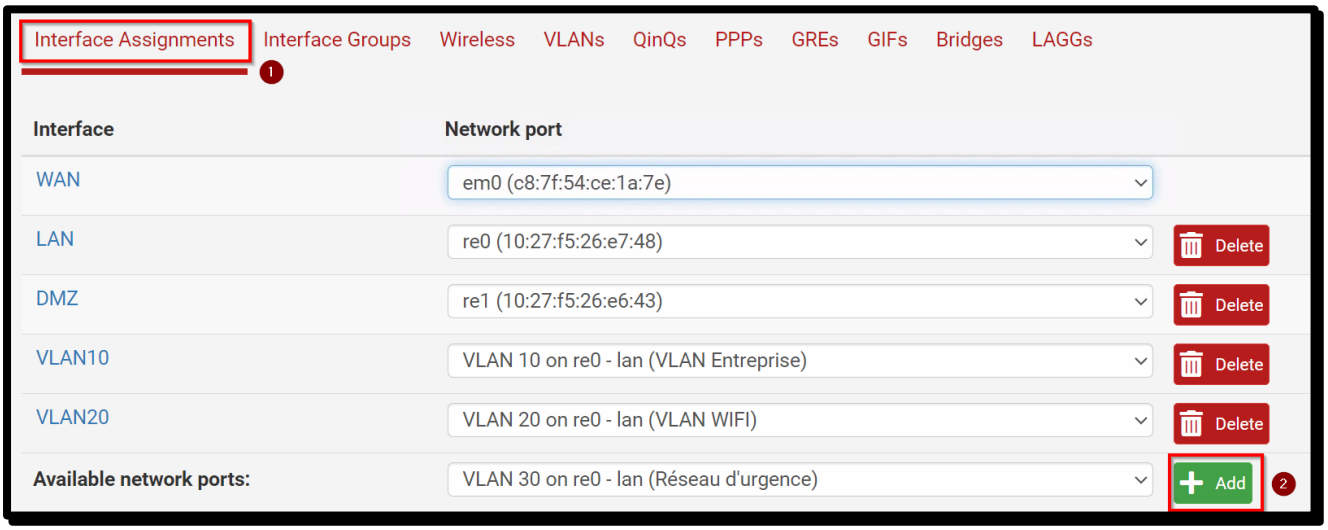
Configuration du VLAN 20



Configuration du VLAN 30

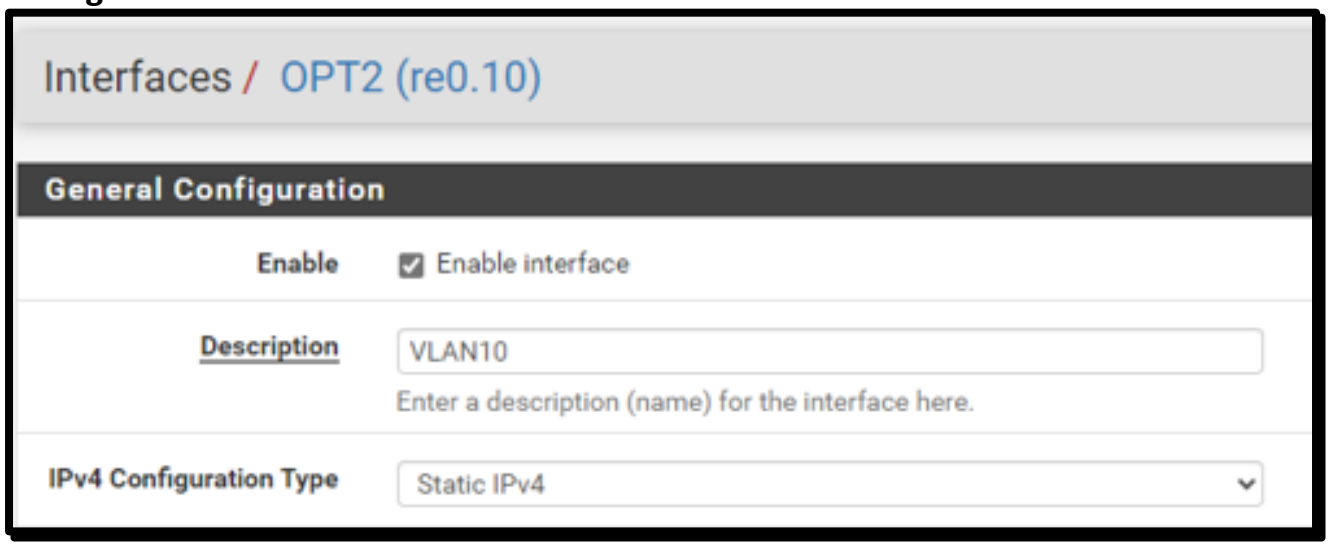


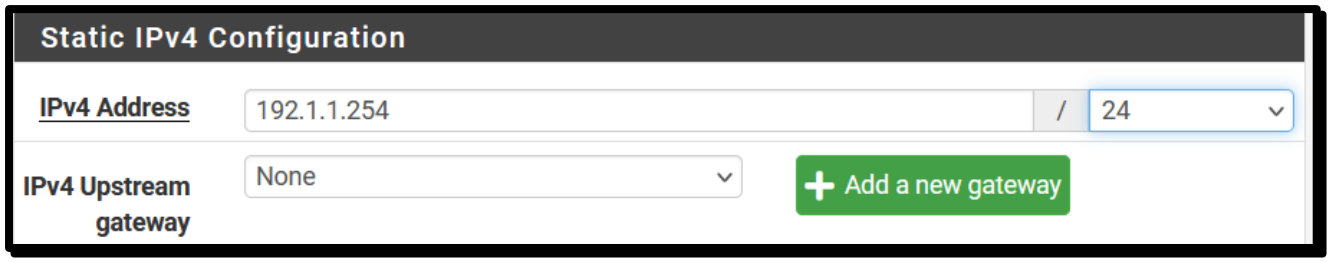
2. Activation des VLANs dans **Interface Assignements**.



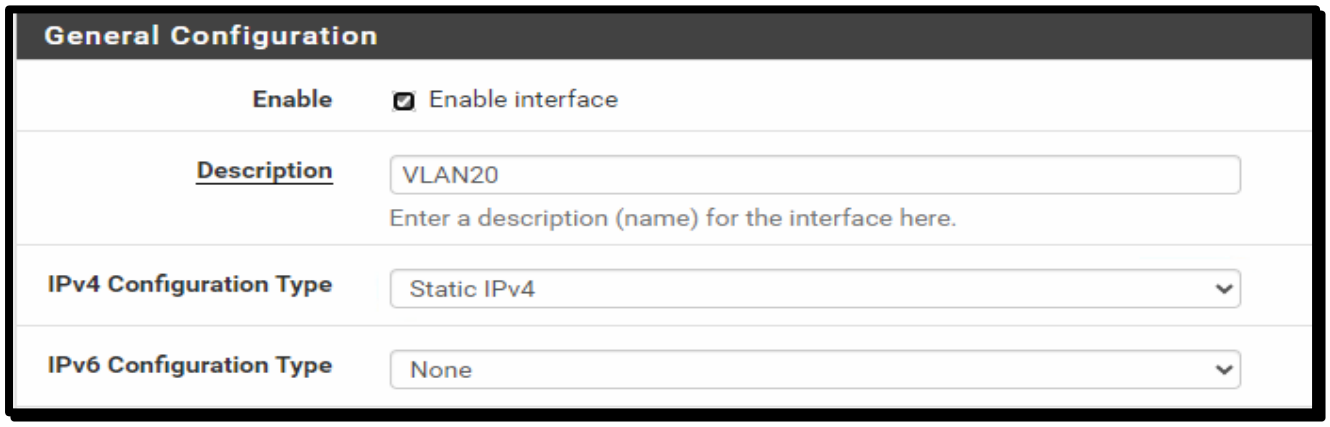
3. Finalement, nous allons configurer chacun des VLANs en leur cliquant dessus comme cela est indiqué ici :

Configuration VLAN10

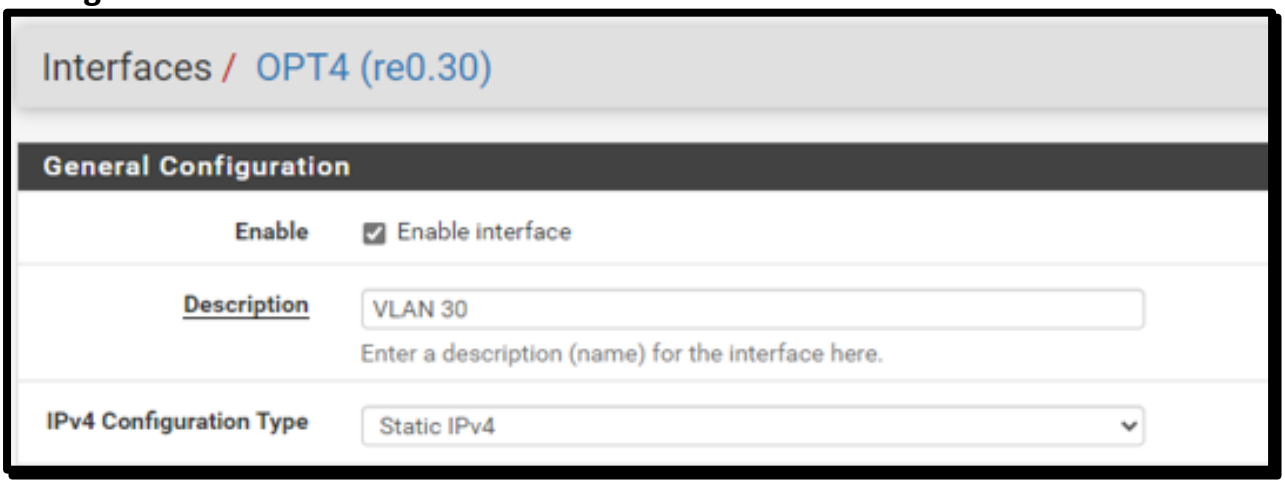




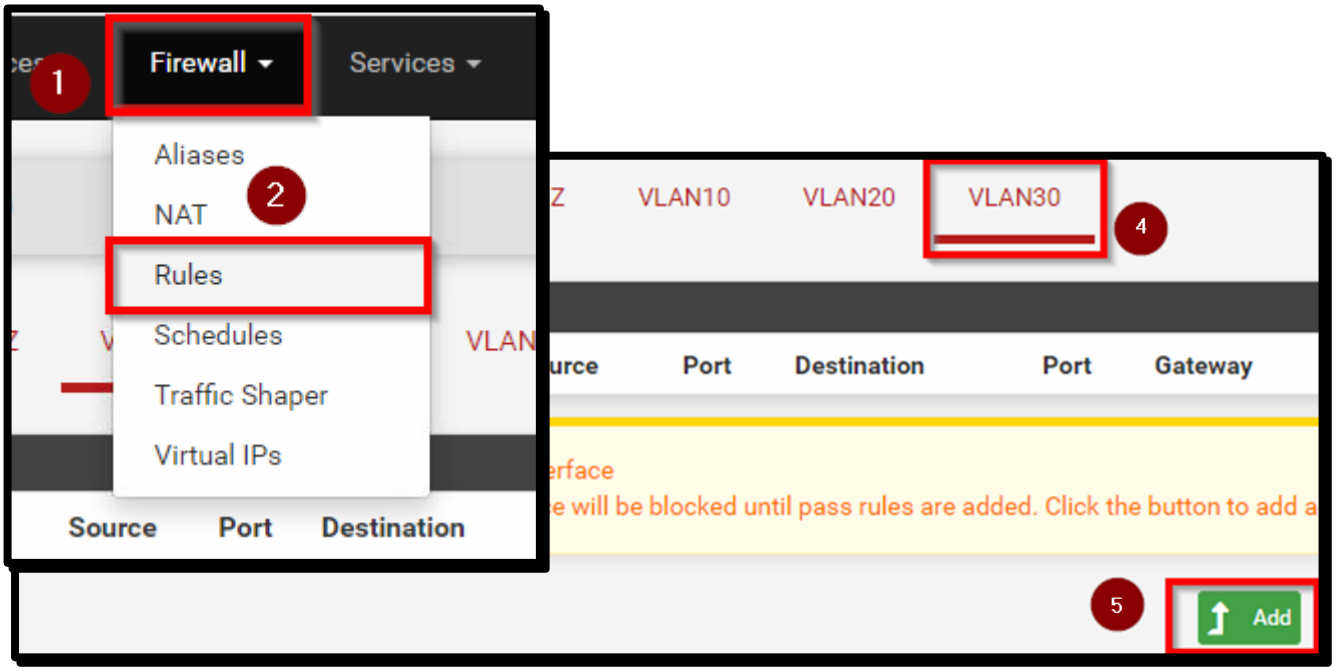
Configuration VLAN20



Configuration VLAN30

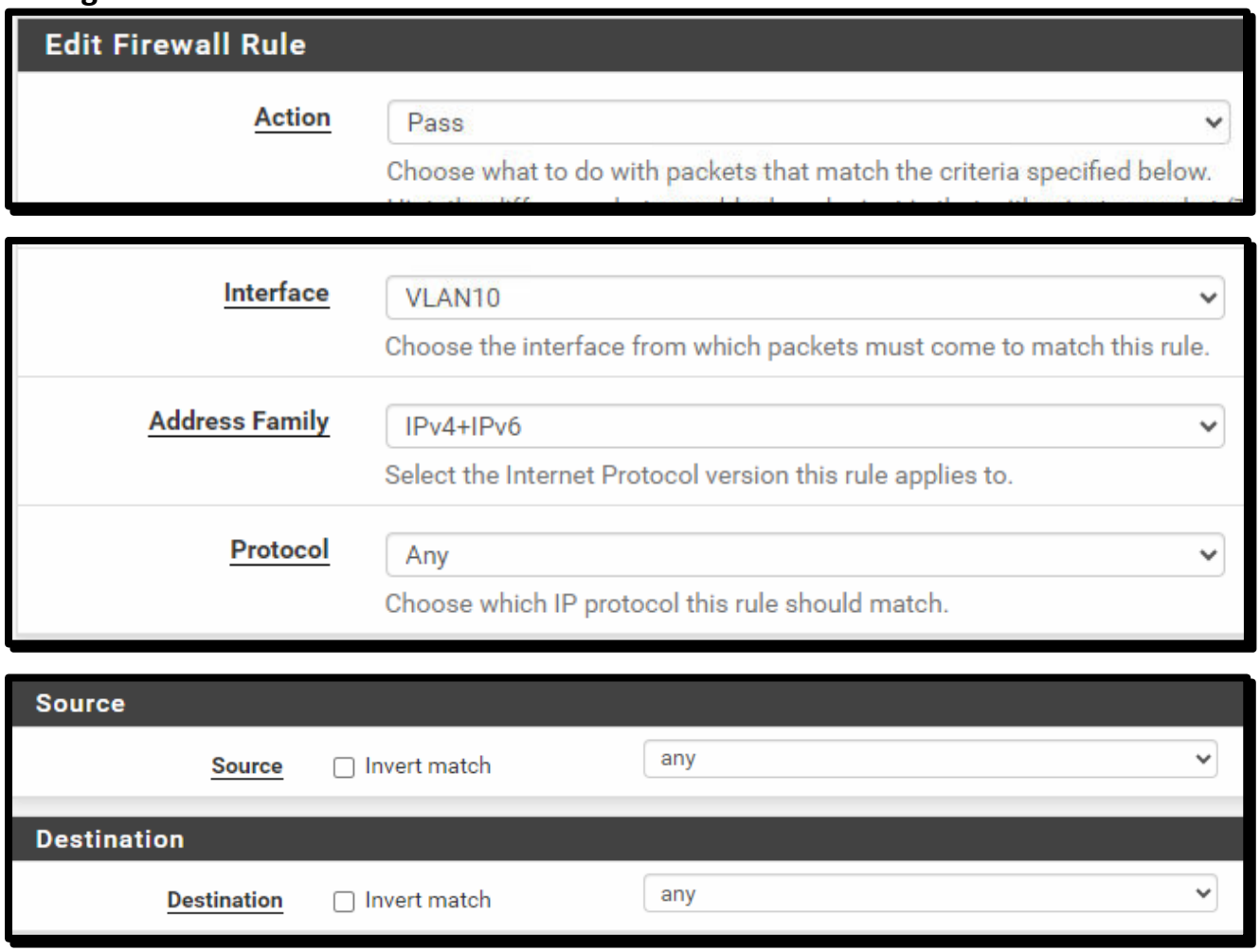


4. Après avoir activé les **VLANs** dans **Interface Assignements**, nous configurons chacun d'entre eux en définissant les règles nécessaires dans **Firewall** -> **Rules**.

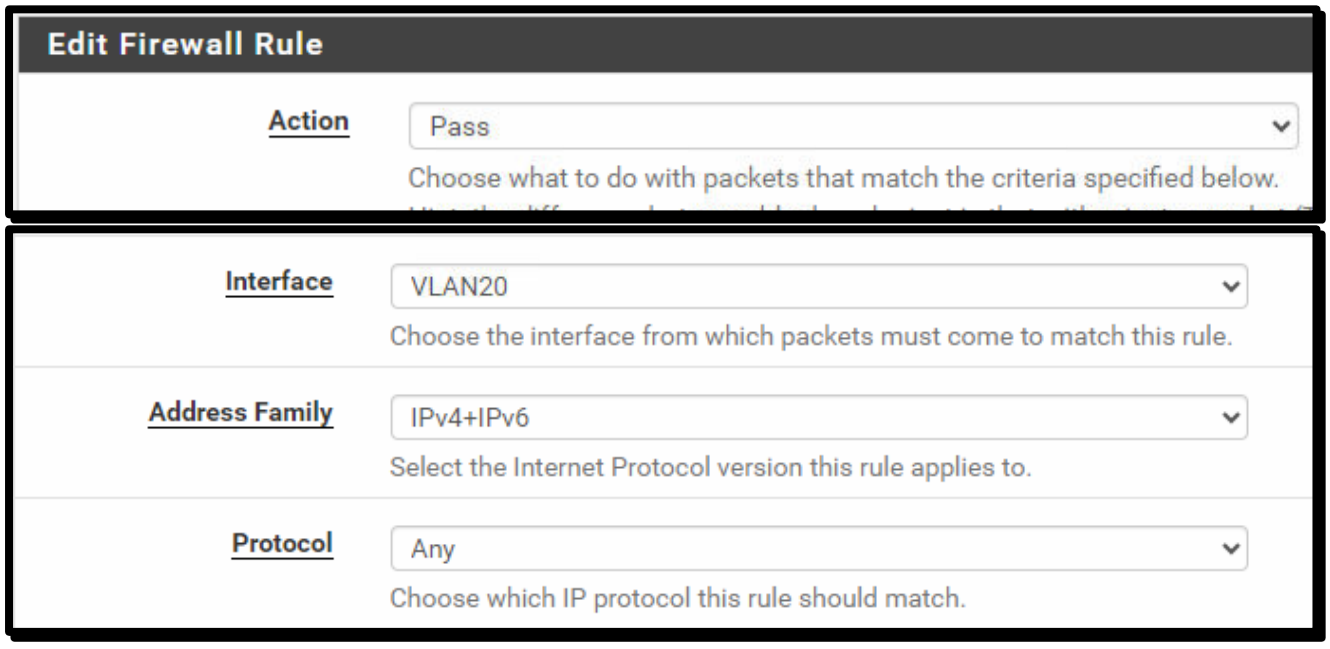


Ainsi nous configurons chacun de nos VLANs comme cela est indiqué ici :

