Configurer l'équilibreur de charge de la communauté pfSense pour ECE

Table des matières

Introduction

Ce document décrit les étapes de configuration et de configuration de pfSense Community Edition en tant qu'équilibreur de charge pour la messagerie instantanée et la messagerie électronique d'entreprise (ECE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ECE 12.x.
- PfSense Community Edition

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CEE 12.6 1)
- pfSense Community Edition 2.7.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Installer PfSense

Présentation de la solution

pfSense Community Edition est un produit multifonction qui fournit un pare-feu, un équilibreur de charge, un scanneur de sécurité et de nombreux autres services dans un seul serveur. pfSense est construit sur Free BSD et a une configuration matérielle minimale. L'équilibreur de charge est une implémentation de HAProxy et une interface utilisateur graphique facile à utiliser est fournie pour configurer le produit.

Vous pouvez utiliser cet équilibreur de charge avec le portail de gestion du centre de contacts (CCMP) et le portail ECE. Ce document présente les étapes de configuration de pfSense pour ECE.

Préparation

Étape 1. Télécharger le logiciel pfSense

Utilisez le site Web pfSense pour télécharger l'image du programme d'installation iso.

Étape 2. Configurer la VM

Configurez une machine virtuelle avec la configuration minimale requise :

· Processeur compatible amd64 64 bits (x86-64)

· 1 Go ou plus de RAM

· Disque dur de 8 Go ou plus (SSD, HDD, etc.)

· Une ou plusieurs cartes d'interface réseau compatibles

· Lecteur USB amorçable ou lecteur optique haute capacité (DVD ou BD) pour l'installation initiale

Pour une installation en laboratoire, une seule interface réseau (NIC) est requise. Il existe plusieurs façons d'exécuter l'appliance, mais la plus simple consiste à utiliser une seule carte réseau, également appelée mode à un bras. En mode à un bras, une seule interface communique

avec le réseau. Bien qu'il s'agisse d'une méthode simple et adaptée à un TP, elle n'est pas la plus sûre.

Pour une configuration plus sécurisée de l'appliance, vous devez disposer d'au moins deux cartes réseau. Une carte réseau est l'interface WAN et communique directement avec l'Internet public. La deuxième carte réseau est l'interface LAN et communique avec le réseau interne de l'entreprise. Vous pouvez également ajouter des interfaces supplémentaires pour communiquer avec différentes parties du réseau qui ont des règles de sécurité et de pare-feu différentes. Par exemple, vous pouvez avoir une carte réseau connectée à l'Internet public, une connexion au réseau DMZ où se trouvent tous les serveurs Web accessibles en externe et une troisième carte réseau connectée au réseau d'entreprise. Cela vous permet de permettre aux utilisateurs internes et externes d'accéder en toute sécurité au même ensemble de serveurs Web qui sont conservés dans une DMZ. Assurez-vous de bien comprendre les implications de toute conception en matière de sécurité avant sa mise en oeuvre. Consultez un ingénieur en sécurité pour vous assurer que les meilleures pratiques sont suivies pour votre mise en oeuvre spécifique.

Installation

Étape 1. Montage de l'ISO sur la machine virtuelle

Étape 2. Mettez la machine virtuelle sous tension et suivez les instructions d'installation.

Reportez-vous à ce document pour obtenir des instructions détaillées.

Configuration du réseau

Vous devez attribuer des adresses IP à l'appliance pour poursuivre la configuration.

Remarque : ce document présente un appareil configuré en mode un bras.

Étape 1. Configuration des VLAN

Si vous avez besoin de la prise en charge VLAN, répondez y à la première question. Sinon, répondez n.

Étape 2. Attribuer une interface WAN

L'interface WAN est le côté non sécurisé de l'appliance en mode bibras et la seule interface en mode un bras. Entrez le nom de l'interface lorsque vous y êtes invité.

Étape 3. Attribution de l'interface LAN

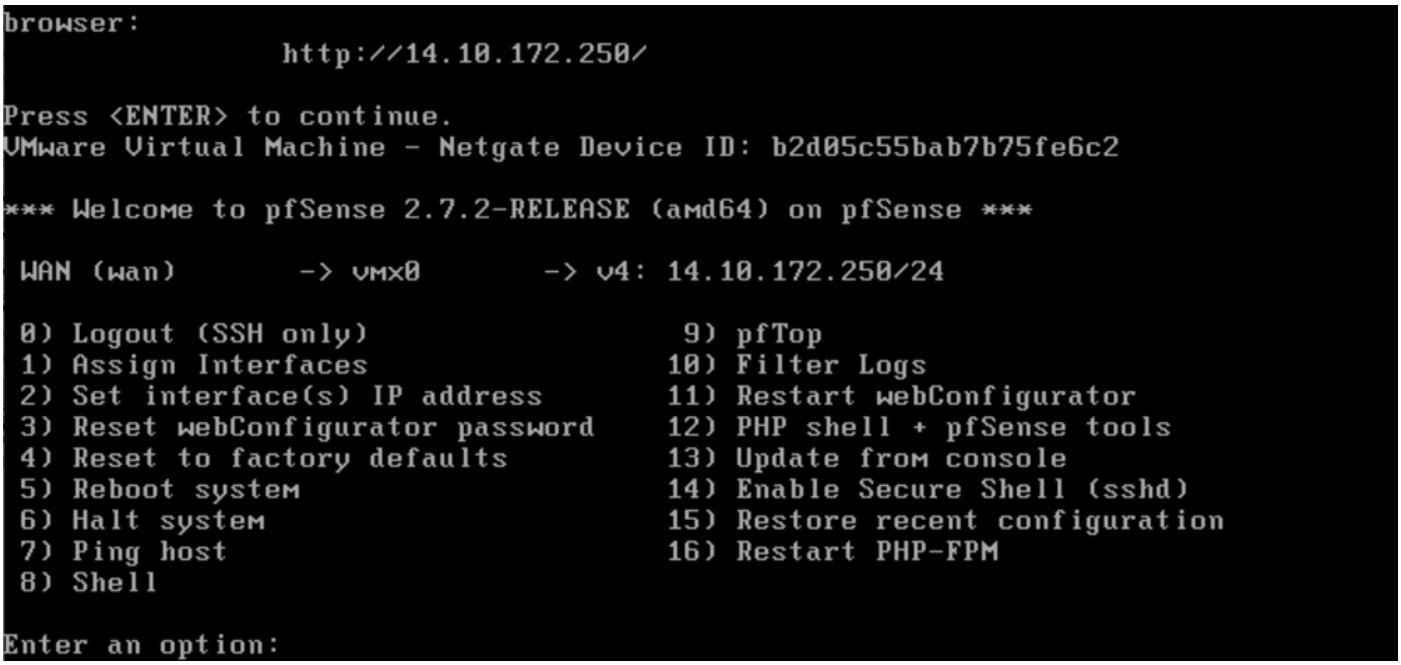
L'interface LAN est le côté sécurisé de l'appliance en mode bibras. Si nécessaire, entrez le nom de l'interface lorsque vous y êtes invité.

Étape 4. Affecter d'autres interfaces

Configurez toutes les autres interfaces nécessaires à votre installation spécifique. Ces options sont facultatives et peu courantes.

Étape 5. Attribuer une adresse IP à l'interface de gestion

Si votre réseau prend en charge le protocole DHCP, l'adresse IP attribuée s'affiche dans l'écran de la console.

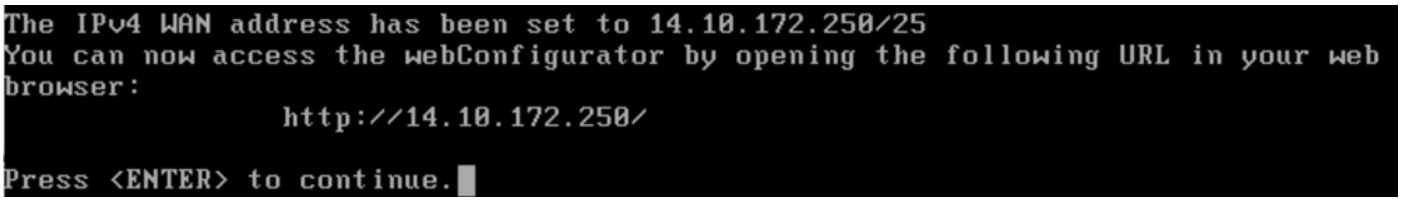


Console PfSense

Si aucune adresse n'est attribuée ou si vous souhaitez attribuer une adresse spécifique, procédez comme suit.

1. Sélectionnez l'option 2 dans le menu de la console.
2. Répondez n pour désactiver DHCP.
3. Saisissez l'adresse IPv4 de l'interface WAN.
4. Entrez le masque de réseau en nombre de bits. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Saisissez l'adresse de la passerelle pour l'interface WAN.
6. Si vous souhaitez que cette passerelle soit la passerelle par défaut de l'appliance, répondez y à l'invite de la passerelle, sinon répondez n.
7. Configurez la carte réseau pour IPv6 si vous le souhaitez.
8. Désactivez le serveur DHCP sur l'interface.
9. Répondez y pour activer HTTP sur le protocole webConfigurator. Ceci est utilisé dans les étapes suivantes.

Vous recevez ensuite une confirmation que les paramètres ont été mis à jour.

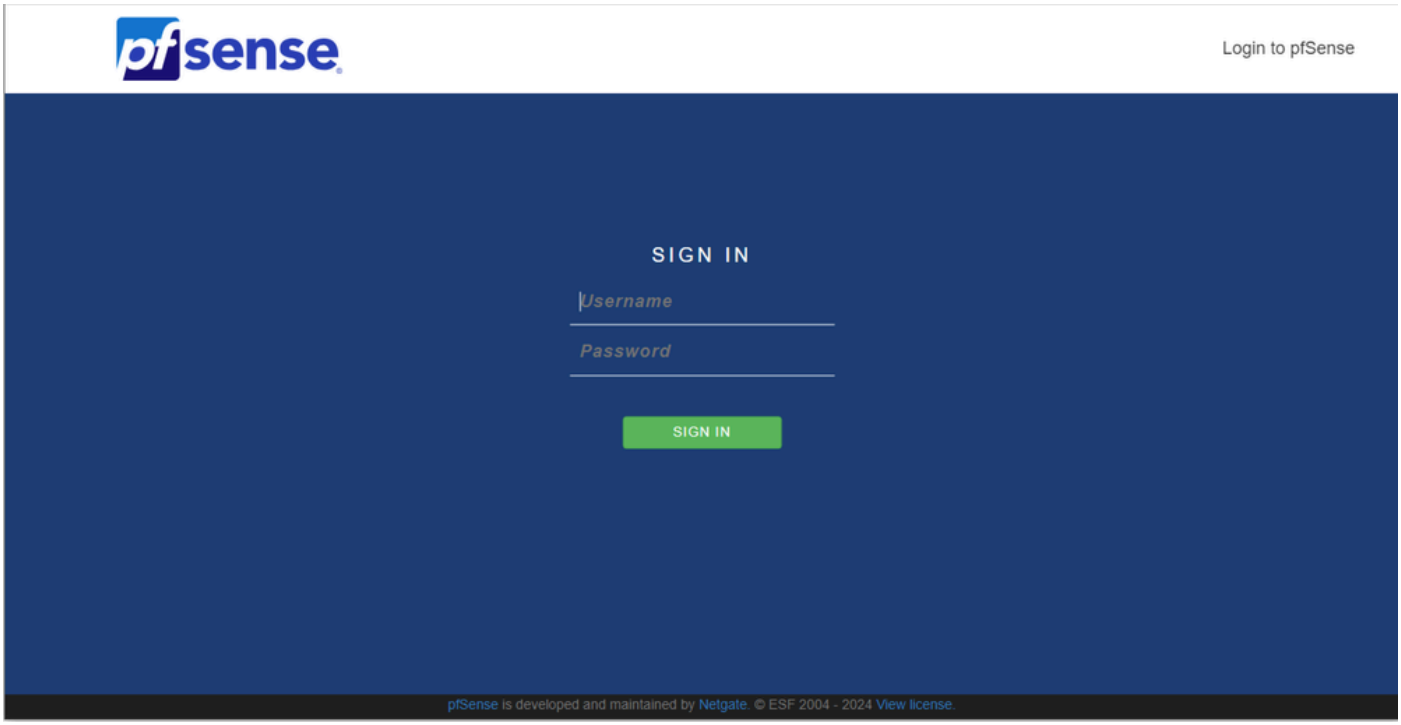


Confirmation de pfSense

Terminer la configuration initiale

Étape 1. Ouvrez un navigateur Web et accédez à : http://<ip_address_of_appliance>

Remarque : vous devez utiliser HTTP et non HTTPS au départ.

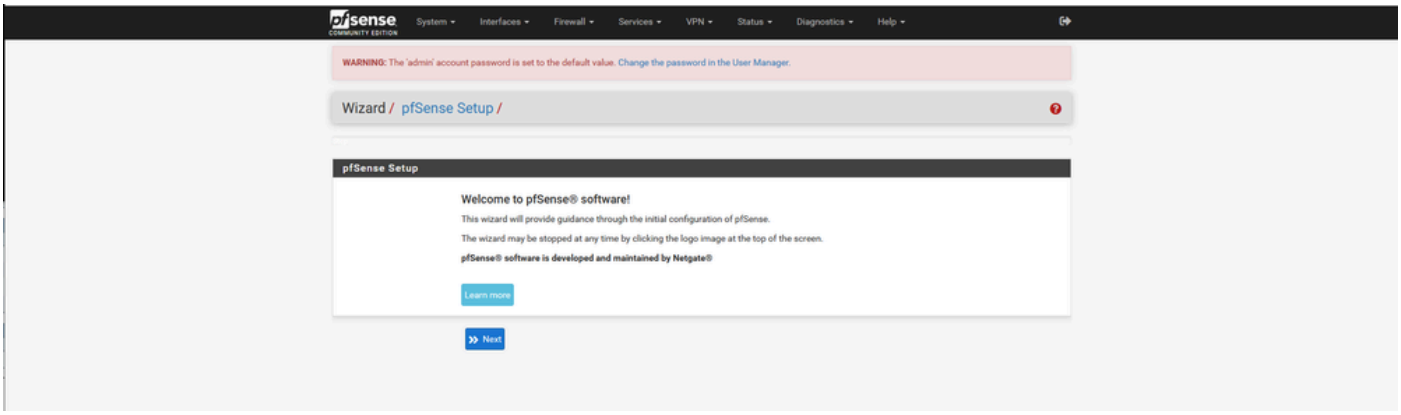


Connexion administrateur pfSense

Étape 2. Connectez-vous avec la connexion par défaut de admin / pfSense

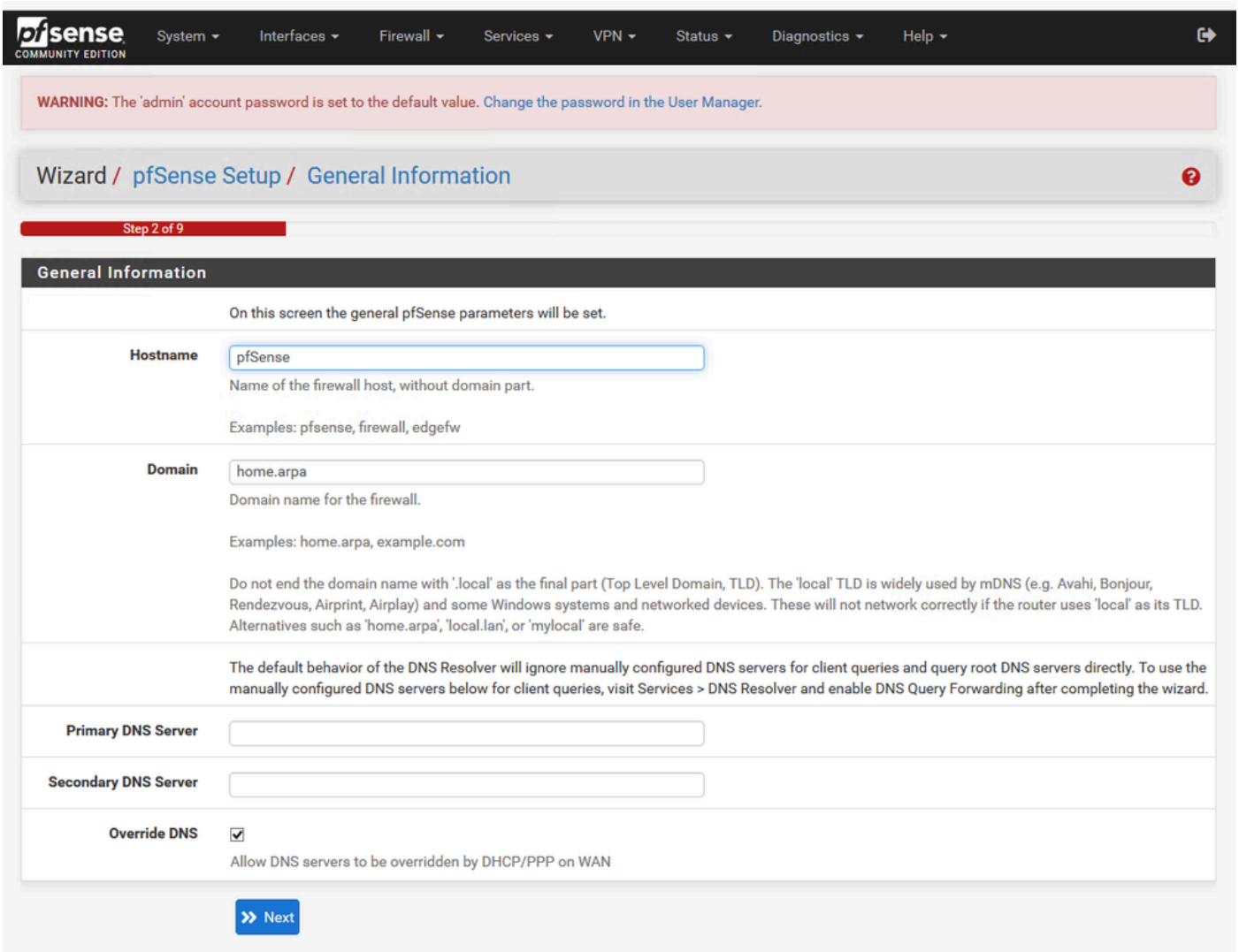
Étape 3. Terminer la configuration initiale

Cliquez sur Suivant dans les deux premiers écrans.



Assistant de configuration de pfSense - 1

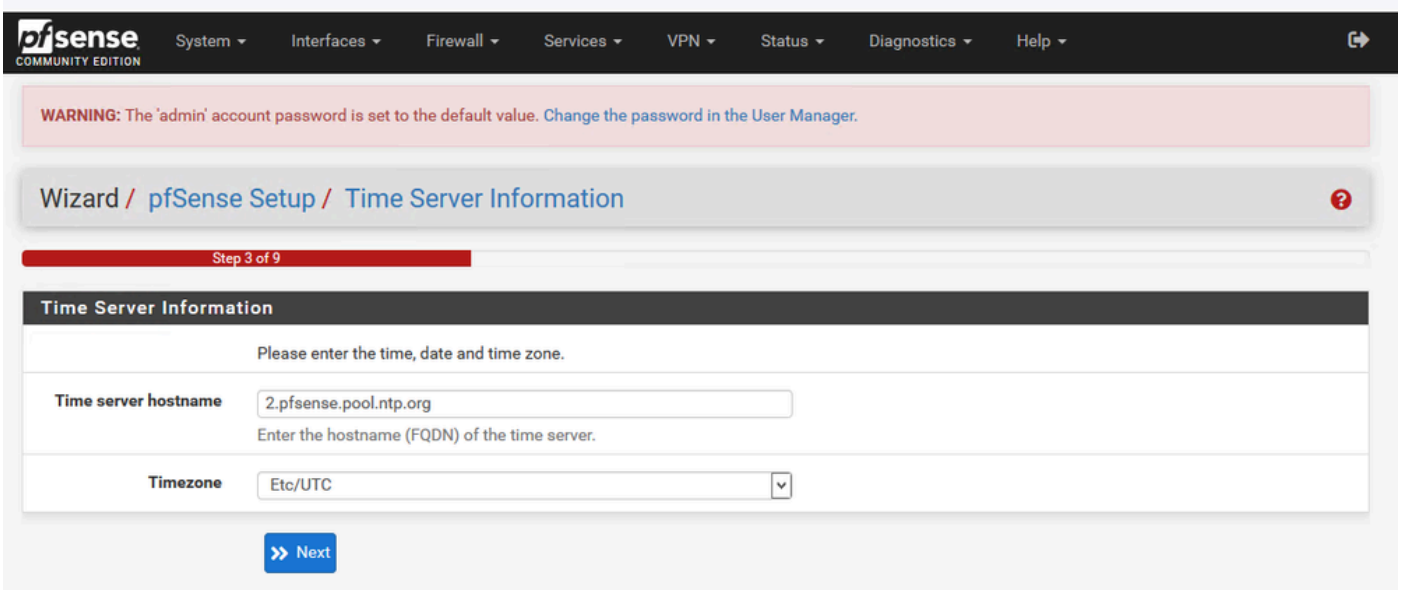
Fournissez le nom d'hôte, le nom de domaine et les informations du serveur DNS.



Assistant de configuration pfSense - 2

Validez les informations d'adresse IP. Si vous avez choisi DHCP pour la première fois, vous pouvez le modifier maintenant.

Fournissez le nom d'hôte du serveur NTP Time et sélectionnez le fuseau horaire correct dans la liste déroulante.



