PfSense Community-taakverdeling voor ECE configureren

Inhoud

Inleiding

Dit document beschrijft de stappen om pfSense Community Edition te configureren en in te stellen als een taakverdeling voor Enterprise Chat en Email (ECE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ECE 12.x
- PFSense Community Edition

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- ECE 12.6(1)
- PFSense Community Edition 2.7.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Installeer PFSense

Overzicht van oplossing

pfSense Community Edition is een multifunctioneel product dat een firewall, taakverdeling, security scanner en veel andere services in één server biedt. pfSense is gebaseerd op gratis BSD en heeft minimale hardwarevereisten. De taakverdeling is een implementatie van HAProxy en er is een eenvoudig te gebruiken GUI om het product te configureren.

U kunt deze taakverdeling gebruiken met zowel ECE als Contact Center Management Portal (CCMP). Dit document bevat de stappen voor het configureren van pfSense voor ECE.

Voorbereiding

Stap 1. Download de PFSense-software

Gebruik de pfSense website om het installatiebestand van de iso te downloaden.

Stap 2. VM configureren

Een VM configureren met de minimumvereisten:

· 64-bits amd64 (x86-64) compatibele CPU

· 1 GB of meer RAM

· 8 GB of groter schijfstation (SSD, HDD, enz.)

· Een of meer compatibele netwerkinterfacekaarten

· Opstartbaar USB-station of optisch station met hoge capaciteit (DVD of BD) voor eerste installatie

Voor installatie in een lab is slechts één netwerkinterface (NIC) vereist. Er zijn verschillende manieren om het apparaat uit te voeren, maar het eenvoudigst is een enkele NIC, ook wel one-arm mode genoemd. In één-arm modus is er één interface die communiceert met het netwerk. Hoewel dit een makkelijke manier is en geschikt voor een lab, is het niet de meest veilige manier.

Een veiligere manier om het apparaat te configureren is door ten minste twee NIC's te hebben. Eén NIC is de WAN-interface en communiceert rechtstreeks met het openbare internet. De tweede NIC is de LAN-interface en communiceert met het interne bedrijfsnetwerk. U kunt ook extra interfaces toevoegen om te communiceren met verschillende delen van het netwerk die verschillende beveiligings- en firewallregels hebben. U kunt bijvoorbeeld een NIC verbinden met het openbare internet, een verbinding maken met het DMZ-netwerk waar alle extern toegankelijke webservers zijn, en een derde NIC verbinding maken met het bedrijfsnetwerk. Hierdoor hebt u interne en externe gebruikers veilig toegang tot dezelfde set webservers die in een DMZ worden bewaard. Zorg ervoor dat u de veiligheidsimplicaties van elk ontwerp begrijpt voordat het wordt geïmplementeerd. Raadpleeg een security engineer om er zeker van te zijn dat de best practices voor uw specifieke implementatie worden gevolgd.

Installatie

Stap 1. De ISO op de VM monteren

Stap 2. Schakel de VM in en volg de aanwijzingen voor installatie.

Raadpleeg dit document voor stapsgewijze instructies.

Netwerkinstelling

U moet IP-adressen aan het apparaat toewijzen om door te gaan met de configuratie.

Opmerking: in dit document wordt een apparaat weergegeven dat in de modus met één arm is geconfigureerd.

Stap 1. VLAN’s configureren

Als u VLAN-ondersteuning nodig hebt, beantwoord dan de eerste vraag. Zo niet, antwoord nr.

Stap 2. WAN-interface toewijzen

De WAN-interface is de niet-beveiligde kant van het apparaat in de modus met twee armen en de enige interface in de modus met één arm. Voer de interfacenaam in wanneer dit wordt gevraagd.