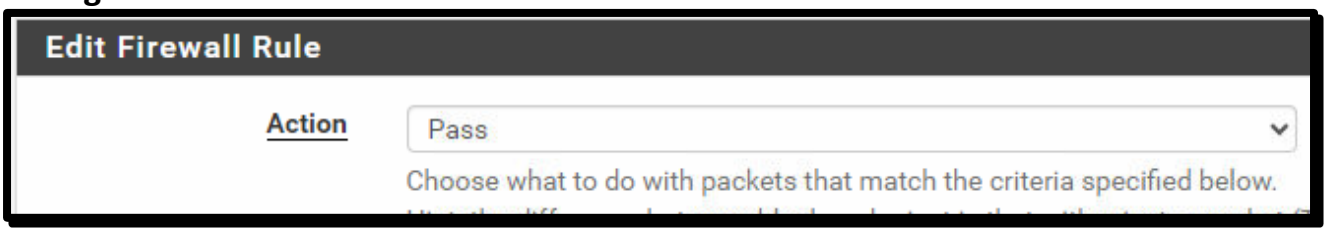
Configuration VLAN10

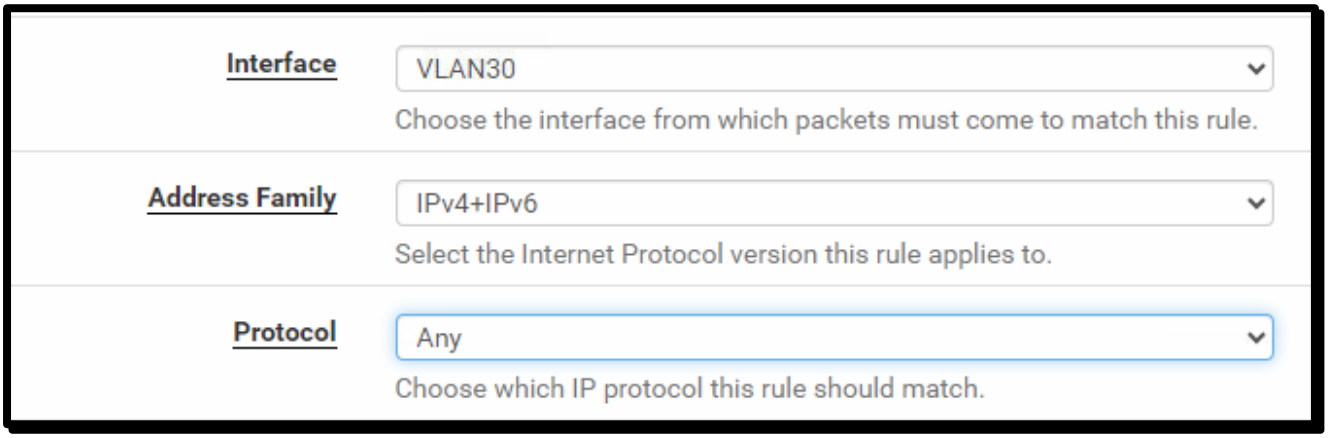


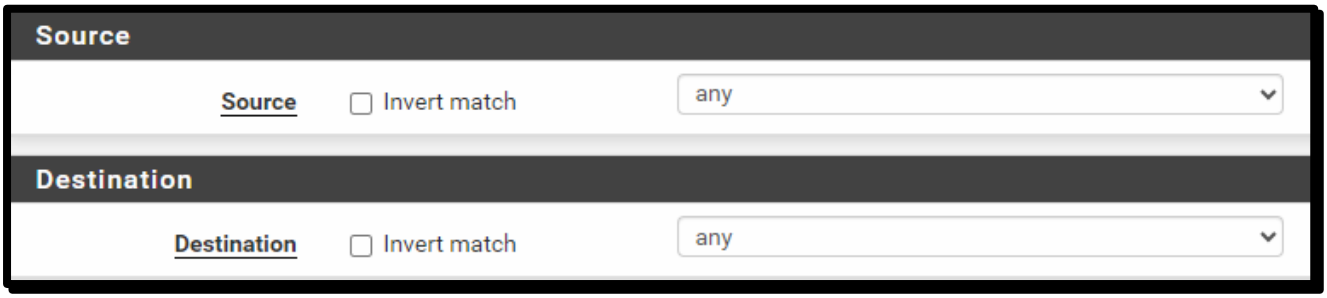
Configuration VLAN20



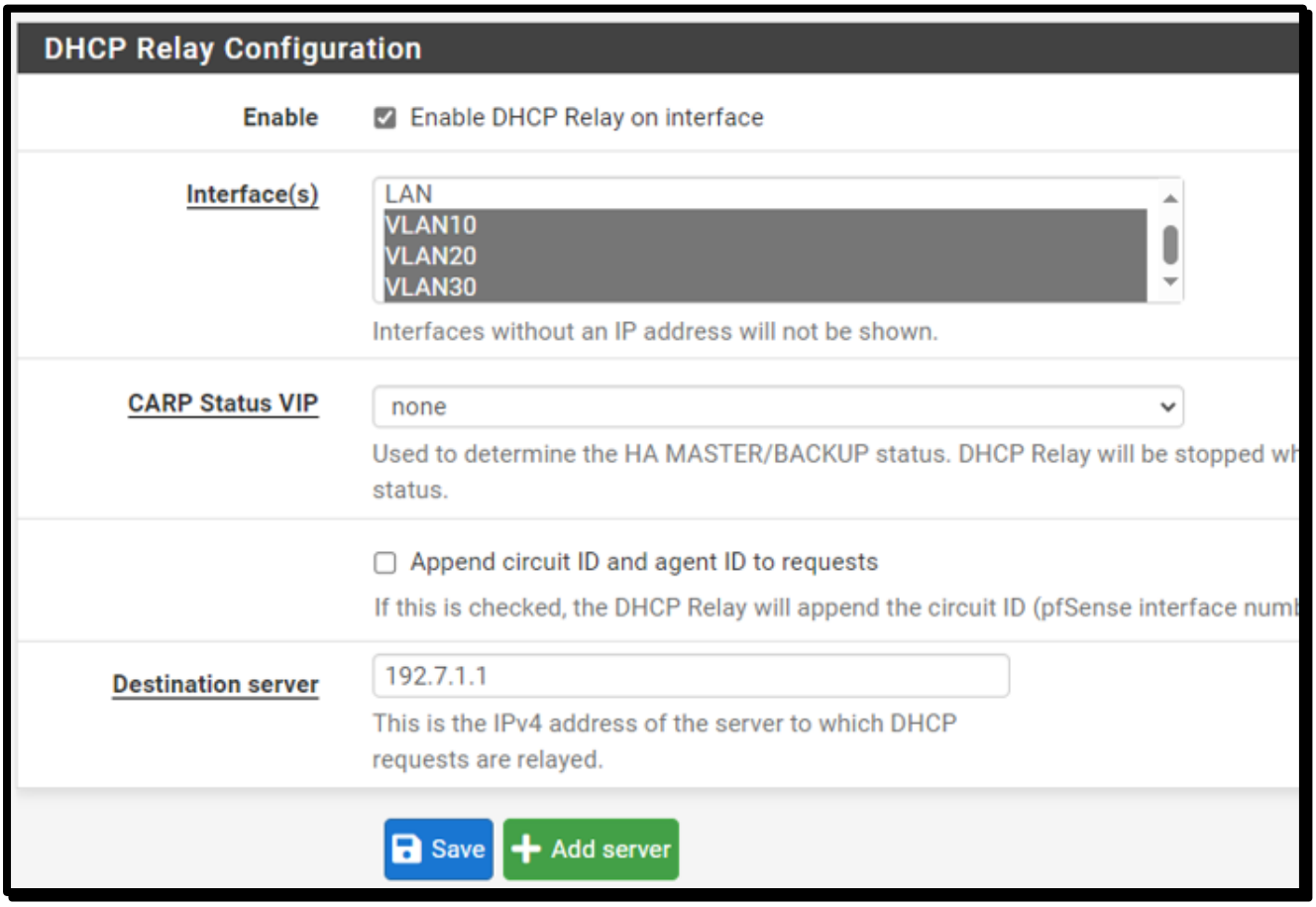
Configuration VLAN30



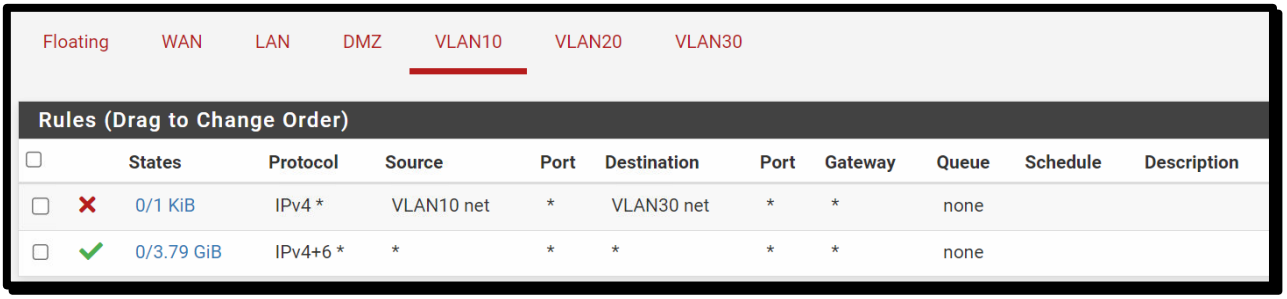


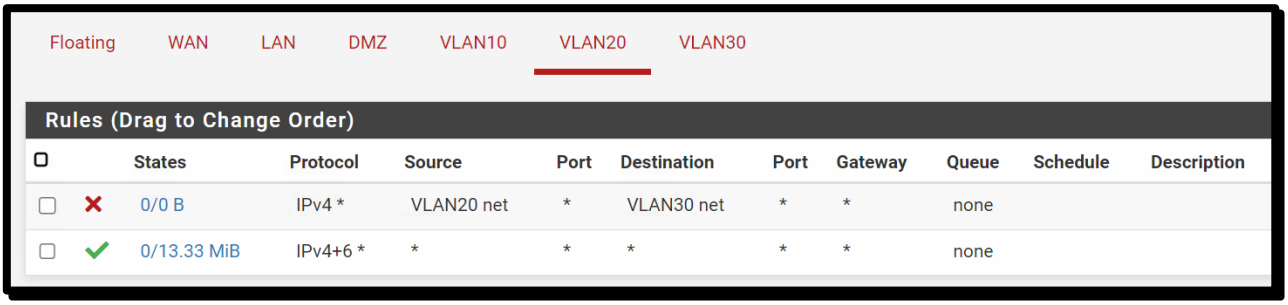


5. Nous ajoutons un DHCP Relay pour canaliser les plages d'adresses IP configurées sur notre serveur AD1 (**Services** -> **DHCP Relay**).



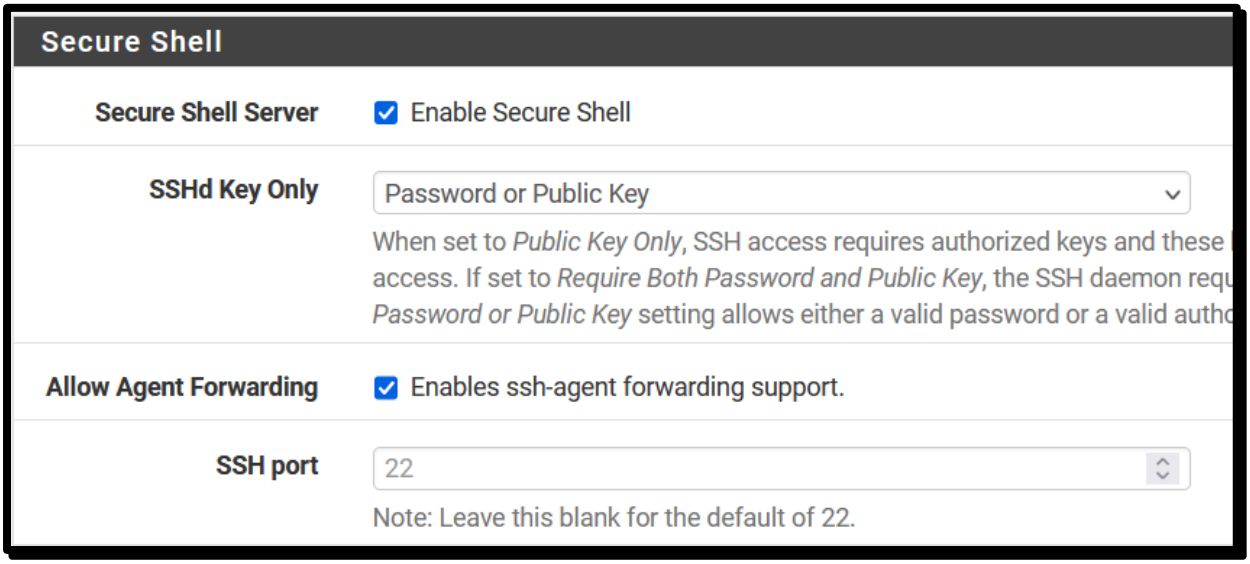
6. Nous interdisons la communication sortante depuis les **VLANs 20** et **10** vers le **VLAN 30** pour des raisons de sécurité.



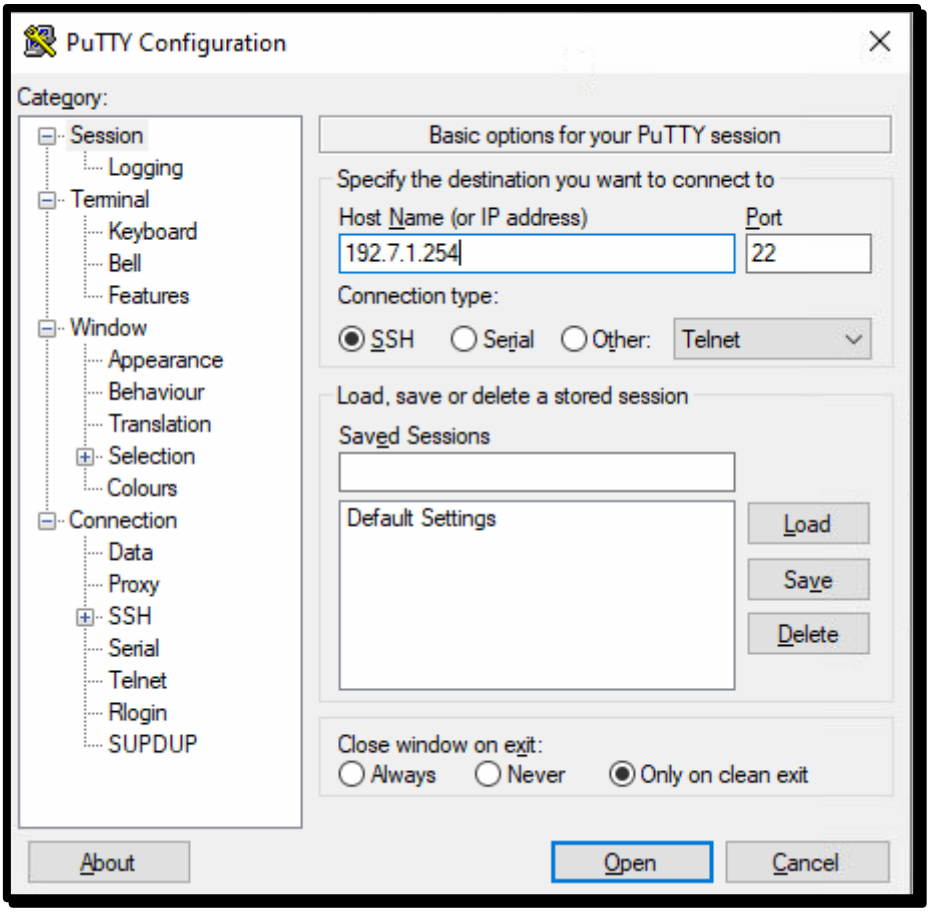


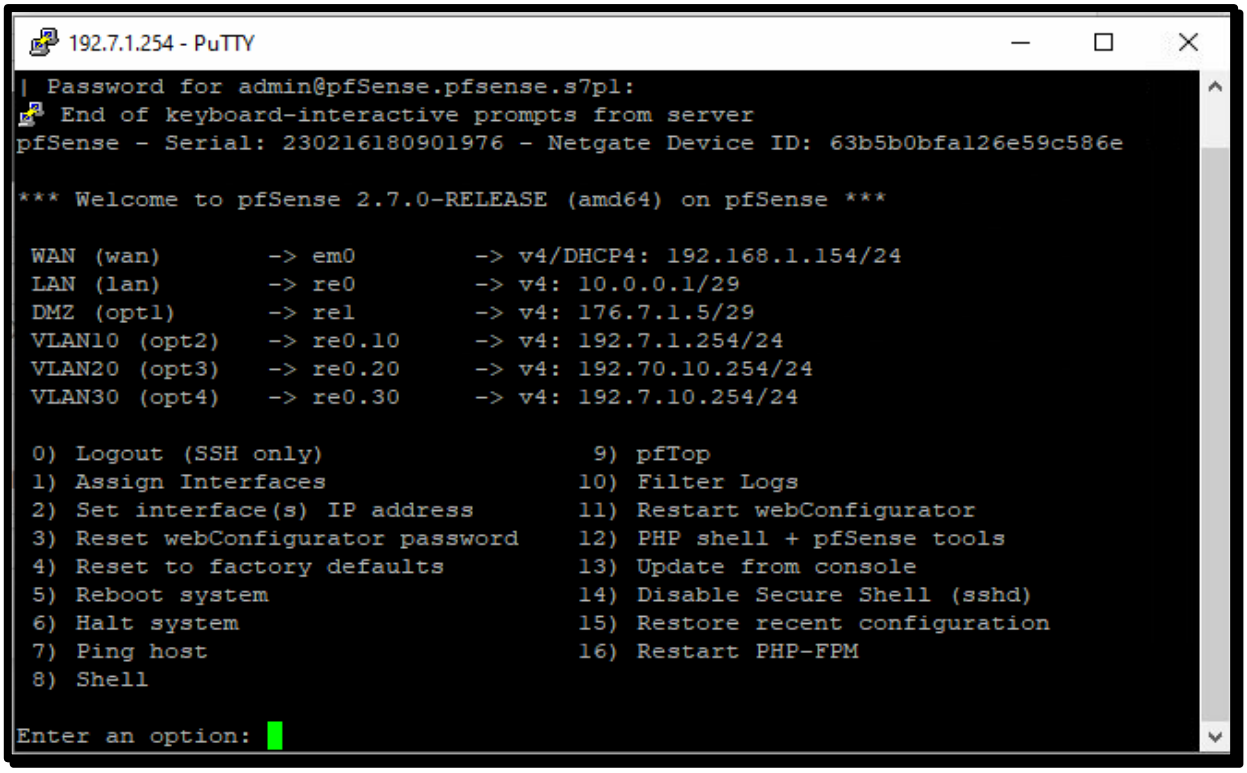
2.1.4. Configuration de la connexion en SSH

1. Pour accéder à pfSense via SSH, nous configurons cette fonctionnalité dans **System** -> **Advanced** -> **Admin Access**.



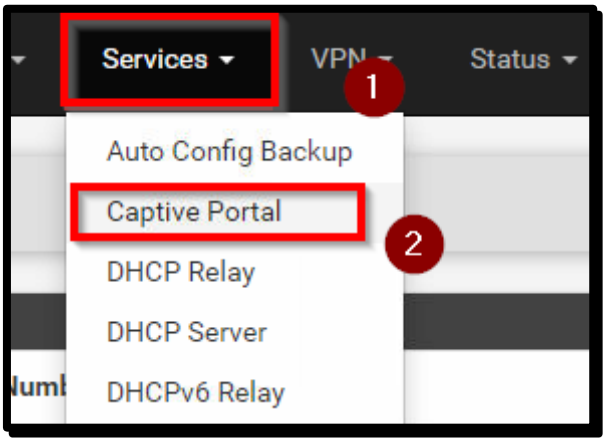
2. Après avoir configuré l'accès SSH côté pfSense, nous y accédons via un outil tel que PuTTY.