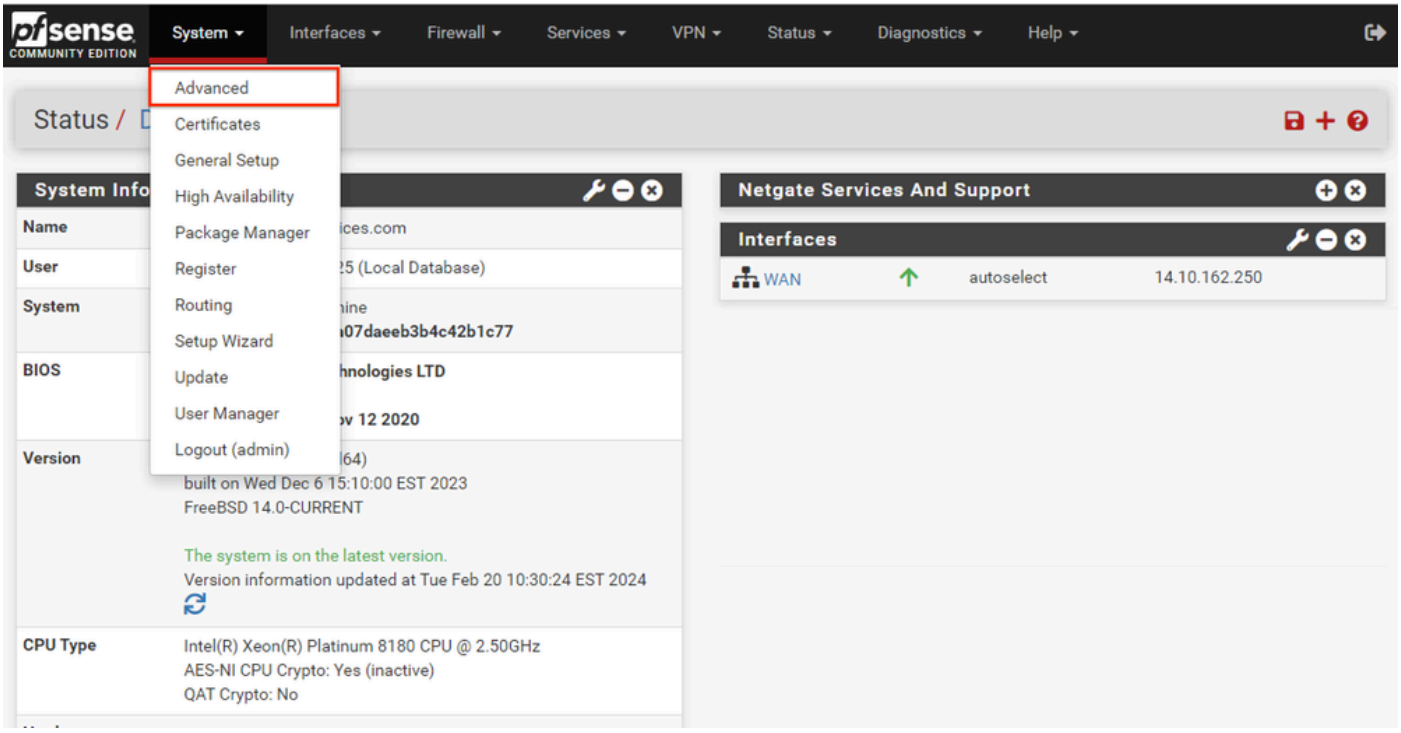
Assistant de configuration de pfSense - 3

Poursuivez l'Assistant de configuration jusqu'à la fin. L'interface GUI redémarre et vous êtes redirigé vers la nouvelle URL une fois terminée.

Configuration des paramètres d'administration de base

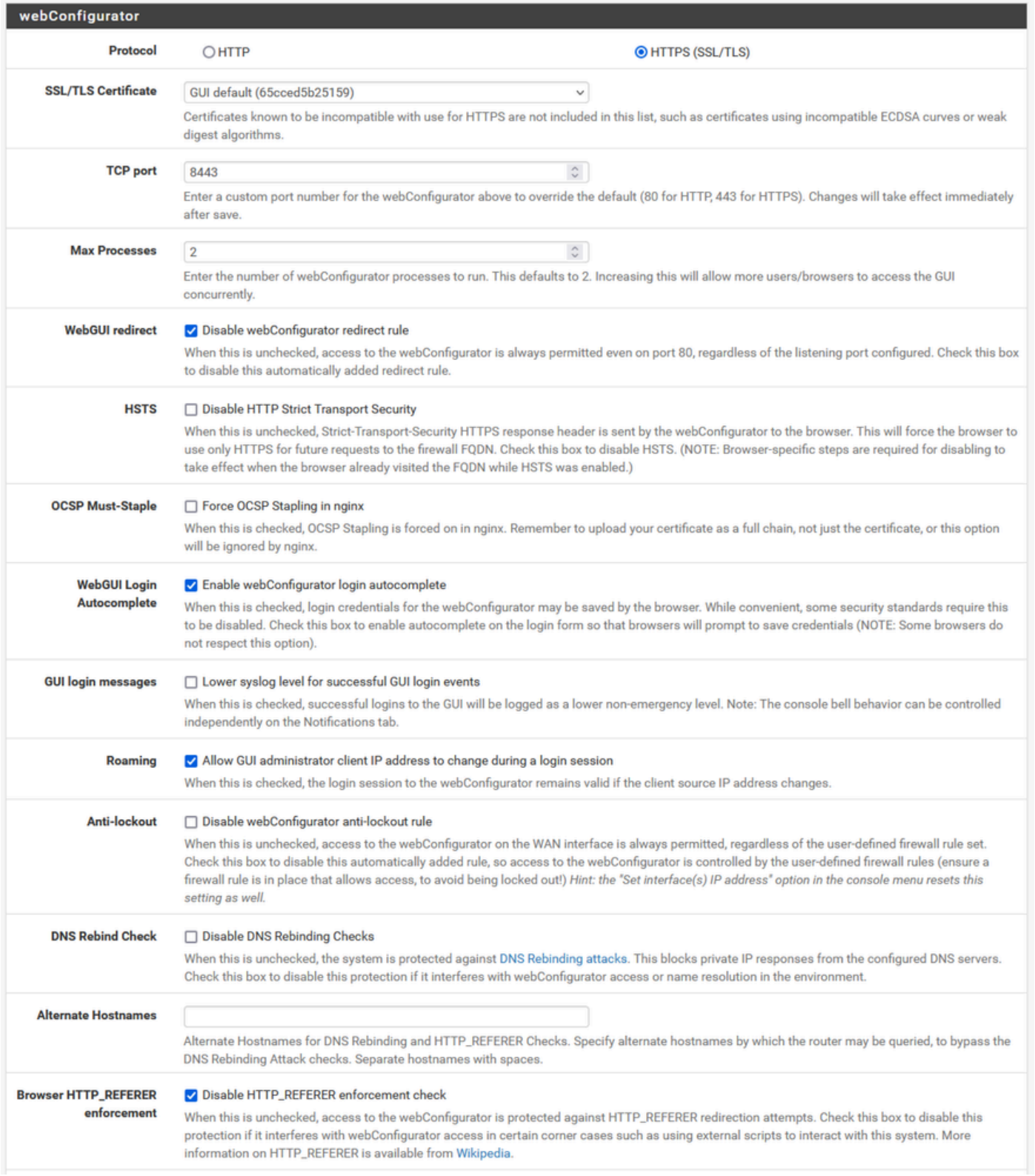
Étape 1. Connectez-vous à l'interface admin

Étape 2. Sélectionnez Avancé dans le menu déroulant Système



Interface utilisateur graphique pfSense - Liste déroulante Admin

Étape 3. Mettre à jour les paramètres webConfigurator



Interface utilisateur graphique pfSense - Configuration admin

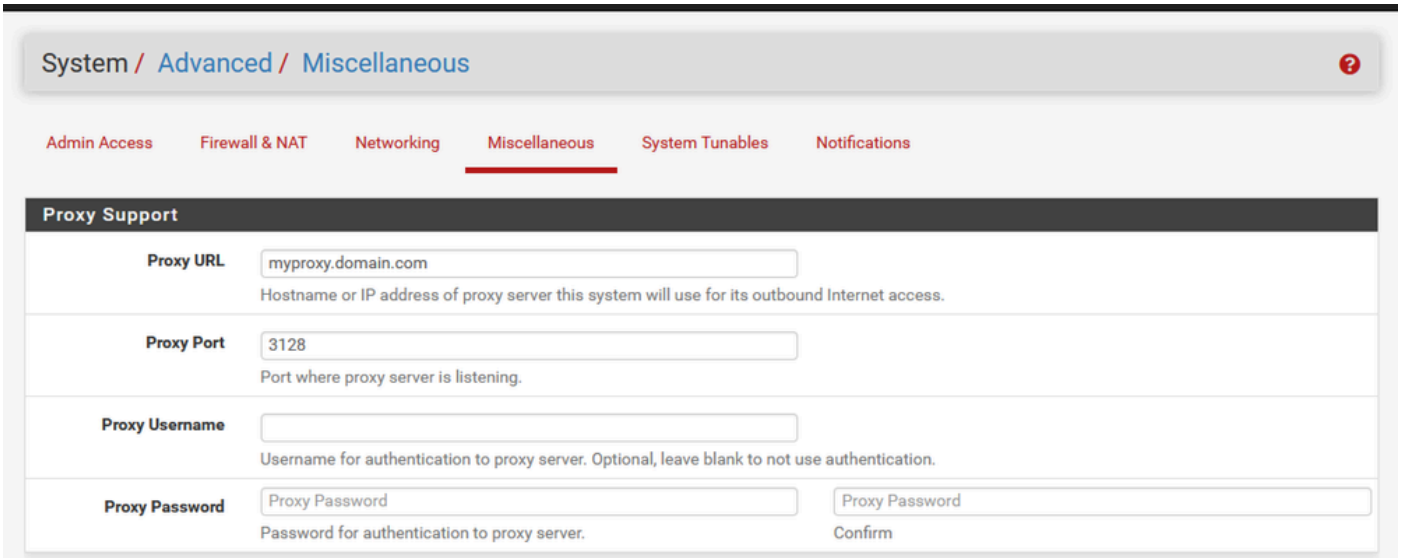
1. Sélectionnez le protocole HTTPS (SSL/TLS).
2. À ce stade, laissez le certificat SSL/TLS au certificat auto-signé.
3. Remplacez le port TCP par un port autre que le port 443 pour mieux sécuriser l'interface et éviter les problèmes de chevauchement de ports.
4. Sélectionnez l'option de redirection WebGUI pour désactiver l'interface d'administration sur le port 80.
5. Sélectionnez l'option d'application Browser HTTP_REFERER.

6. Activez Secure Shell en sélectionnant l'option Enable Secure Shell.

Remarque : assurez-vous de sélectionner le bouton Enregistrer avant de continuer. Vous êtes ensuite redirigé vers le nouveau lien https.

Étape 4. Configurez le serveur proxy si nécessaire

Si nécessaire, configurez les informations de proxy dans l'onglet Miscellaneous (Divers). Pour terminer l'installation et la configuration, l'appliance doit disposer d'un accès à Internet.



Interface utilisateur graphique pfSense - Configuration du proxy

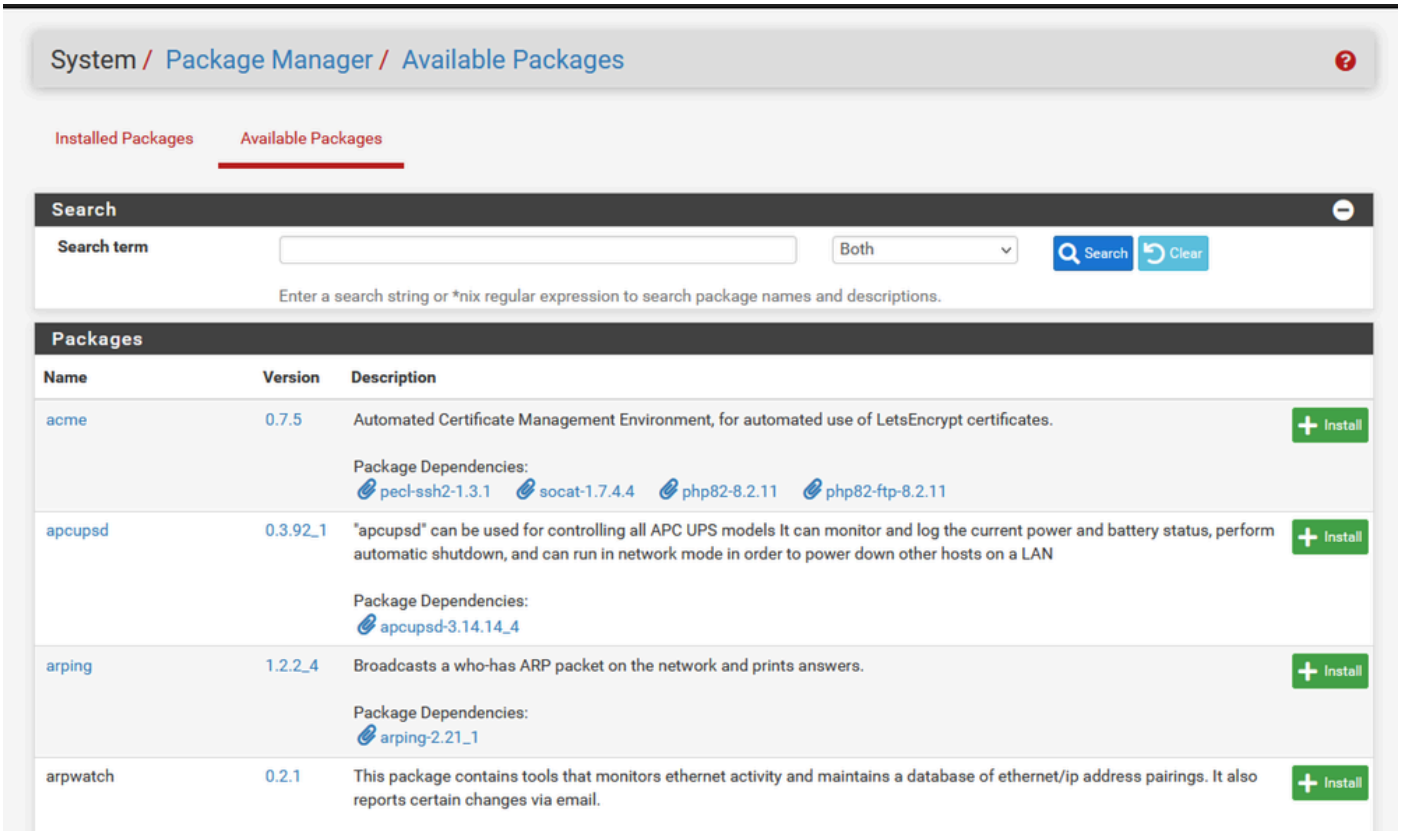
Remarque : assurez-vous de sélectionner le bouton Enregistrer après avoir effectué les modifications.

Ajouter les packages requis

Étape 1. Sélectionnez Système > Gestionnaire de package

Étape 2. Sélectionner les packages disponibles

Remarque : le chargement de tous les packages disponibles peut prendre quelques minutes. Si ce délai expire, vérifiez que les serveurs DNS sont correctement configurés. Souvent, un redémarrage de l'appliance corrige la connectivité Internet.



Interface utilisateur graphique pfSense - Liste de packages

Étape 3. Rechercher et installer les packages requis

1. haproxy
2. Open-VM-Tools

Remarque : ne sélectionnez pas le package haproxy-devel.

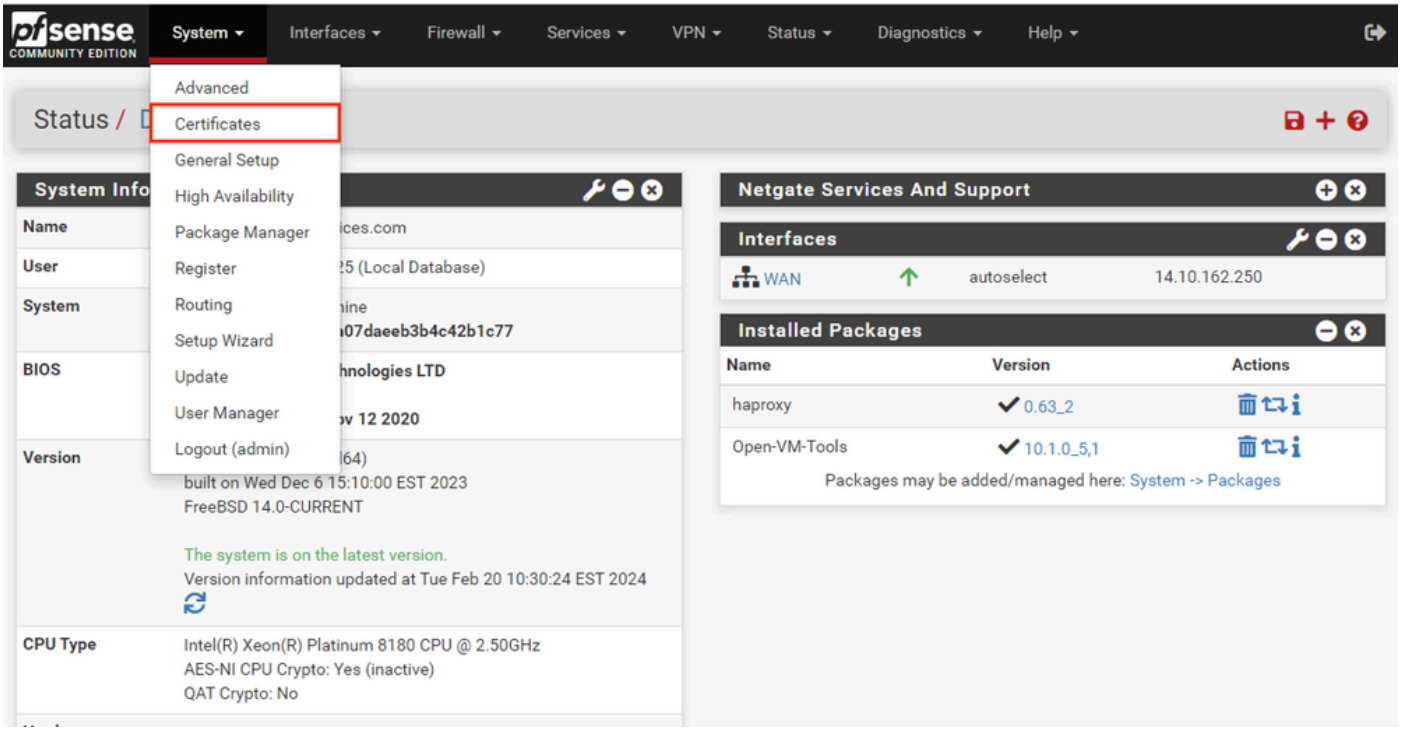
Configurer les certificats

pfSense peut créer un certificat auto-signé ou s'intégrer à une autorité de certification publique, une autorité de certification interne ou agir en tant qu'autorité de certification et émettre des certificats signés par une autorité de certification. Ce guide présente les étapes à suivre pour intégrer à une autorité de certification interne.

Avant de commencer cette section, assurez-vous que vous disposez de ces éléments.

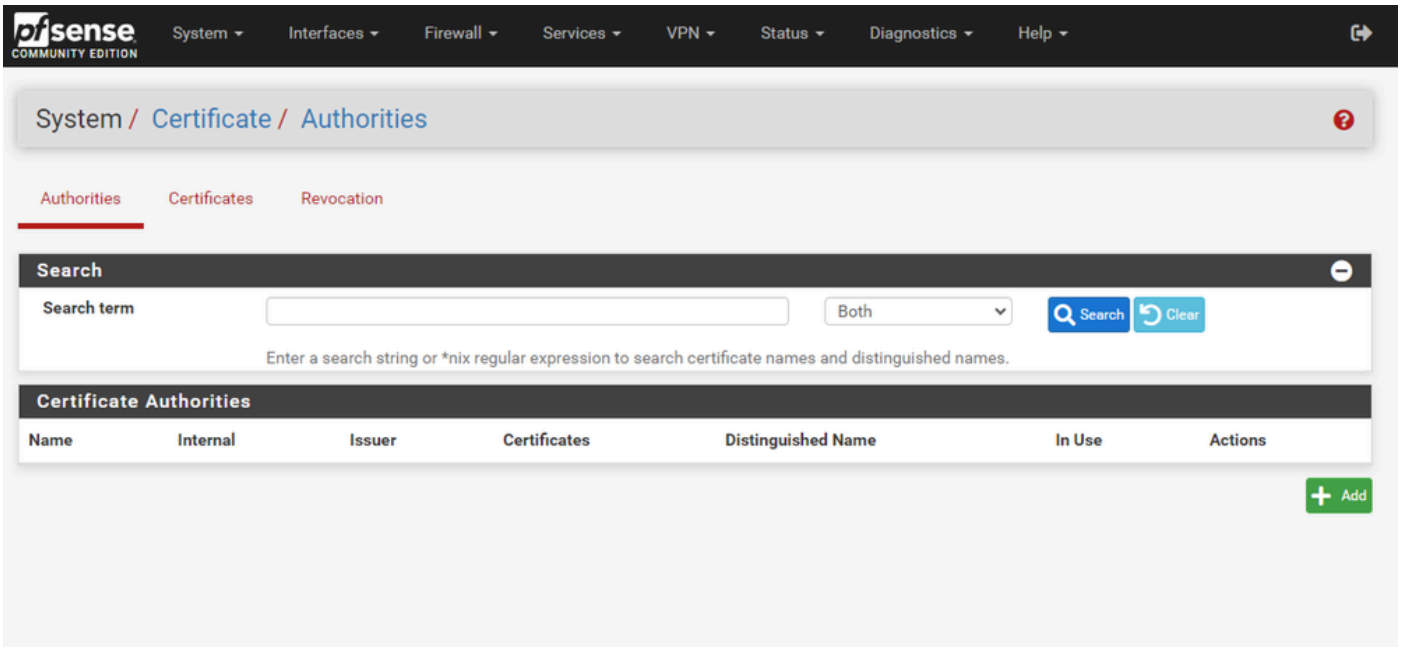
1. Certificat racine pour CA enregistré au format PEM ou codé en base 64.
2. Tous les certificats intermédiaires (parfois appelés certificats d'émission) pour l'autorité de certification sont enregistrés au format PEM ou au format codé Base-64.

