

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Installer PfSense](#)

[Présentation de la solution](#)

[Préparation](#)

[Installation](#)

[Configuration du réseau](#)

[Terminer la configuration initiale](#)

[Configuration des paramètres d'administration de base](#)

[Ajouter les packages requis](#)

[Configurer les certificats](#)

[Ajouter des adresses IP virtuelles](#)

[Configurer le pare-feu](#)

[Configurer HAProxy](#)

[Concepts HAProxy](#)

[Paramètres HAProxy initiaux](#)

[Configurer le serveur principal HAProxy](#)

[Configurer le frontal HAProxy](#)

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.

```
browser:
      http://14.10.172.250/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: b2d05c55bab7b75fe6c2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx0      -> v4: 14.10.172.250/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
```

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.

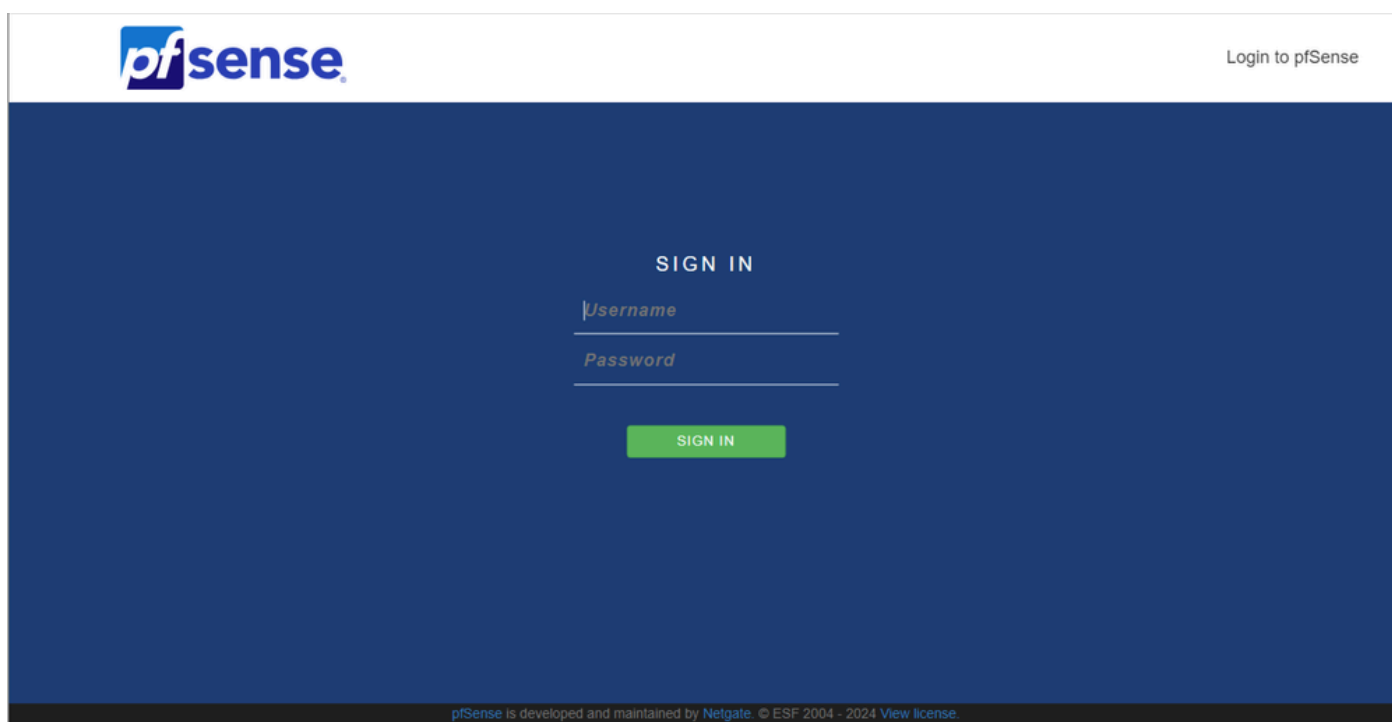
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://14.10.172.250/
Press <ENTER> to continue.
```

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.

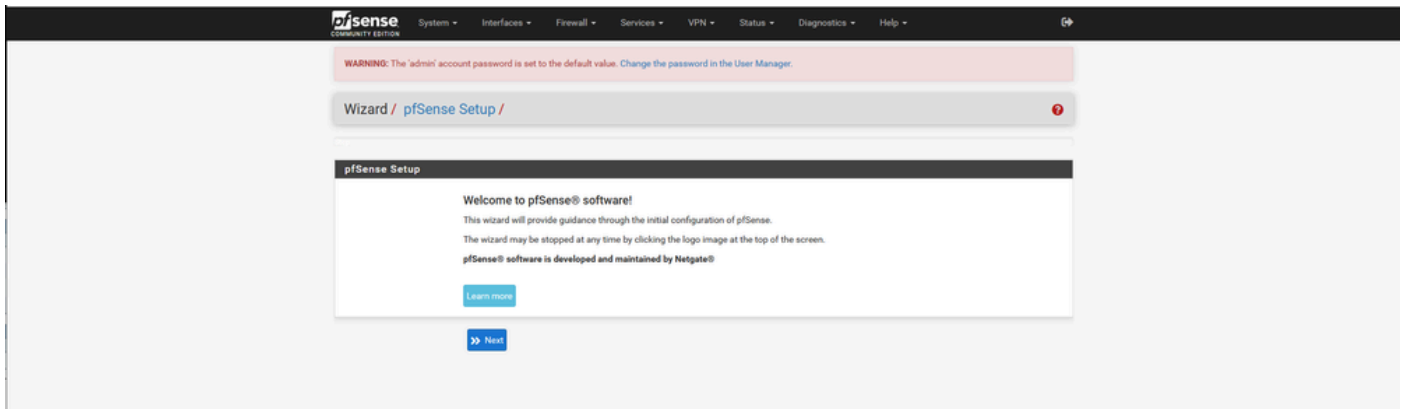


Connexion administrateur pfSense

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

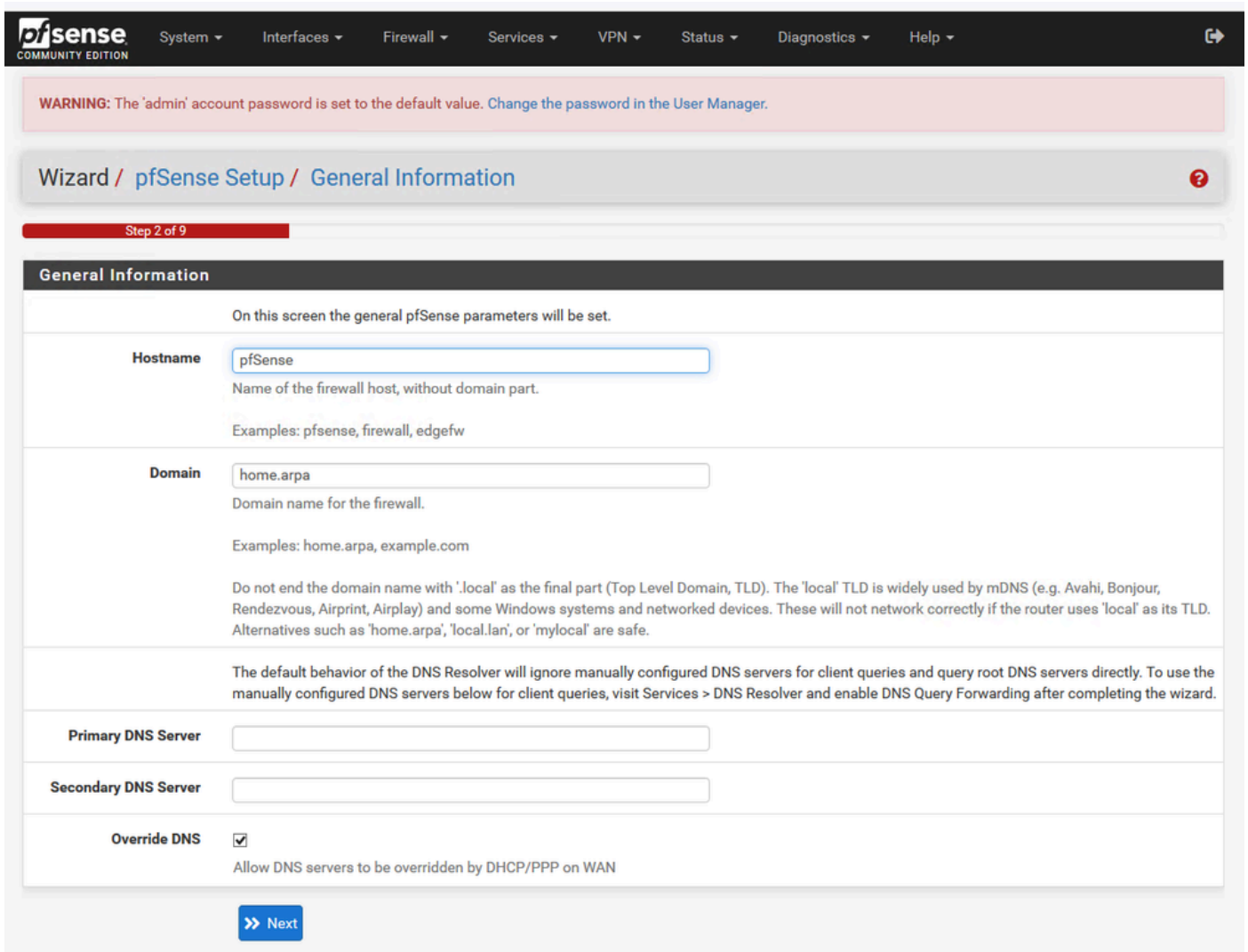
Étape 3. Terminer la configuration initiale

Cliquez sur Suivant dans les deux premiers écrans.



Assistant de configuration de pfSense - 1

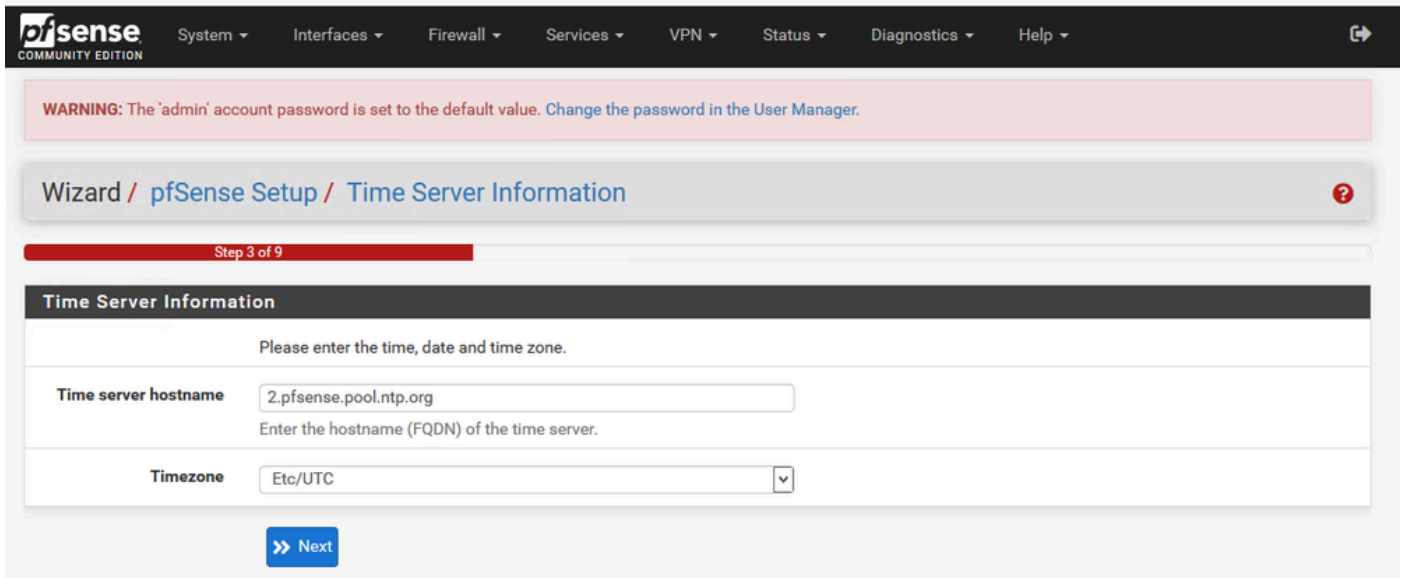
Fournissez le nom d'hôte, le nom de domaine et les informations du serveur DNS.



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.



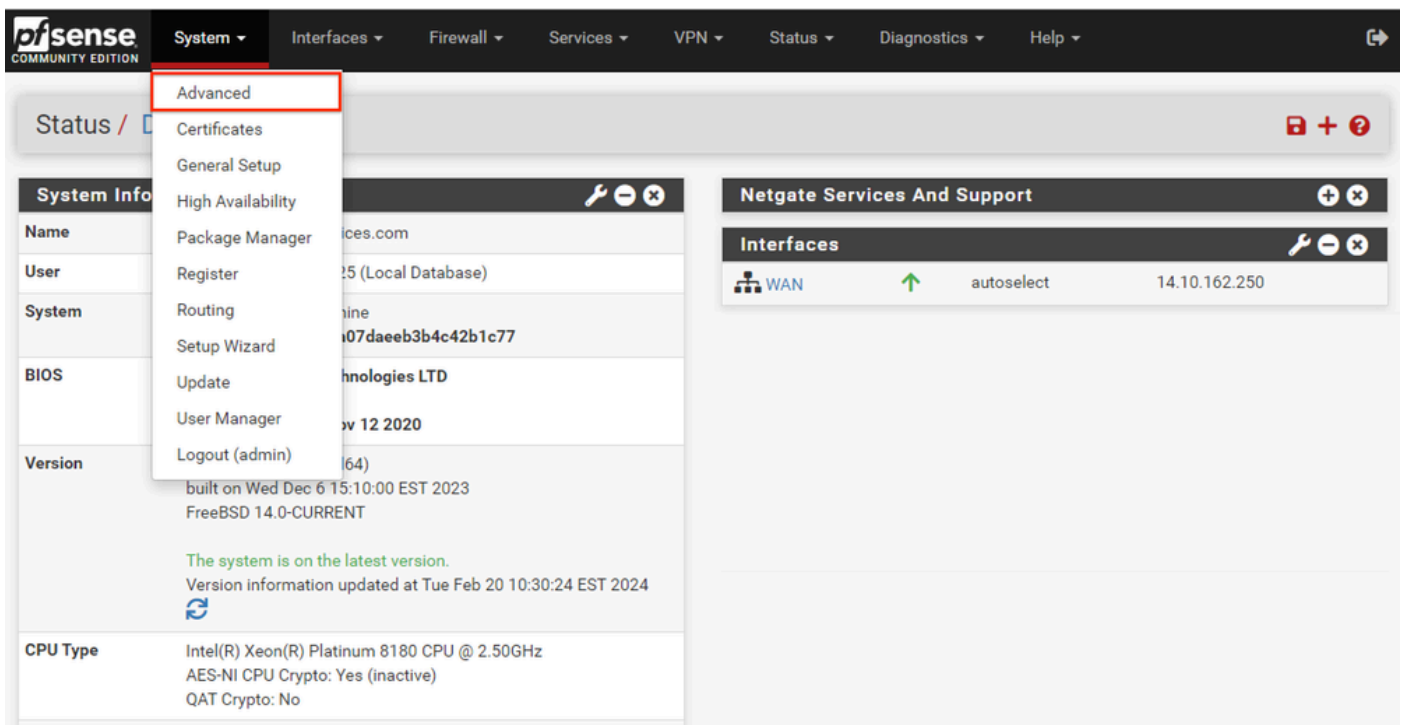
Assistant de configuration de pfSense - 3

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

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	<input type="text" value="GUI default (65cced5b25159)"/> <p>Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</p>
TCP port	<input type="text" value="8443"/> <p>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</p>
Max Processes	<input type="text" value="2"/> <p>Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.</p>
WebGUI redirect	<input checked="" type="checkbox"/> Disable webConfigurator redirect rule <p>When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.</p>
HSTS	<input type="checkbox"/> Disable HTTP Strict Transport Security <p>When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)</p>
OCSP Must-Staple	<input type="checkbox"/> Force OCSP Stapling in nginx <p>When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.</p>
WebGUI Login Autocomplete	<input checked="" type="checkbox"/> Enable webConfigurator login autocomplete <p>When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).</p>
GUI login messages	<input type="checkbox"/> Lower syslog level for successful GUI login events <p>When this is checked, successful logins to the GUI will be logged as a lower non-emergency level. Note: The console bell behavior can be controlled independently on the Notifications tab.</p>
Roaming	<input checked="" type="checkbox"/> Allow GUI administrator client IP address to change during a login session <p>When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes.</p>
Anti-lockout	<input type="checkbox"/> Disable webConfigurator anti-lockout rule <p>When this is unchecked, access to the webConfigurator on the WAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) <i>Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.</i></p>
DNS Rebind Check	<input type="checkbox"/> Disable DNS Rebinding Checks <p>When this is unchecked, the system is protected against DNS Rebinding attacks. This blocks private IP responses from the configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in the environment.</p>