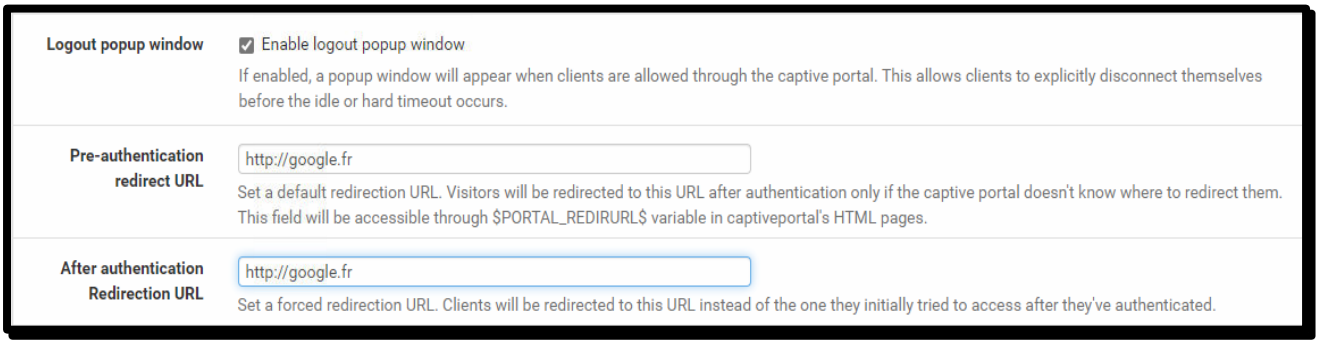
2.1.5. Configuration de Portail Captif

1. Pour configurer le portail captif, nous nous rendrons dans **Services -> Captive Portal -> Add**

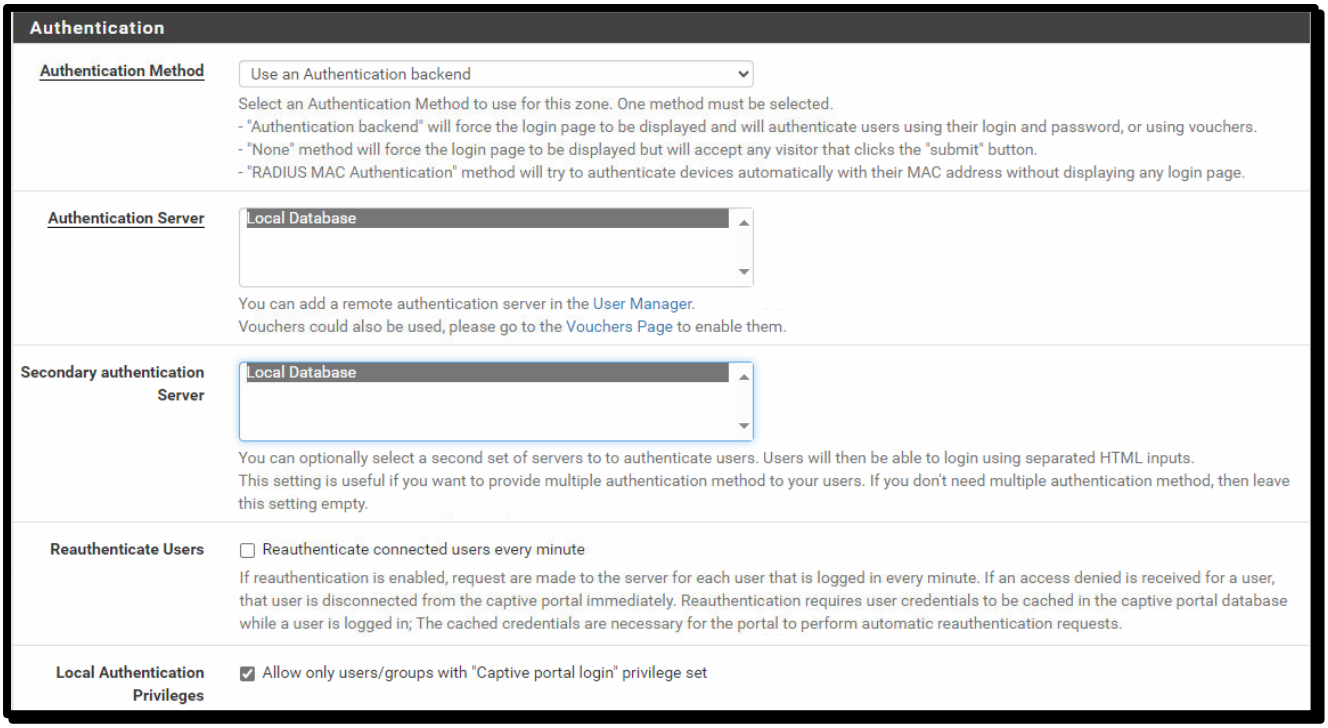


2. Nous configurons l'interface réseau sur laquelle le portail captif sera utilisé (dans notre cas, VLAN20).

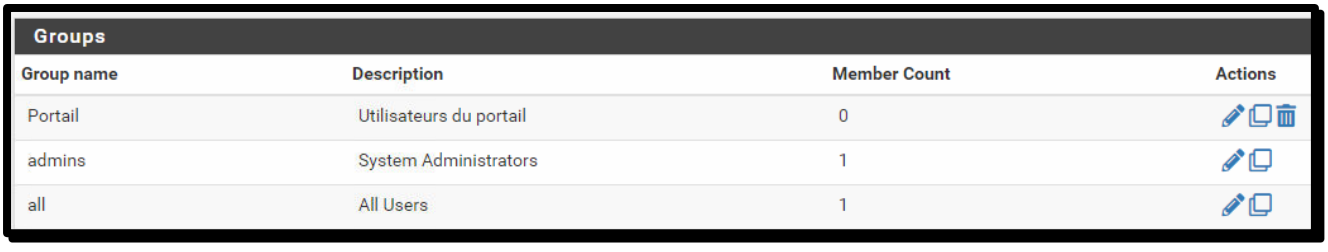
3. Nous activons une fenêtre contextuelle ainsi que le site par défaut, dans notre cas Google.



4. Ensuite, nous configurons le serveur d'authentification.

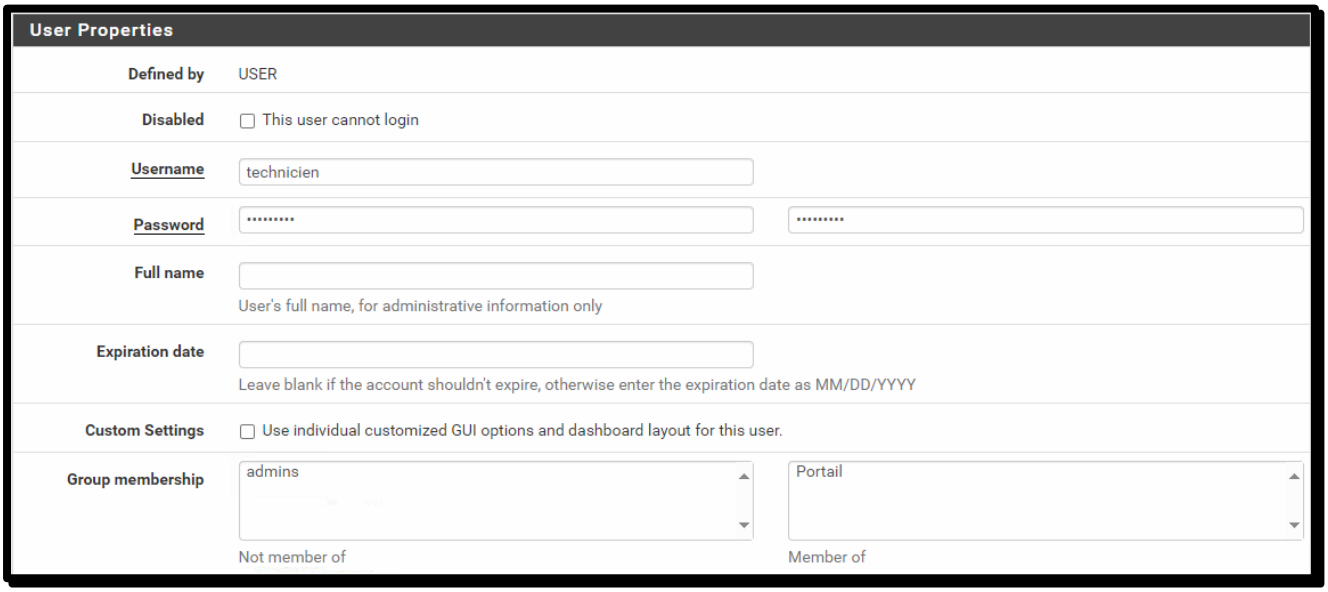


5. Nous ajoutons le groupe d'utilisateurs ayant accès au portail captif (**System** -> **User Manager** -> **Groups** -> **Add**) et nous lui attribuons les privilèges nécessaires.



Nous la modifions pour qu'elle aurait les privilèges de « **User – Services: Captive Portal login »**

6. Enfin, nous créons un profil utilisateur qui aura les droits d'accès au portail captif (**System** -> **User Manager** -> **User**).

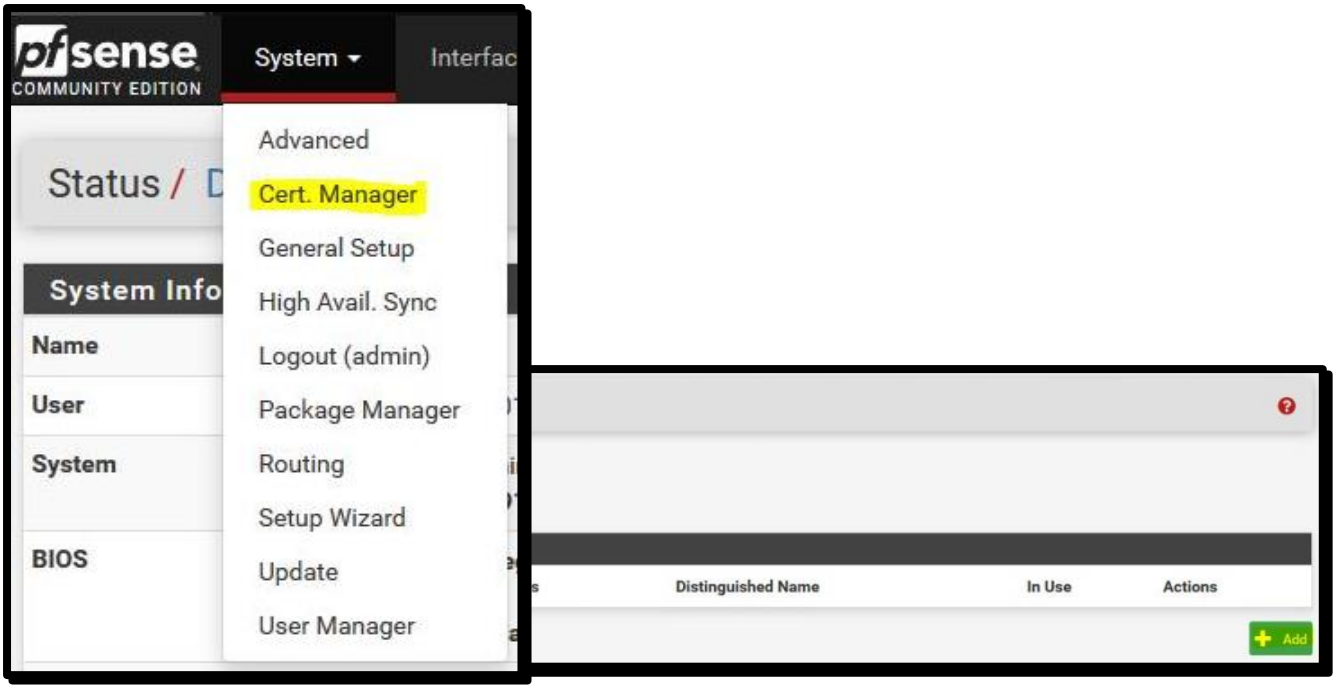


2.1.6. Configuration du VPN

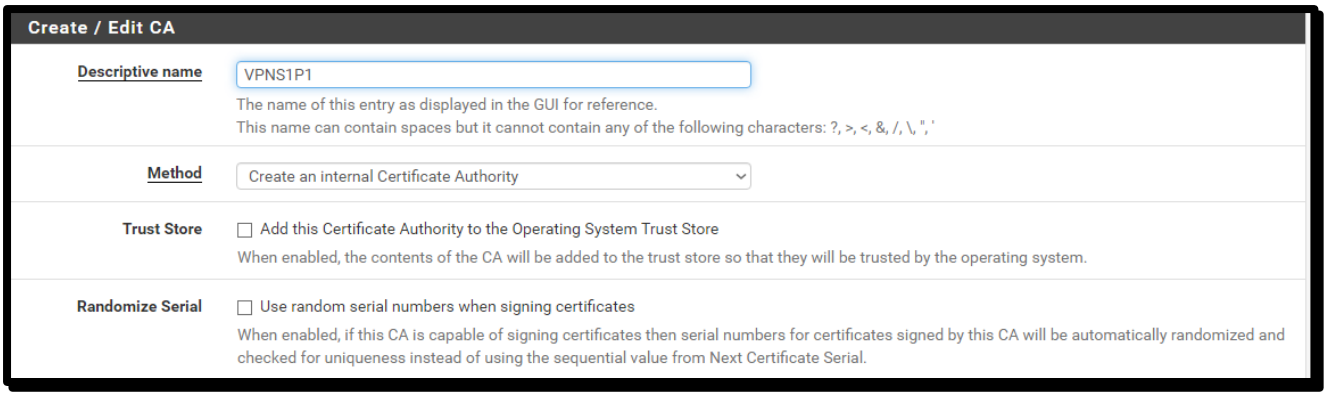
Pour accéder à distance à notre réseau, nous allons configurer l'accès via un VPN (Réseau Virtuel Privé), qui nous offre un accès sécurisé.

2.1.6.1 Création d'autorité de certificat

1. Accédez à **Système** -> **Cert**. **Manager**, puis cliquez sur "**Add**" pour créer un certificat nécessaire pour le VPN.



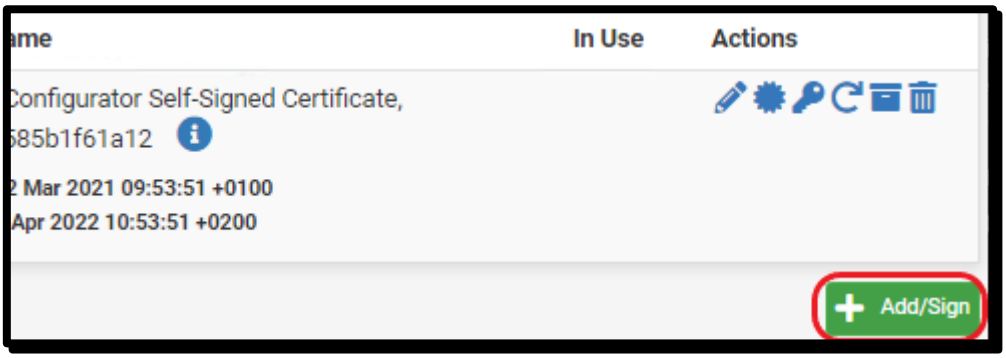
2. Choisissez un nom pour votre autorité de certification, par exemple "**VPNS1P1**", et conservez les autres paramètres par défaut. Enregistrez ensuite.



Voici le certificat que nous venons de créer :

2.1.6.2 Création de certificat

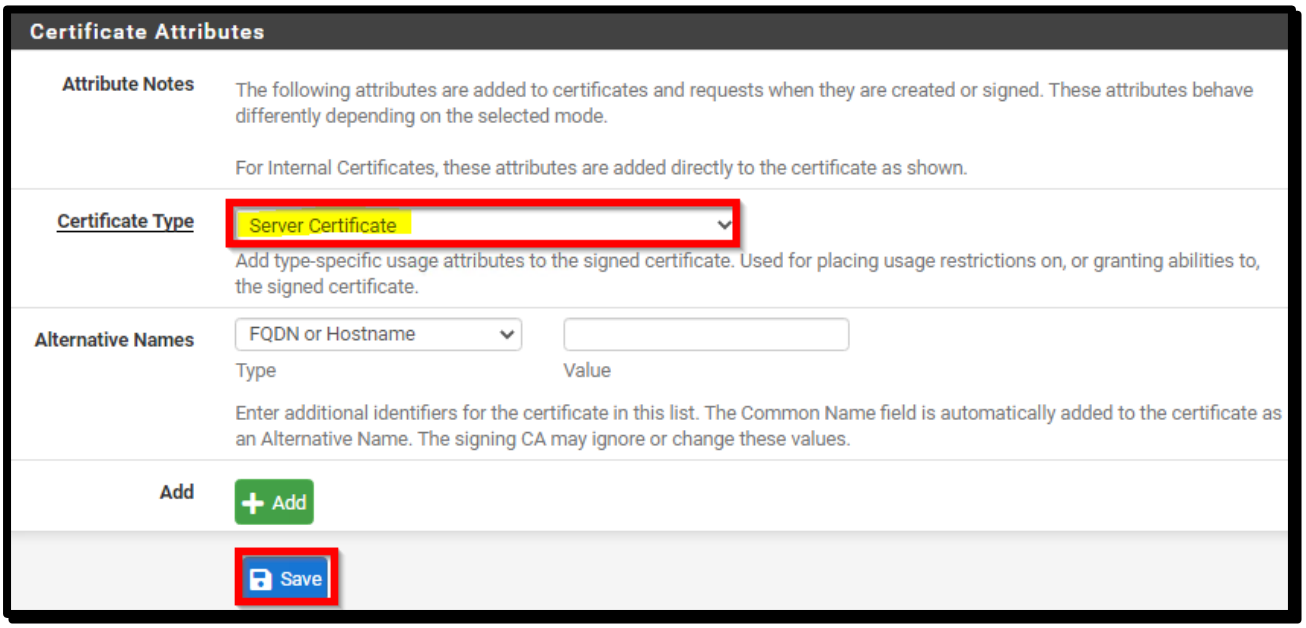
1. Sous l'autorité de certification créée précédemment, cliquez sur "**Add/Sign**" pour créer un certificat.



2. Sélectionnez "**Certificat interne**" comme méthode et nommez-le, par exemple, "**Certificat VPN**".

3. Choisissez l'autorité de certification que vous avez créée précédemment.

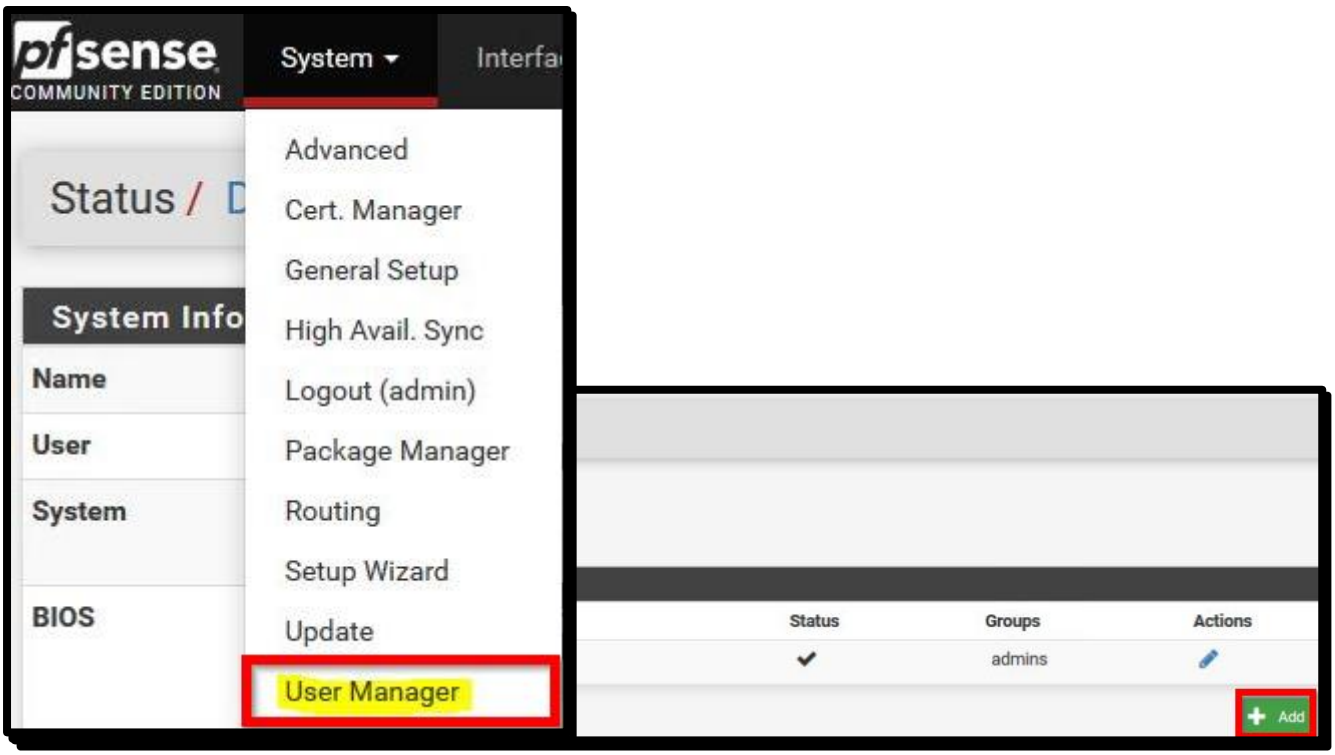
4. Configurez le type de certificat comme étant "**Certificat de serveur**" et enregistrez-le.



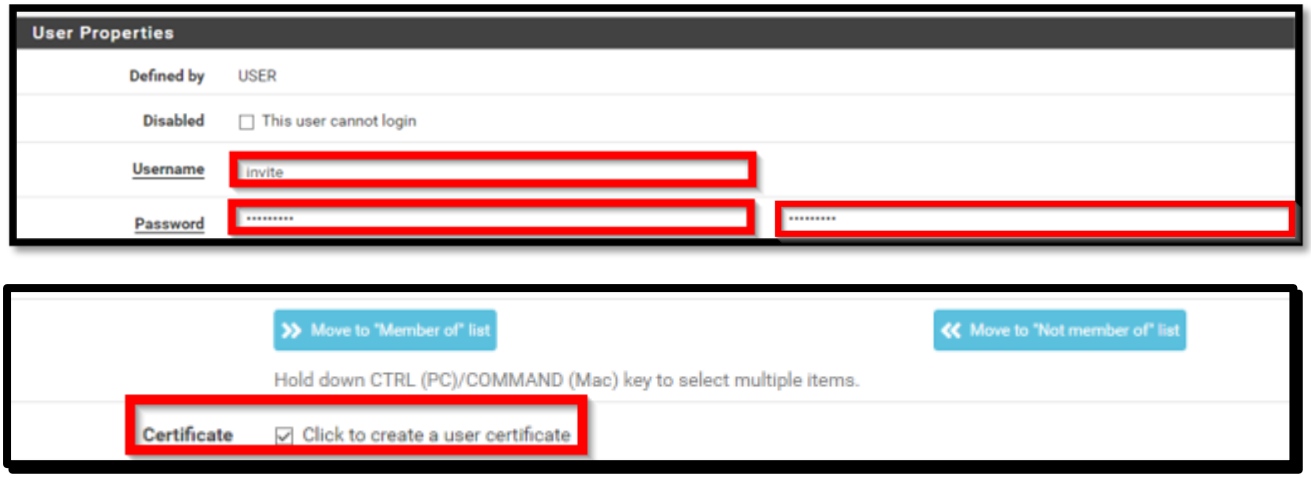
Voici notre certificat que nous venons de créer :

2.1.6.3 Création des Utilisateurs du VPN

1. Accédez à **Système** -> **User Manager** et cliquez sur "**ADD**" pour ajouter des utilisateurs VPN.



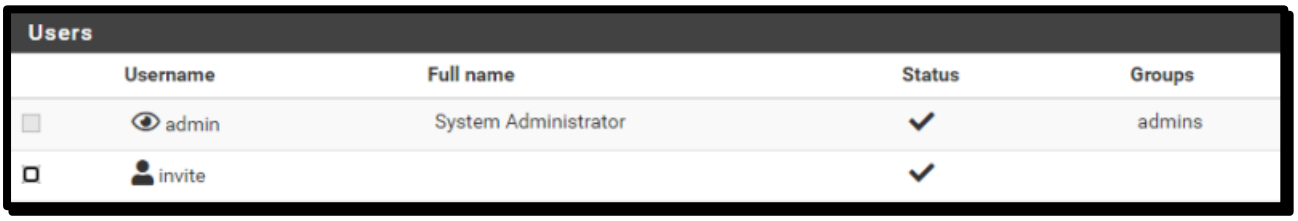
2. Saisissez l'identifiant de l'utilisateur et le mot de passe, puis cochez "**Créer un certificat utilisateur**".