Étape 1. Sélectionnez Certificats dans le menu déroulant Système



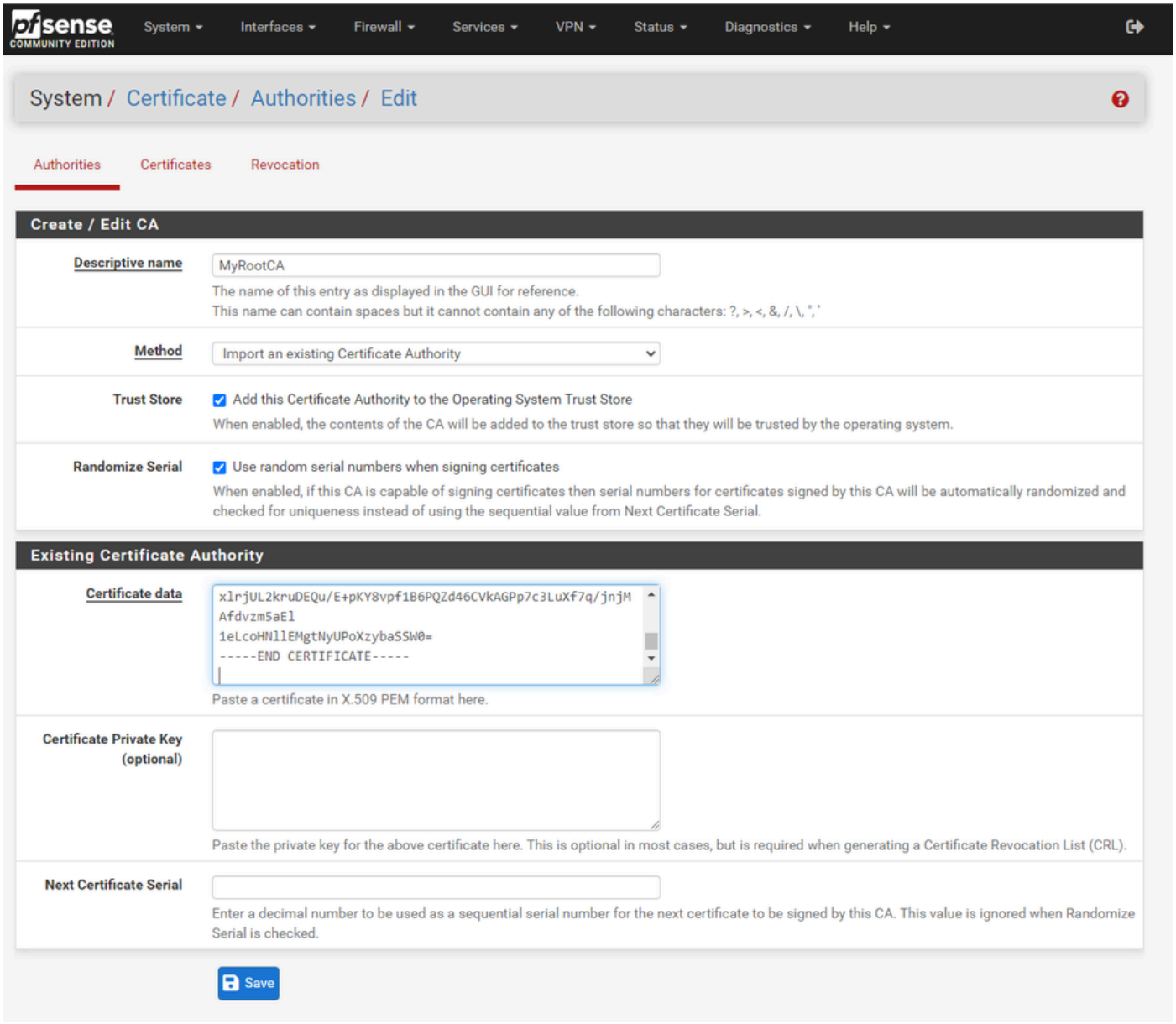
Interface utilisateur graphique pfSense - Liste déroulante Certificats

Étape 2. Importer le certificat racine CA



Interface utilisateur graphique pfSense - Liste des certificats CA

Cliquez sur le bouton Ajouter.



Interface graphique utilisateur pfSense - Importation CA

Comme l'illustre l'image :

1. Fournissez un nom unique et descriptif

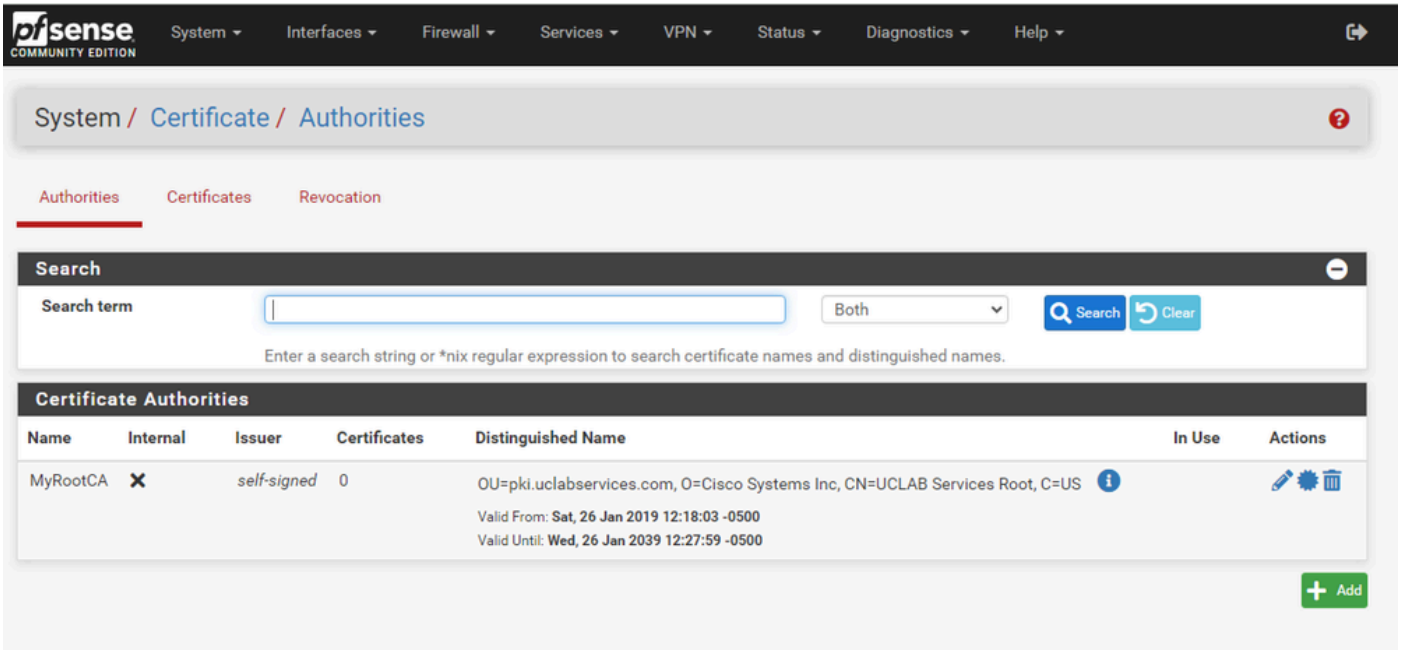
2. Sélectionnez Importer une autorité de certification existante dans la liste déroulante Méthode.

3. Assurez-vous que les cases à cocher Magasin sécurisé et Série aléatoire sont activées.

4. Collez l'intégralité du certificat dans la zone de texte Données du certificat. Assurez-vous d'inclure des lignes -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----.

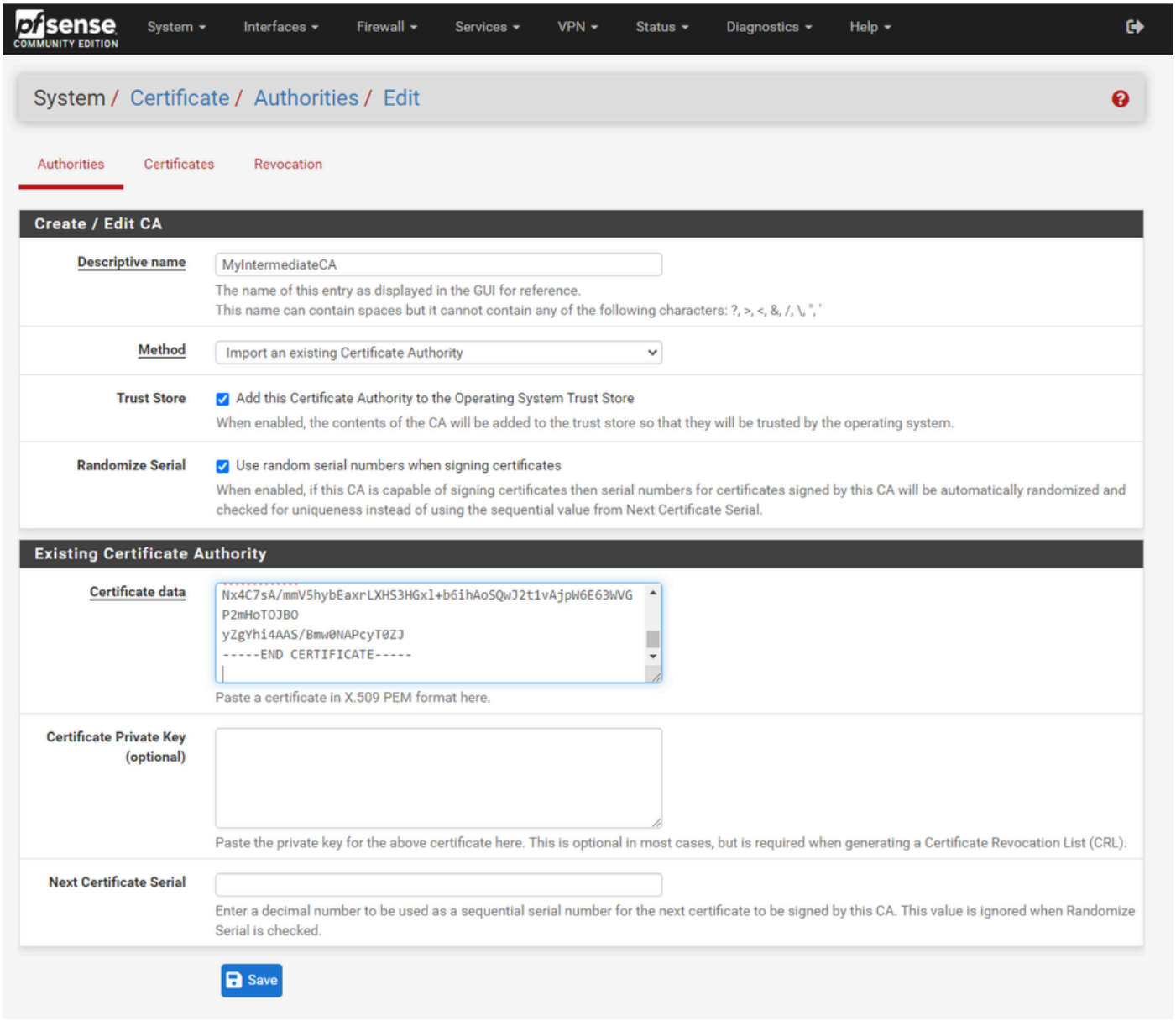
5. Sélectionnez Enregistrer.

6. Vérifiez que le certificat est importé comme indiqué dans l'image.



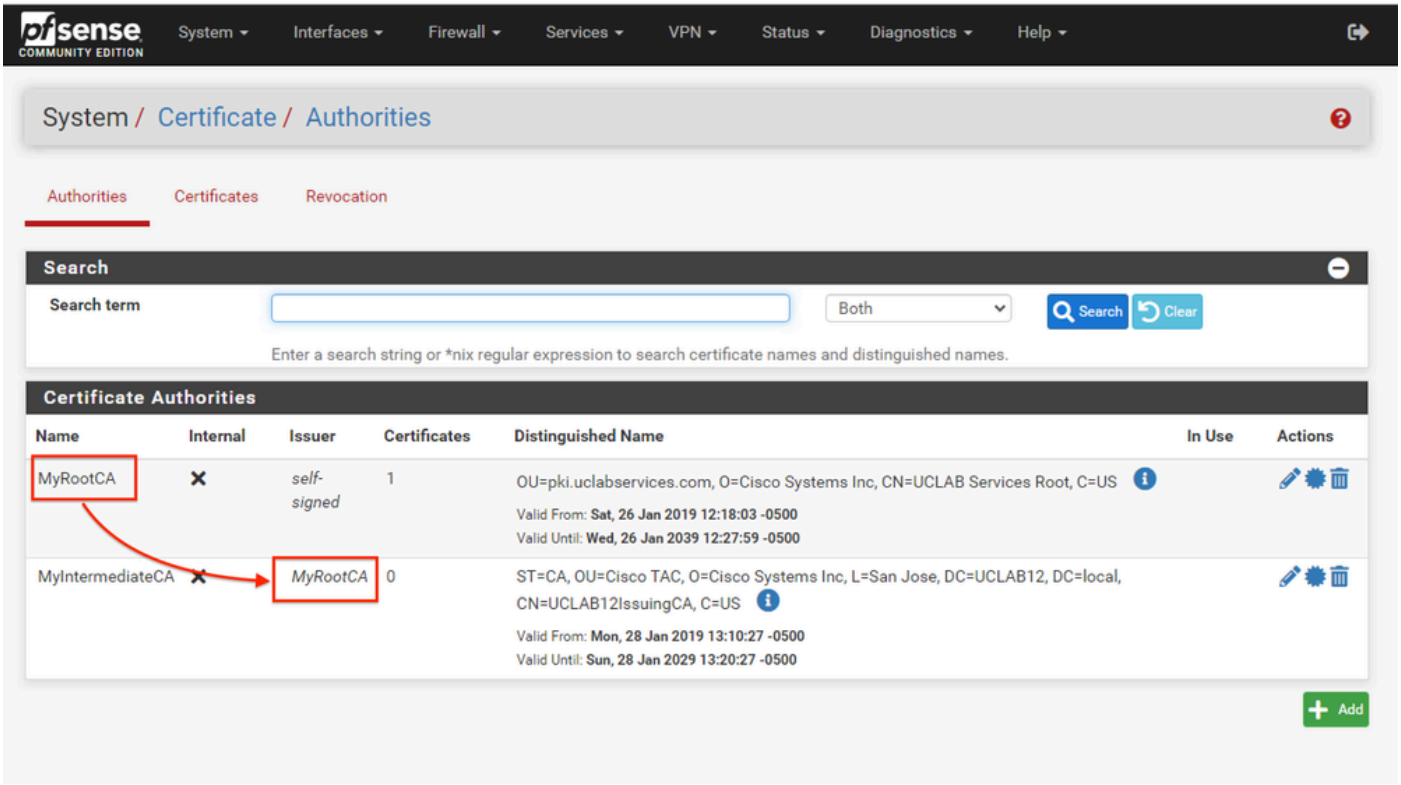
Interface utilisateur graphique pfSense - Liste CA

Étape 3. Importer le certificat intermédiaire CA



Interface graphique utilisateur pfSense - Importation intermédiaire CA

Répétez les étapes pour importer le certificat d'autorité de certification racine et importer le certificat d'autorité de certification intermédiaire.



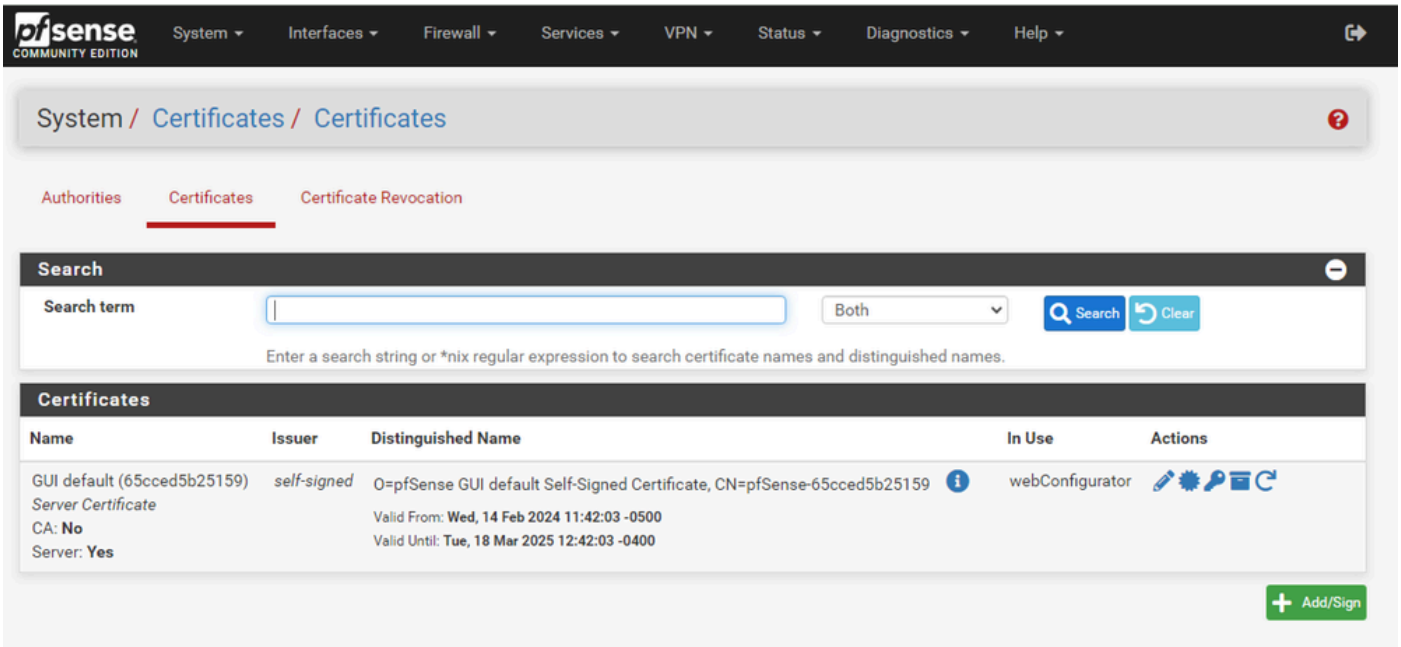
Interface graphique utilisateur pfSense - Liens CA

Vérifiez les autorités de certification pour vous assurer que l'intermédiaire est correctement enchaîné au certificat racine comme indiqué dans l'image.

Étape 4. Créer et exporter un CSR pour le site Web à charge équilibrée

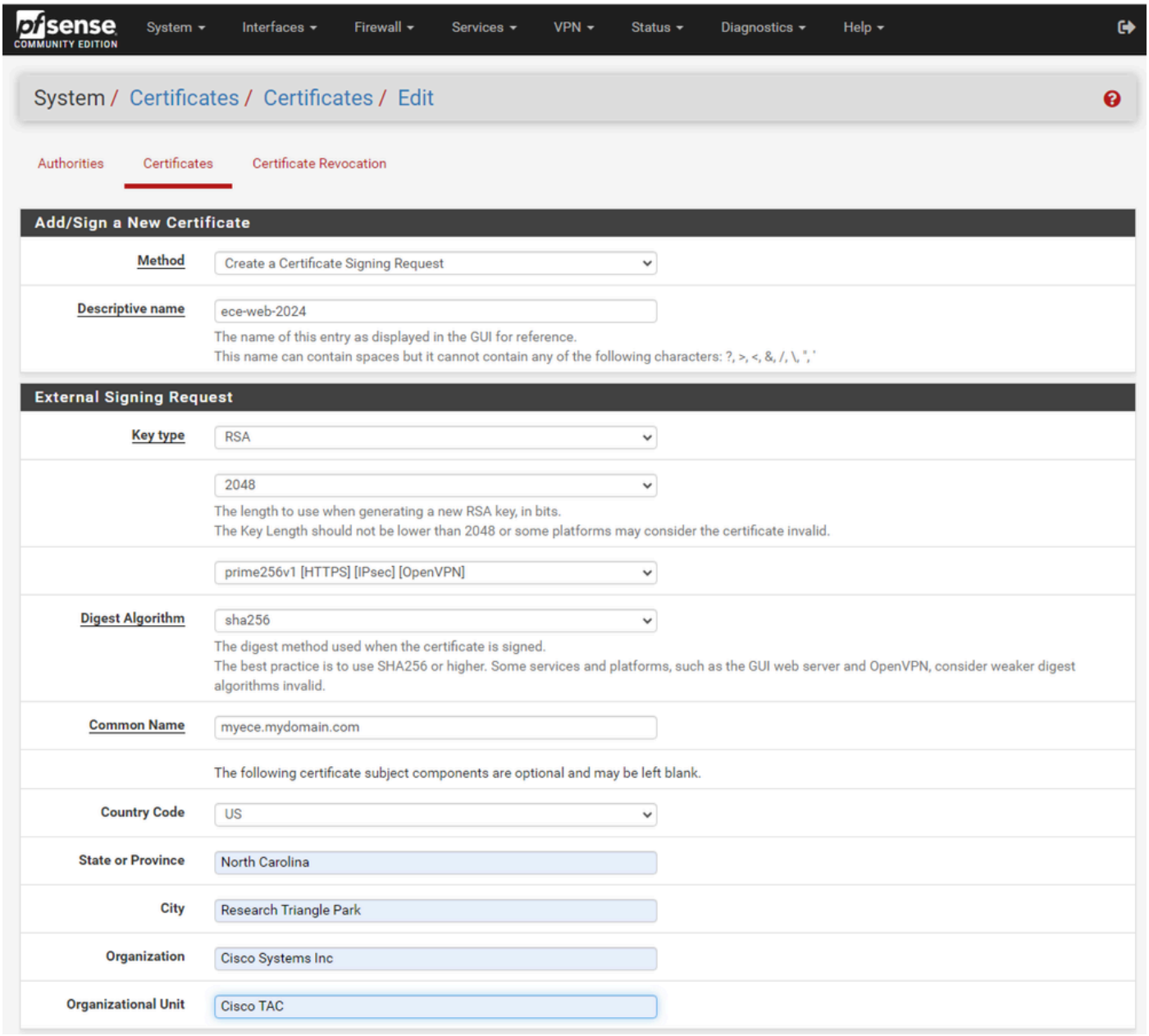
Cette section décrit les étapes à suivre pour créer un CSR, exporter le CSR, puis importer le certificat signé. Si vous disposez déjà d'un certificat au format PFX, vous pouvez importer ce certificat. Consultez la documentation de pfSense pour connaître ces étapes.