Alternate Hostnames	<input type="text"/> <p>Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.</p>
Browser HTTP_REFERER enforcement	<input checked="" type="checkbox"/> Disable HTTP_REFERER enforcement check <p>When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.</p>

Interface utilisateur graphique pfSense - Configuration admin

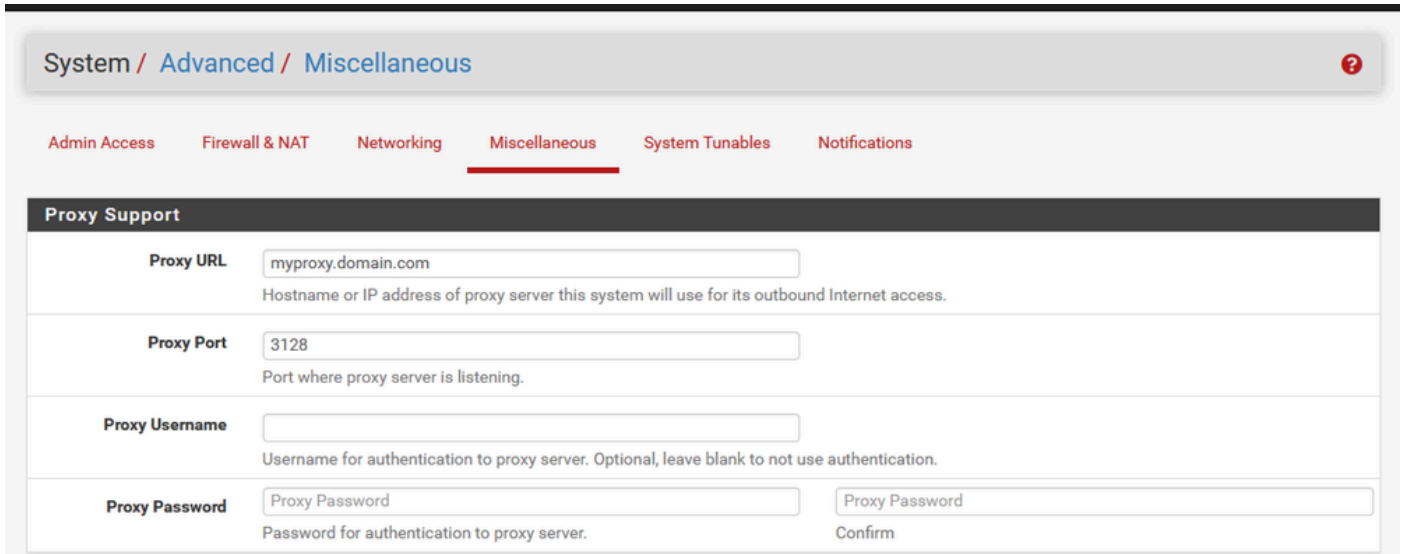
1. Sélectionnez le protocole HTTPS (SSL/TLS).
2. À ce stade, laissez le certificat SSL/TLS au certificat auto-signé.
3. Remplacez le port TCP par un port autre que le port 443 pour mieux sécuriser l'interface et éviter les problèmes de chevauchement de ports.
4. Sélectionnez l'option de redirection WebGUI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



System / Advanced / Miscellaneous

Admin Access Firewall & NAT Networking **Miscellaneous** System Tunables Notifications

Proxy Support


Proxy URL
Hostname or IP address of proxy server this system will use for its outbound Internet access.

Proxy Port
Port where proxy server is listening.

Proxy Username
Username for authentication to proxy server. Optional, leave blank to not use authentication.

Proxy Password
Password for authentication to proxy server. Confirm


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.

System / Package Manager / Available Packages ?

Available Packages

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11	<input type="button" value="+ Install"/>
apcupsd	0.3.92_1	*apcupsd* can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Package Dependencies: apcupsd-3.14.14_4	<input type="button" value="+ Install"/>
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arping-2.21_1	<input type="button" value="+ Install"/>
arpwatch	0.2.1	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	<input type="button" value="+ Install"/>

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.

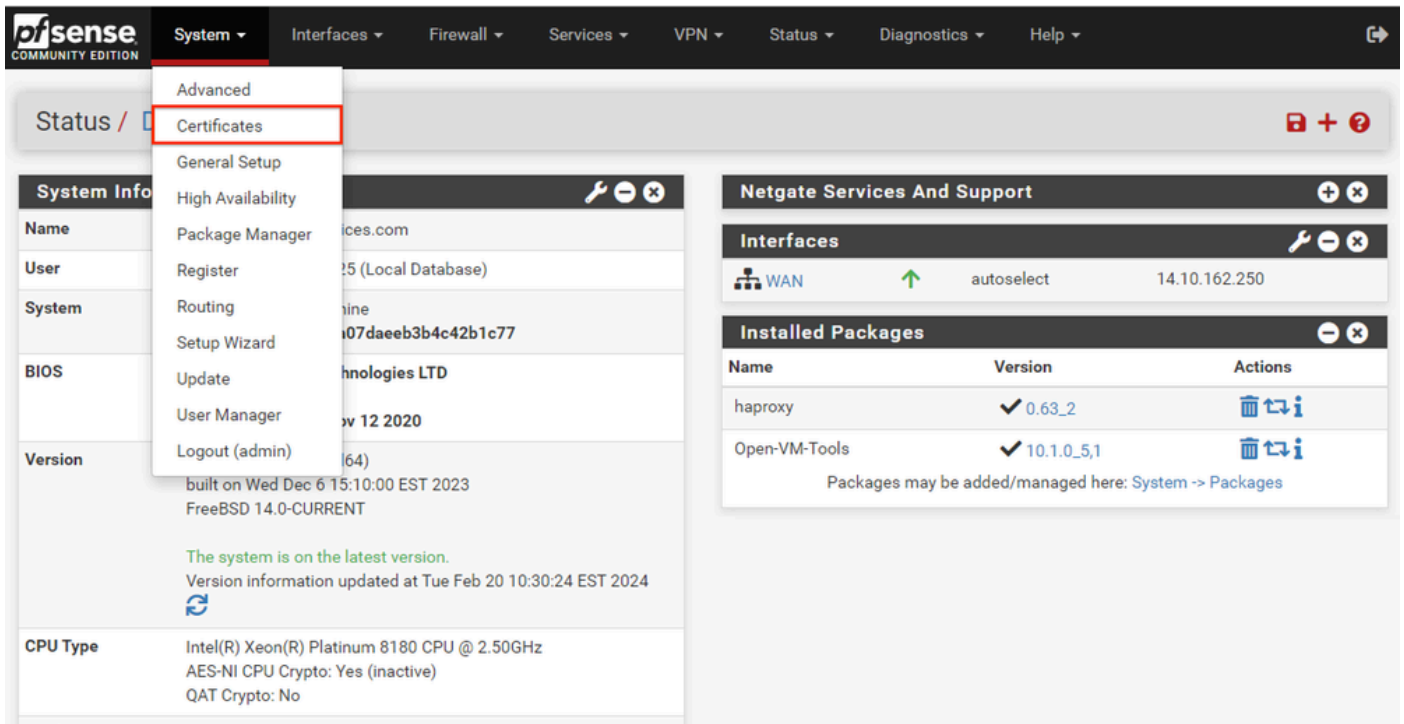
Configurer les certificats

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.

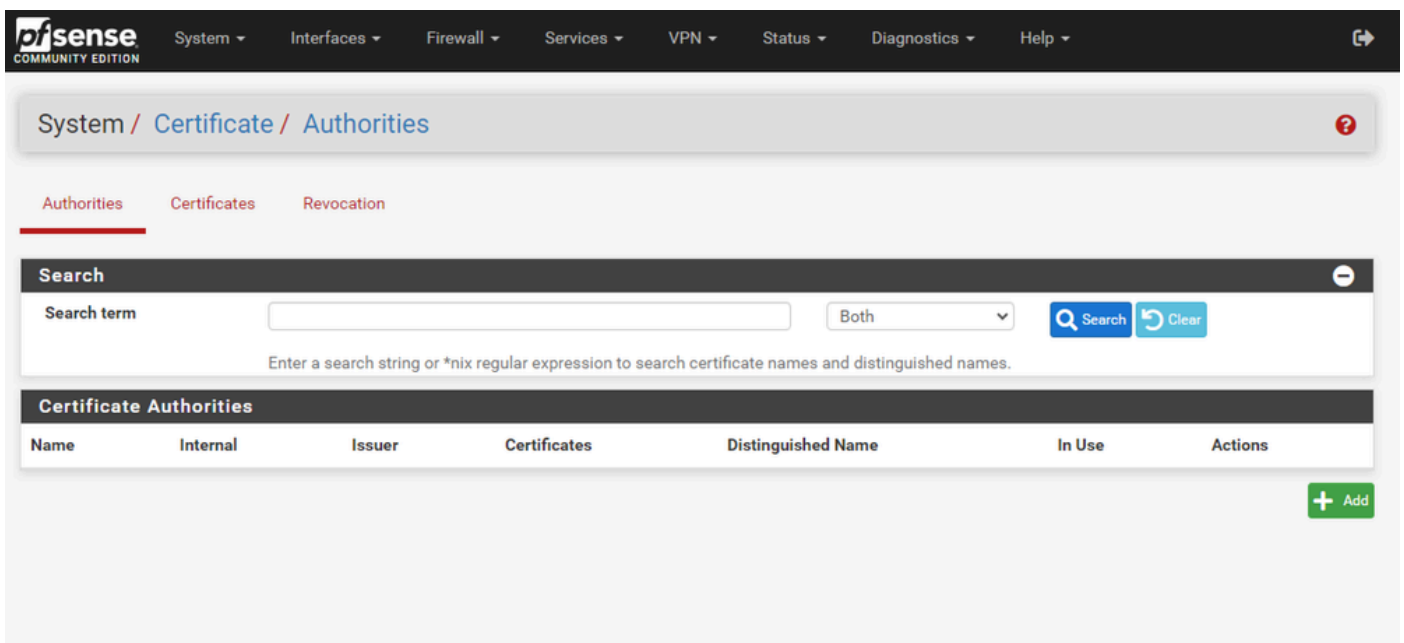
1. Certificat racine pour CA enregistré au format PEM ou codé en base 64.
2. Tous les certificats intermédiaires (parfois appelés certificats d'émission) pour l'autorité de certification sont enregistrés au format PEM ou au format codé Base-64.

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.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate / Authorities / Edit ?

Authorities Certificates Revocation

Create / Edit CA

Descriptive name
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
 When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data
 Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)
 Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial
 Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

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.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate / Authorities ?

Authorities Certificates Revocation

Search ⊖

Search term Both Q Search ↺ Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
MyRootCA	✘	self-signed	0	OU=pki.uclabservices.com, O=Cisco Systems Inc, CN=UCLAB Services Root, C=US i Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500		✎ ⚙ 🗑

+ Add

Interface utilisateur graphique pfSense - Liste CA

Étape 3. Importer le certificat intermédiaire CA

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data
Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

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.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
MyRootCA	✗	self-signed	1	OU=pki.uclabservices.com, O=Cisco Systems Inc, CN=UCLAB Services Root, C=US Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500	<input type="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>