3. Saisissez le nom du certificat et sélectionnez l'autorité de certification précédemment créée. Enregistrez les paramètres.

Puis nous cliquons sur le bouton **Save**.

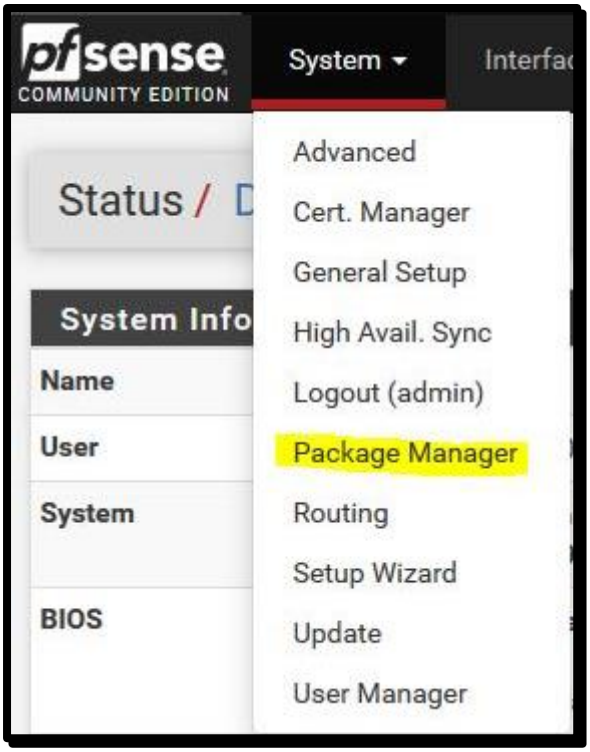
Voici l'utilisateur du VPN que nous venons de créer :

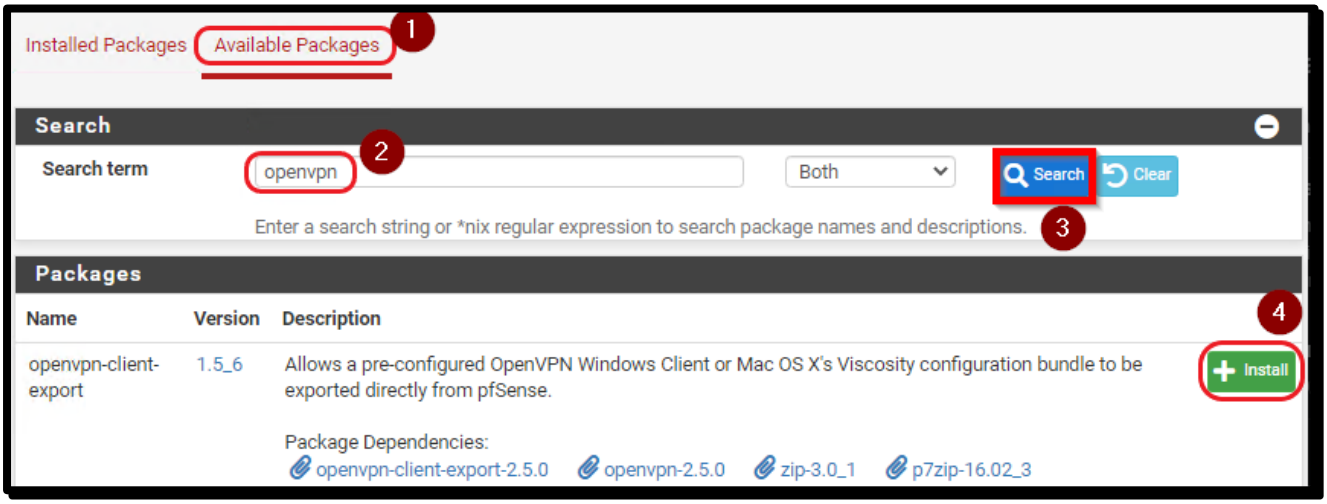


2.1.6.4 Installation et configuration du serveur OpenVPN

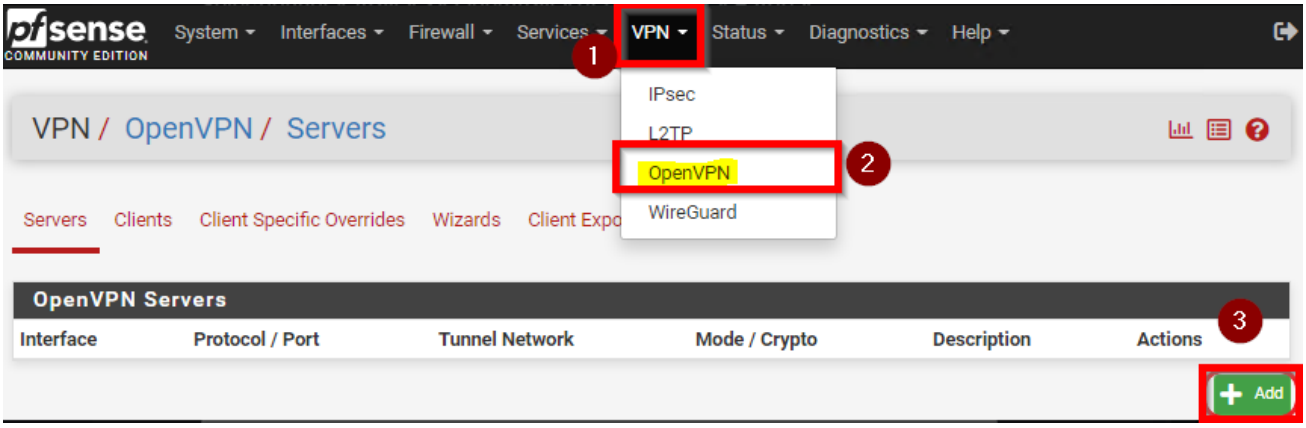
Il s'agit d'un utilitaire pour exporter la configuration client au format .ovpn.

1. Allez dans **Système** -> **Gestionnaire de paquets** -> **Paquets disponibles**, recherchez "**openvpn**" et installez-le.

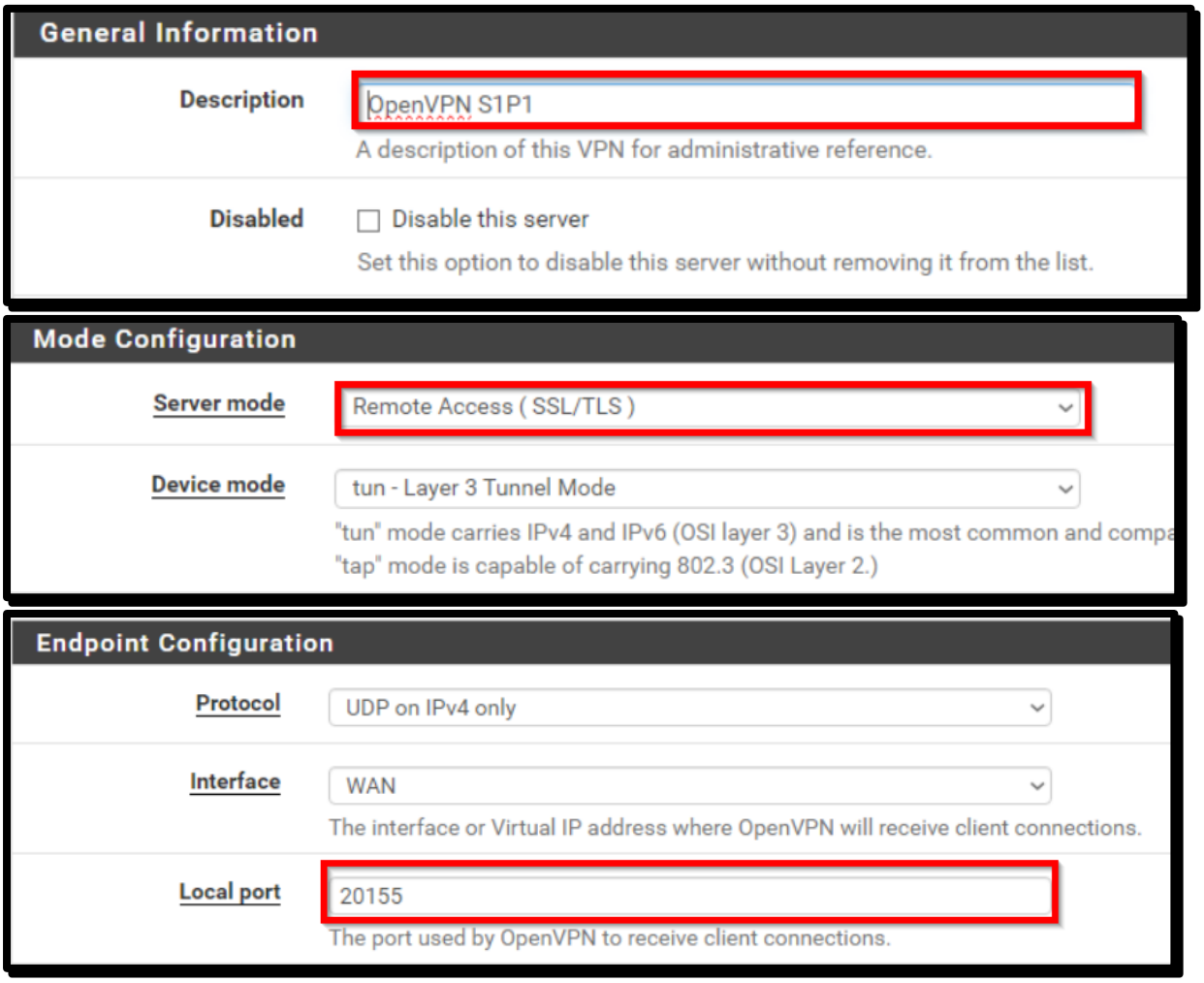




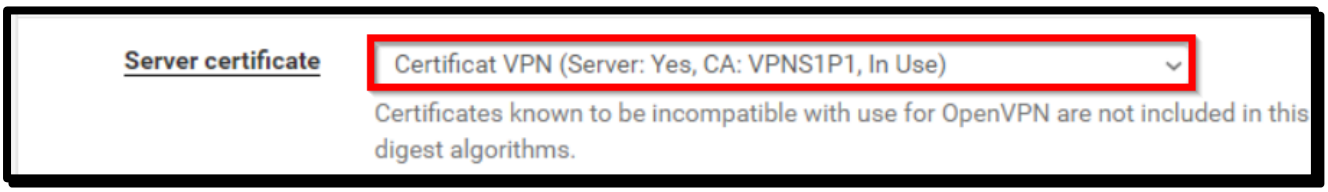
2. Configurez le serveur en allant dans **VPN** -> **OpenVPN** -> **Ajouter**.



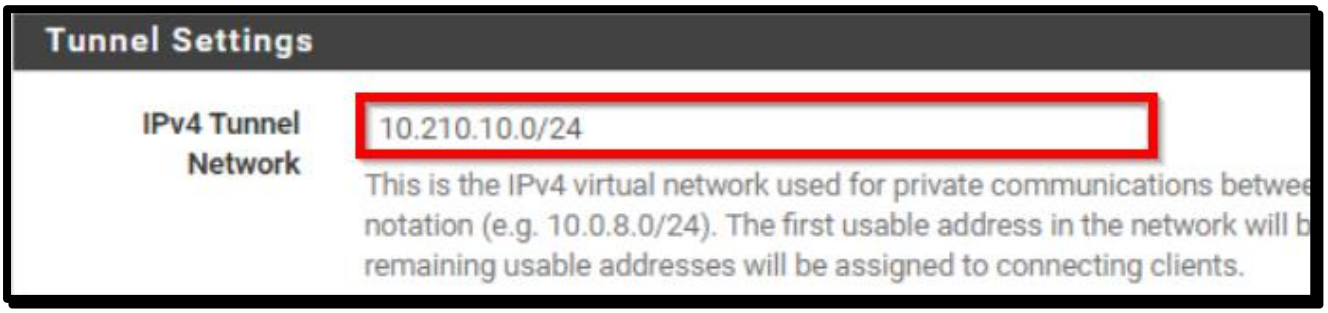
3. Configurez le nom du serveur, le mode en "**Accès distant (SSL/TLS)**", et spécifiez le port local.

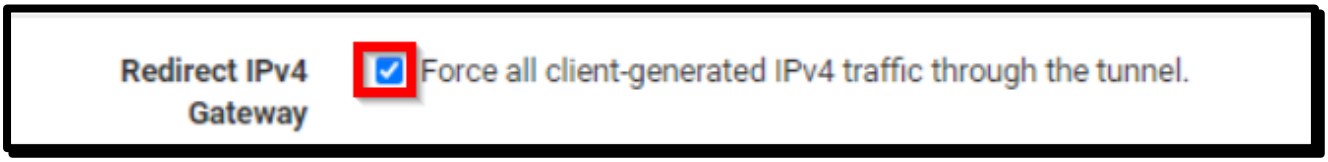


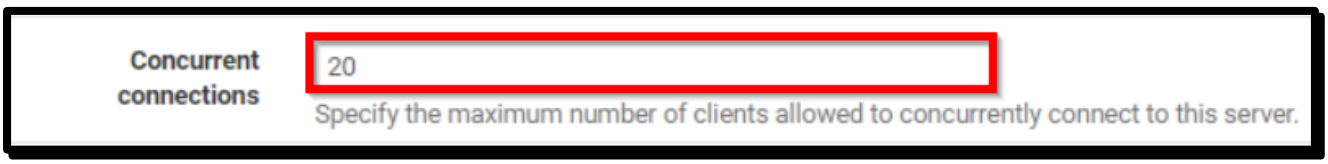
4. Dans la section **'Paramètres cryptographiques'**, nous allons choisir **VPNS1P1** comme notre « **Autorité de certification homologue** » et le certificat du serveur comme « **Certificat VPN** » :



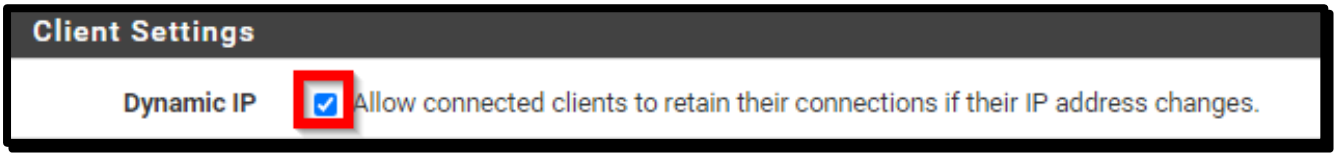
5. Dans la section **'Paramètres du tunnel'**, nous allons configurer **l'IPv4 Tunnel Network** sur 10.210.10.0/24 (adresse du réseau VPN). Nous allons cocher la case **'Rediriger la passerelle IPv4'**. Ensuite, nous allons paramétrer le nombre de **'Connexions simultanées'** sur 20, correspondant au nombre de connexions pouvant être établies simultanément.





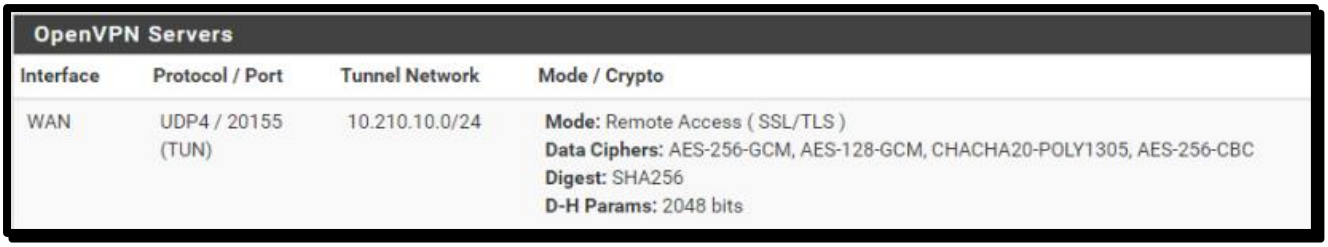


6. Dans la section **Client Settings**, nous allons cocher la case **Dynamic IP** :



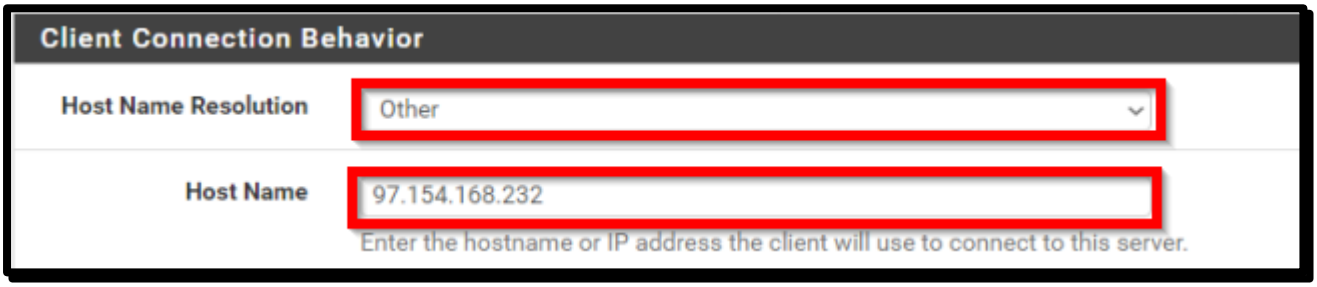
7. Dans la section **Advanced Configuration** nous mettons le valeur **auth-nocache**, ce qui signifie que les identifiants ne seront pas mis en cache :

Après avoir apporté toutes ces modifications, nous pouvons enfin sauvegarder nos changements. Notre serveur VPN est maintenant créé :

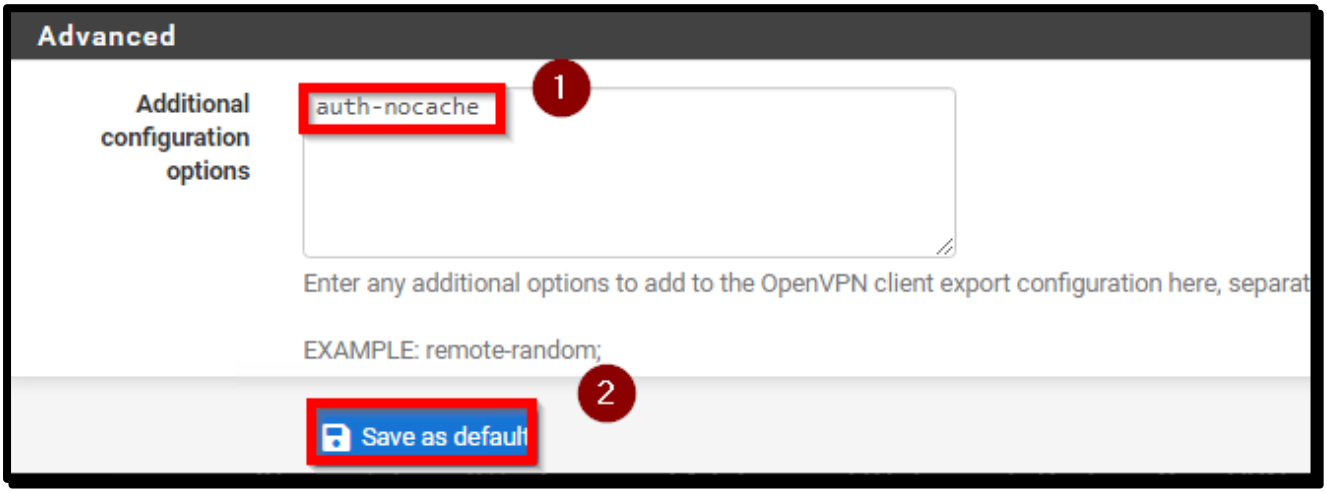


2.1.6.5 Exportation de la configuration VPN pour le Client

1. Pour exporter la configuration de notre client OpenVPN, nous allons dans **VPN** -> **OpenVPN** -> **Export client**, où nous allons configurer le champ de **résolution de nom d'hôte** en "**Autre**" et le champ de **nom d'hôte** en l'adresse IP publique de notre WAN, dans notre cas 97.154.168.232.