1. Sélectionnez le menu Certificats, puis le bouton Ajouter/Signer.



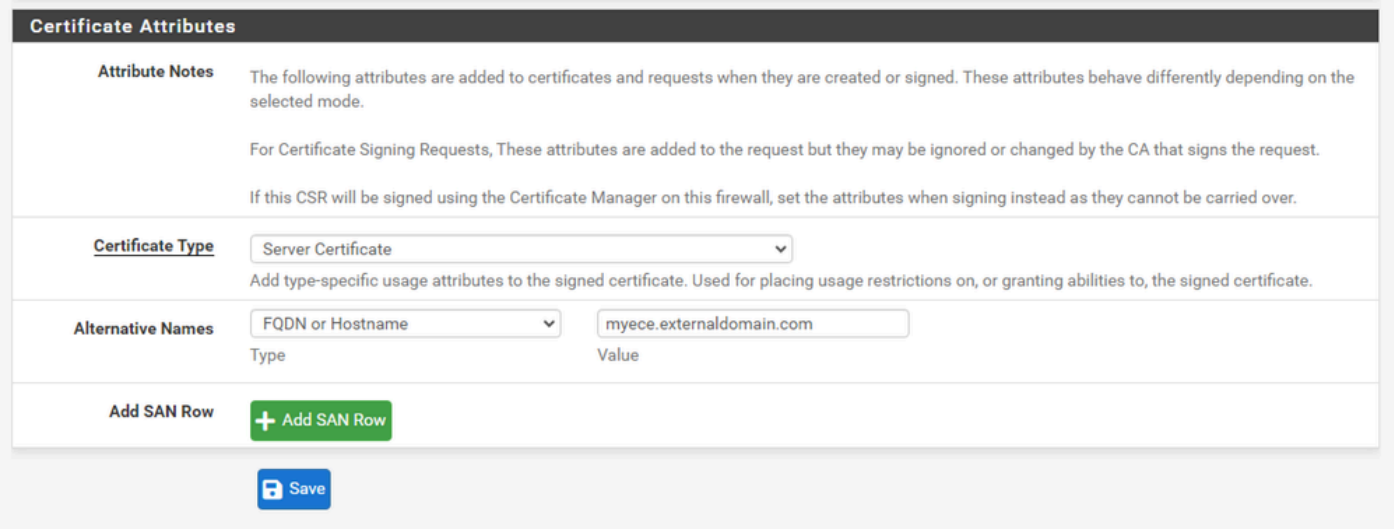
Interface utilisateur graphique pfSense - Liste des certificats

2. Remplissez le formulaire de demande de signature de certificat.



Interface utilisateur graphique pfSense - Création de CSR

- Méthode : sélectionnez Créer une demande de signature de certificat dans la liste déroulante
- Descriptive Name : saisissez un nom pour le certificat
- Type de clé et algorithme Digest : vérifiez qu'ils correspondent à vos besoins
- Nom commun : fournissez le site Web du nom de domaine complet
- Fournir les informations de certificat restantes requises pour votre environnement



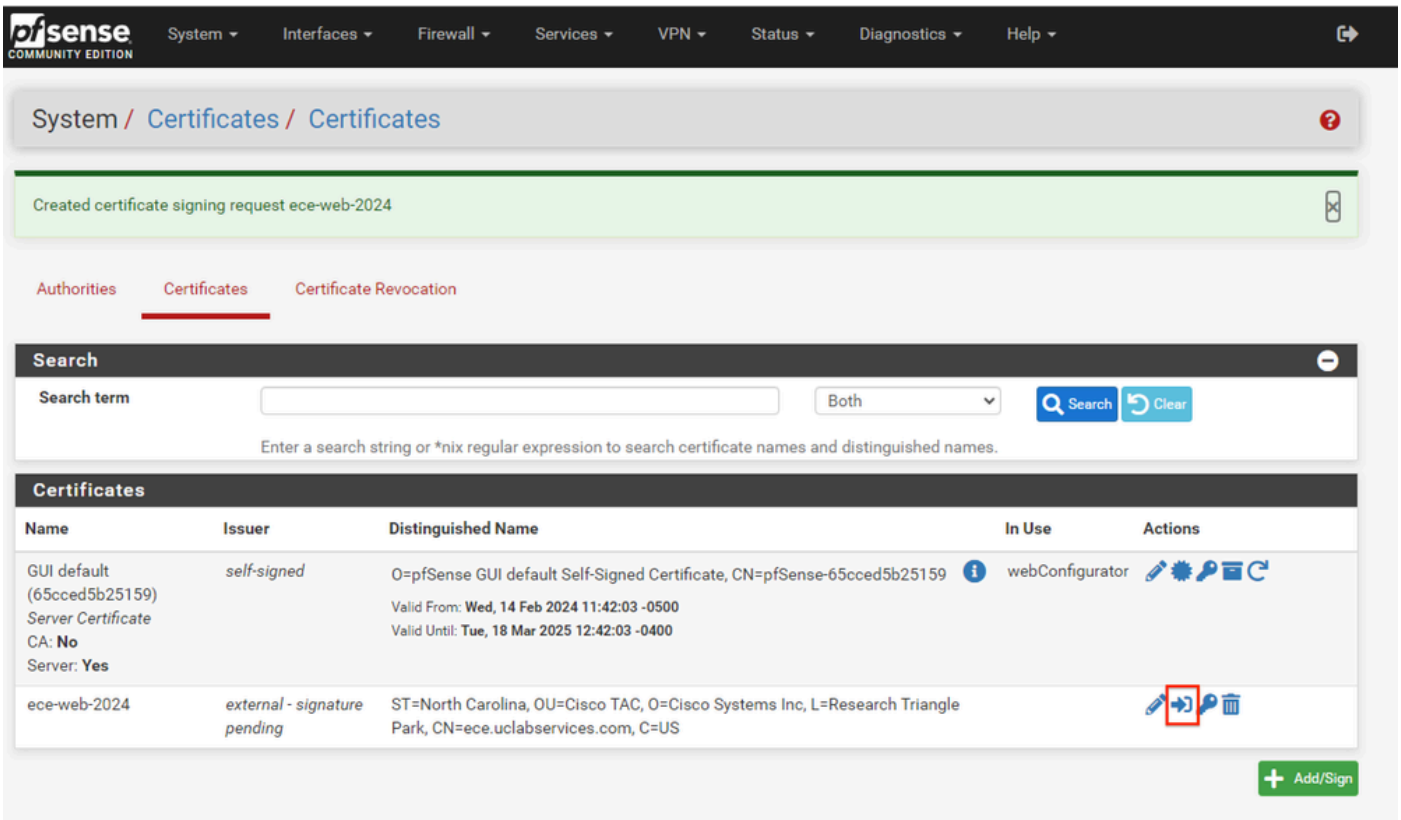
Interface utilisateur graphique pfSense - CSR Advanced

- Certificate Type : sélectionnez Server Certificate dans la liste déroulante.
- Autres noms : indiquez tout autre nom de sujet (SAN) requis pour votre mise en oeuvre.

Remarque : le nom commun est automatiquement ajouté au champ SAN. Il vous suffit d'ajouter les noms supplémentaires requis.

Sélectionnez Enregistrer une fois que tous les champs sont corrects.

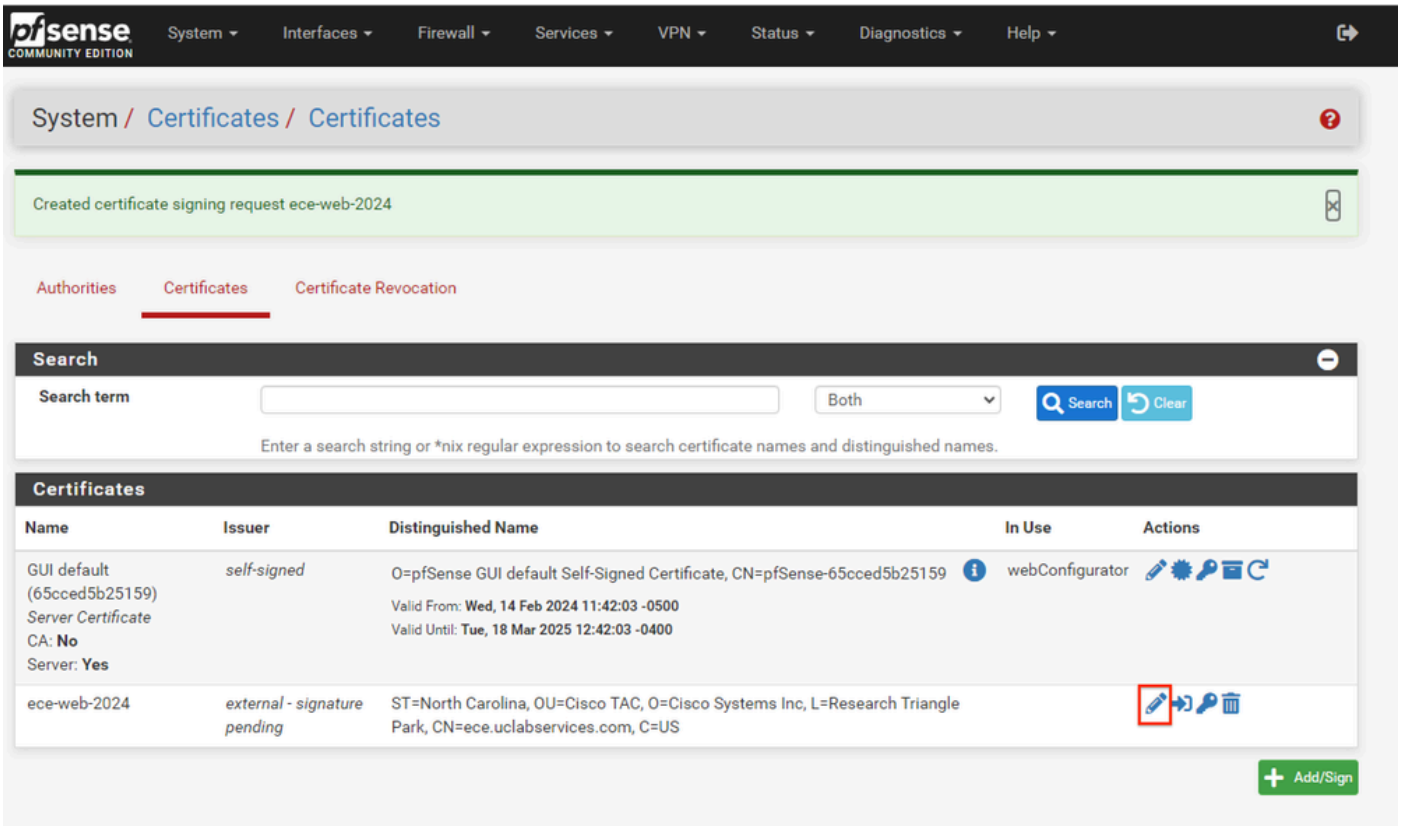
3. Exportez le CSR dans un fichier.



Interface utilisateur graphique pfSense - Exportation CSR

Cliquez sur le bouton Exporter pour enregistrer le CSR, puis signez-le avec votre autorité de certification. Une fois que vous avez le certificat signé, enregistrez-le dans un fichier PEM ou Base-64 pour terminer le processus.

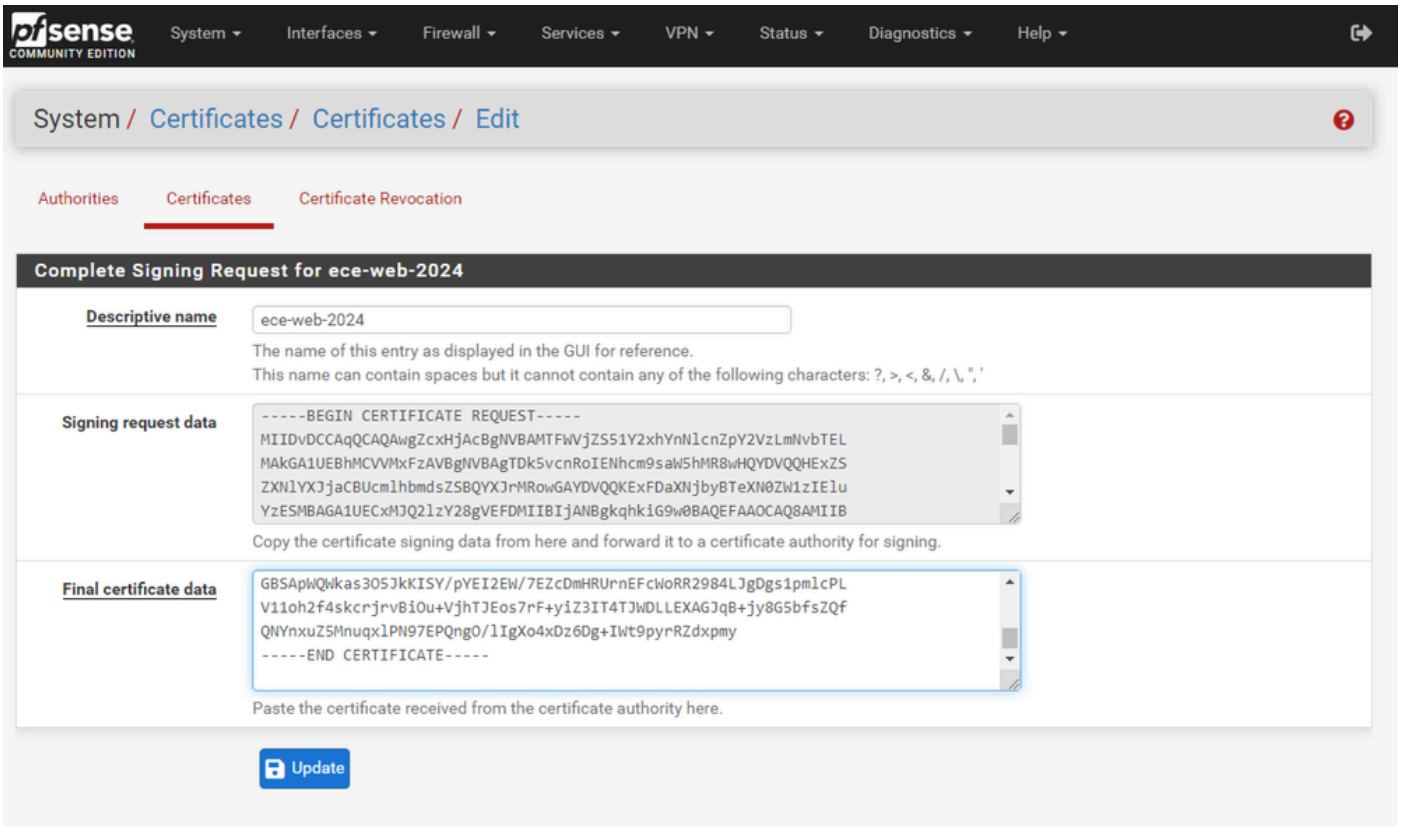
4. Importez le certificat signé.



Interface utilisateur graphique pfSense - Importation de certificat

Sélectionnez l'icône Crayon pour importer le certificat signé.

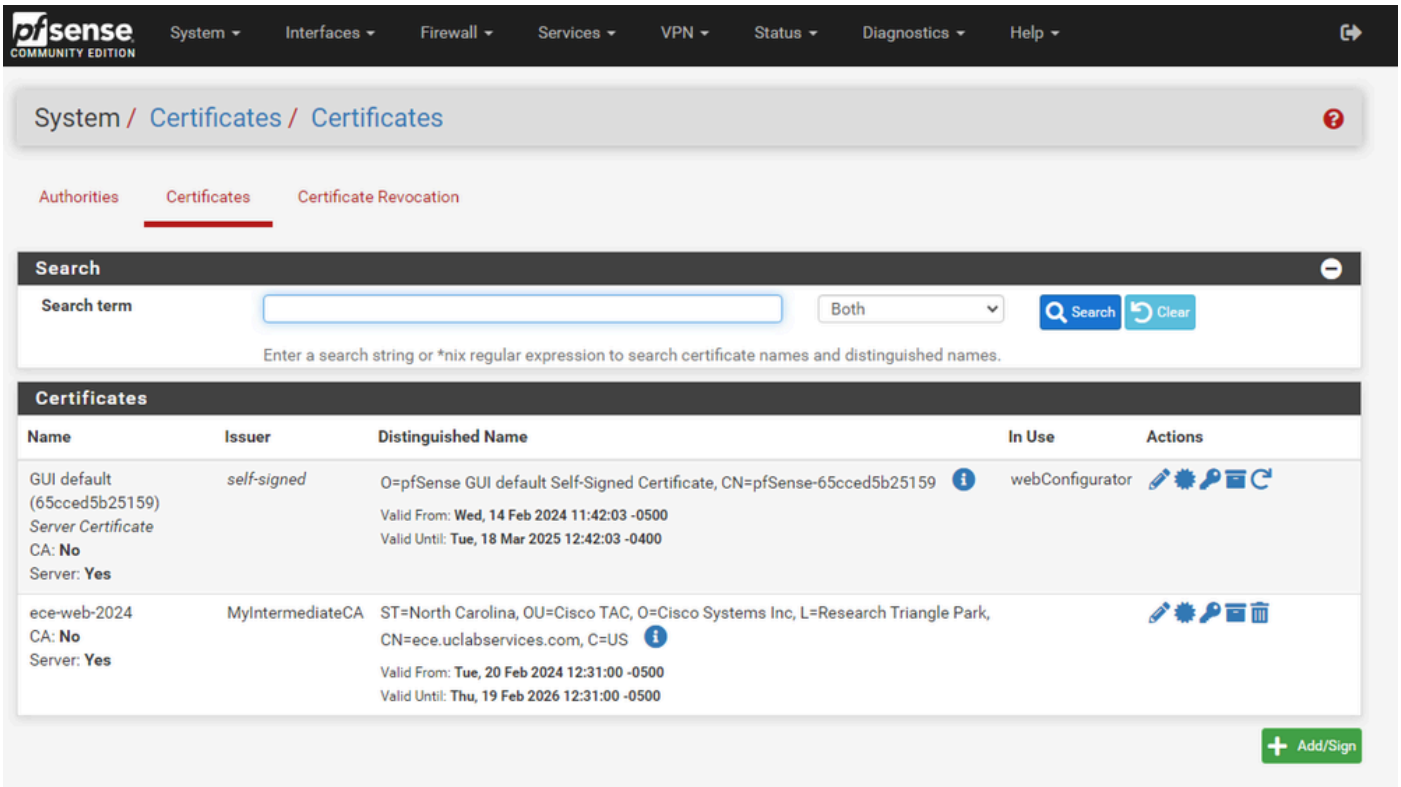
5. Collez les données du certificat dans le formulaire.



Interface utilisateur graphique pfSense - Importation de certificat

Sélectionnez Update pour enregistrer le certificat.

6. Vérifiez les données du certificat pour vous assurer qu'elles sont correctes.



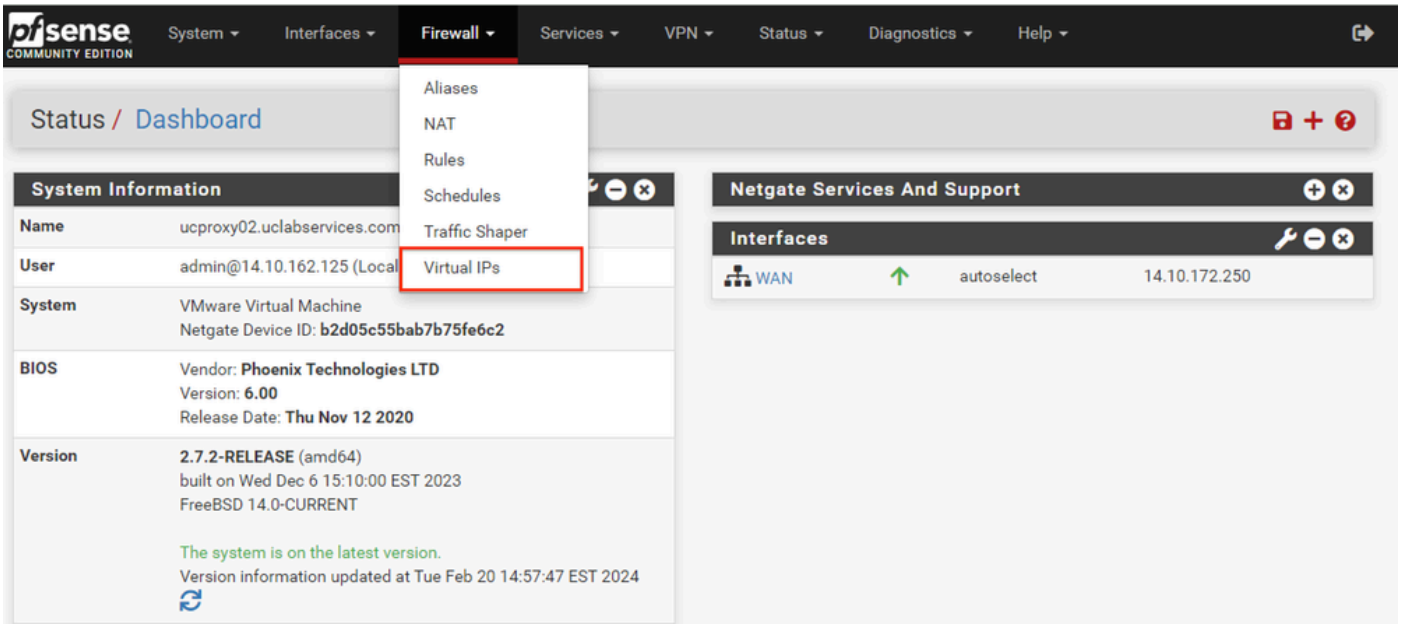
Interface utilisateur graphique pfSense - Liste de certificats

7. Répétez cette procédure si vous souhaitez héberger plusieurs sites sur ce pfSense.

Ajouter des adresses IP virtuelles

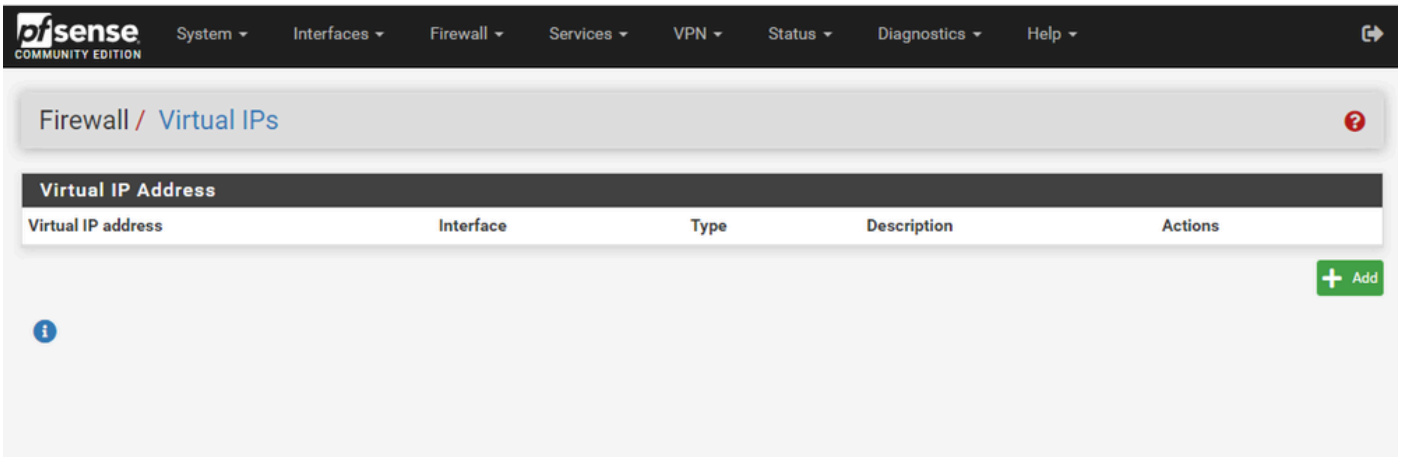
Au moins une adresse IP est requise pour héberger des sites Web sur le PfSense. Dans pfSense, cette opération est effectuée avec des adresses IP virtuelles (VIP).