MyIntermediateCA	✗	MyRootCA	0	ST=CA, OU=Cisco TAC, O=Cisco Systems Inc, L=San Jose, DC=UCLAB12, DC=local, CN=UCLAB12IssuingCA, C=US Valid From: Mon, 28 Jan 2019 13:10:27 -0500 Valid Until: Sun, 28 Jan 2029 13:20:27 -0500	<input type="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>

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.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65ccd5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65ccd5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	<input type="button" value="i"/> webConfigurator	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="key"/> <input type="button" value="refresh"/>

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

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create a Certificate Signing Request

Descriptive name ece-web-2024
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

External Signing Request

Key type RSA

2048
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.

prime256v1 [HTTPS] [IPsec] [OpenVPN]

Digest Algorithm sha256
The digest method used when the certificate 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.

Common Name myece.mydomain.com
The following certificate subject components are optional and may be left blank.

Country Code US

State or Province North Carolina

City Research Triangle Park

Organization Cisco Systems Inc

Organizational Unit Cisco TAC

- 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

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Certificate Signing Requests, These attributes are added to the request but they may be ignored or changed by the CA that signs the request.

If this CSR will be signed using the Certificate Manager on this firewall, set the attributes when signing instead as they cannot be carried over.


Certificate Type
 Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names
 Type Value

Add SAN Row

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.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates ?










Created certificate signing request ece-web-2024 ⌵

Authorities Certificates Certificate Revocation

Search -

Search term

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	i webConfigurator	    
ece-web-2024	external - signature pending	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US		   

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.

System / Certificates / Certificates

Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	<input checked="" type="checkbox"/> webConfigurator	<input type="button" value="Info"/> <input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Export"/> <input type="button" value="Import"/>
ece-web-2024	external - signature pending	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US	<input type="checkbox"/>	<input checked="" type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Export"/> <input type="button" value="Import"/>

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.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Complete Signing Request for ece-web-2024

Descriptive name
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ', "

Signing request data

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDvDCCAQCAQAwgZcxHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
MAkGA1UEBhMCVVMxZzAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMR0wGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
YzESMBAQA1UECzMDQ2LzY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

 Copy the certificate signing data from here and forward it to a certificate authority for signing.

Final certificate data