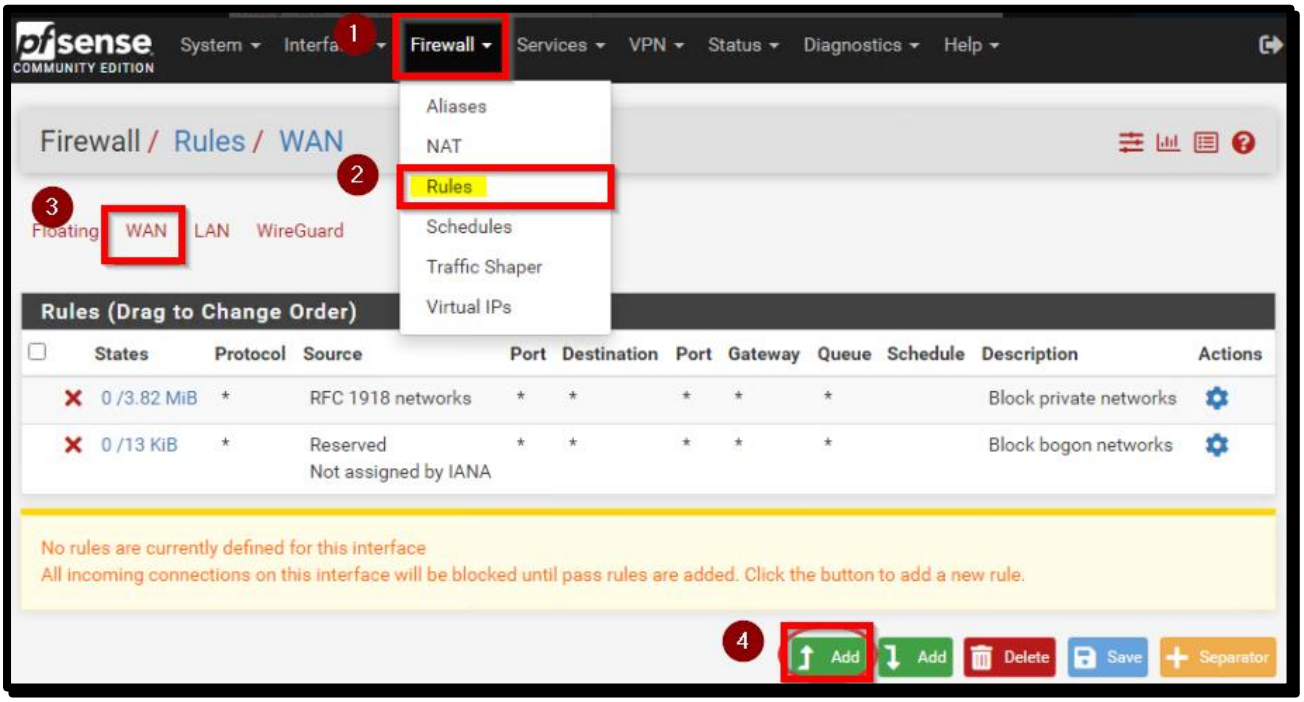
2. Dans la section **'Avancé'**, nous allons saisir les mêmes paramètres que ceux utilisés dans la configuration du serveur VPN et nous cliquons sur 'Save as default' :



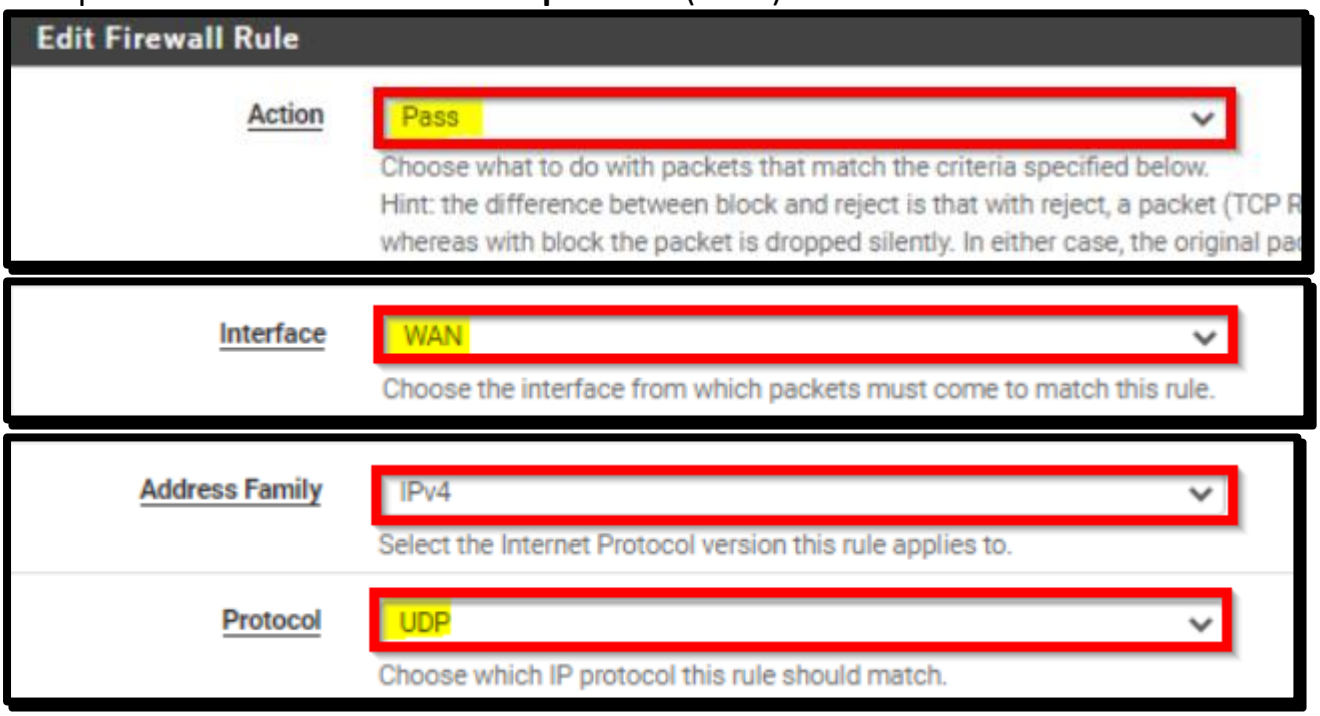
3. Enfin, toujours sur la même page, nous allons télécharger la configuration de notre OpenVPN. Soit uniquement le fichier de configuration si nous disposons déjà d'un client, soit avec le logiciel client si nous n'en avons pas encore :

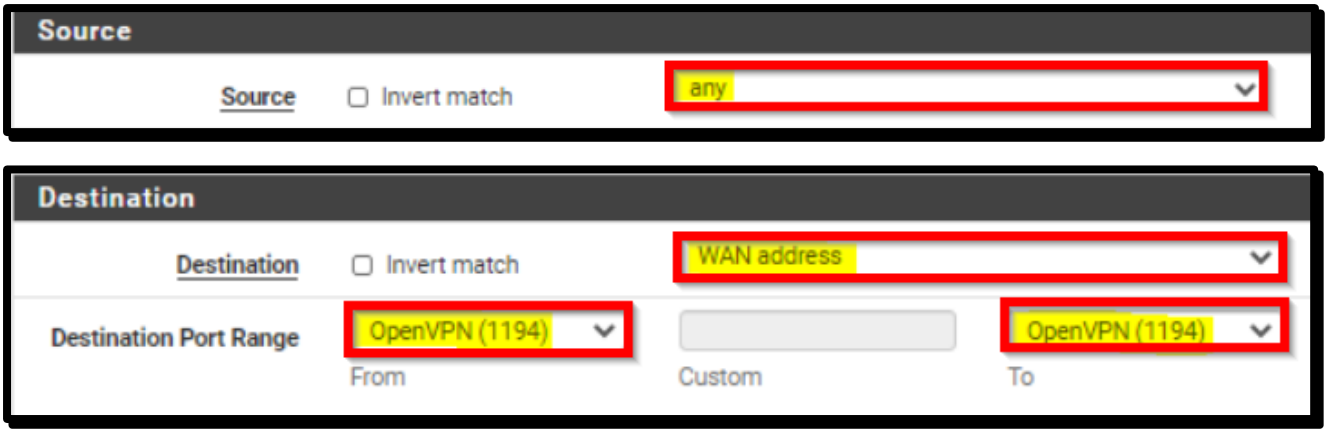
2.1.6.6 Configuration du Pare-Feu (NAT)

1. Pour permettre le passage par le WAN, nous devrons configurer les règles de pare-feu. Pour ce faire, nous nous rendrons dans les **règles** de **pare-feu** -> **WAN**, où nous cliquerons sur **Ajouter**.



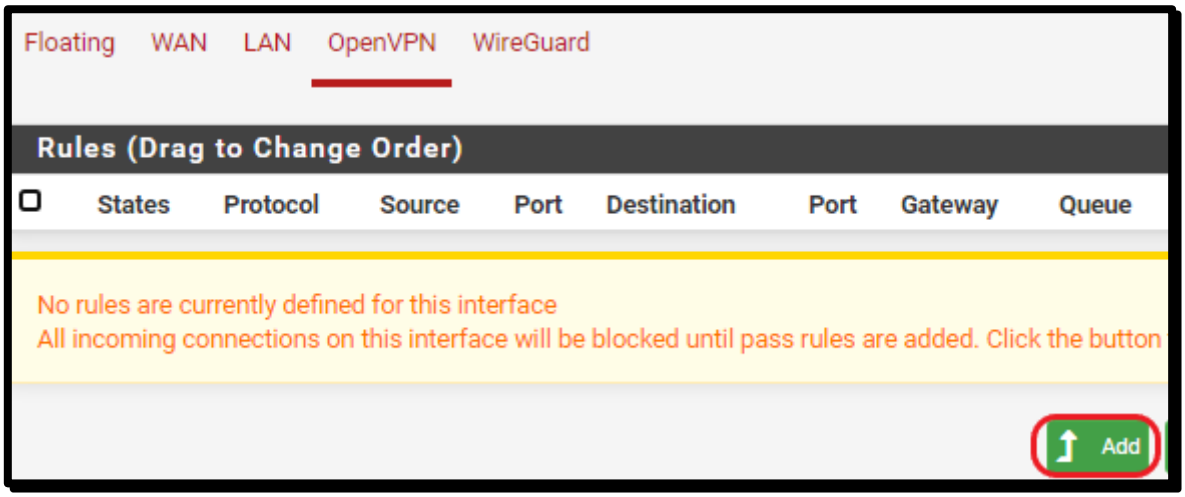
2. Là-dedans, nous allons autoriser le passage du protocole **UDP** à travers notre **WAN** et le port de destination de notre **OpenVPN** (1194) :



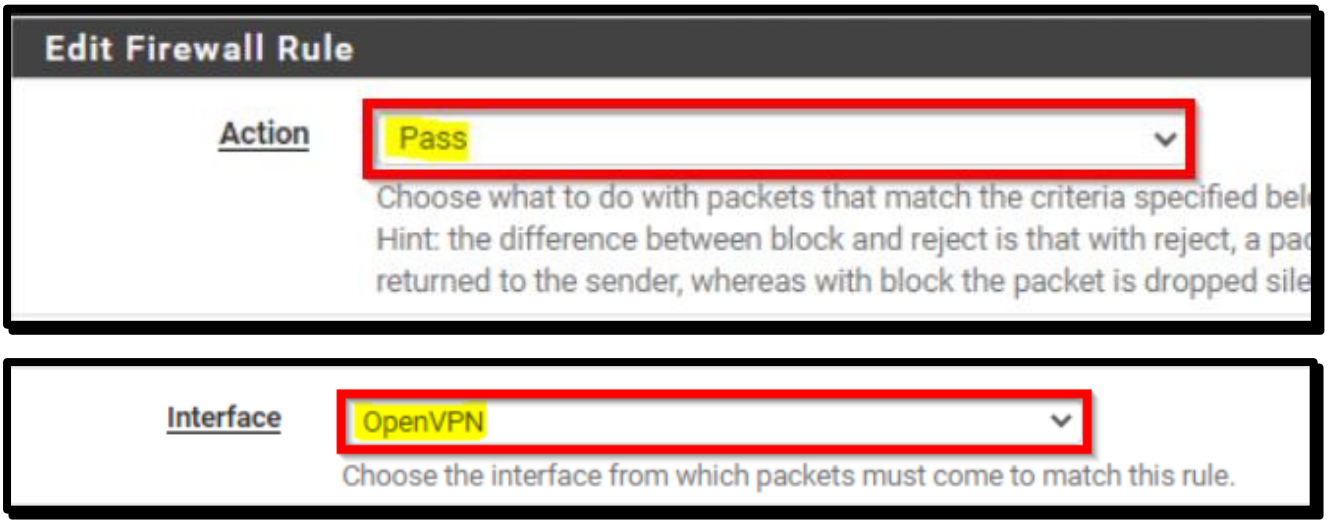


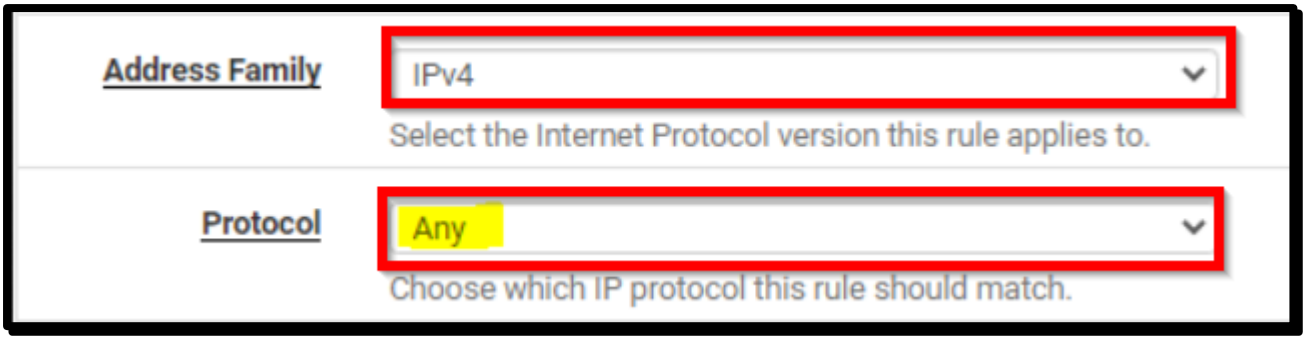
On sauvegarde les changements.

3. Ensuite, nous allons configurer les règles de pare-feu de l'interface OpenVPN en accédant à **'Firewall'** -> **'Rules'** -> **'OpenVPN'**, où nous cliquons sur **Ajouter** :



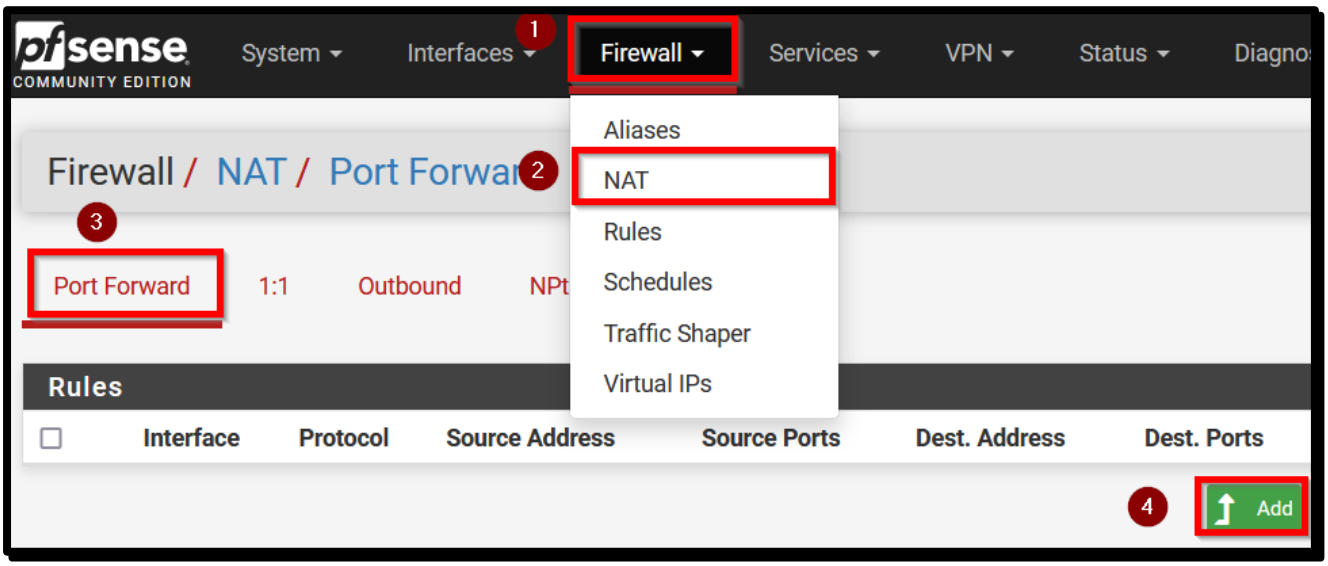
4. Là-dedans, nous allons mettre les paramètres suivants :



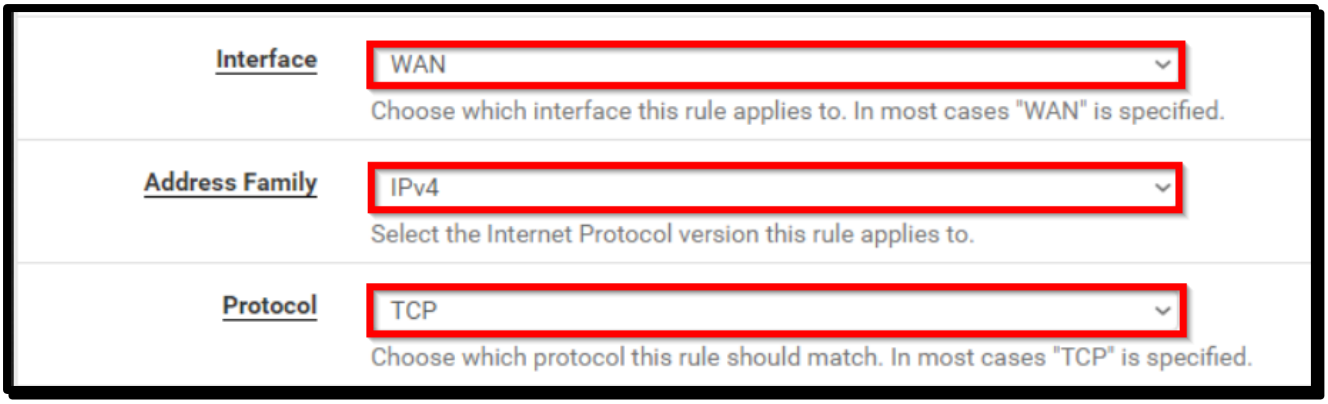


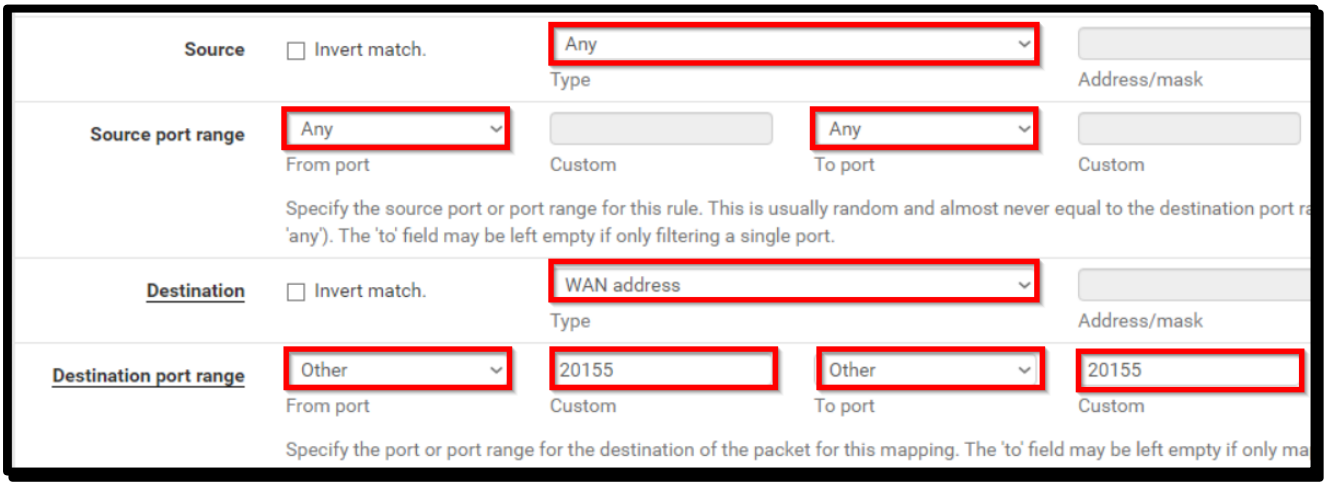
5. Ensuite, nous nous rendons dans **Interfaces** -> **Assignations**, où nous ajoutons notre interface **OpenVPN**.