Stap 3. Wijs de LAN interface toe

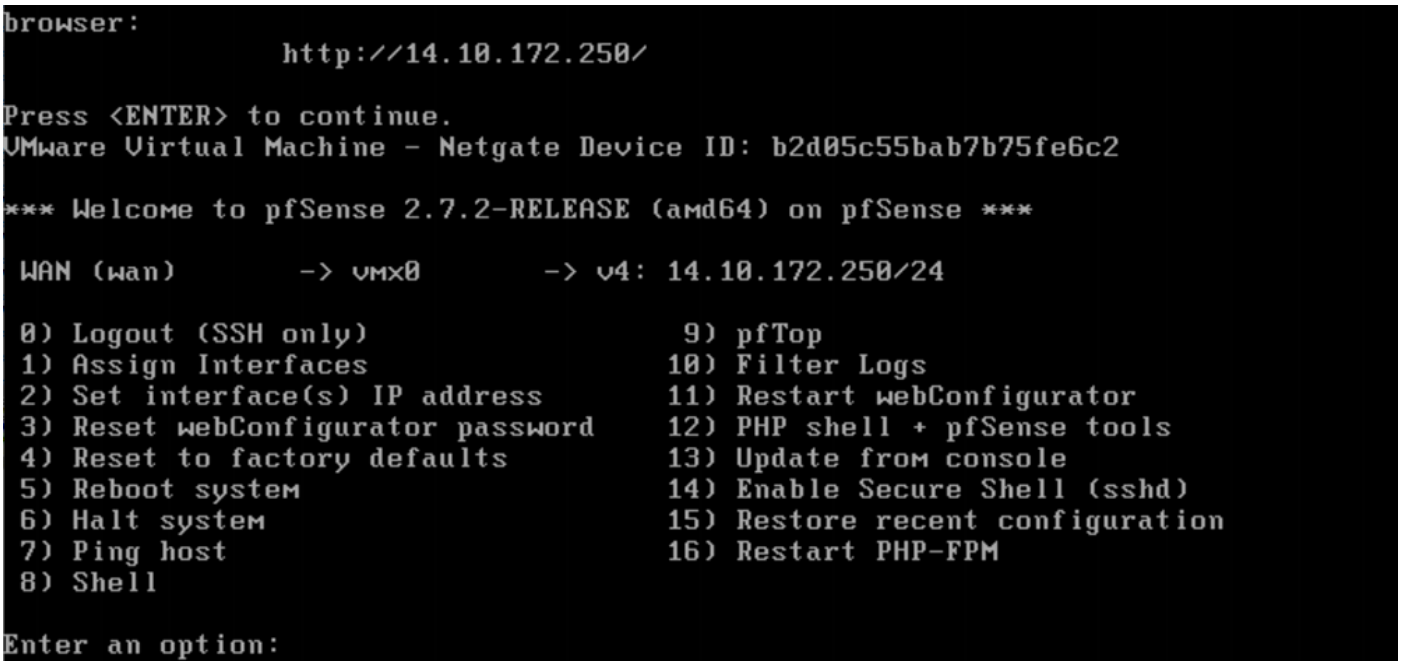
De LAN-interface is de beveiligde kant van het apparaat in de modus met twee armen. Indien nodig voert u de interfacenaam in wanneer dit wordt gevraagd.

Stap 4. Andere interfaces toewijzen

Configureer eventuele andere interfaces die u nodig hebt voor uw specifieke installatie. Deze zijn optioneel en niet alledaags.

Stap 5. IP-adres aan een beheerinterface toewijzen

Als uw netwerk DHCP ondersteunt, wordt het toegewezen IP-adres weergegeven in het consolescherm.

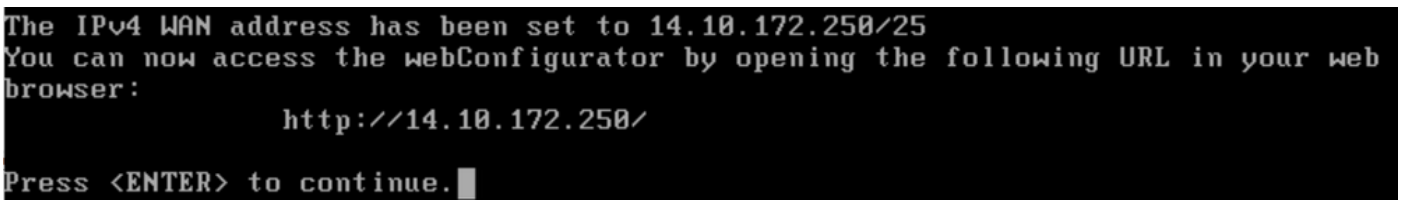


PFSense-console

Als er geen adres is toegewezen of als u een specifiek adres wilt toewijzen, voert u deze stappen uit.

1. Kies optie 2 in het consolemenu.
2. Antwoord op: DHCP uitschakelen.
3. Voer het IPv4-adres voor de WAN-interface in.
4. Geef het netmasker op voor de bittellingen. (24 = 255,255,255,0, 16 = 255,255,0,0, 8 = 255,0,0,0)
5. Voer het gatewayadres voor de WAN-interface in.
6. Als u wilt dat deze gateway de standaardgateway voor het apparaat wordt, antwoordt u op de gatewayprompt, anders antwoordt u op.
7. Configureer de NIC voor IPv6 indien gewenst.
8. DHCP-server op de interface uitschakelen.
9. Antwoord door HTTP in te schakelen op het webConfigurator-protocol. Dit wordt gebruikt in de volgende stappen.

U ontvangt vervolgens een bevestiging dat de instellingen zijn bijgewerkt.