```
GBSAPwQkcas305JkKISY/pYEI2EW/7EZcDmHRURnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yiZ3IT4TJwDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5Mnuqx1PN97EPQngO/1IgXo4xDz6Dg+Iwt9pyrRZdxpmy
-----END CERTIFICATE-----
```

 Paste the certificate received from the certificate authority here.

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.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term Both ▾

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	webConfigurator	
ece-web-2024 CA: No Server: Yes	MyIntermediateCA	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US Valid From: Tue, 20 Feb 2024 12:31:00 -0500 Valid Until: Thu, 19 Feb 2026 12:31:00 -0500		

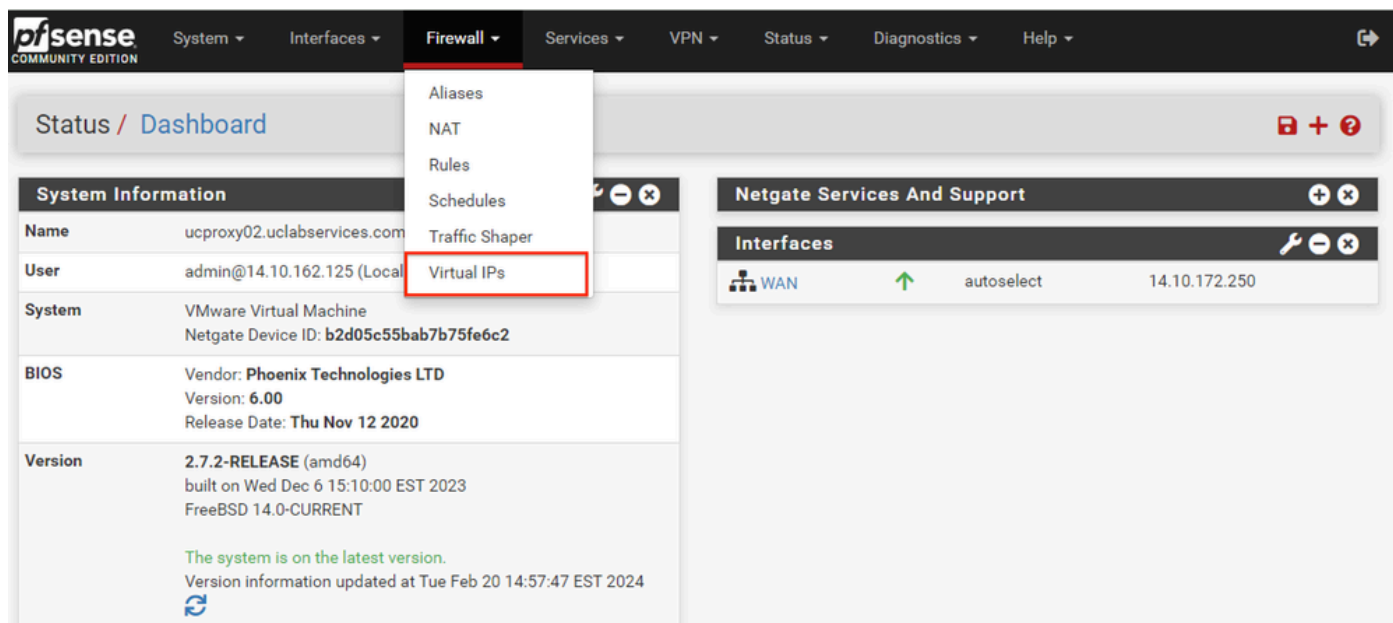
Interface utilisateur graphique pfSense - Liste de certificats

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

Ajouter des adresses IP virtuelles

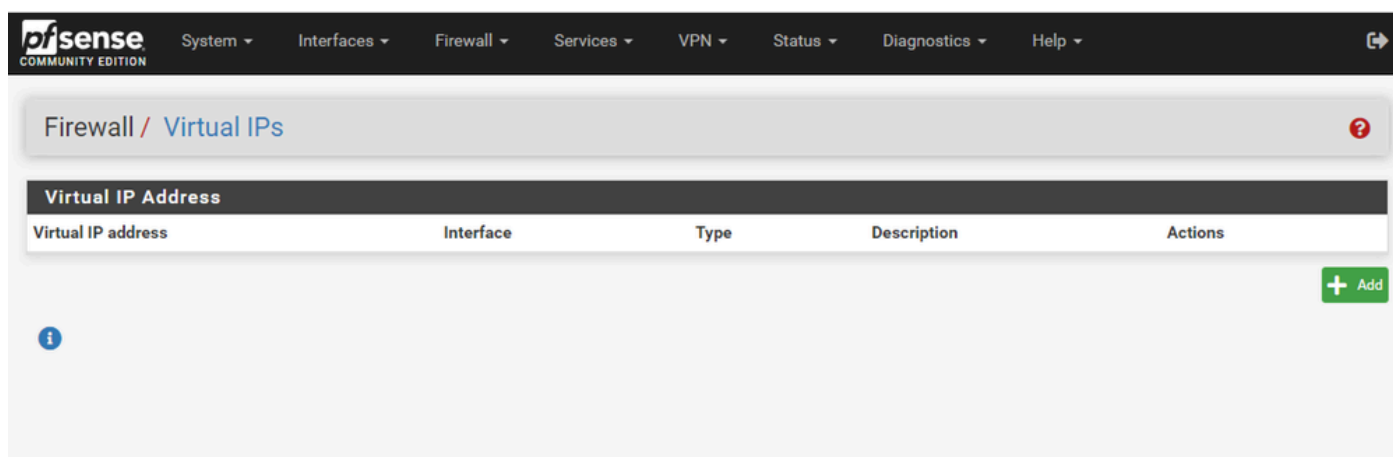
Au moins une adresse IP est requise pour héberger des sites Web sur le PfSense. Dans pfSense, cette opération est effectuée avec des adresses IP virtuelles (VIP).

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

[System](#) ▾ [Interfaces](#) ▾ [Firewall](#) ▾ [Services](#) ▾ [VPN](#) ▾ [Status](#) ▾ [Diagnostics](#) ▾ [Help](#) ▾

Firewall / [Virtual IPs](#) / [Edit](#)

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface

Address type

Address(es) /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.

Advertising frequency

Base Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

Interface utilisateur graphique pfSense - Configuration VIP

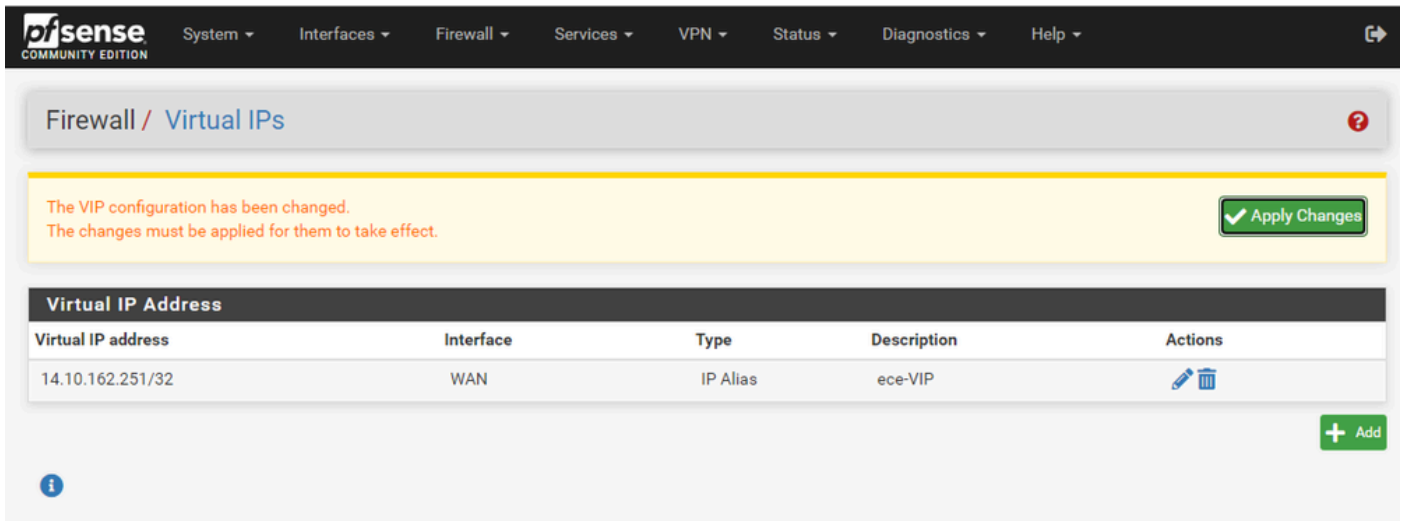
Utilisez ces informations pour ajouter un VIP.

- 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



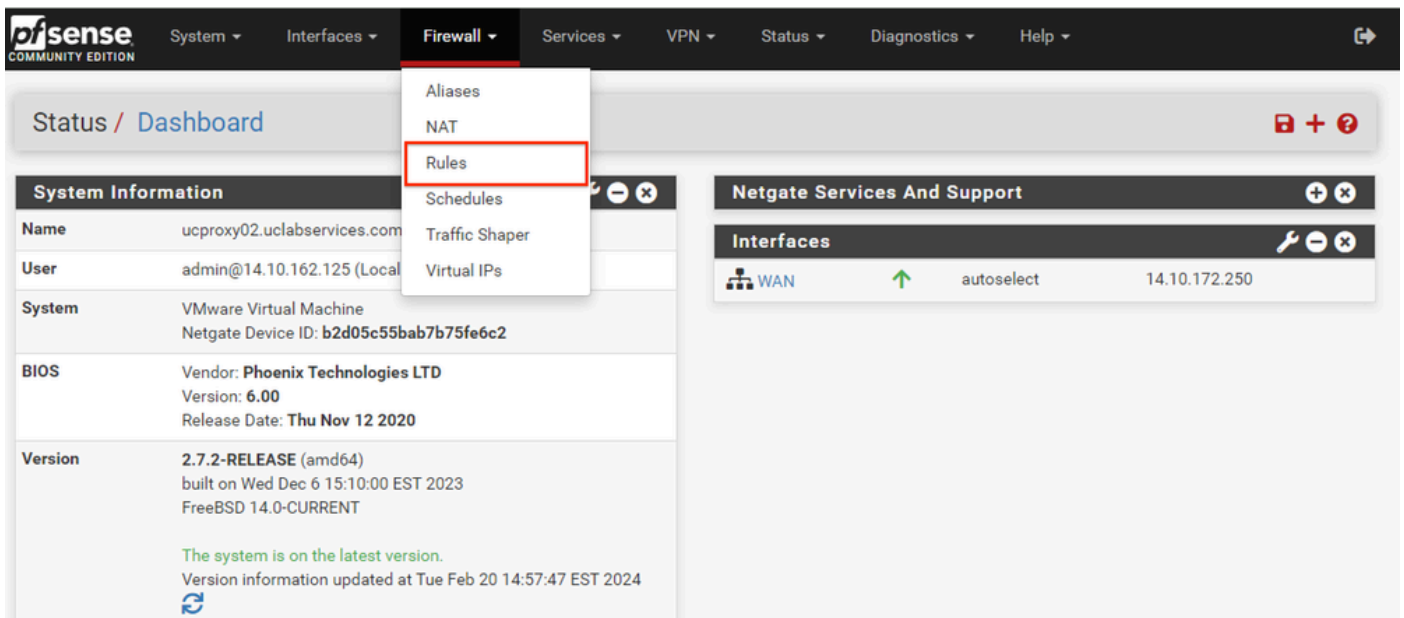
Interface utilisateur graphique pfSense - Liste VIP

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

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / WAN

Floating WAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/13.35 MiB	*	*	*	WAN Address	8443 22	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/3.63 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

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

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action ▾
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface ▾
Choose the interface from which packets must come to match this rule.

Address Family ▾
Select the Internet Protocol version this rule applies to.

Protocol ▾
Choose which IP protocol this rule should match.

Source

Source Invert match ▾ / ▾

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match ▾ / ▾

Destination Port Range ▾ ▾
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

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 : laissez 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.

The screenshot shows the 'Edit Firewall Rule' configuration page in pfSense. The page is divided into several sections:

- Action:** Set to 'Block'. A hint explains the difference between block and reject.
- Disabled:** A checkbox for 'Disable this rule' is unchecked.
- Interface:** Set to 'WAN'.
- Address Family:** Set to 'IPv4'.
- Protocol:** Set to 'TCP'.
- Source:** Includes an 'Invert match' checkbox (unchecked), a dropdown for 'Any', and a 'Source Address' field. A 'Display Advanced' button is present.
- Destination:** Includes an 'Invert match' checkbox (unchecked), a dropdown for 'Any', and a 'Destination Address' field. The 'Destination Port Range' section has 'From' and 'To' dropdowns set to '(other)', with 'Custom' input fields for each.
- Extra Options:** Includes a 'Log' checkbox (checked) with a hint about local log space. The 'Description' field contains the text 'Drop all other inbound traffic'. An 'Advanced Options' section with a 'Display Advanced' button is also visible.

At the bottom of the form is a blue 'Save' button.

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 : laissez 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