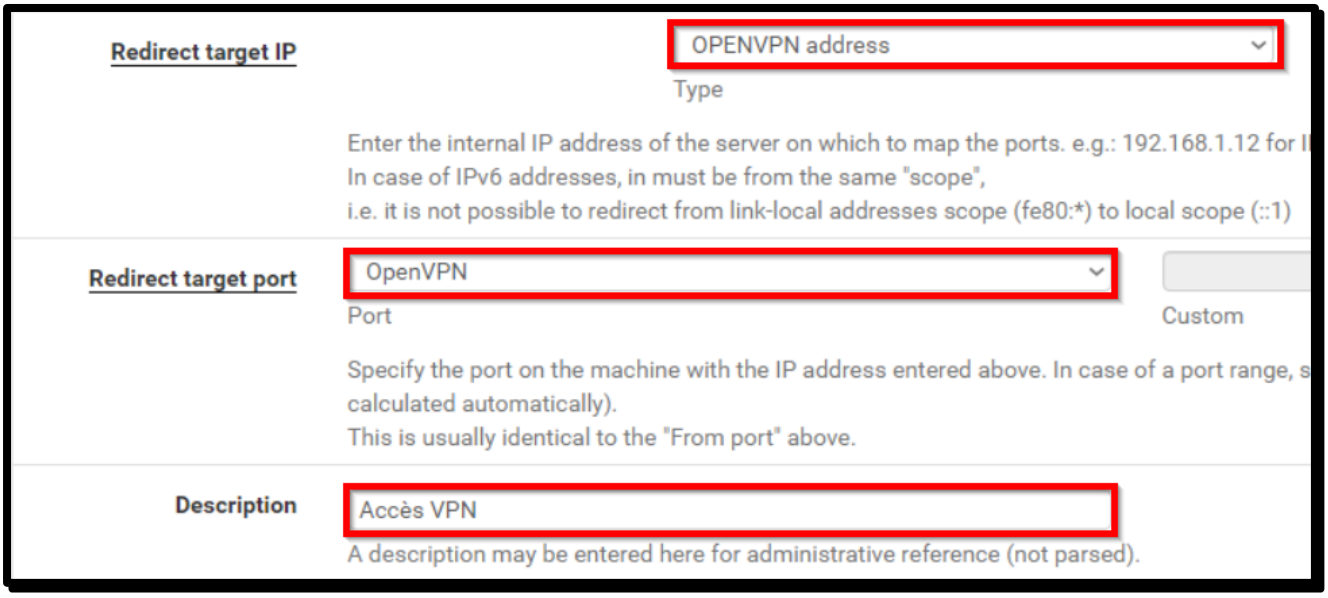
6. Puis, dans **Firewall -> NAT -> Port Forward**, nous cliquons sur **Add :**



7. Sur la page qui s'affiche, nous allons configurer les paramètres suivants :



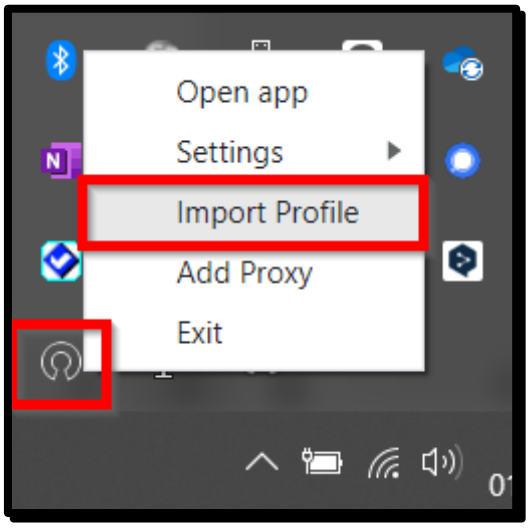




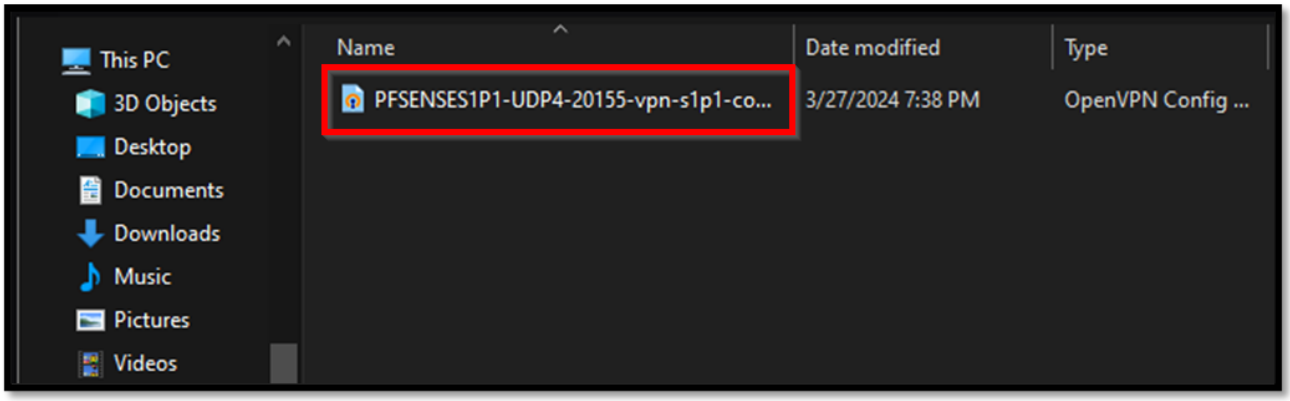
Finalement nous sauvegardons les changements.

2.1.6.7 Les tests

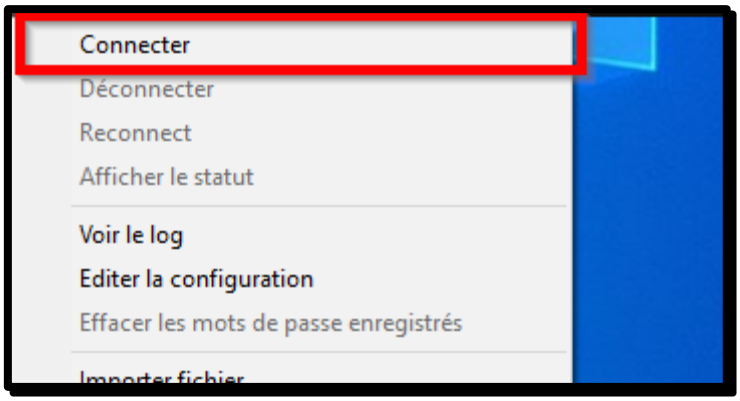
1. Pour tester la fonctionnalité, nous avons téléchargé le fichier de configuration de notre client. Pour l'appliquer, nous allons faire un clic droit sur notre barre des tâches, puis sélectionner '**Importer le fichier**…' :



Ensuite, nous choisissons le fichier à importer :



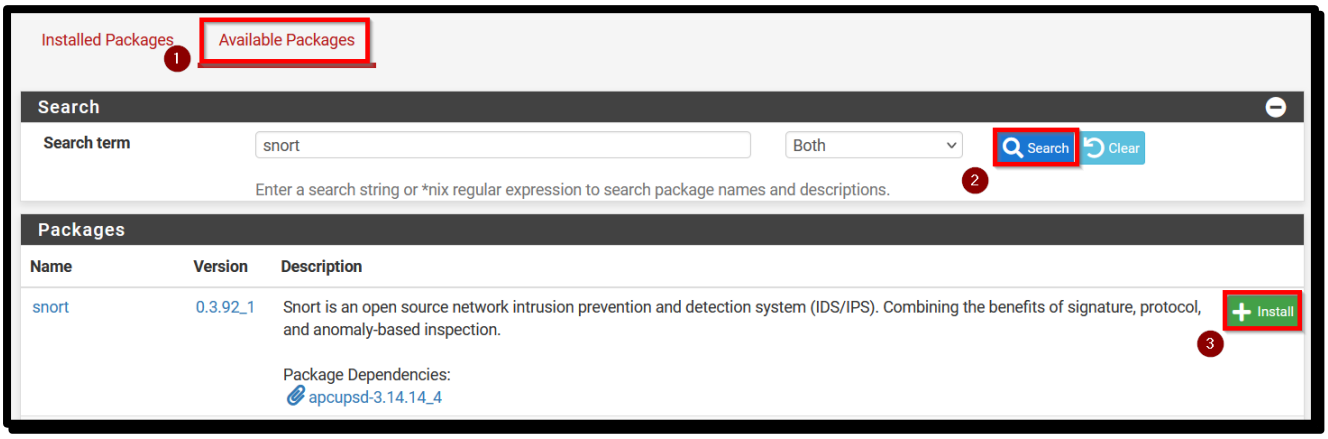
2. Après la mise en place de notre configuration, nous allons tout simplement cliquer encore une fois sur notre barre des tâcher afin de choisir le bouton **Connecter** :



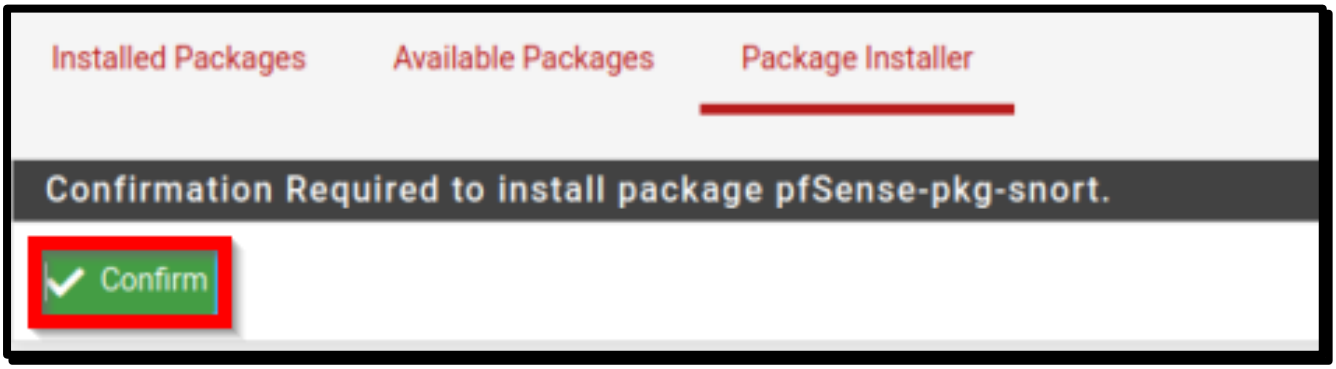
2.1.7. Installation de SNORT

SNORT est un logiciel qui nous permet la détection et la protection contre les menaces. Tout comme OpenVPN, c'est une extension installable via le gestionnaire des paquets.

1. Pour commencer notre installation, nous allons dans **Système** -> **Gestionnaire de paquets** -> **Paquets disponibles**, où nous allons rechercher notre extension en tapant le mot-clé « snort » dans la barre de recherche et cliquer sur le bouton **Installer** :

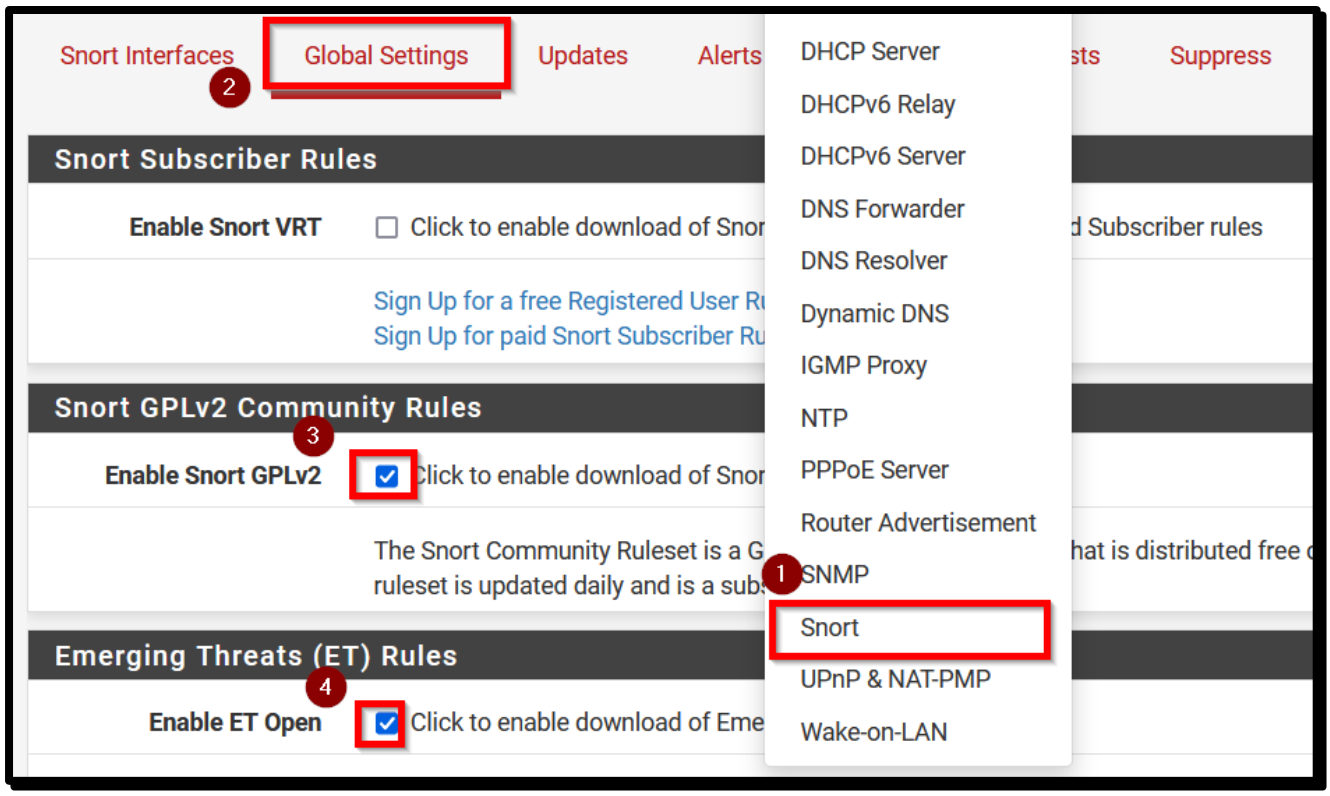


Puis nous le confirmons :

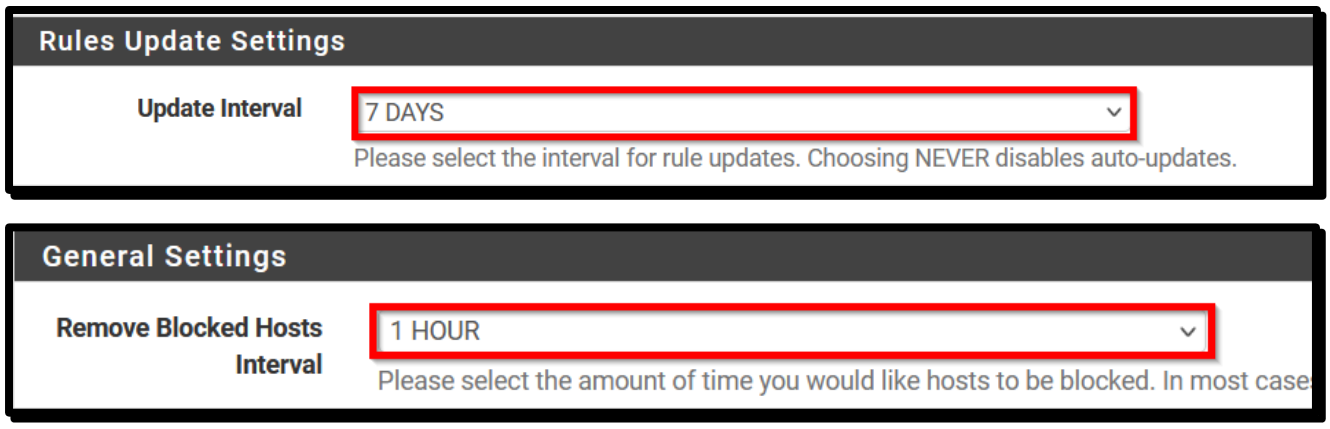


2. Une fois l'installation achevée, nous nous rendons dans **Services** -> **Snort** -> **Paramètres globaux**, où nous choisissons les listes de règles définissant les méthodes de détection des menaces :

Dans notre cas nous allons prendre le paquet communautaire **GPLv2** et **ET Open** :

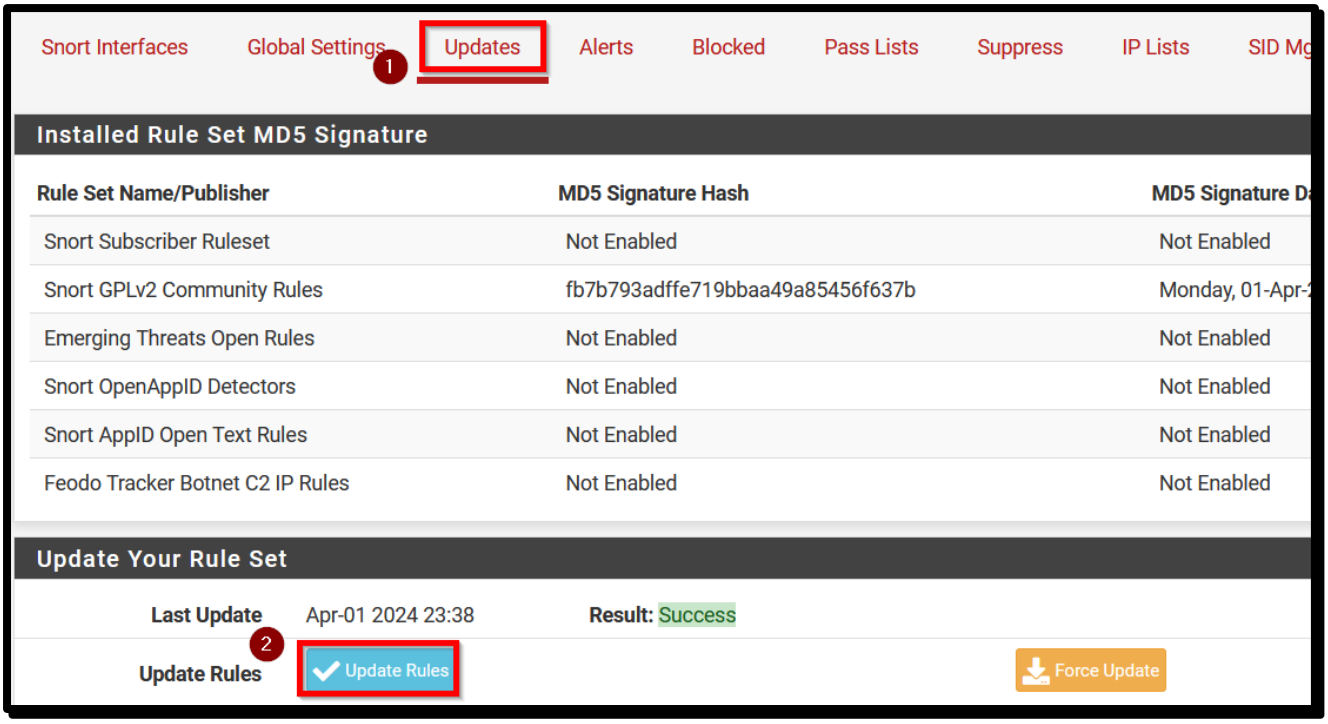


3. Ensuite, un peu plus bas sur la même page, nous sélectionnons l'intervalle des mises à jour ainsi que l'option de blocage d'accès à notre réseau en cas d'activité suspecte :

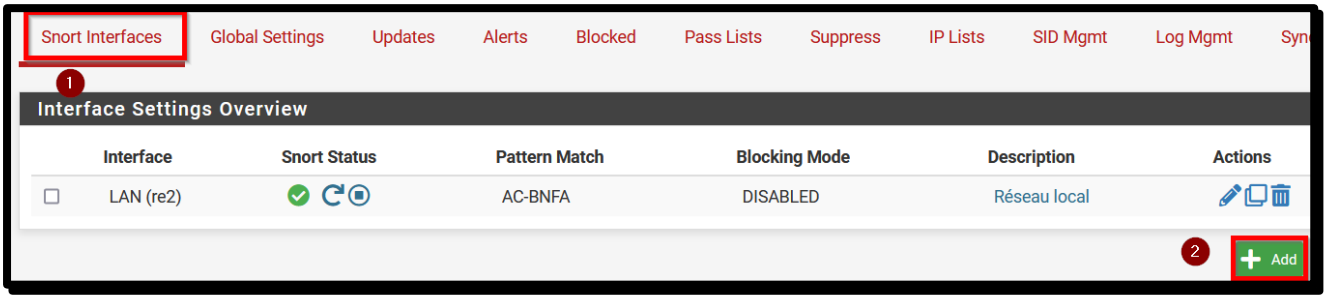


Après cela, nous sauvegardons nos changements.