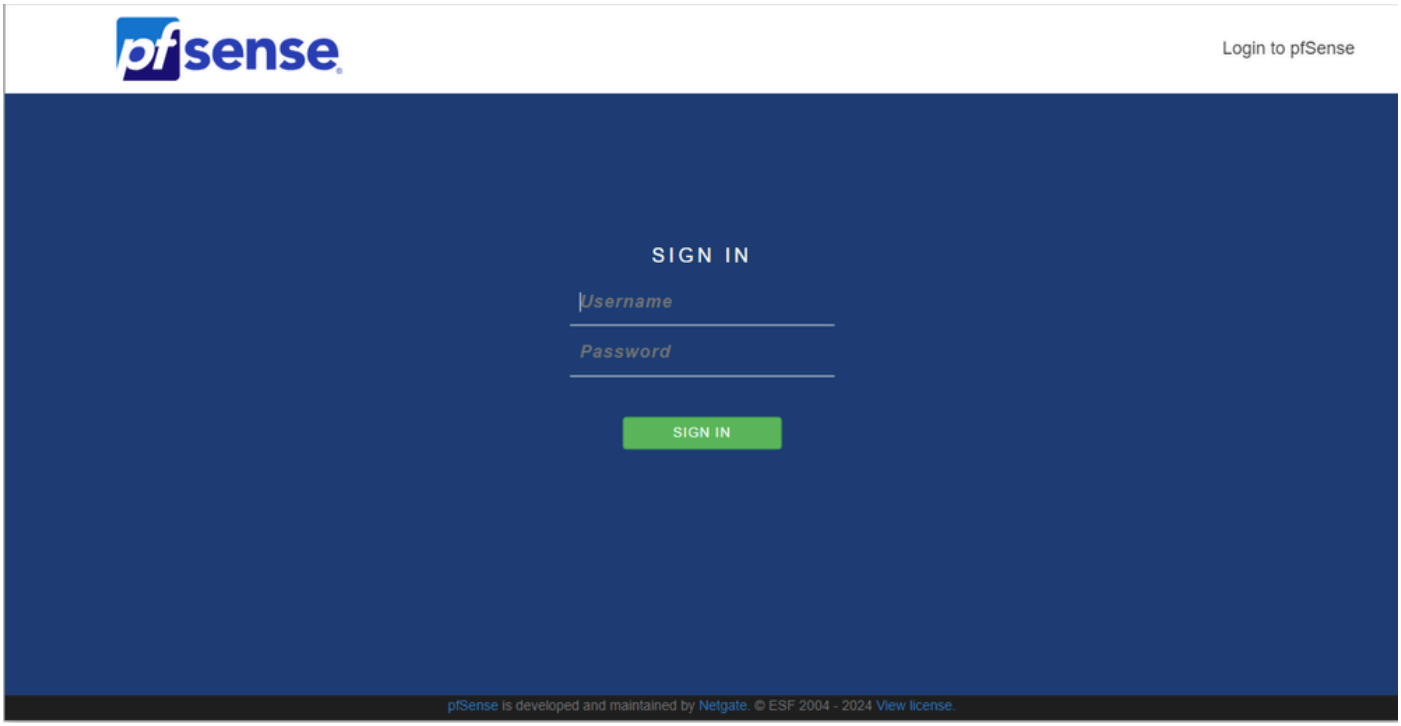


PFSense-bevestiging

Eerste configuratie voltooien

Stap 1. Open een webbrowser en navigeer naar: http://<ip_address_of_application>

✎ Opmerking: u moet eerst HTTP en niet HTTPS gebruiken.