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/13.51 MiB	*	*	*	WAN Address	8443 22	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/3.65 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	14.10.162.251	443 (HTTPS)	*	none		Allow ECE HTTPS	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	none		Drop all other inbound traffic	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

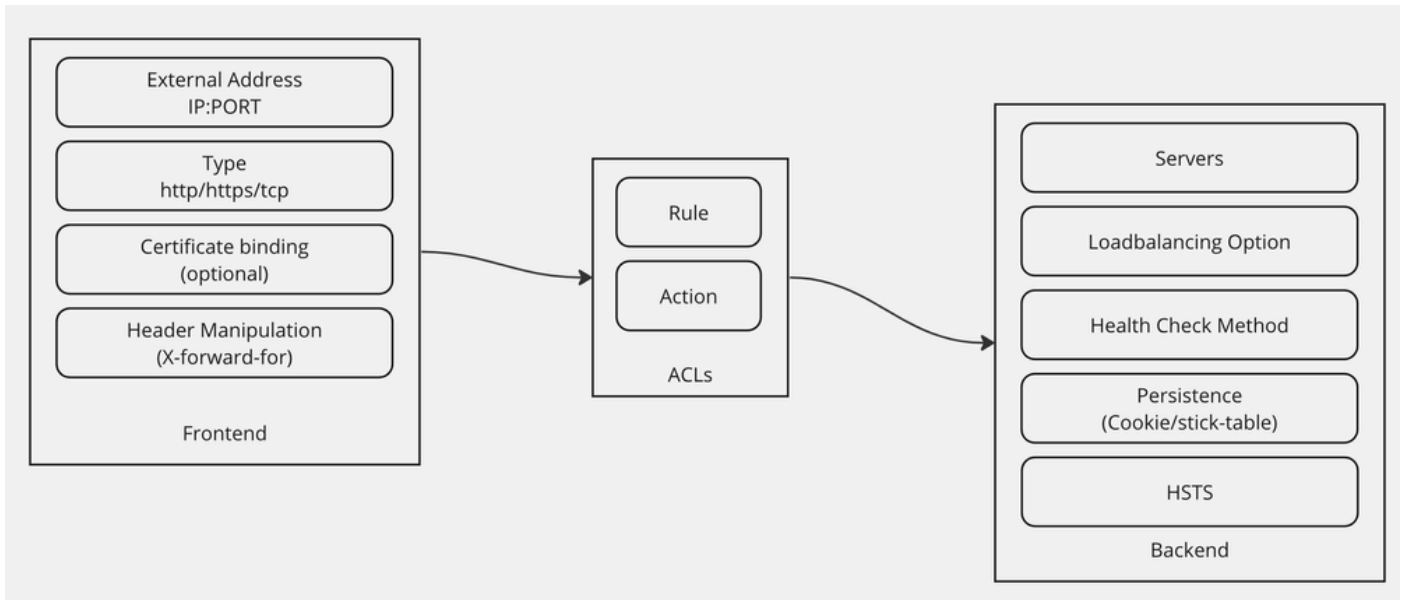
Interface utilisateur graphique pfSense - Liste des règles de pare-feu

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

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the following items: System, Interfaces, Firewall, Services (selected), VPN, Status, Diagnostics, and Help. Below the navigation bar, the main content area is divided into two columns. The left column contains a 'System Information' table, and the right column contains a 'Netgate Services And Support' section.

System Information	
Name	ucproxy02.uclabservices.com
User	admin@14.10.162.125 (Local Database)
System	VMware Virtual Machine Netgate Device ID: b2d05c55bab7b75fe6c2
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 15:10:00 EST 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 14:00:00 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

The 'Services' menu is open, showing a list of services. The 'HAProxy' option is highlighted with a red box. Other services listed include Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, NTP, PPPoE Server, Router Advertisement, SNMP, and Wake-on-LAN.

The 'Netgate Services And Support' section shows the contract type as 'Community Support' and 'Community Support Only'. Below this, there is a section titled 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES'. The text explains that users who purchased their pfSense gateway firewall appliance from Netgate and elected 'Community Support' at the point of sale or installed pfSense on their own hardware, have access to various community support resources. This includes the 'NETGATE RESOURCE LIBRARY'. The text also mentions that users may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription, which is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

Interface utilisateur graphique pfSense - Liste déroulante HAProxy

Étape 2. Configurer les paramètres de base

General settings

 Enable HAProxy

Installed version 2.8.3-86e043a
Maximum connections

per process.

Sets the maximum per-process number of concurrent connections to X.
NOTE: setting this value too high will result in HAProxy not being able to allocate enough memory.

Current 'System Tunables' settings.

'kern.maxfiles': **30767**

'kern.maxfilesperproc': **27684**

Full memory usage will only show after all connections have actually been used.

When setting a high amount of allowed simultaneous connections you will need to add and or increase the following two 'System Tunables' kern.maxfiles and kern.maxfilesperproc. For HAProxy alone set these to at least the number of allowed connections * 2 + 31. So for 100.000 connections these need to be 200.031 or more to avoid trouble, take into account that handles are also used by other processes when setting kern.maxfiles.

Connections	Memory usage
1	50 kB
1.000	48 MB
10.000	488 MB
100.000	4,8 GB

Calculated for plain HTTP connections, using ssl offloading will increase this.

Number of threads to start per process

Defaults to 1 if left blank (1 CPU core(s) detected).

FOR NOW, THREADS SUPPORT IN HAPROXY 1.8 IS HIGHLY EXPERIMENTAL AND IT MUST BE ENABLED WITH CAUTION AND AT YOUR OWN RISK.

Reload behaviour
 Force immediate stop of old process on reload. (closes existing connections)

Note: when this option is selected, connections will be closed when haproxy is restarted. Otherwise the existing connections will be served by the old haproxy process until they are closed. Checking this option will interrupt existing connections on a restart (which happens when the configuration is applied, but possibly also when pfSense detects an interface coming up or a change in its ip-address.)

Reload stop behaviour