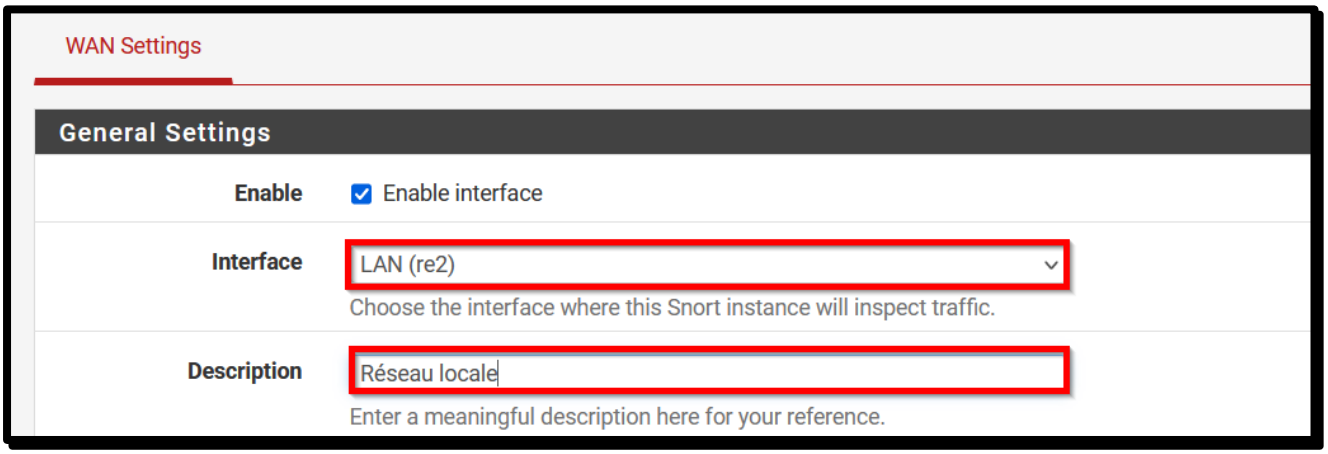
4. Ensuite, nous allons dans **Services -> Snort -> Updates,** afin de mettre à jour notre nouveau service installé :



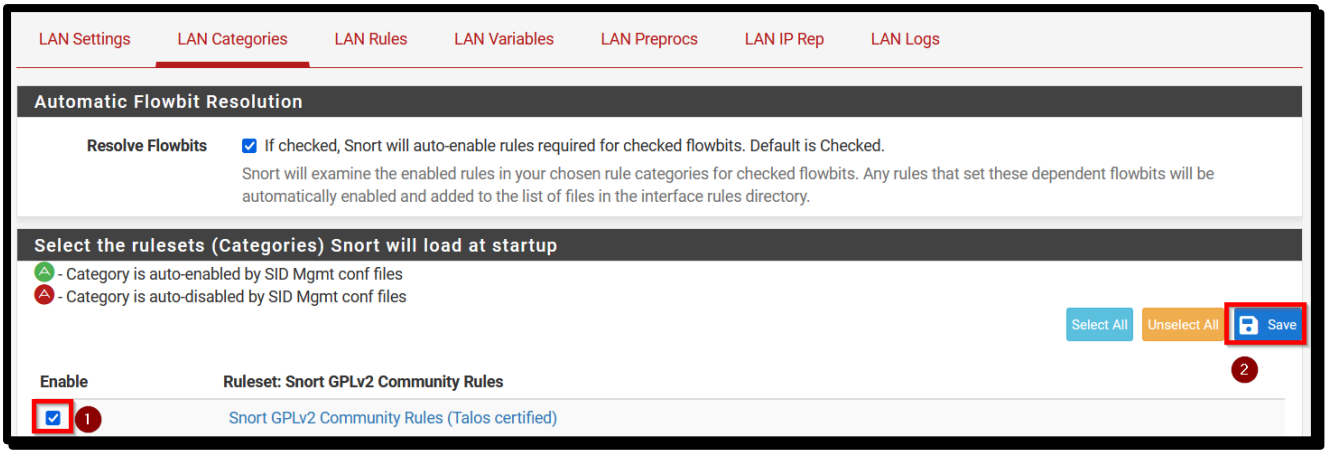
5. Une fois la mise à jour terminée, nous nous rendons dans **Services -> Snort -> Snort Interfaces**, afin d'ajouter une interface d'écoute :



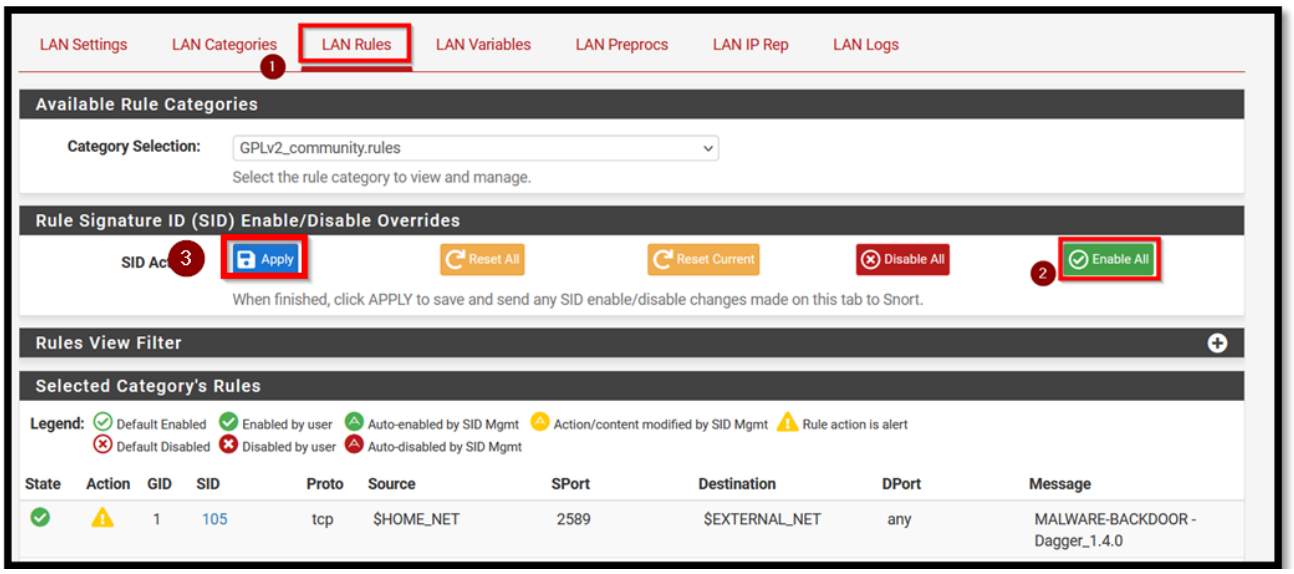
Nous sélectionnons l'interface sur laquelle Snort écoutera ainsi que sa description :



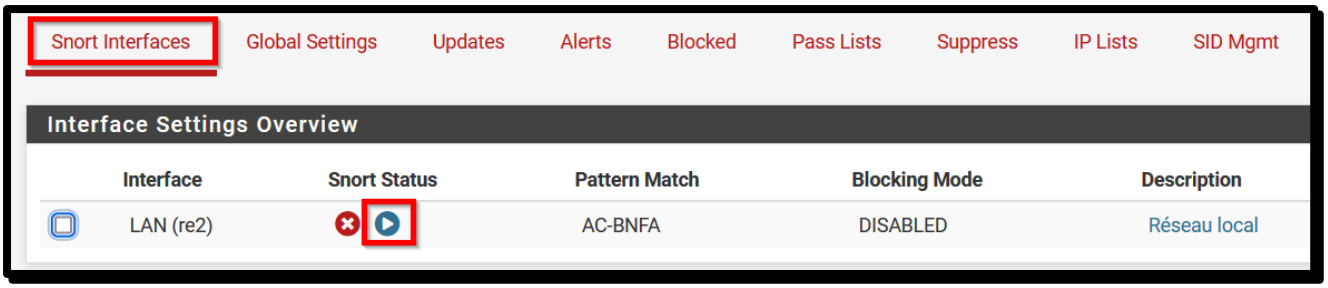
6. Une fois paramètres sauvegardés, nous allons dans **Services -> Snort -> Interface Settings -> LAN – Catégories** de règle qu'on vient de créer, afin de les activer :



7. Après les avoir activées, nous avons la possibilité d'activer les règles une par une sur la page **Règles LAN**. Dans notre cas, nous avons choisi d'activer toutes les règles :



8. Lorsque nos règles sont correctement paramétrées, nous devrons nous rendre sur la page **Snort Interfaces** afin d'activer le mode d'écoute :

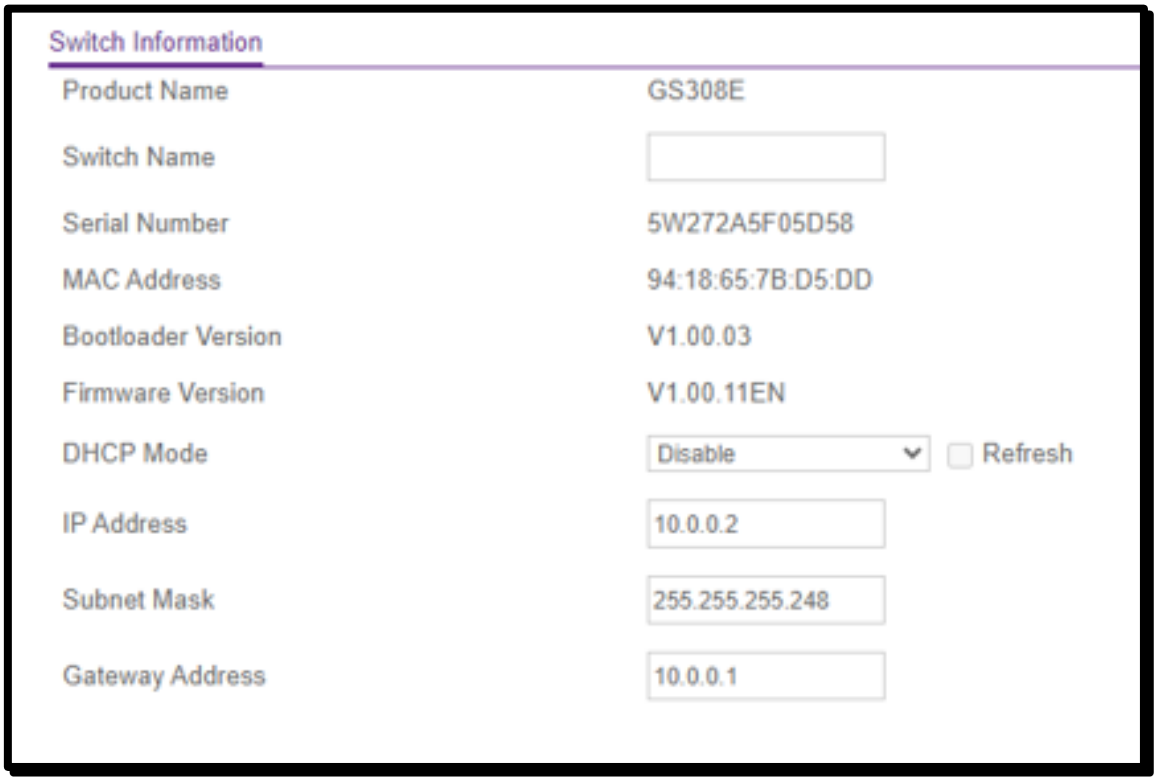


Notre service de détection d'intrusion est désormais prêt à être utilisé!

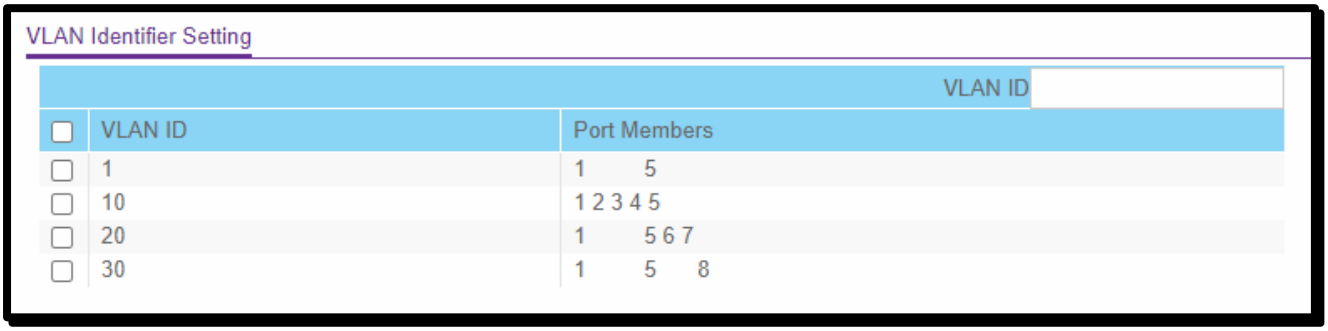
2.2.Netgear

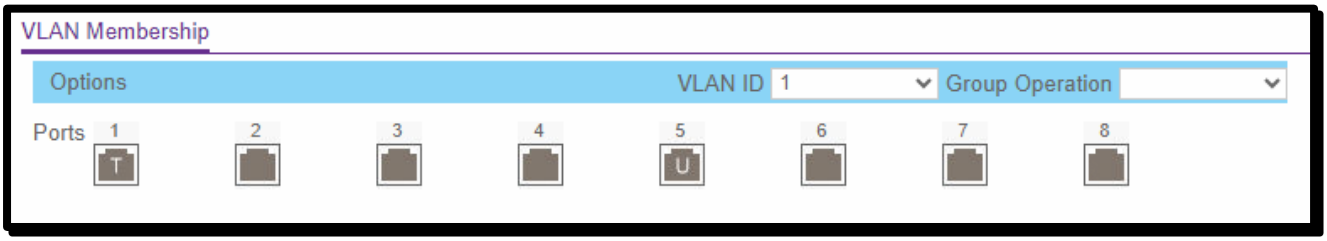
2.2.1 Configuration Basique

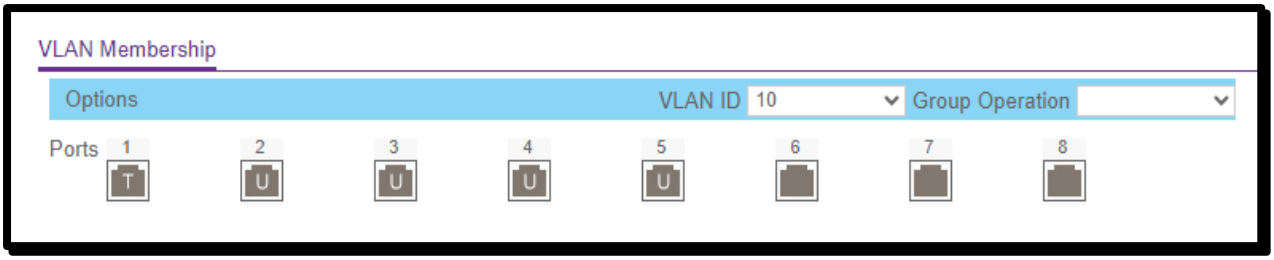
1. L'adresse d'usine de notre switch est **192.168.0.239**. Nous changeons également le mot de passe en **Azerty13!** (mot de passe par défaut : « **password** »). Nous réglons notre commutateur sur **10.0.0.2/29**.

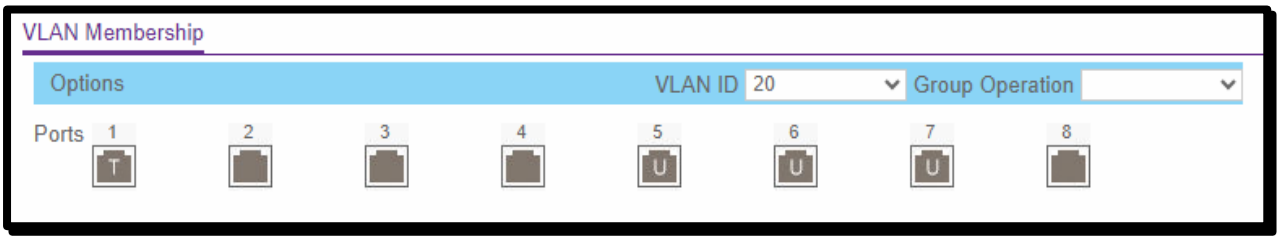


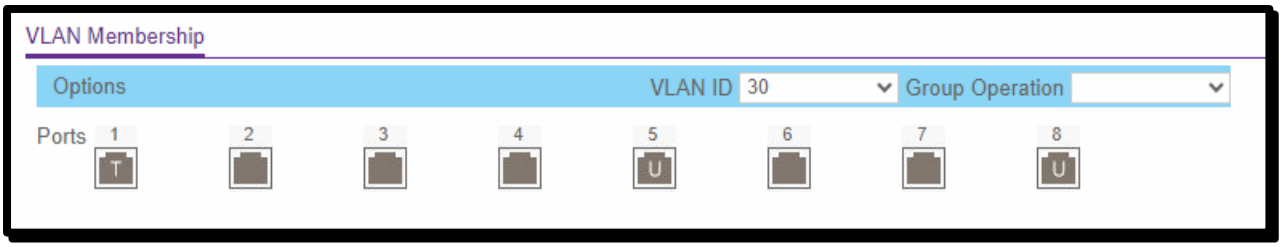
2. Configuration des VLANS dans « **VLAN** -> **802.1Q** -> **VLAN Configuration** ».