Étape 1. Sélectionnez Virtual IPs dans la liste déroulante Firewall



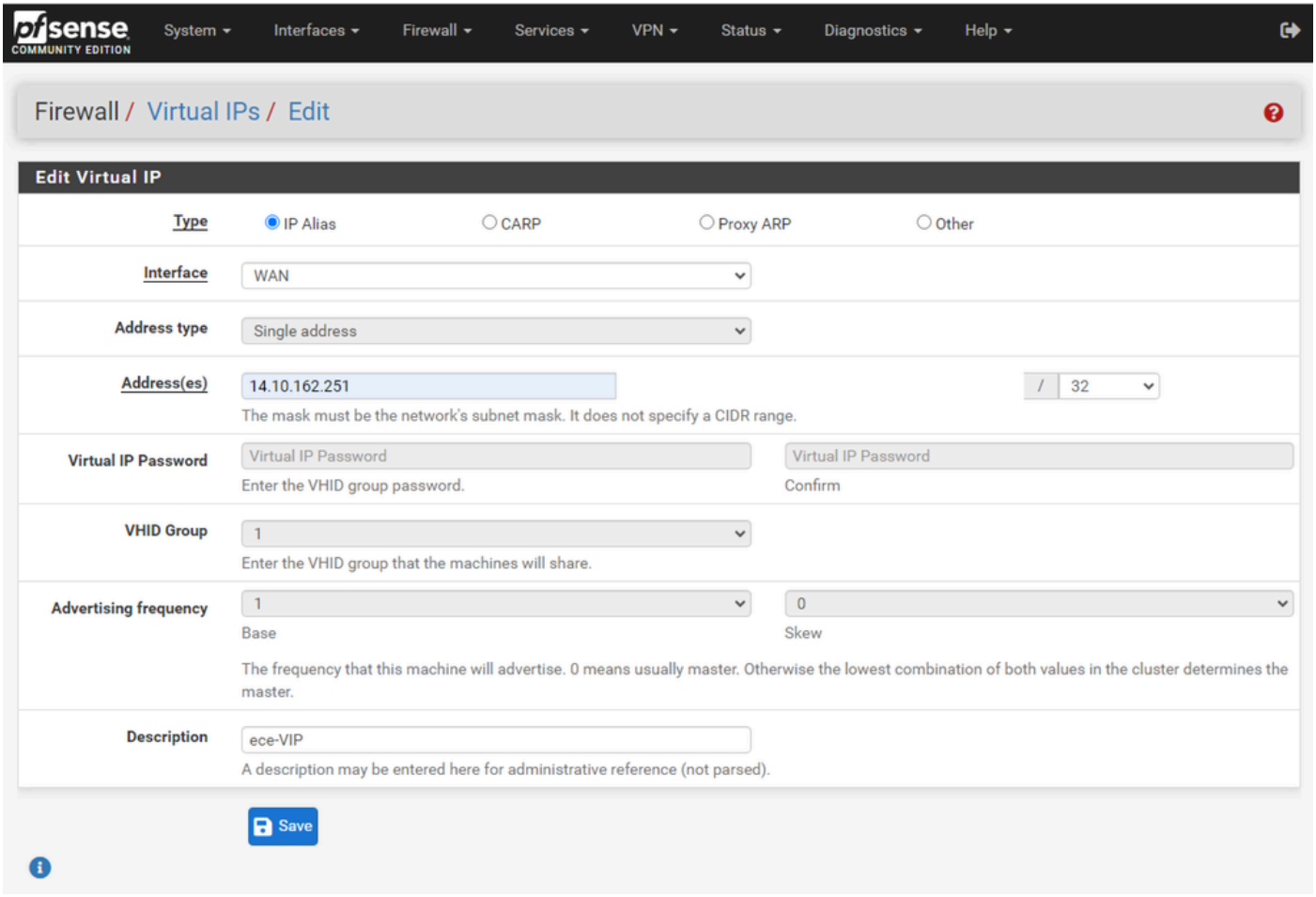
Interface utilisateur graphique pfSense - Liste déroulante VIP

Étape 2. Cliquez sur le bouton Ajouter



Interface utilisateur graphique pfSense - Page de renvoi VIP

Étape 3. Fournir les informations d'adresse



Interface utilisateur graphique pfSense - Configuration VIP

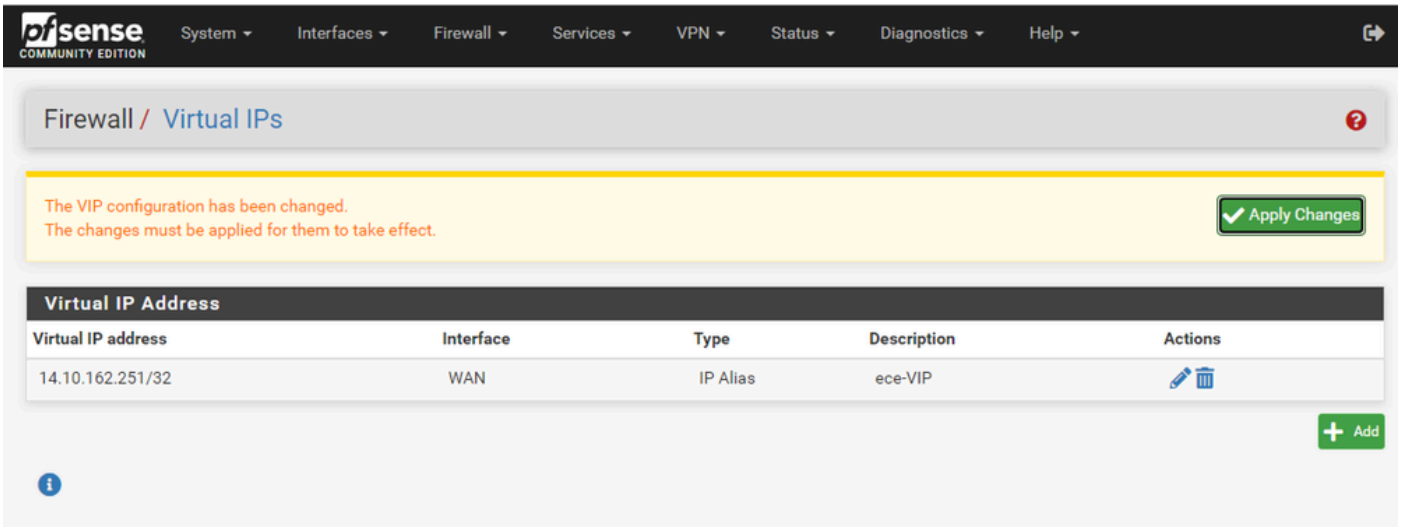
Utilisez ces informations pour ajouter un VIP.

- Type : sélectionnez l'alias IP
- Interface : sélectionnez l'interface pour cette adresse IP à diffuser
- Address(es) : saisissez l'adresse IP
- Address Mask : pour les adresses IP utilisées pour l'équilibrage de charge, le masque doit être /32
- Description : fournissez un court texte pour faciliter la compréhension de la configuration ultérieurement

Sélectionnez Enregistrer pour valider la modification.

Répétez cette opération pour chaque adresse IP requise pour votre configuration.

Étape 4. Appliquer la configuration



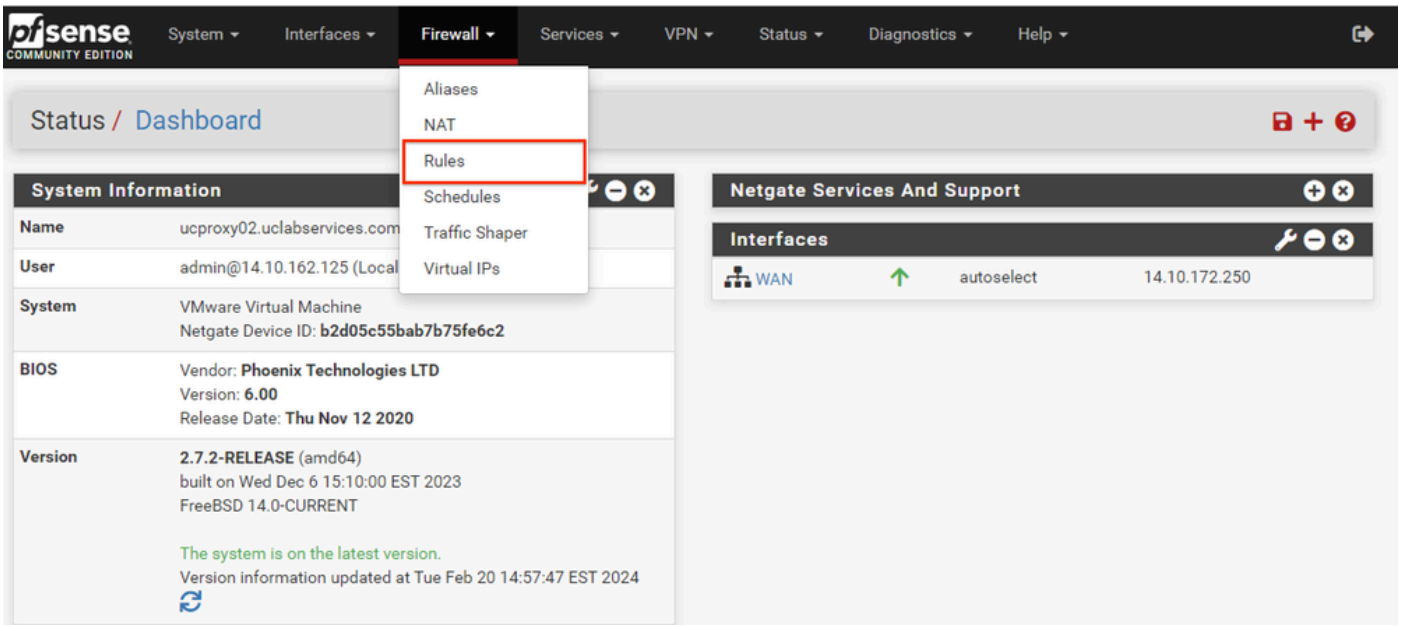
Interface utilisateur graphique pfSense - Liste VIP

Cliquez sur le bouton Appliquer les modifications après l'ajout de tous les VIP.

Configurer le pare-feu

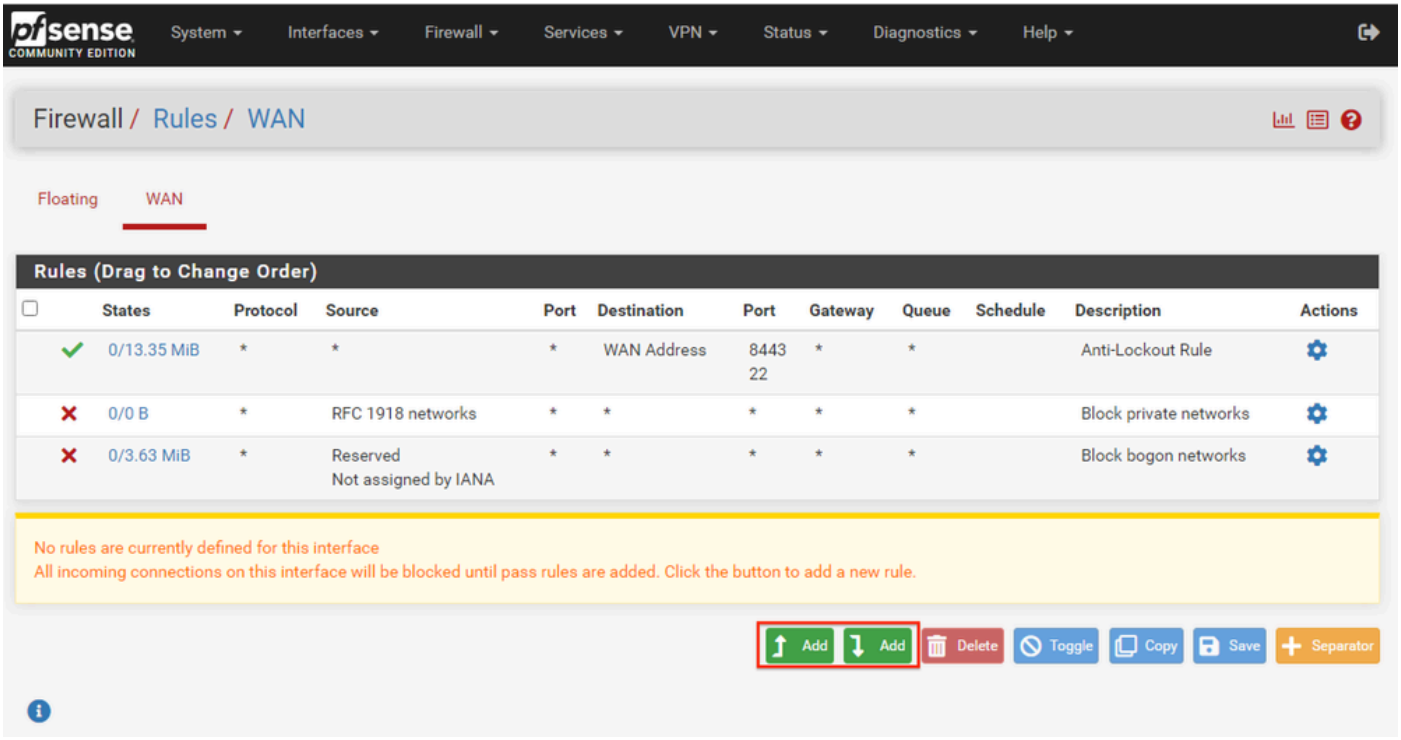
pfSense dispose d'un pare-feu intégré. Le jeu de règles par défaut est très limité. Avant la mise en production de l'appliance, assurez-vous de créer une stratégie de pare-feu complète.

Étape 1. Sélectionnez Règles dans la liste déroulante Pare-feu



Interface utilisateur graphique pfSense - Liste déroulante Règles de pare-feu

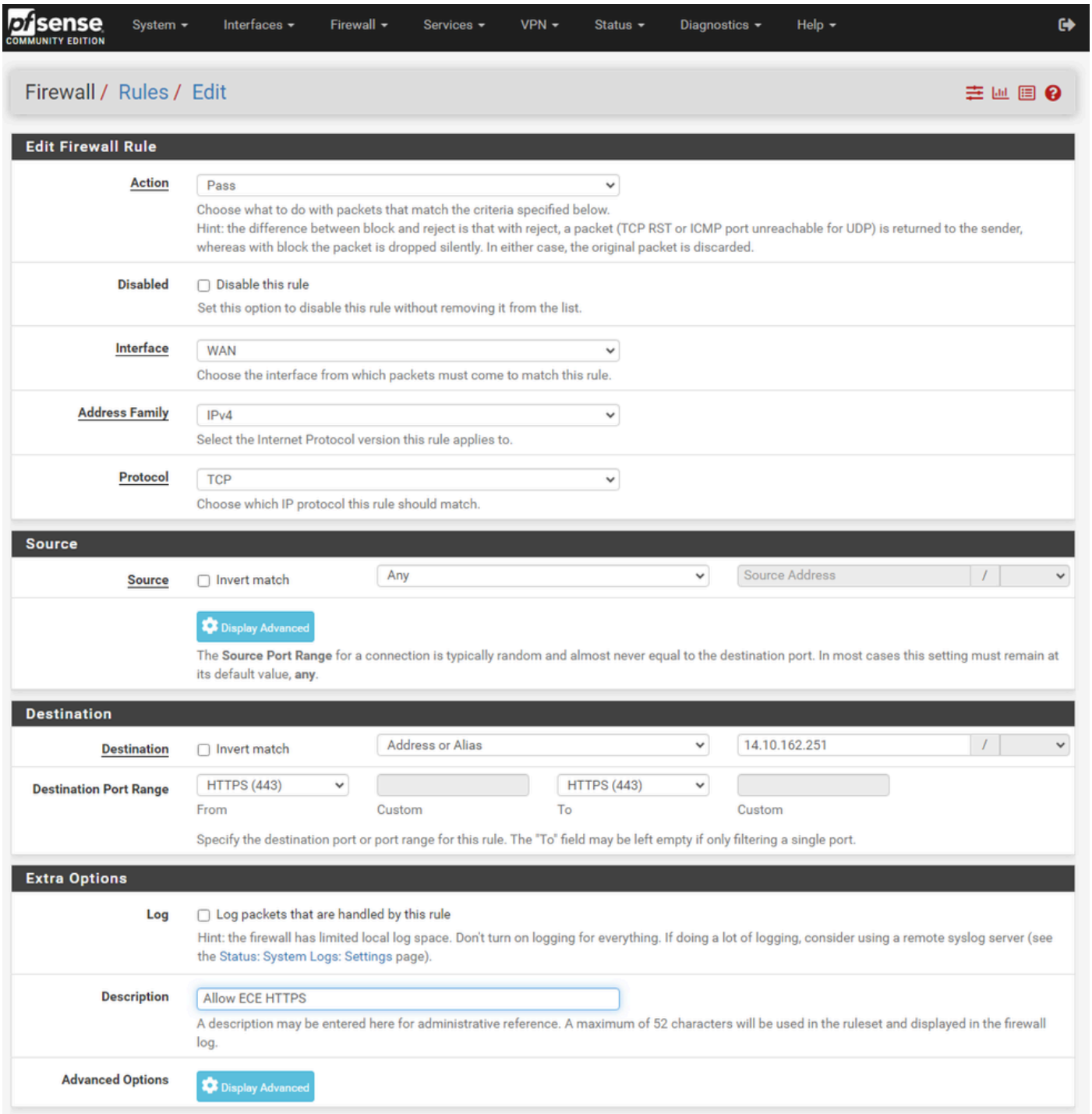
Étape 2. Sélectionnez l'un des boutons Ajouter



Interface utilisateur graphique pfSense - Liste des règles de pare-feu

Notez qu'un bouton ajoute la nouvelle règle au-dessus de la ligne sélectionnée tandis que l'autre ajoute la règle au-dessous de la règle sélectionnée. L'un ou l'autre bouton peut être utilisé pour la première règle.

Étape 3. Créer une règle de pare-feu pour autoriser le trafic vers le port 443 pour l'adresse IP



Interface utilisateur graphique pfSense - Configuration de la règle de passe de pare-feu

Utilisez les informations pour créer la règle.