Defines the maximum time allowed to perform a clean soft-stop. Defaults to 15 minutes, but could also be defined in different units like 30s, 15m, 3h or 1d.

Carp monitor

Monitor carp interface and only run haproxy on the firewall which is MASTER.

Stats tab, 'internal' stats port

Internal stats port

EXAMPLE: 2200

Sets the internal port to be used for the stats tab. This is bound to 127.0.0.1 so will not be directly exposed on any LAN/WAN/other interface. It is used to internally pass through the stats page. Leave this setting empty to remove the "HAProxyLocalStats" item from the stats page and save a little on resources.

Internal stats refresh rate

Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

Sticktable page refresh rate

Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

Interface utilisateur graphique pfSense - Paramètres principaux HAProxy

Cochez la case Activer HAProxy.

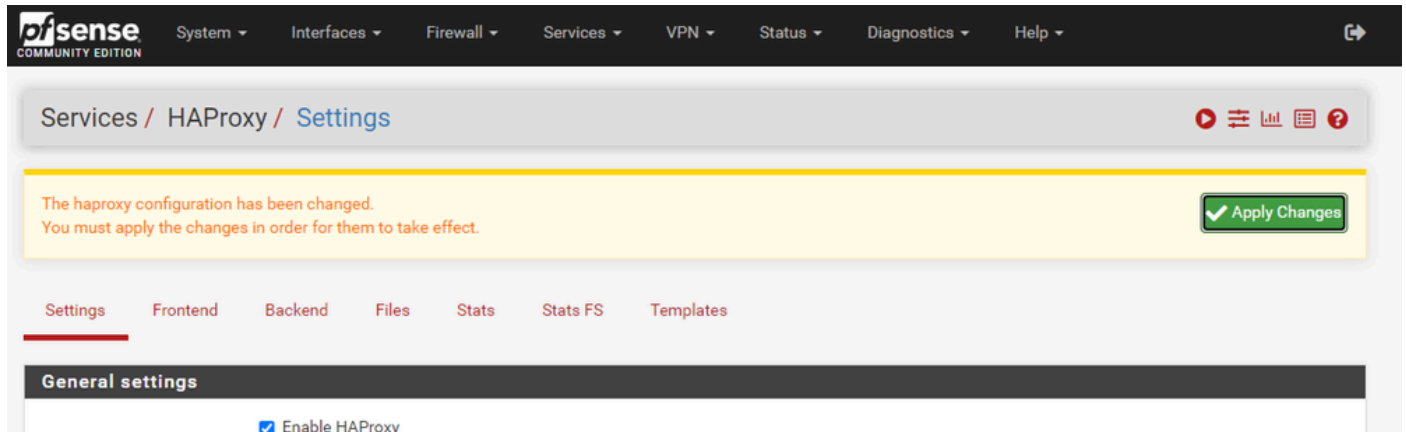
Saisissez une valeur pour le paramètre Nombre maximal de connexions. Reportez-vous au tableau de cette section pour plus de détails sur la mémoire requise.

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.



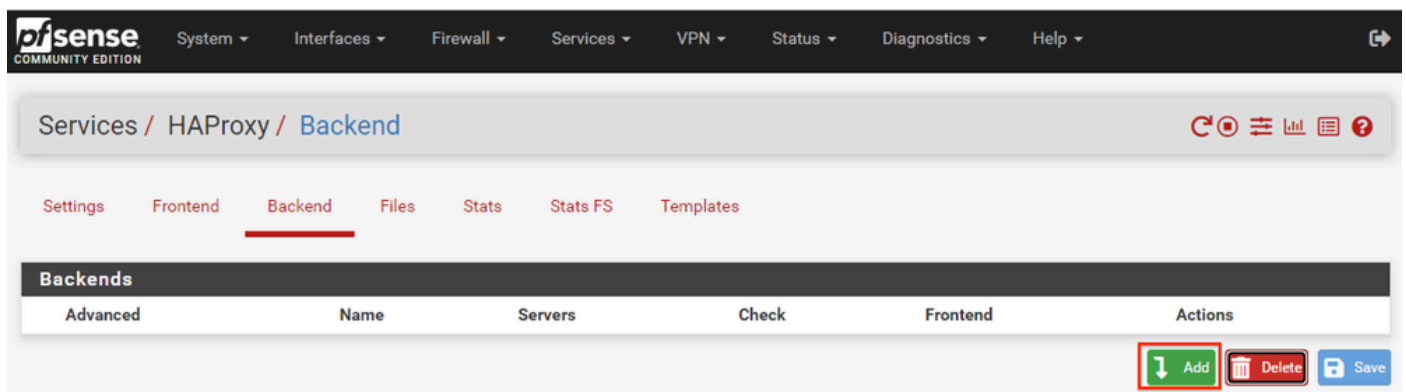
The screenshot shows the pfSense web interface for the HAProxy Settings page. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation, the breadcrumb trail reads 'Services / HAProxy / Settings'. A yellow notification banner at the top states: 'The haproxy configuration has been changed. You must apply the changes in order for them to take effect.' To the right of this banner is a green 'Apply Changes' button. Below the notification, there are tabs for 'Settings', 'Frontend', 'Backend', 'Files', 'Stats', 'Stats FS', and 'Templates'. The 'Settings' tab is currently selected. Underneath, there is a section titled 'General settings' with a checkbox labeled 'Enable HAProxy' which is checked.

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

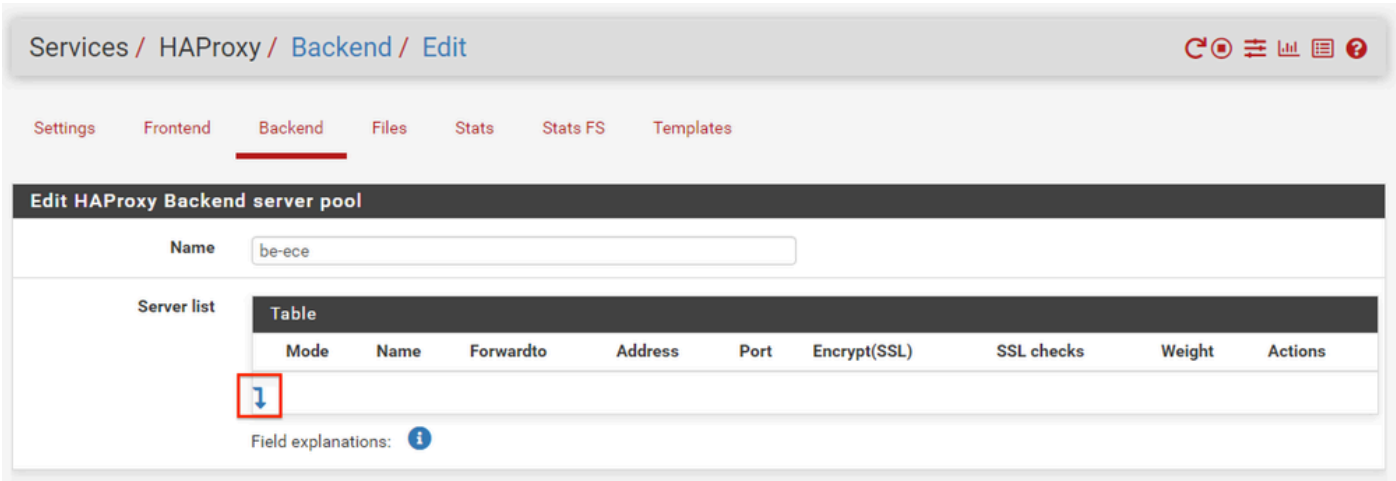
Commencez par le back-end. La raison en est que le serveur frontal doit faire référence à un serveur principal. Vérifiez que vous avez sélectionné le menu principal.



The screenshot shows the pfSense web interface for the HAProxy Backend page. The navigation menu at the top is the same as in the previous screenshot. The breadcrumb trail now reads 'Services / HAProxy / Backend'. The 'Backend' tab is selected. Below the tabs, there is a section titled 'Backends' which contains a table with columns: 'Advanced', 'Name', 'Servers', 'Check', 'Frontend', and 'Actions'. At the bottom right of the table, there are three buttons: 'Add' (highlighted with a red box), 'Delete', and 'Save'.

Interface utilisateur graphique pfSense - HAProxy Add Backend

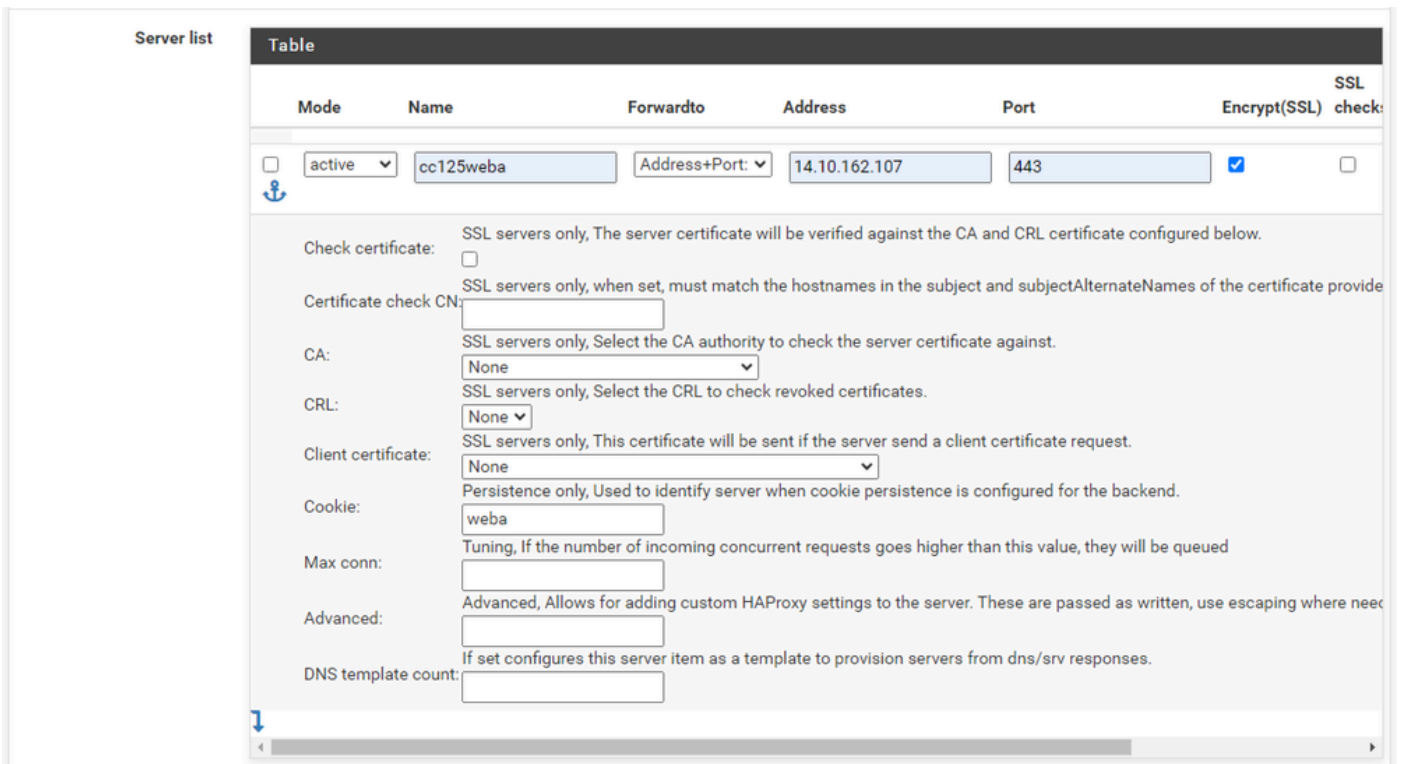
Cliquez sur le bouton Ajouter.



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.

Loadbalancing options (when multiple servers are defined)

Balance

None
This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.

Round robin
Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Static Round Robin
Each server is used in turns, according to their weights. This algorithm is as similar to roundrobin except that it is static, which means that changing a server's weight on the fly will have no effect. On the other hand, it has no design limitation on the number of servers, and when a server goes up, it is always immediately reintroduced into the farm, once the full map is recomputed. It also uses slightly less CPU to run (around -1%).

Least Connections
The server with the lowest number of connections receives the connection. Round-robin is performed within groups of servers of the same load to ensure that all servers will be used. Use of this algorithm is recommended where very long sessions are expected, such as LDAP, SQL, TSE, etc... but is not very well suited for protocols using short sessions such as HTTP. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Source