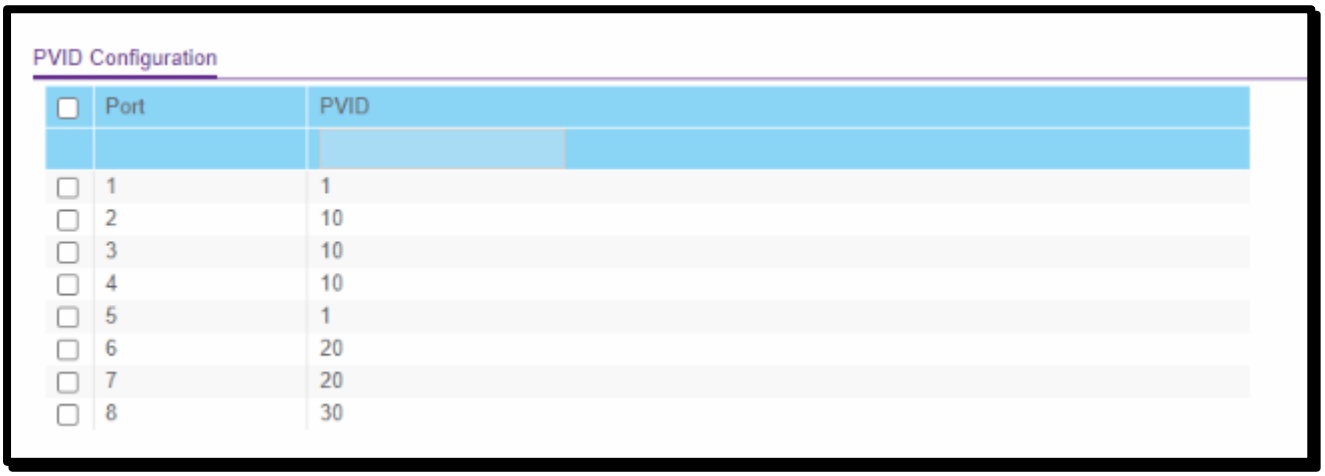








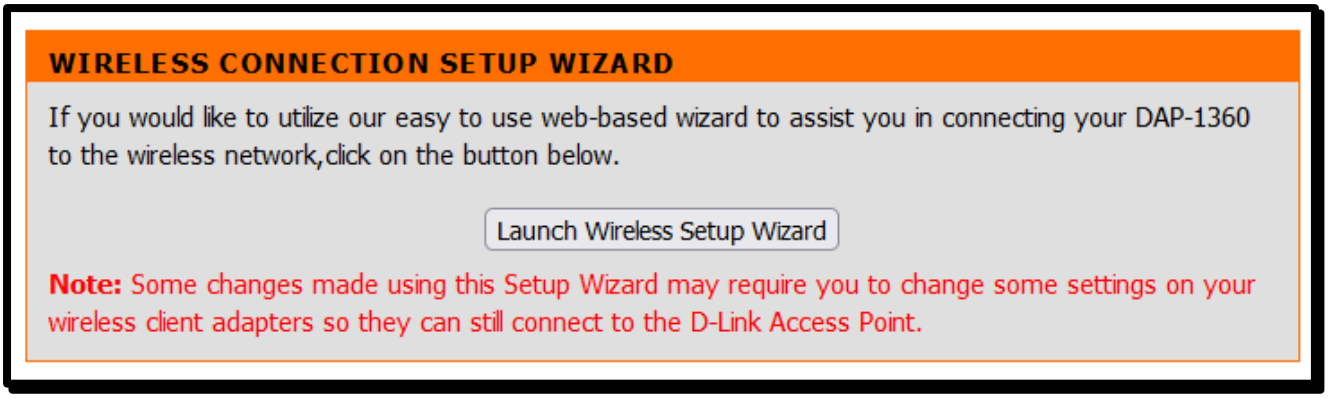




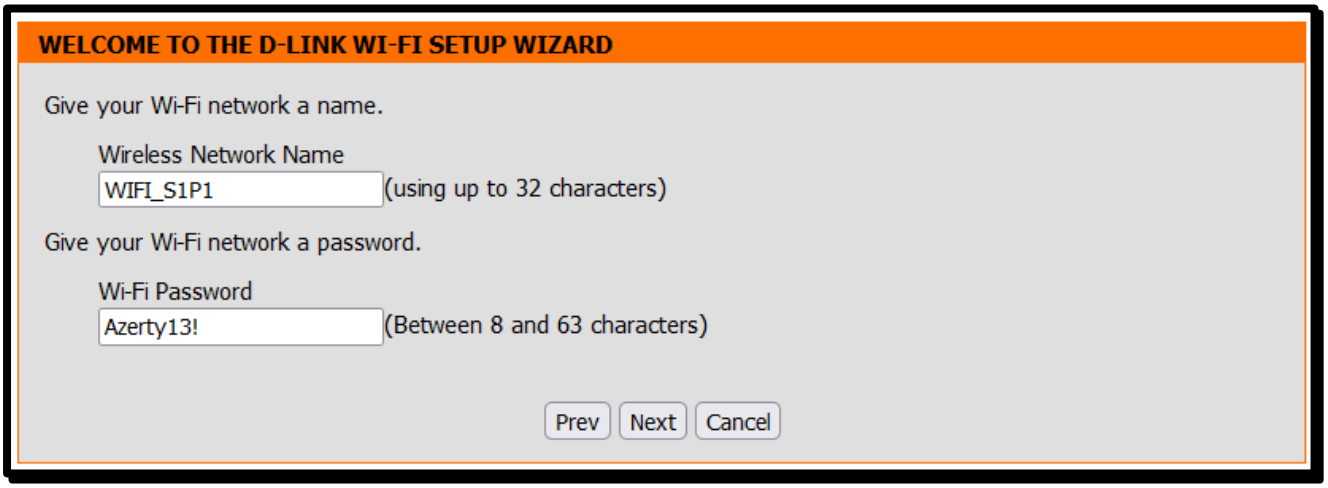
2.3. D-Link

2.3.1 Configuration Basique

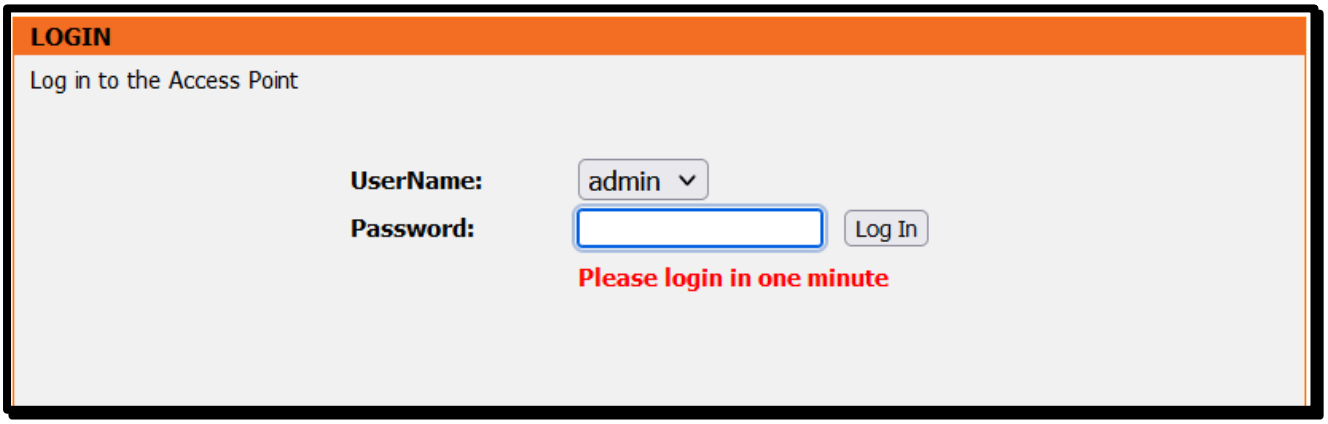
1. Pour accéder à notre DAP-1360, nous utilisons l'adresse http://192.168.0.50/.



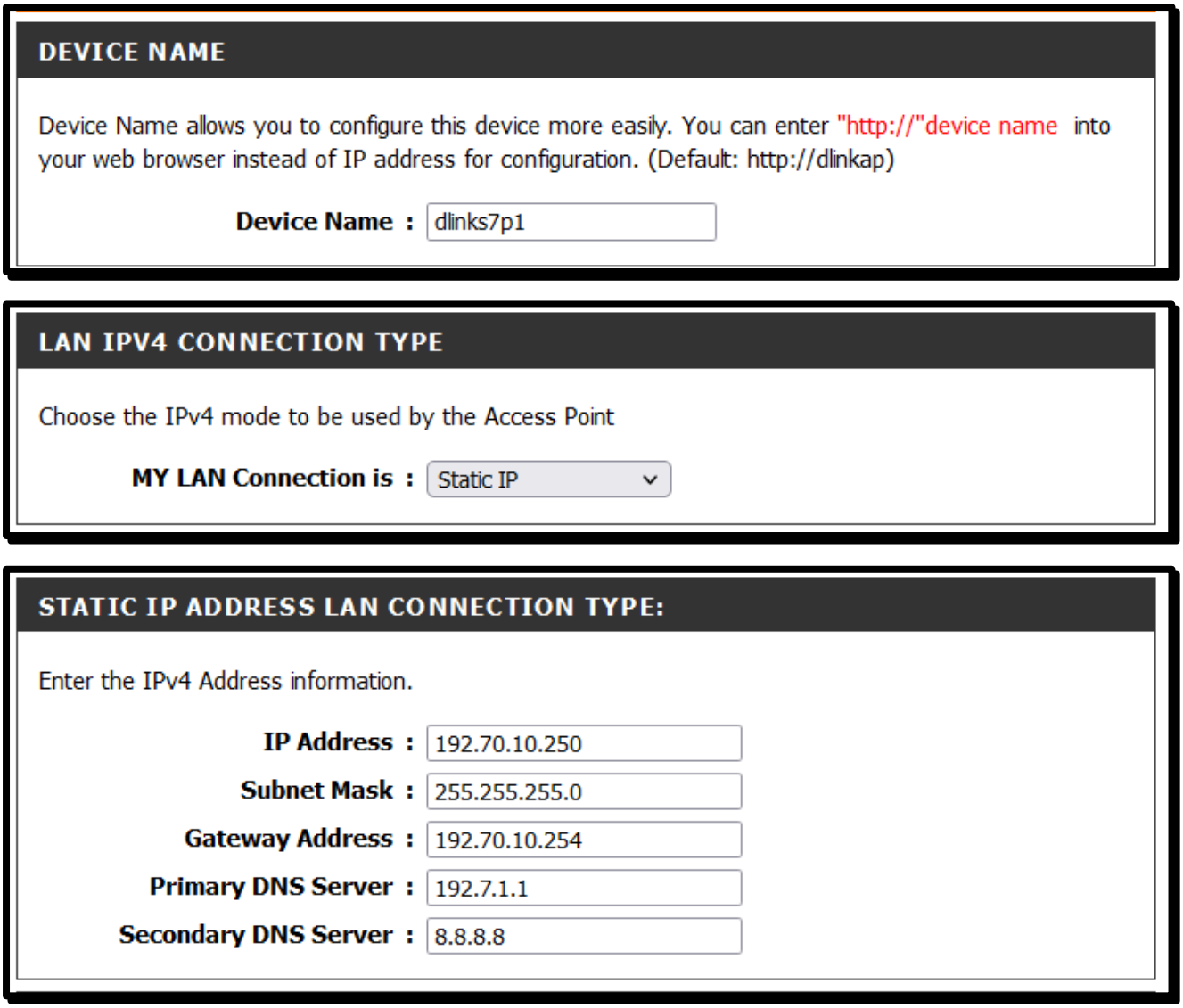
2. Configuration du point d'accès selon les indications.



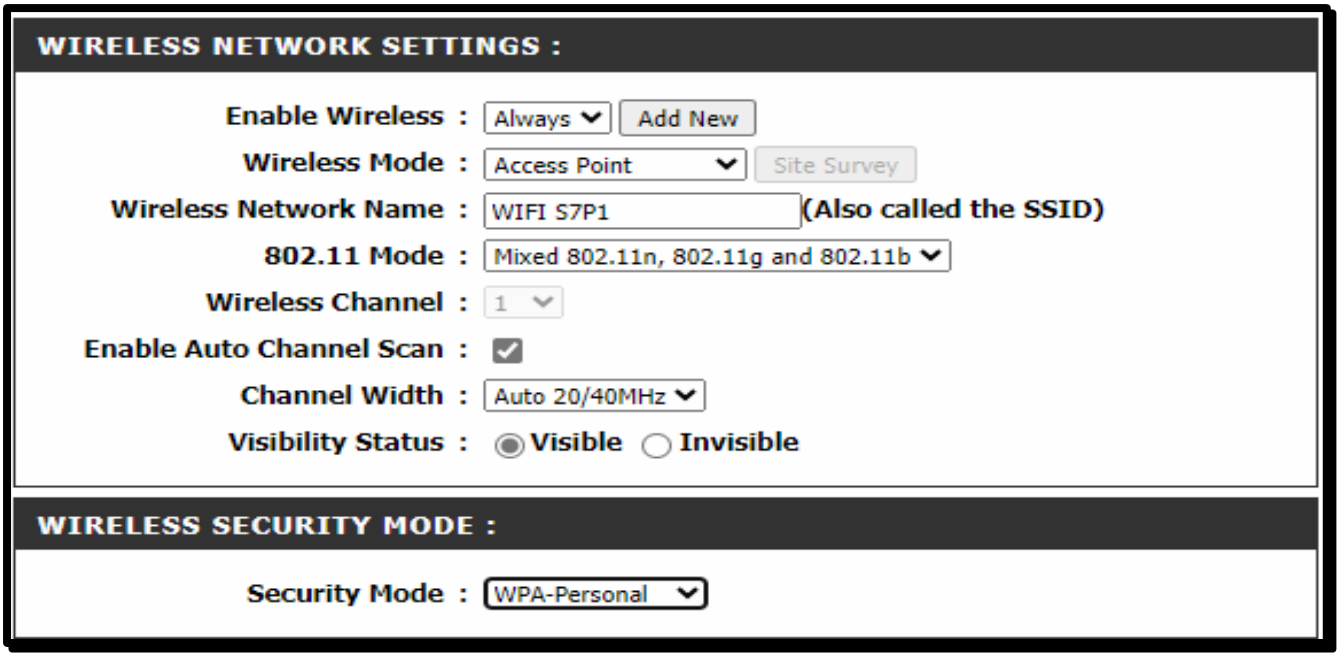
3. Après le redémarrage nous allons nous connecter avec le compte admin sans le mot de passe.



4.

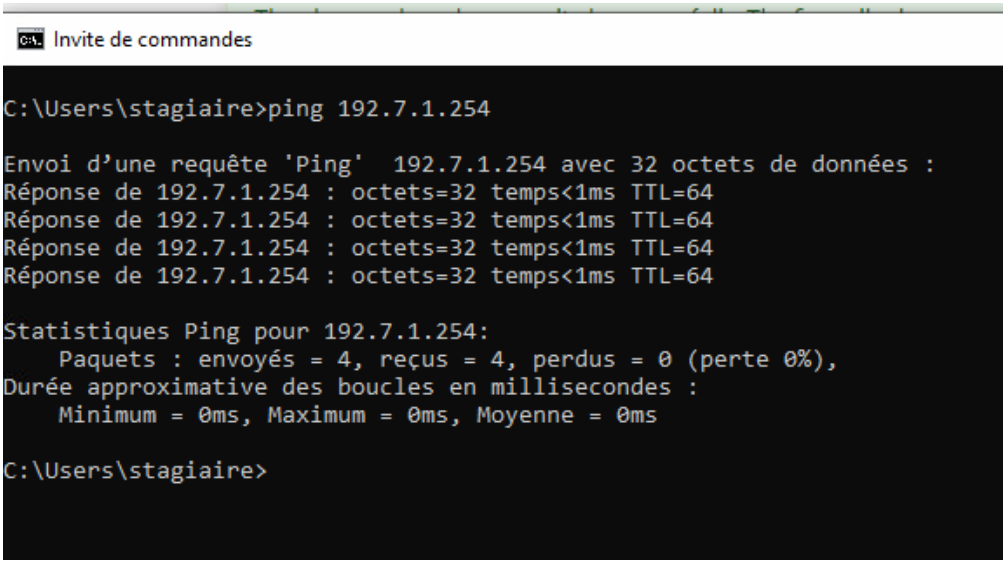


3. Configuration d'accès sans fil :

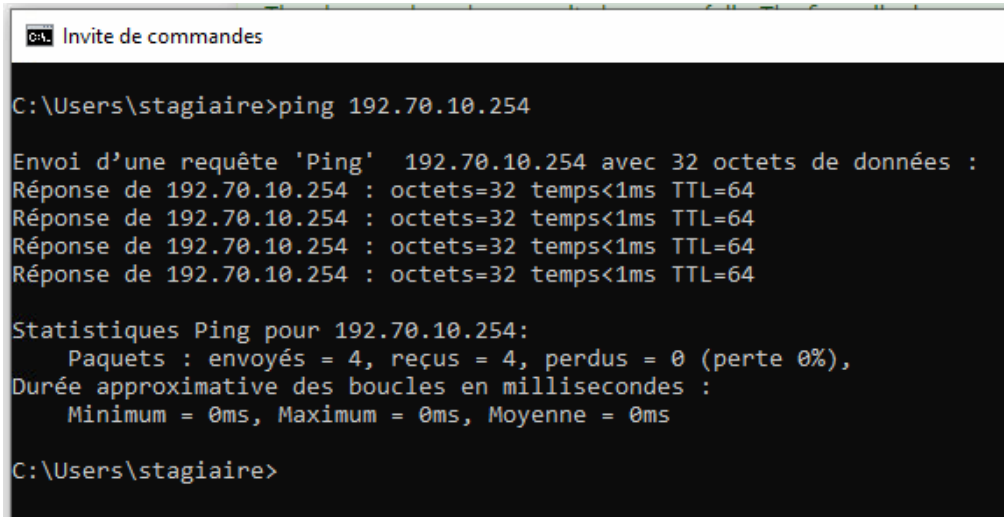


3. Les Tests

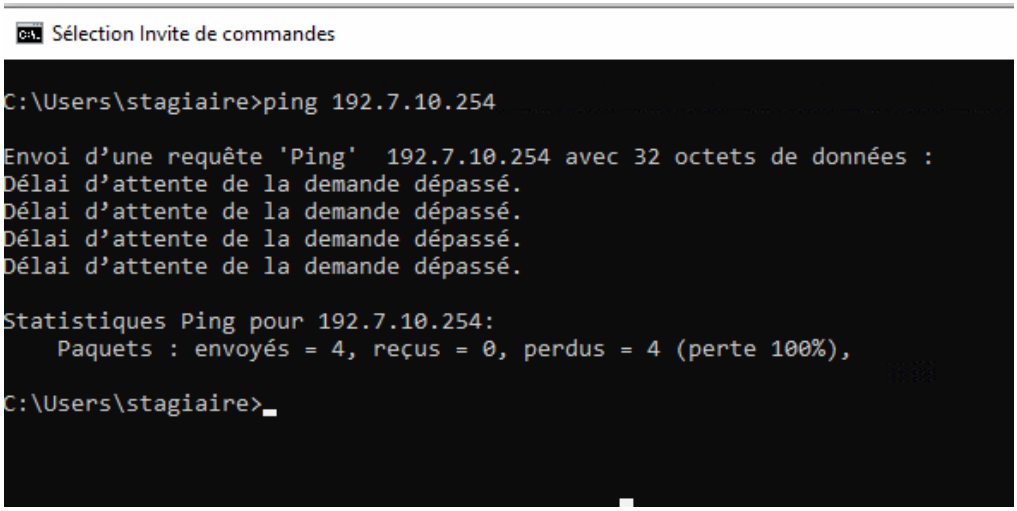
1. Tentative d'accès du VLAN10 vers le VLAN10 :



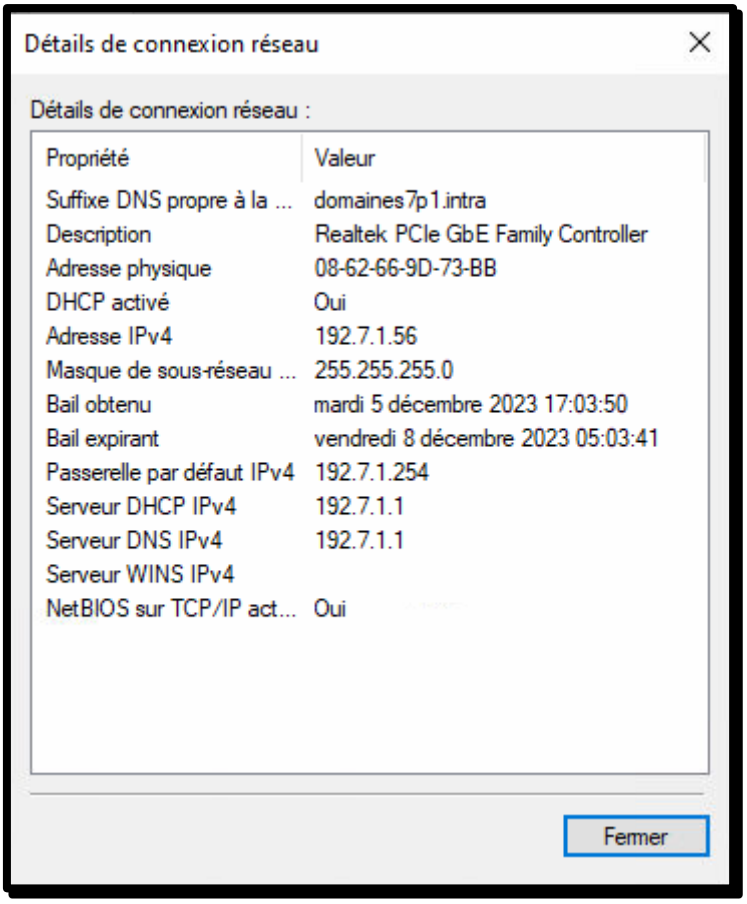
2. Tentative d'accès du VLAN10 vers le VLAN20 :

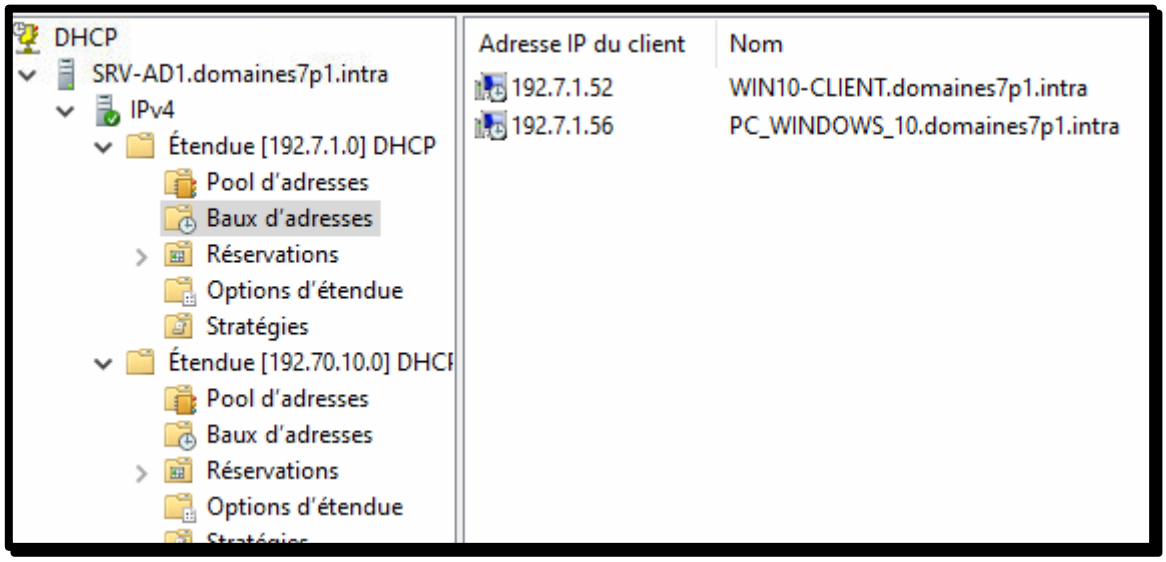


3. Tentative d'accès du VLAN10 vers le VLAN30 :



4. L'adresse DHCP attribuée correspond bien à l'étendue du VLAN10.


Détails de connexion réseau
Détails de connexion réseau :
Propriété
Valeur
Suffixe DNS propre à la ...
domaines7p1.intra
Description
Realtek PCIe GbE Family Controller
Adresse physique
08-62-66-9D-73-BB
DHCP activé
Oui
Adresse IPv4
192.7.1.56
Masque de sous-réseau ...
255.255.255.0
Bail obtenu
mardi 5 décembre 2023 17:03:50
Bail expirant
vendredi 8 décembre 2023 05:03:41
Passerelle par défaut IPv4
192.7.1.254
Serveur DHCP IPv4
192.7.1.1
Serveur DNS IPv4
192.7.1.1
Serveur WINS IPv4
NetBIOS sur TCP/IP act...
Oui
Fermer


DHCP
SRV-AD1.domaines7p1.intra
IPv4
Étendue [192.7.1.0] DHCP
Pool d'adresses
Baux d'adresses
Réservations
Options d'étendue
Stratégies
Étendue [192.70.10.0] DHCP
Pool d'adresses
Baux d'adresses
Réservations
Options d'étendue
Adresse IP du client
Nom
192.7.1.52
WIN10-CLIENT.domaines7p1.intra
192.7.1.56
PC_WINDOWS_10.domaines7p1.intra