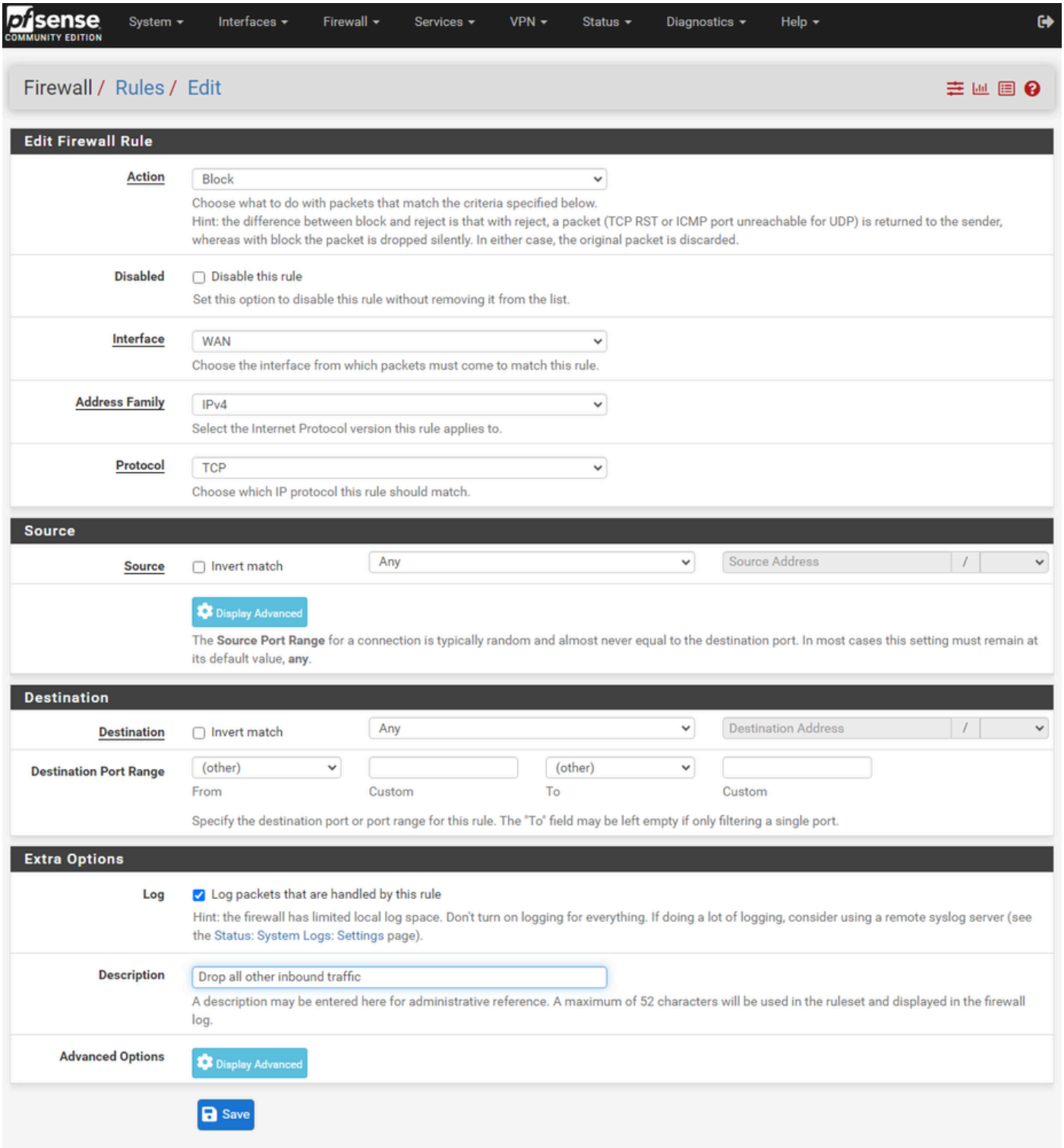
- Action : sélectionnez Pass (Réussite)
- Interface : sélectionnez l'interface à laquelle la règle s'applique
- Famille d'adresses et protocole : sélectionnez les options appropriées
- Source : laisser la valeur Tous sélectionnée
- Destination : sélectionnez Address ou Alias dans la liste déroulante Destination, puis saisissez l'adresse IP à laquelle la règle s'applique
- Destination Port Range : sélectionnez HTTPS (443) dans les listes déroulantes From et To
- Log : cochez cette case pour consigner tous les paquets qui correspondent à cette règle pour la comptabilisation

- Description : fournissez du texte pour faire référence à la règle ultérieurement

Sélectionnez Enregistrer.

Étape 4. Créer une règle de pare-feu pour abandonner tout autre trafic vers le PfSense

Cliquez sur le bouton Ajouter pour insérer la règle sous la nouvelle règle créée.



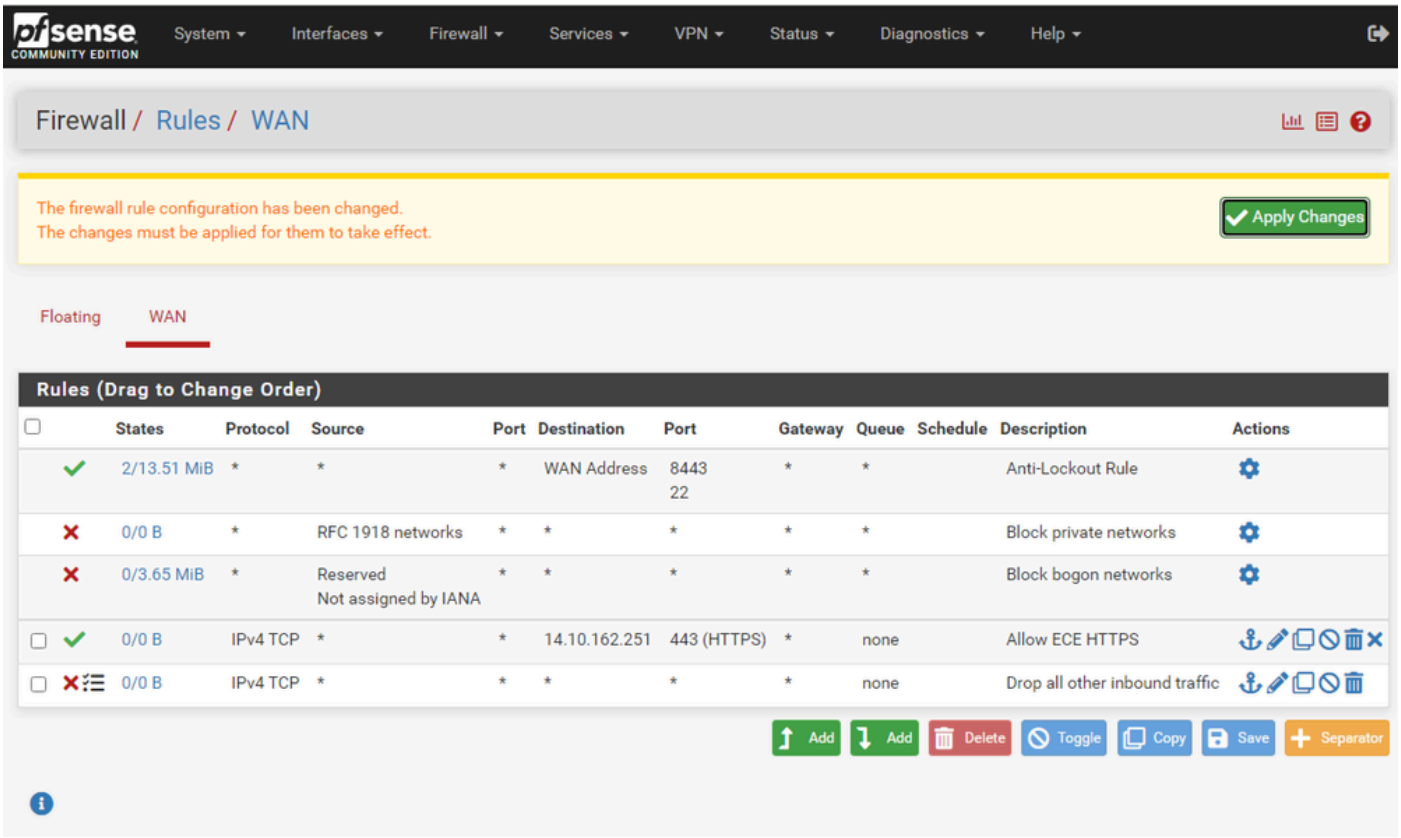
Interface utilisateur graphique pfSense - Configuration de la règle d'abandon du pare-feu

- Action : sélectionnez Bloquer

- Interface : sélectionnez l'interface à laquelle la règle s'applique
- Famille d'adresses et protocole : sélectionnez les options appropriées
- Source : laisser la valeur Tous sélectionnée
- Destination : laissez la valeur Tous sélectionnée
- Log : cochez cette case pour consigner tous les paquets qui correspondent à cette règle pour la comptabilisation
- Description : fournissez du texte pour faire référence à la règle ultérieurement

Sélectionnez Enregistrer.

Étape 5. Vérifiez les règles et assurez-vous que la règle de blocage se trouve en bas



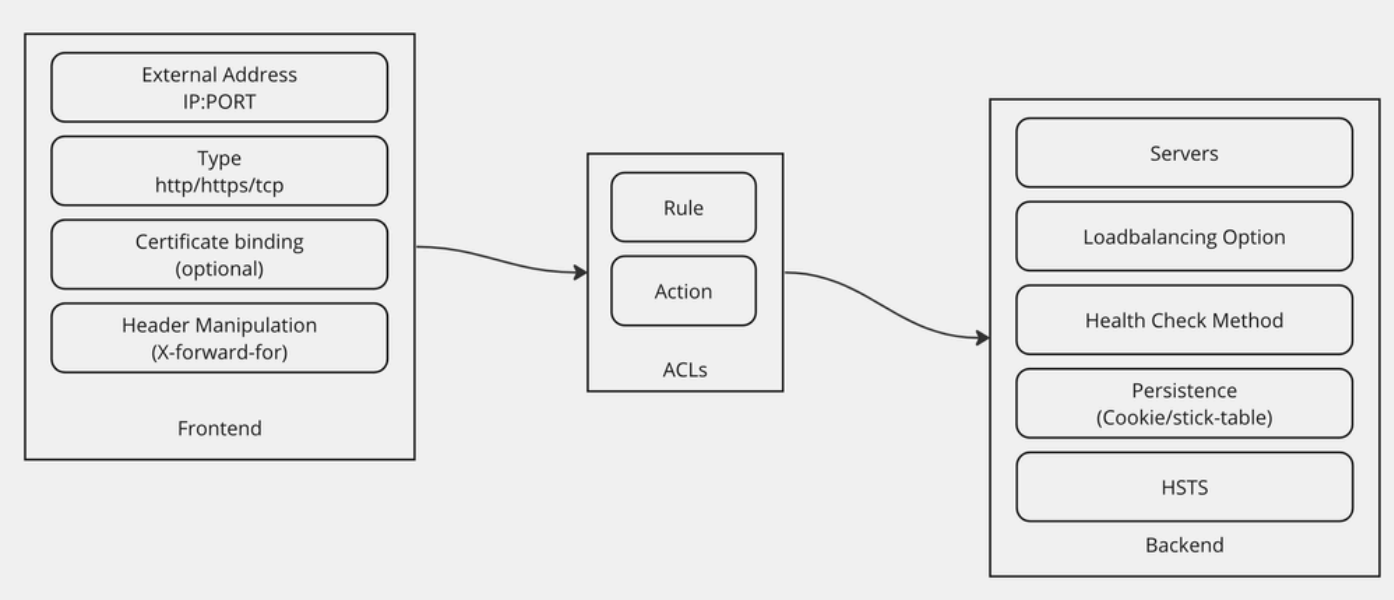
Interface utilisateur graphique pfSense - Liste des règles de pare-feu

Si nécessaire, faites glisser les règles pour les trier.

Sélectionnez Apply Changes une fois que les règles de pare-feu sont dans l'ordre requis pour votre environnement.

Configurer HAProxy

Concepts HAProxy



Concepts HAProxy

HAProxy est mis en oeuvre avec un modèle frontal/principal.

Le frontal définit le côté du proxy avec lequel les clients communiquent.

Le frontal se compose d'une combinaison IP et port, d'une liaison de certificat et peut implémenter une manipulation d'en-tête.

Le serveur principal définit le côté du proxy qui communique avec les serveurs Web physiques.

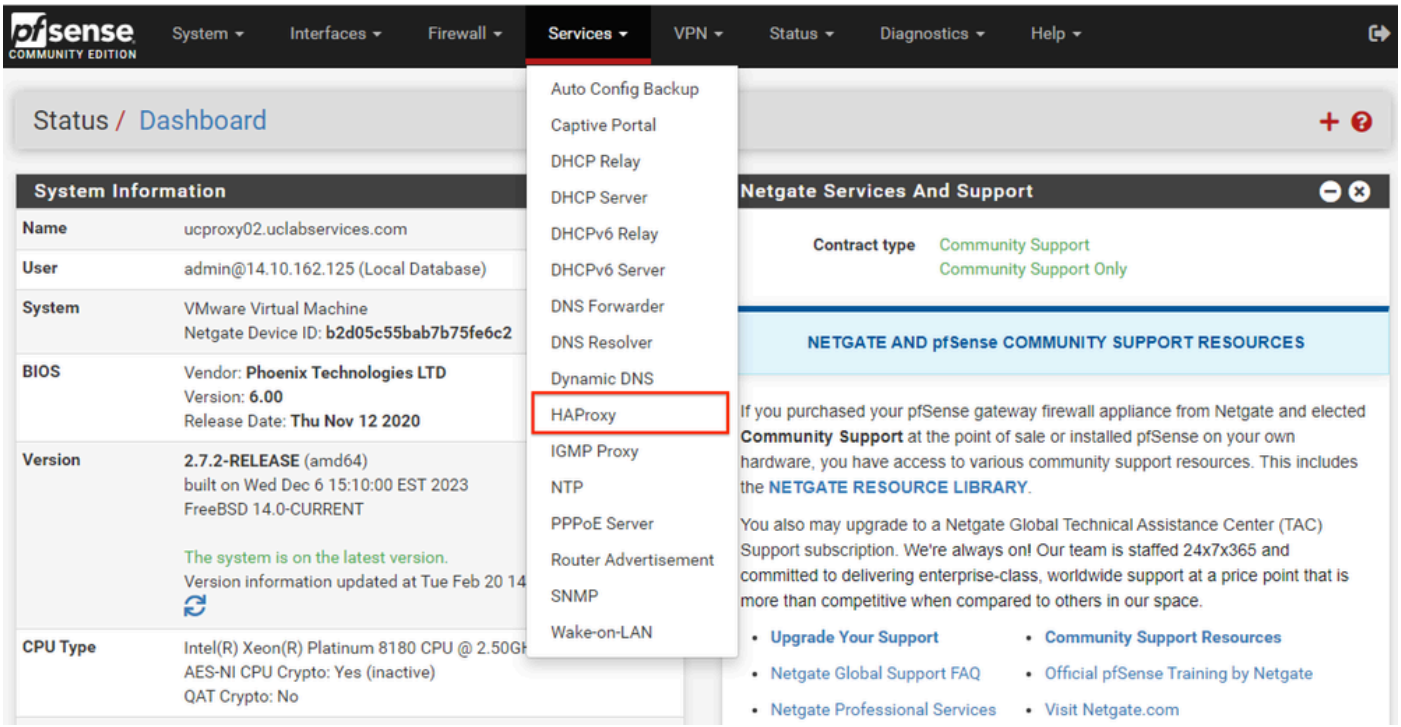
Le serveur principal définit les serveurs et les ports réels, la méthode d'équilibrage de charge pour l'affectation initiale, les contrôles d'intégrité et la persistance.

Un frontal sait avec quel backend communiquer, soit par un backend dédié, soit en utilisant des listes de contrôle d’accès.

Les listes de contrôle d’accès peuvent créer différentes règles de sorte qu’un frontal donné puisse communiquer avec différents backends en fonction de différents éléments.

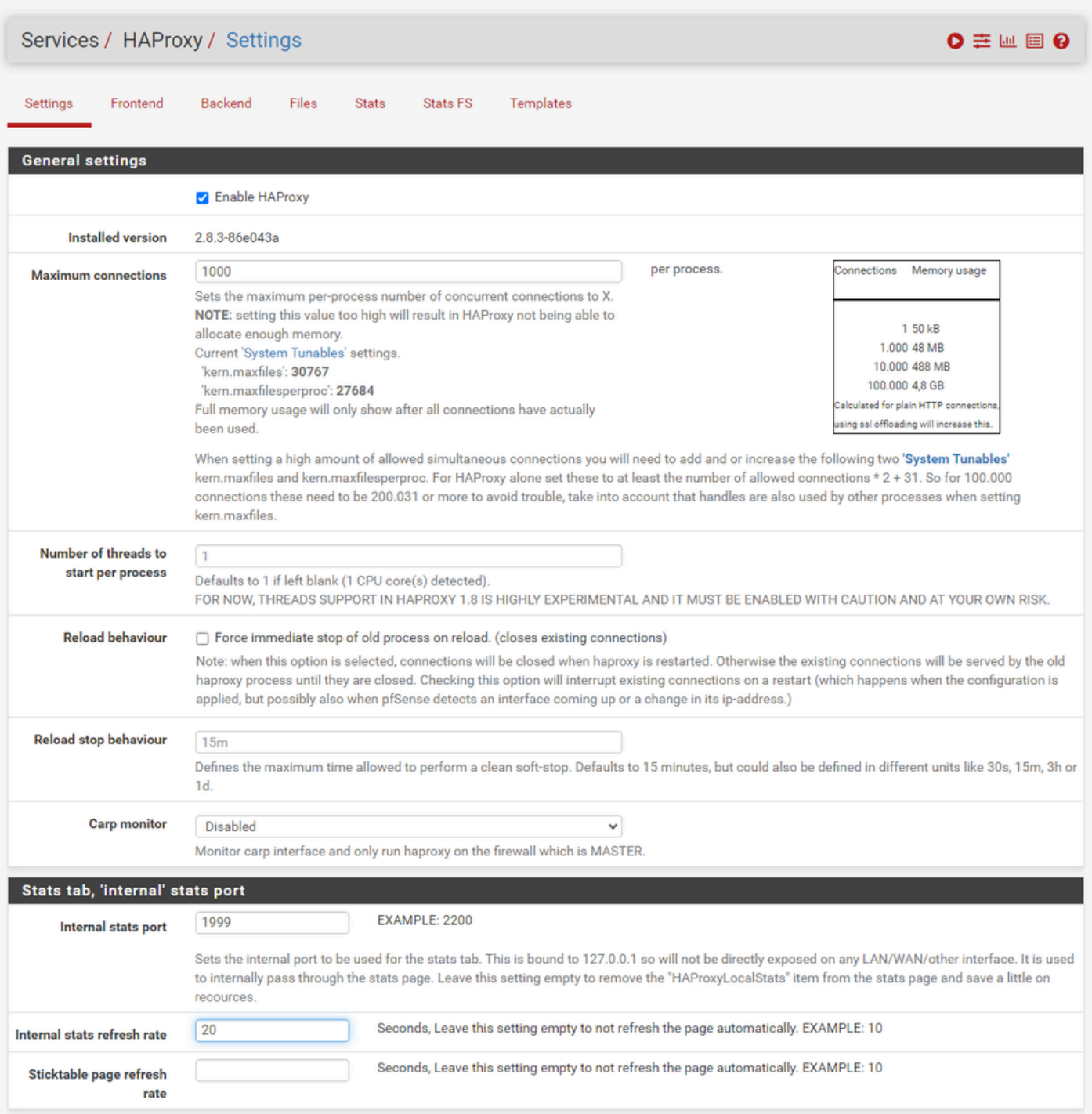
Paramètres HAProxy initiaux

Étape 1. Sélectionnez HAProxy dans la liste déroulante Services



Interface utilisateur graphique pfSense - Liste déroulante HAProxy

Étape 2. Configurer les paramètres de base



Interface utilisateur graphique pfSense - Paramètres principaux HAProxy

Cochez la case Activer HAProxy.

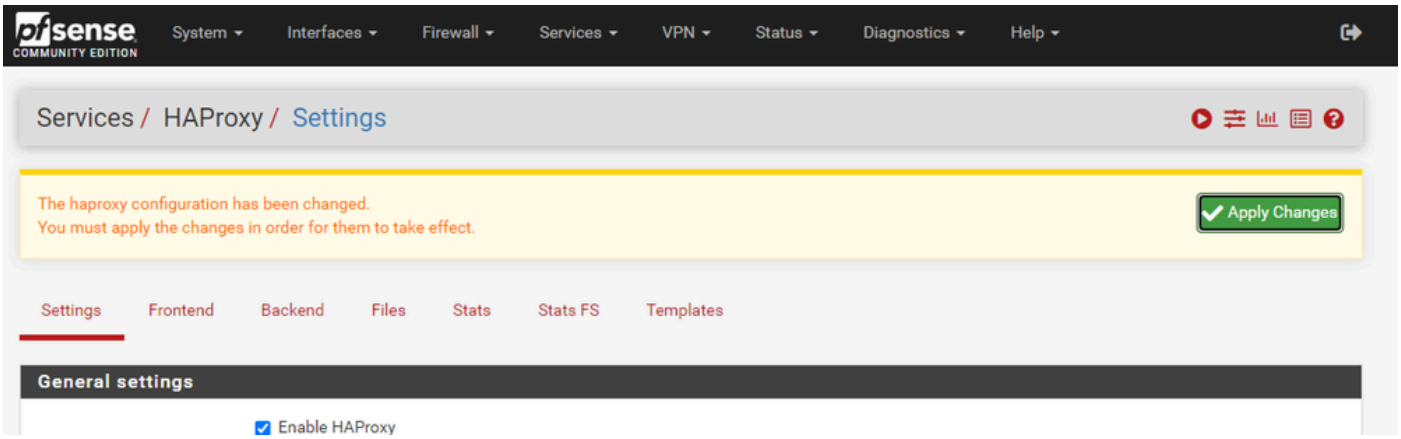
Saisissez une valeur pour le paramètre Nombre maximal de connexions. Reportez-vous au tableau de cette section pour plus de détails sur la mémoire requise.

Saisissez une valeur pour le port d'état interne. Ce port est utilisé pour afficher les statistiques HAProxy sur l'appliance, mais n'est pas exposé en dehors de l'appliance.

Saisissez une valeur pour le taux de rafraîchissement des statistiques internes.

Vérifiez la configuration restante et mettez-la à jour en fonction de votre environnement.

Sélectionnez Enregistrer.

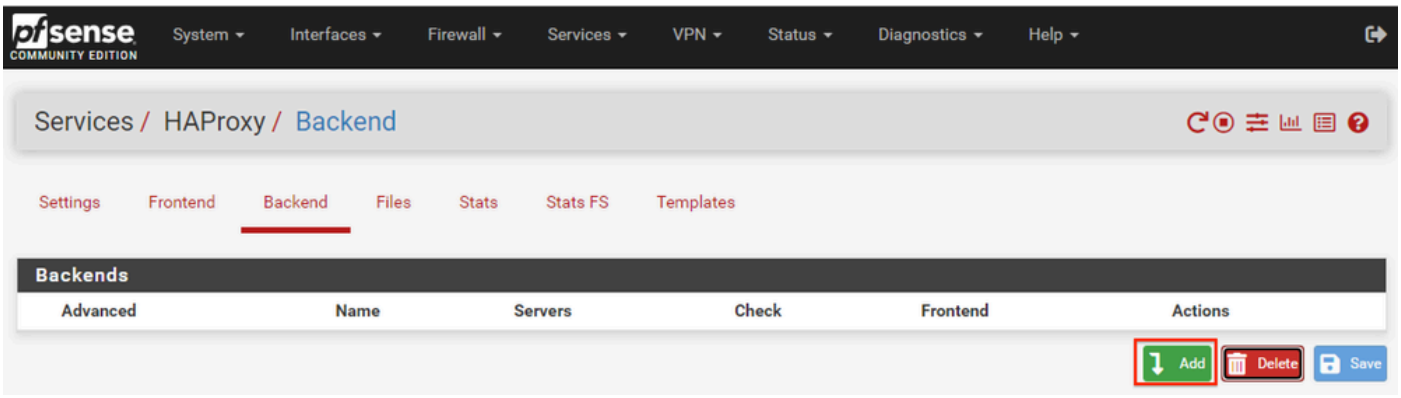


Interface utilisateur graphique pfSense - HAProxy Appliquer les modifications

Remarque : les modifications de configuration ne sont pas activées tant que vous n'avez pas sélectionné le bouton Appliquer les modifications. Vous pouvez apporter plusieurs modifications à la configuration et les appliquer toutes simultanément. La configuration n'a pas besoin d'être appliquée pour être utilisée dans une autre section.