The source IP address is hashed and divided by the total weight of the running servers to designate which server will receive the request. This ensures that the same client IP address will always reach the same server as long as no server goes down or up. If the hash result changes due to the number of running servers changing, many clients will be directed to a different server. This algorithm is generally used in TCP mode where no cookie may be inserted. It may also be used on the Internet to provide a best-effort stickyness to clients which refuse session cookies. This algorithm is static, which means that changing a server's weight on the fly will have no effect.

Uri (HTTP backends only)
This algorithm hashes either the left part of the URI (before the question mark) or the whole URI (if the "whole" parameter is present) and divides the hash value by the total weight of the running servers. The result designates which server will receive the request. This ensures that the same URI will always be directed to the same server as long as no server goes up or down. This is used with proxy caches and anti-virus proxies in order to maximize the cache hit rate. Note that this algorithm may only be used in an HTTP backend.

Len (optional)
The "len" parameter indicates that the algorithm should only consider that many characters at the beginning of the URI to compute the hash.

Depth (optional)
The "depth" parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request.

Allow using whole URI including url parameters behind a question mark.

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.

Access control lists and actions	
Timeout / retry settings	
Connection timeout	60000 The time (in milliseconds) we give up if the connection does not complete within (default 30000).
Server timeout	60000 The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).
Retries	2 After a connection failure to a server, it is possible to retry, potentially on another server. This is useful if health-checks are too rare and you don't want the clients to see the failures. The number of attempts to reconnect is set by the "retries" parameter.
Health checking	
Health check method	HTTP <small>HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).</small>
Check frequency	 milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	<input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged. By default, failed health check are logged if server is UP and successful health checks are logged if server is DOWN, so the amount of additional information is limited.
Http check method	GET <small>OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the webserver and is less easy to filter out of its logs.</small>
Url used by http check requests.	/system/web/view/platform/common/login/root.jsp?partitionId=1 Defaults to / if left blank.
Http check version	HTTP/1.1\r\nHost:\ ece125.uclabservices.com Defaults to "HTTP/1.0" if left blank. Note that the Host field is mandatory in HTTP/1.1, and as a trick, it is possible to pass it after "\r\n" following the version string like this: <code>HTTP/1.1\r\nHost:\ www</code> Also some hosts might require an accept parameter like this: <code>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</code>

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\nHost:\ {fqdn_of_server}

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

Agent checks

Agent checks Use agent checks
Use a TCP connection to read an ASCII string of the form 100%,75%,drain,down (more about this in the [haproxy manual](#))

Cookie persistence

Cookie Enabled Enables cookie based persistence. (only used on "http" frontends)

Server Cookies **Make sure to configure a different cookie on every server in this backend.**

Cookie Name
The string name to track in Set-Cookie and Cookie HTTP headers.
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASPNET_SessionId

Cookie Mode
Determines how HAProxy inserts/prefixes/replaces or examines cookie and set-cookie headers.
EXAMPLE: with an existing PHPSESSIONID you can for example use "Session-prefix" or to create a new cookie use "Insert-silent".