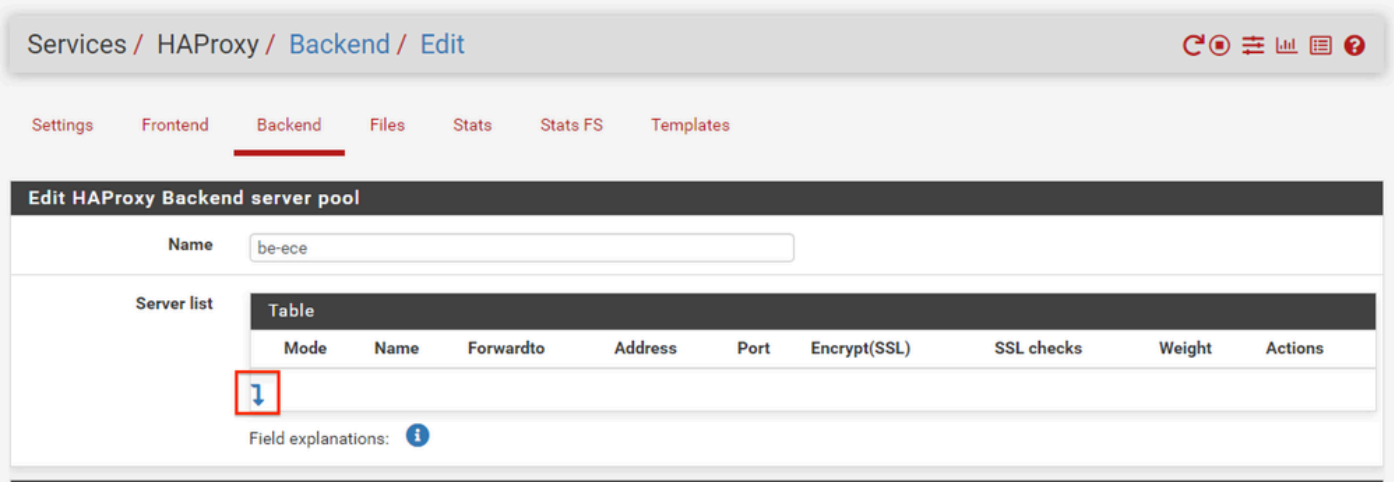
Configurer le serveur principal HAProxy

Commencez par le back-end. La raison en est que le serveur frontal doit faire référence à un serveur principal. Vérifiez que vous avez sélectionné le menu principal.



Interface utilisateur graphique pfSense - HAProxy Add Backend

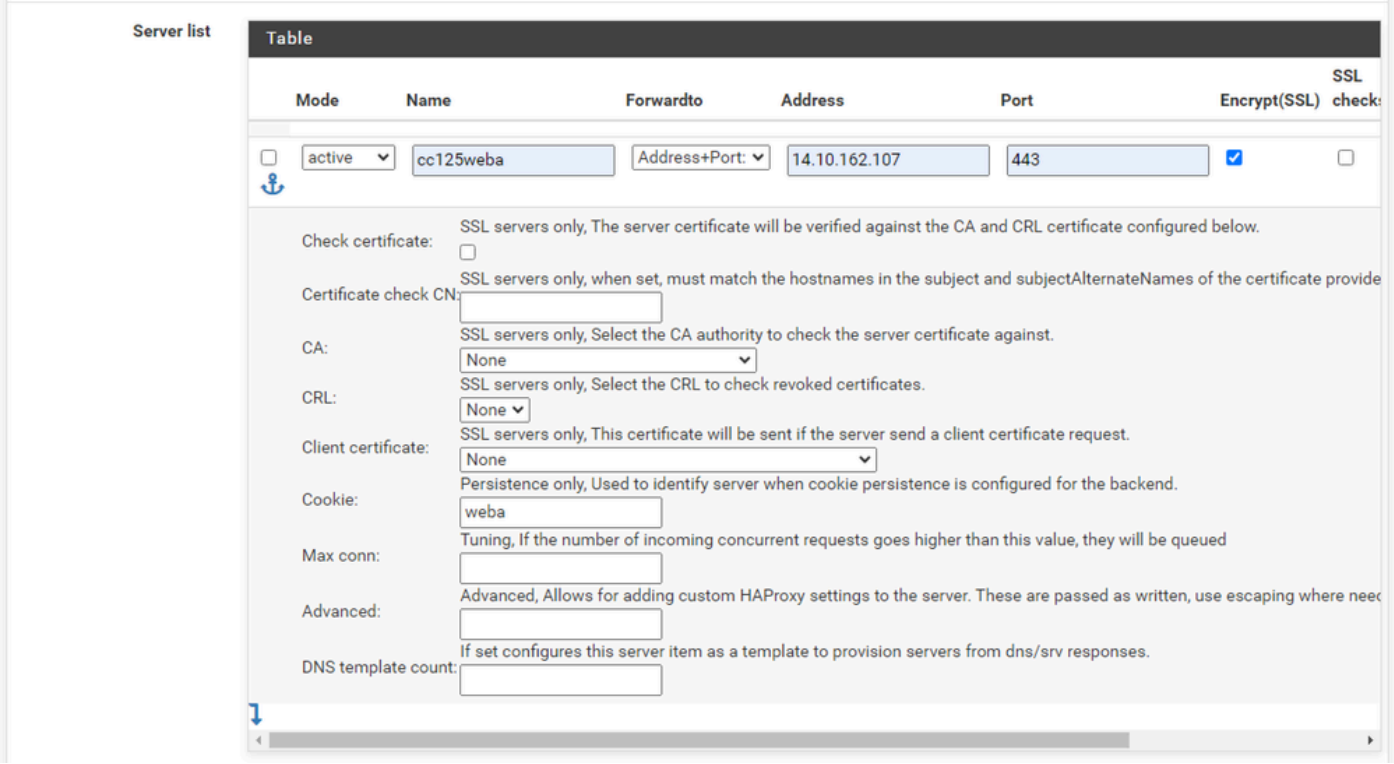
Cliquez sur le bouton Ajouter.



Interface utilisateur graphique pfSense - Démarrage du serveur principal HAProxy

Entrez un nom pour le serveur principal.

Sélectionnez la flèche vers le bas pour ajouter le premier serveur à la liste des serveurs



Serveur principal - Liste des serveurs

Entrez un nom pour référencer le serveur. Il n'est pas nécessaire que ce nom corresponde au nom réel du serveur. Il s'agit du nom affiché sur la page de statistiques.

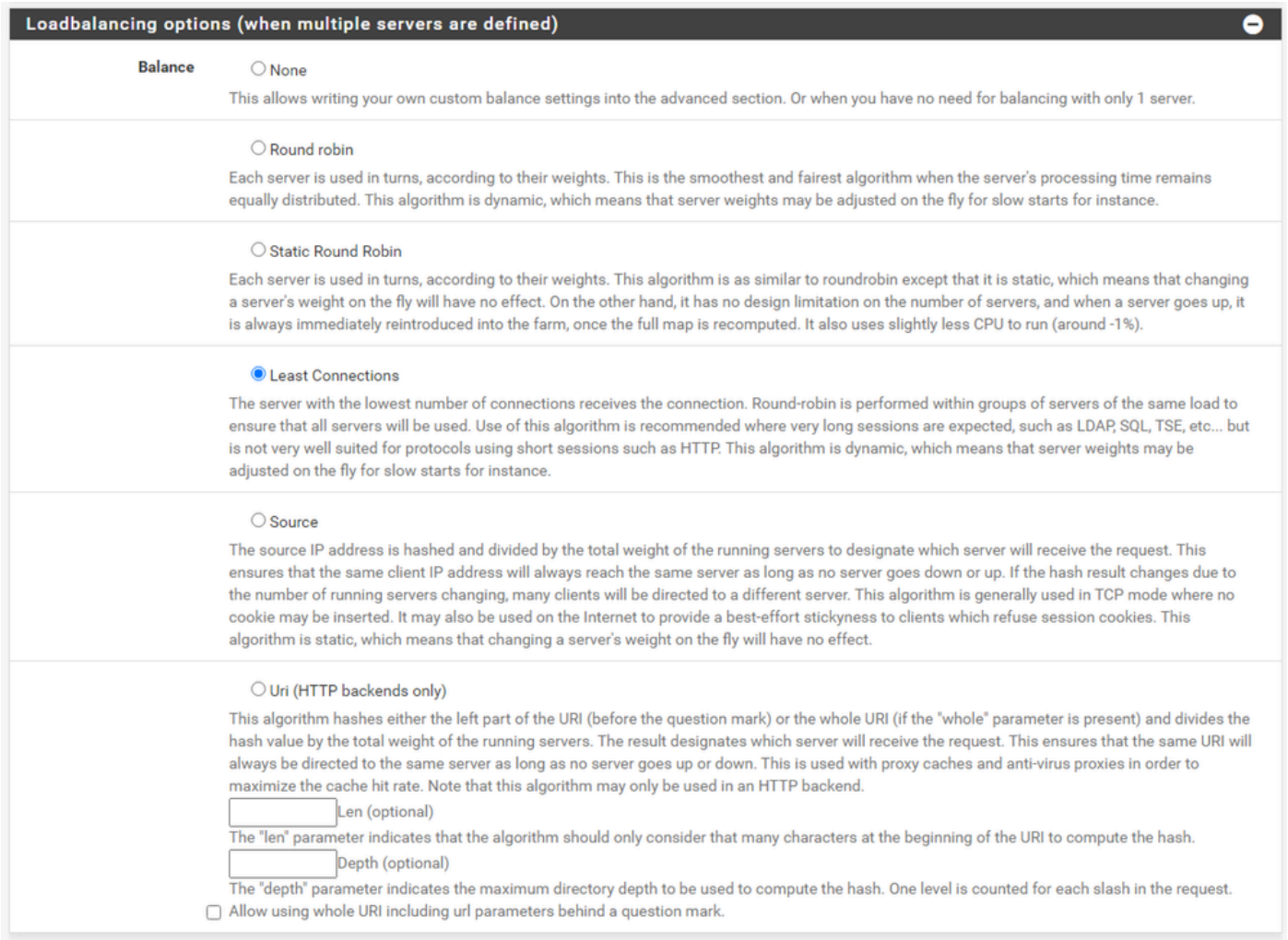
Indiquez l'adresse du serveur. Il peut être configuré en tant qu'adresse IP pour le nom de domaine complet.

Indiquez le port auquel vous souhaitez vous connecter. Il doit s'agir du port 443 pour ECE.

Cochez la case Chiffrer (SSL).

Saisissez une valeur dans le champ Cookie. Il s'agit du contenu du cookie d'adhésivité de session et il doit être unique dans le back-end.

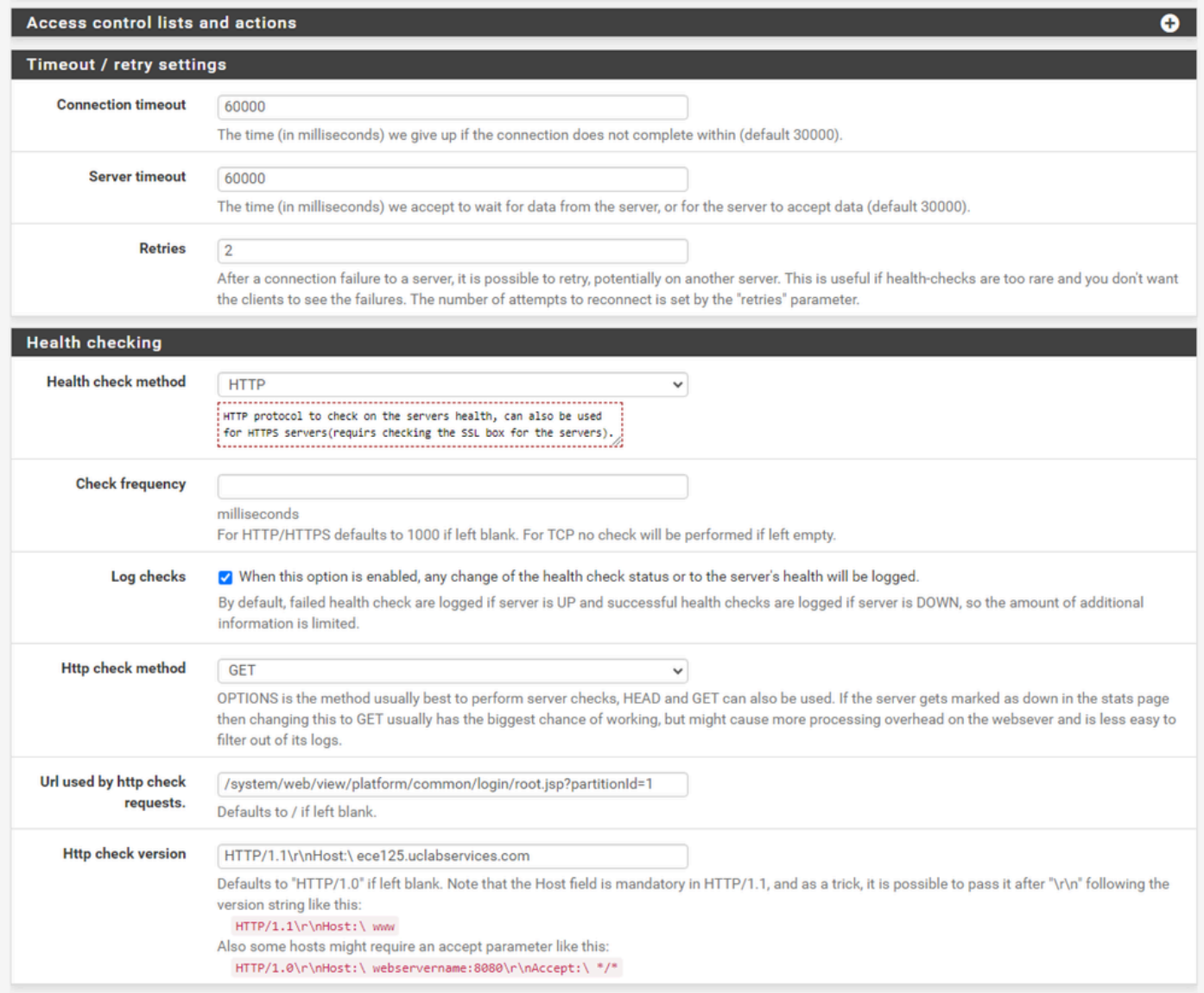
Une fois le premier serveur configuré, sélectionnez la flèche vers le bas pour configurer les autres serveurs Web de l'environnement.



Serveur principal HAProxy - Équilibrage de charge

Configurez les options d'équilibrage de charge.

Pour les serveurs ECE, ce paramètre doit être défini sur Connexions minimales.



Serveur principal HAProxy - Contrôle d'intégrité

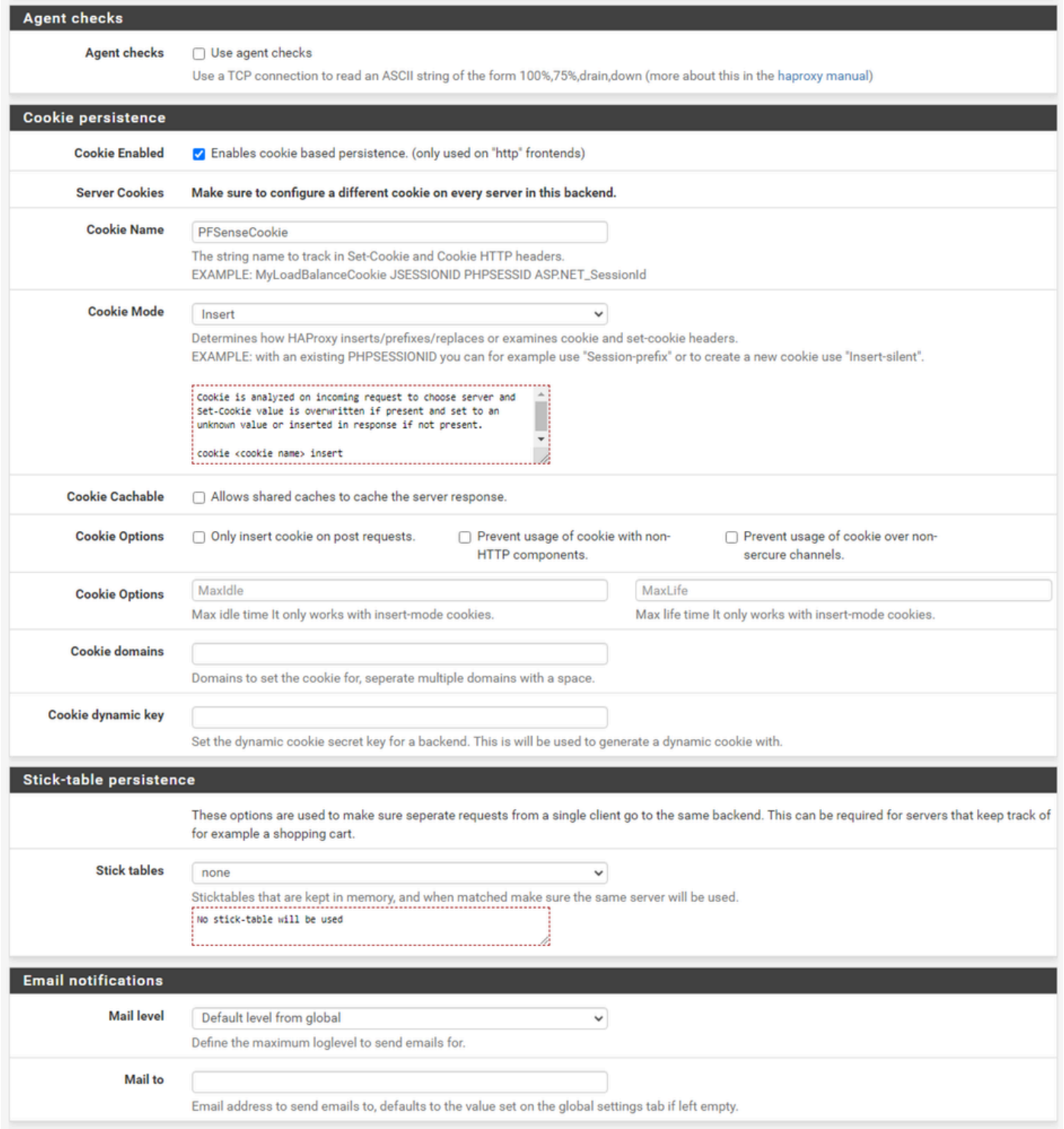
Les listes de contrôle d'accès ne sont pas utilisées dans cette configuration.

Les paramètres de délai d'attente/nouvelle tentative peuvent être conservés dans leur configuration par défaut.

Configurez la section Vérification de l'intégrité.

1. Méthode de contrôle d'intégrité : HTTP
2. Vérifier la fréquence : laisser vide pour utiliser la valeur par défaut toutes les 1 seconde.
3. Vérifications du journal : sélectionnez cette option pour enregistrer les modifications d'intégrité dans les journaux.
4. Méthode de vérification HTTP : sélectionnez GET dans la liste.
5. Url utilisée par les requêtes de vérification http : pour un serveur ECE, entrez /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Version de vérification HTTP : Entrée, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

Veillez à inclure un espace après la barre oblique inverse finale, mais avant le nom de domaine complet du serveur.

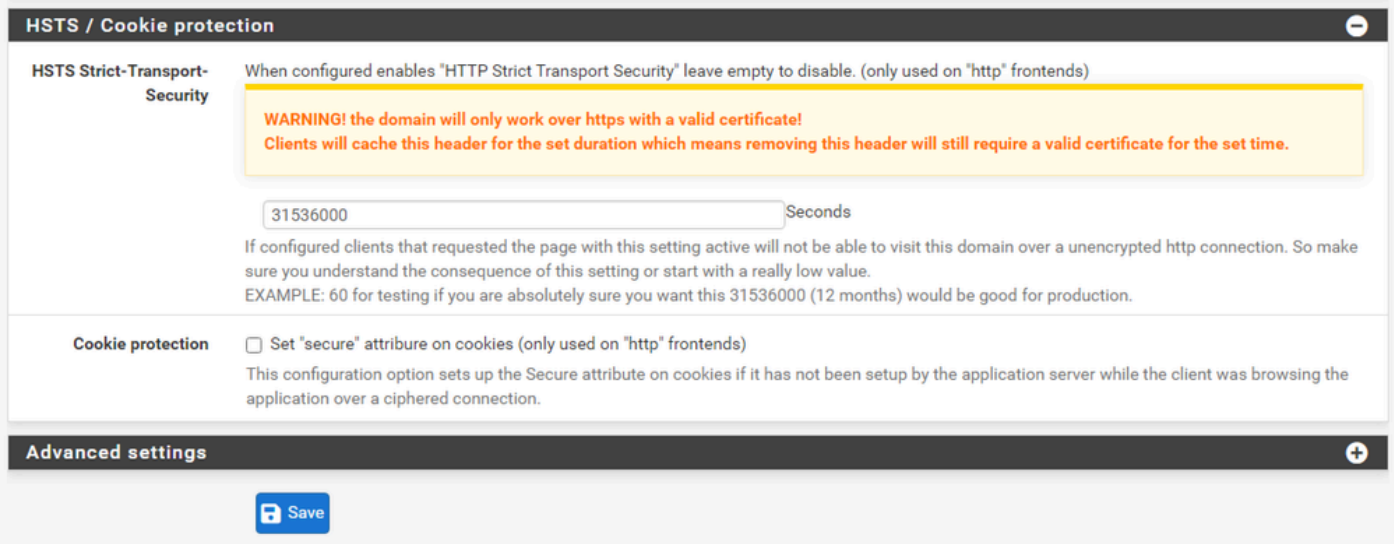


Serveur principal HAProxy - Persistance des cookies

Laissez les vérifications de l'agent désélectionnées.