```
cookie is analyzed on incoming request to choose server and
set-cookie value is overwritten if present and set to an
unknown value or inserted in response if not present.

cookie <cookie name> insert
```

Cookie Cachable Allows shared caches to cache the server response.

Cookie Options Only insert cookie on post requests. Prevent usage of cookie with non-HTTP components. Prevent usage of cookie over non-secure channels.

Cookie Options
Max idle time It only works with insert-mode cookies. Max life time It only works with insert-mode cookies.

Cookie domains
Domains to set the cookie for, separate multiple domains with a space.

Cookie dynamic key
Set the dynamic cookie secret key for a backend. This is will be used to generate a dynamic cookie with.

Stick-table persistence

These options are used to make sure separate requests from a single client go to the same backend. This can be required for servers that keep track of for example a shopping cart.

Stick tables
Sticktables that are kept in memory, and when matched make sure the same server will be used.

```
No stick-table will be used
```

Email notifications

Mail level
Define the maximum loglevel to send emails for.

Mail to
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

Serveur principal HAProxy - Persistence 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.

HSTS / Cookie protection

HSTS Strict-Transport-Security When configured enables "HTTP Strict Transport Security" leave empty to disable. (only used on "http" frontends)

WARNING! the domain will only work over https with a valid certificate!
Clients will cache this header for the set duration which means removing this header will still require a valid certificate for the set time.

31536000 Seconds

If configured clients that requested the page with this setting active will not be able to visit this domain over a unencrypted http connection. So make sure you understand the consequence of this setting or start with a really low value.
EXAMPLE: 60 for testing if you are absolutely sure you want this 31536000 (12 months) would be good for production.

Cookie protection Set "secure" attribute on cookies (only used on "http" frontends)
This configuration option sets up the Secure attribute on cookies if it has not been setup by the application server while the client was browsing the application over a ciphered connection.

Advanced settings

[Save](#)

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.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / HAProxy / Frontend

Settings Frontend Backend Files Stats Stats FS Templates

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
									Add Delete Save

Interface utilisateur graphique pfSense - HAProxy Add Frontend

Sélectionnez le bouton Ajouter.

Settings **Frontend** Backend Files Stats Stats FS Templates

Edit HAProxy Frontend

Name

Description

Status

External address Define what ip:port combinations to listen on for incoming connections.

Table						
	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/>	14.10.162.252 (ece-VIP)	<input type="text"/>	443	<input checked="" type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
 If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define [Virtual IP](#) addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (.). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

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).

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Table						
Name	Expression	CS	Not	Value	Actions	
↓						

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched

Example:

Name	Expression	CS	Not	Value	Actions
Backend1acl	Host matches			www.yourdomain.tld	
addHeaderAc	SSL Client certificate valid				

acl's with the same name will be 'combined' using OR criteria.
 For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table			
Action	Parameters	Condition acl names	Actions
↓			

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

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.

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Table							
	Name	Expression	CS	Not	Value	Actions	
<input type="checkbox"/>		ccmpWS	Host starts with:	no	no	ccmp.uclabservices.com:8085	
<input type="checkbox"/>		ccmpSSL	Host starts with:	no	no	ccmp.uclabservices.com	

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched
 Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

 acl's with the same name will be 'combined' using OR criteria.
 For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACL's](#)

NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table					
	Action	Parameters	Condition acl names	Actions	
<input type="checkbox"/>		Use Backend	See below	ccmpSSL	
		backend: be-uclab-ccmp120-ssl			
<input type="checkbox"/>		Use Backend	See below	ccmpWS	
		backend: be-uclab-ccmp120-ws			

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

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.

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss."

SNI Filter
Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate
Choose the cert to use on this frontend.
 Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 Add ACL for certificate Subject Alternative Names.

OCSP Load certificate ocsp responses for easy certificate validation by the client.
A cron job wil update the ocsp response every hour.

Additional certificates Which of these certificate will be send will be determined by haproxy's SNI recognition. If the browser does not send SNI this will not work properly. (IE on XP is one example, possibly also older browsers or mobile devices).

Table	
Certificates	Actions
<input type="checkbox"/> Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)	
<input type="checkbox"/> Add ACL for certificate Subject Alternative Names.	

Advanced ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: force-ssl3, force-tls10 force-tls11 force-tls12 no-ssl3 no-tls10 no-tls11 no-tls12 no-tls-tickets
Example: no-ssl3 ciphers EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES

Advanced certificate specific ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: alpn, no-ca-names, ecnhe, curves, ciphers, ssl-min-ver and ssl-max-ver
Example: alpn h2,http/1.1 ciphers EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecnhe secp256k1

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.

Services / HAProxy / Frontend

The haproxy configuration has been changed.
You must apply the changes in order for them to take effect.

Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

Frontends									
Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	fe-ece	Frontend for ECE	14.10.162.252:443	https	be-ece (default)	

Add Delete Save

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.