Configurez la persistance des cookies :

1. Cookie Enabled : sélectionnez cette option pour activer la persistance basée sur les cookies.
2. Cookie Name : saisissez un nom pour le cookie.
3. Cookie Mode : sélectionnez Insert dans la liste déroulante.
4. Laissez les autres options non définies.



Serveur principal HAProxy - HSTS

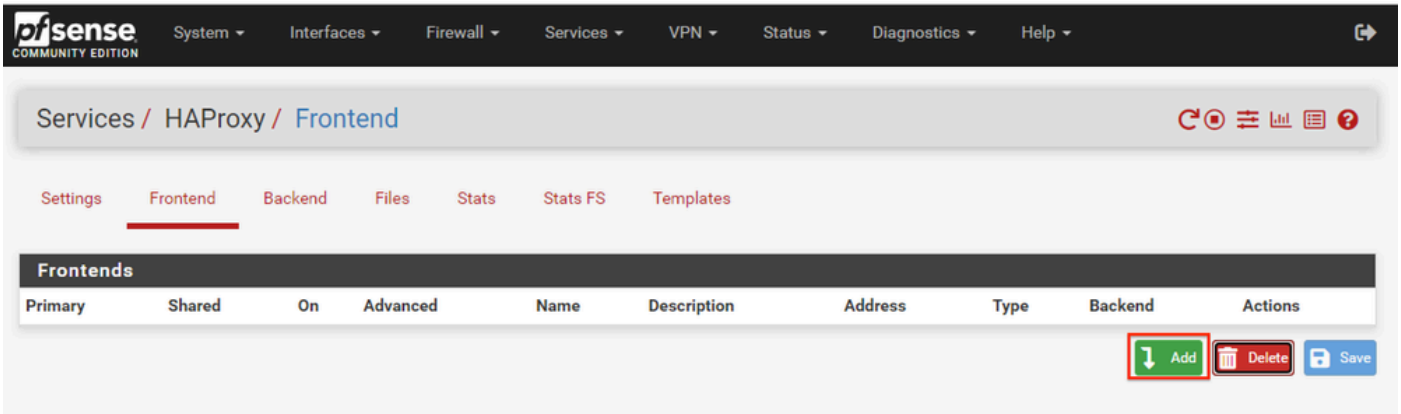
Les autres sections du formulaire de configuration du serveur principal peuvent être conservées dans leurs paramètres par défaut.

Si vous souhaitez configurer HSTS, configurez une valeur de délai d'attente dans cette section. ECE insère également un cookie HSTS de sorte que cette configuration soit redondante.

Sélectionnez, Enregistrer.

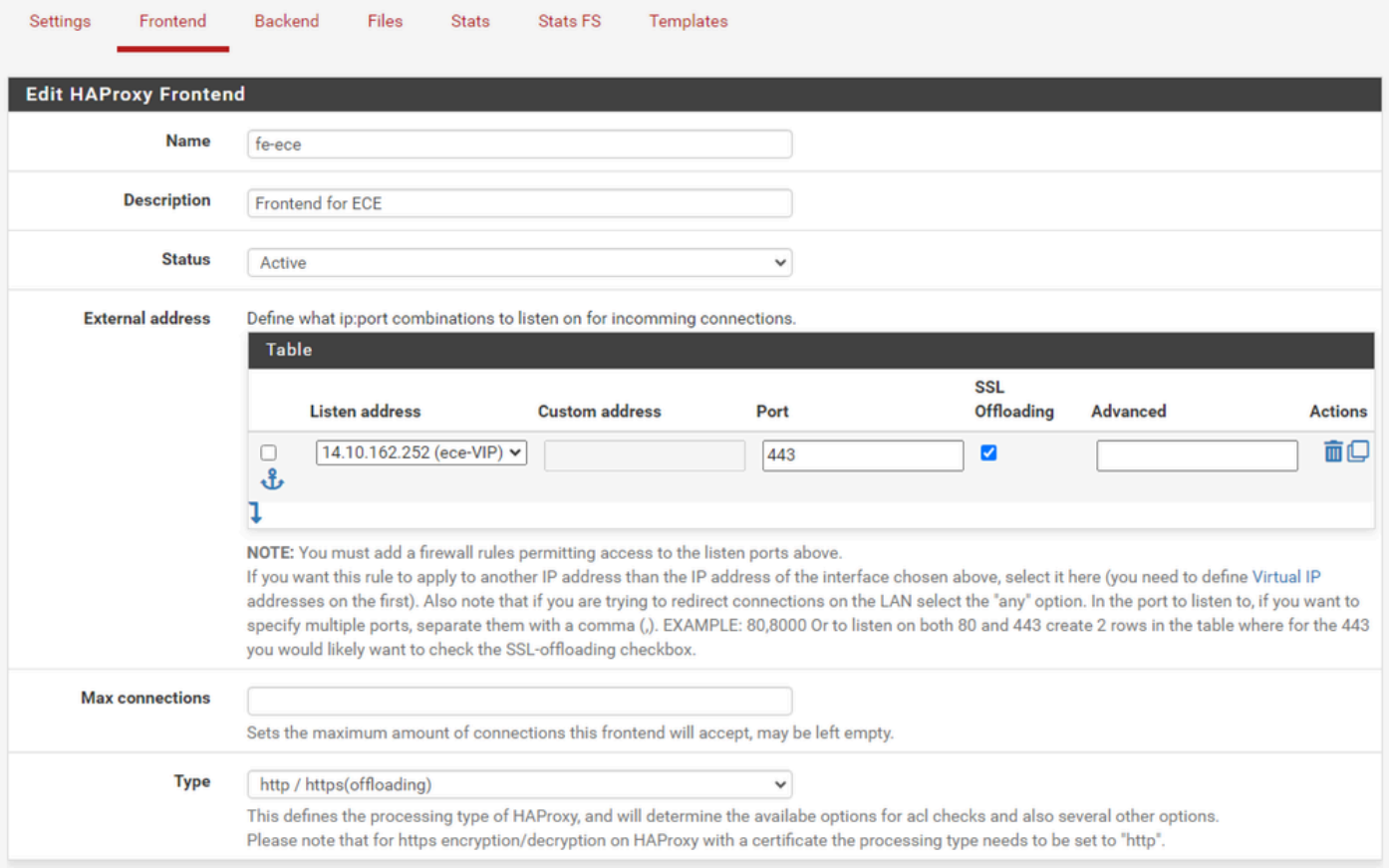
Configurer le frontal HAProxy

Passez au menu Frontend.



Interface utilisateur graphique pfSense - HAProxy Add Frontend

Sélectionnez le bouton Ajouter.



HAProxy - En-tête frontal

Entrez un nom pour le serveur frontal.

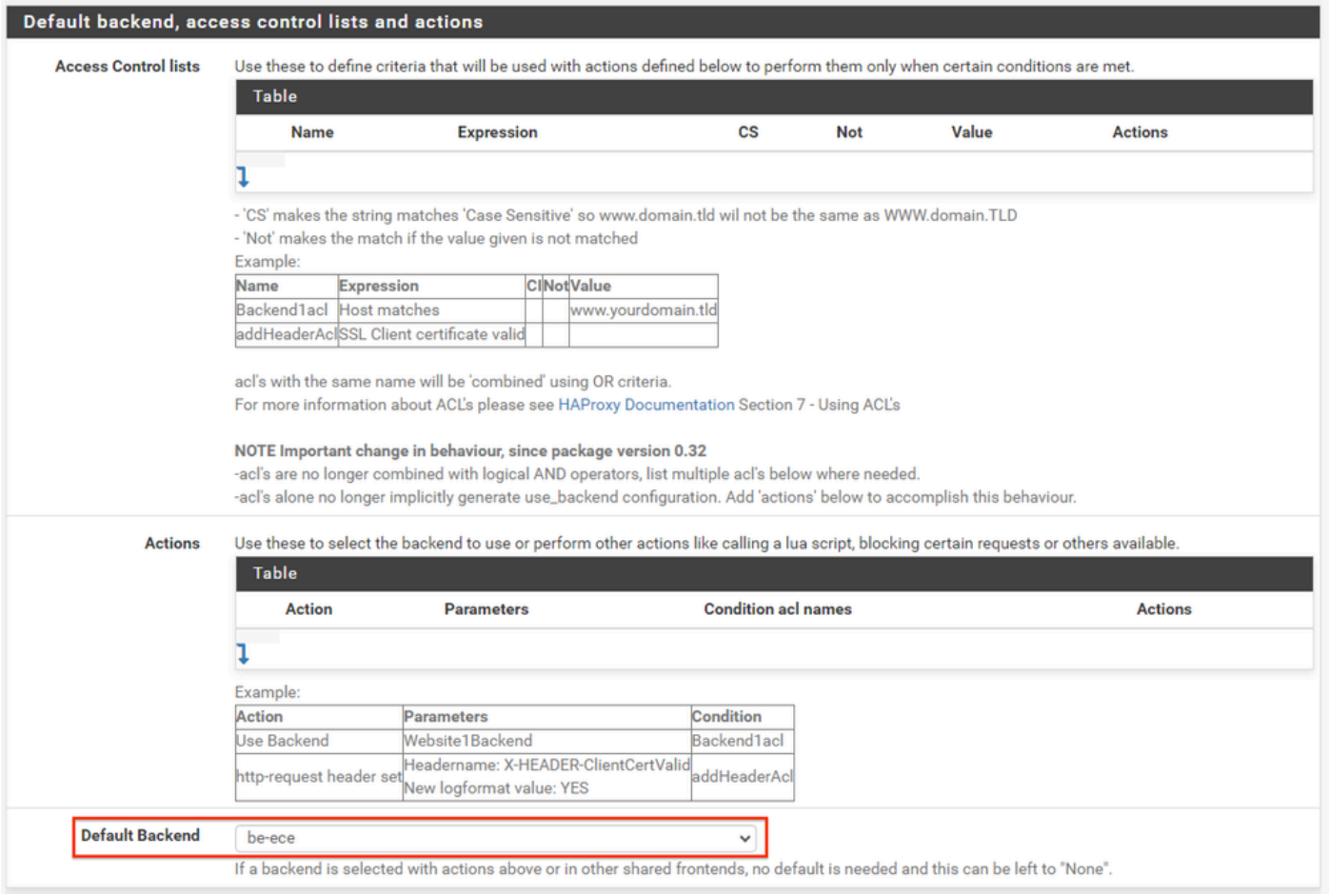
Fournissez une description pour faciliter l'identification ultérieure du serveur frontal.

Dans la table des adresses externes :

1. Listen address : sélectionnez le VIP que vous avez créé pour ce site Web.
2. Port : saisissez 443.
3. SSL Offloading : sélectionnez cette option afin que le cookie de session puisse être inséré.

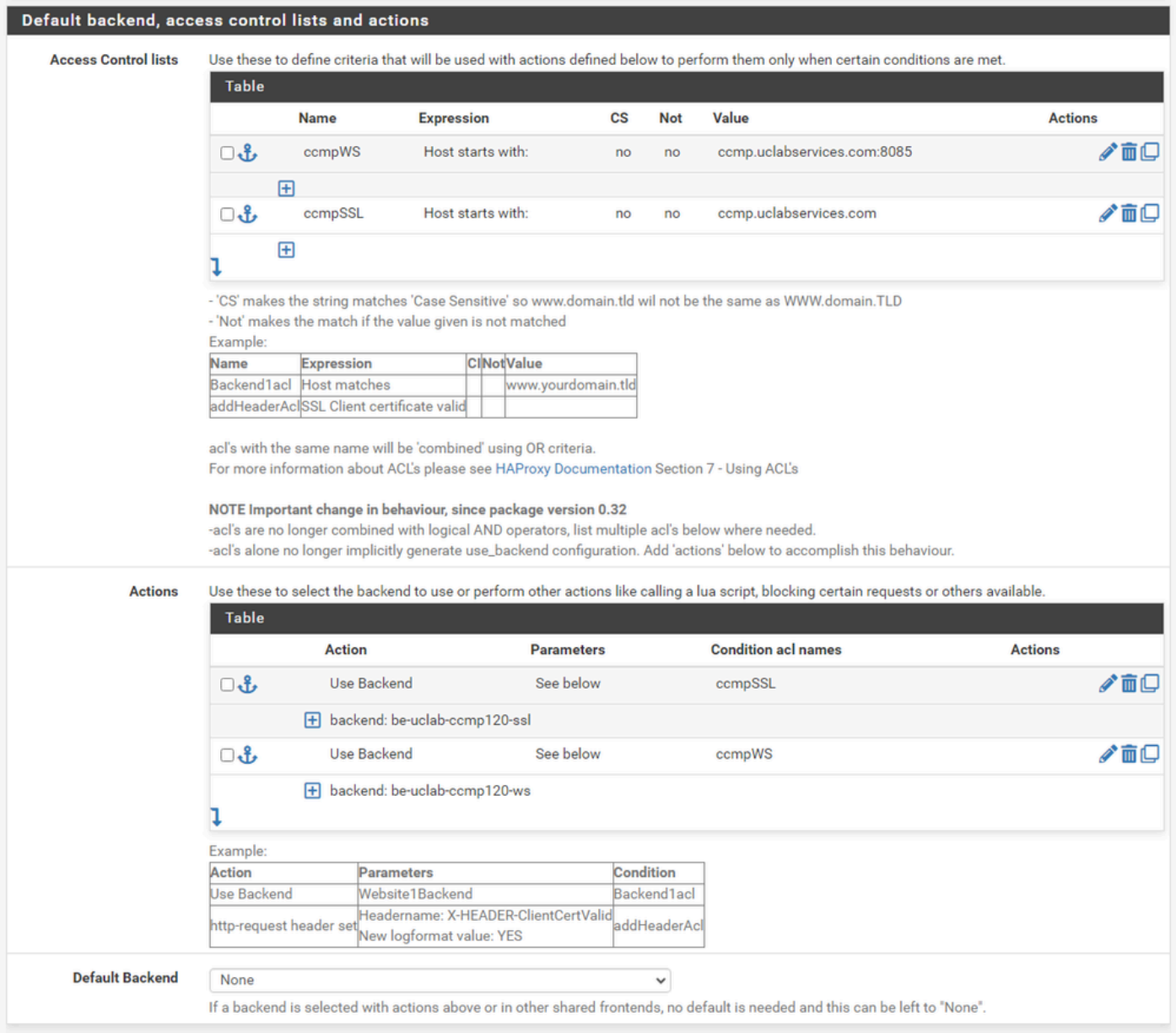
Laissez le champ Max connections vide.

Assurez-vous que le type est sélectionné en tant que http / https(offloading).



HAProxy back-end - Sélection du back-end par défaut

La configuration la plus simple consiste à choisir un serveur principal par défaut dans la liste déroulante. Cette option peut être sélectionnée lorsque le VIP héberge un seul site Web.

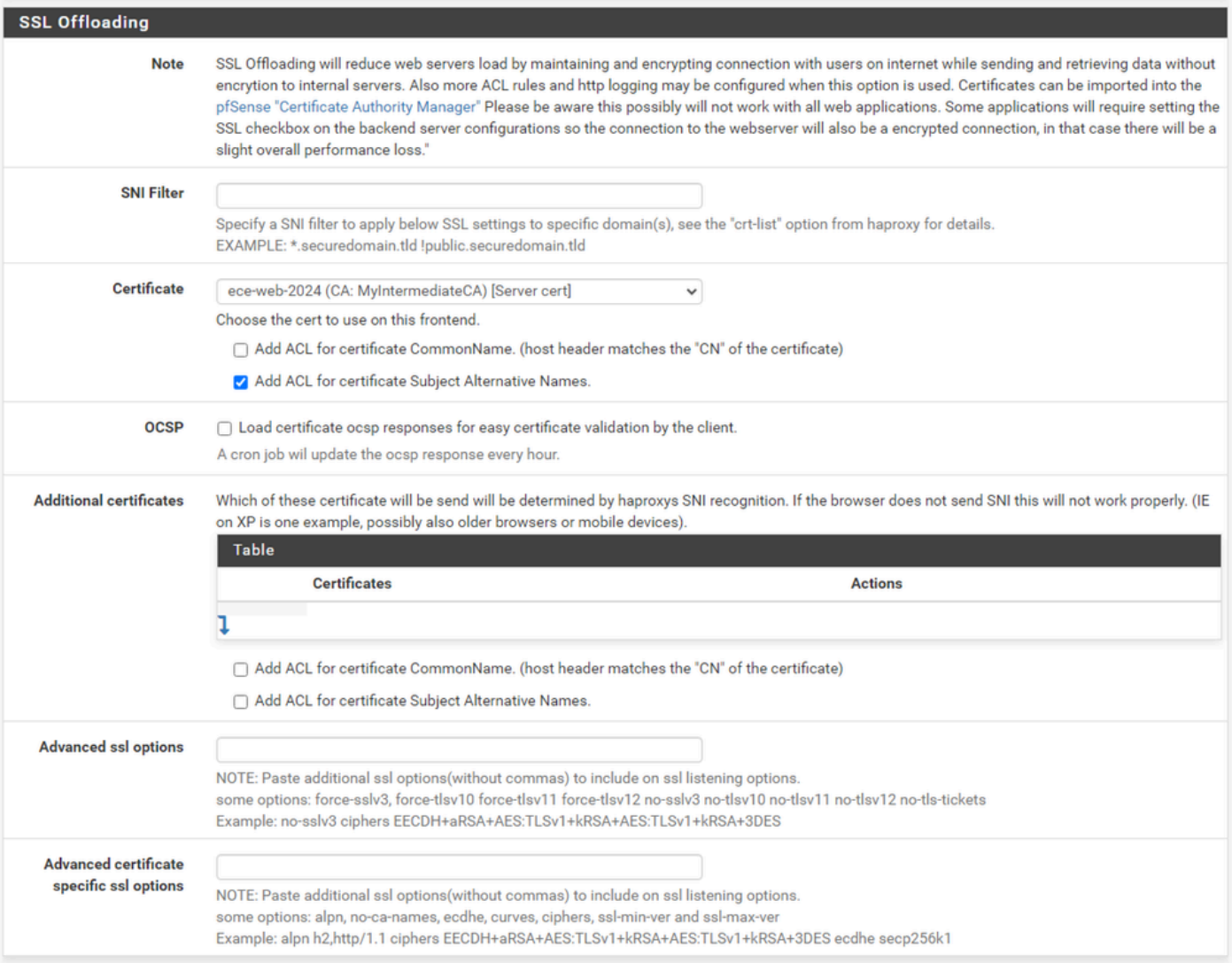


HAProxy principal - ACL avancé

Comme l'illustre l'image, les listes de contrôle d'accès peuvent être utilisées pour rediriger un seul serveur frontal vers plusieurs serveurs principaux en fonction des conditions.

Vous pouvez voir que la liste de contrôle d'accès vérifie si l'hôte de la demande commence par un nom et un numéro de port, ou simplement par le nom. Sur cette base, un serveur principal spécifique est utilisé.

Ce n'est pas courant avec l'ECE.



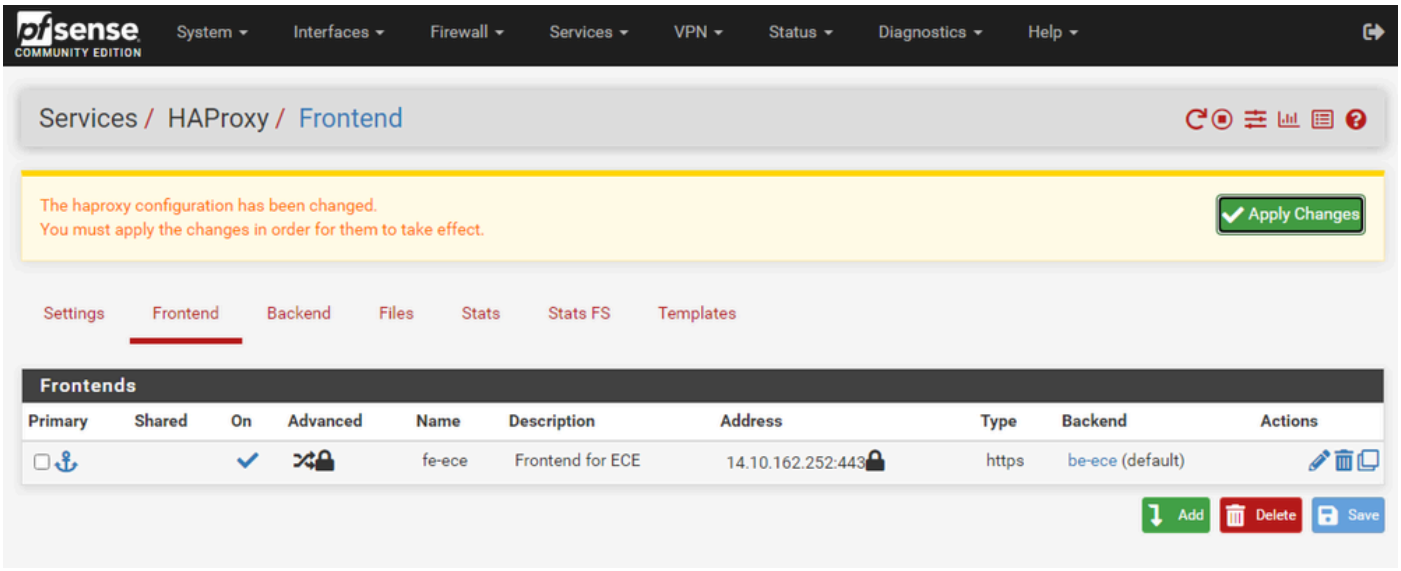
Frontend HAProxy - Liaison de certificat

Dans la section Déchargement SSL, sélectionnez le certificat créé pour être utilisé avec ce site. Ce certificat doit être un certificat de serveur.

Sélectionnez l'option Add ACL for certificate Subject Alternative Names.

Vous pouvez conserver les valeurs par défaut des options restantes.

Sélectionnez Enregistrer à la fin de ce formulaire.



HAProxy - Appliquer la configuration

Sélectionnez Apply Changes pour valider les modifications du serveur frontal et du serveur principal dans la configuration en cours.

Félicitations, vous avez terminé l'installation et la configuration de pfSense.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.