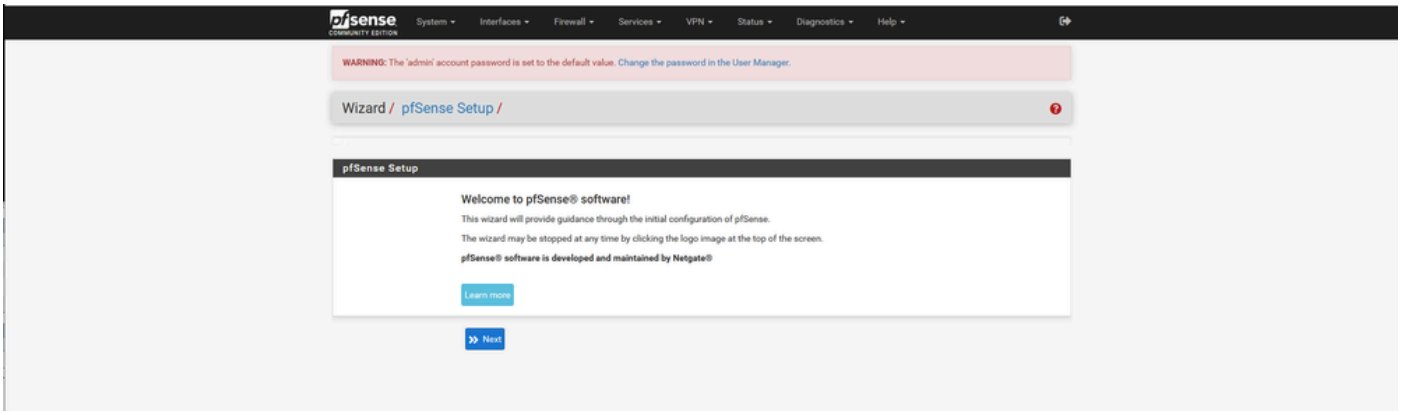


Aanmelden bij PFSense Admin

Stap 2. Login met de standaardlogin van admin / pfSense

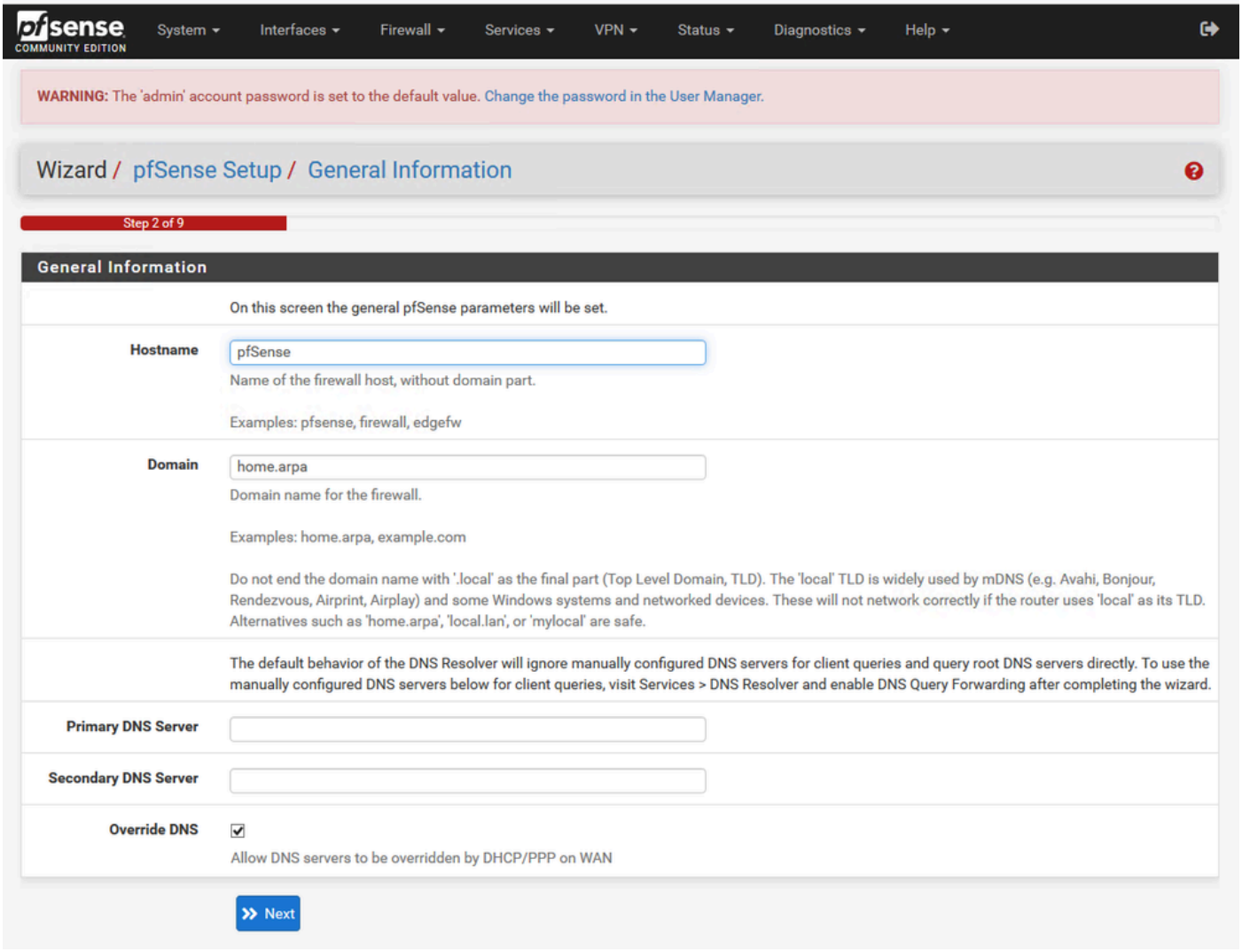
Stap 3. De eerste configuratie voltooien

Klik op volgende door de eerste twee schermen.



Wizard PFSense instellen - 1

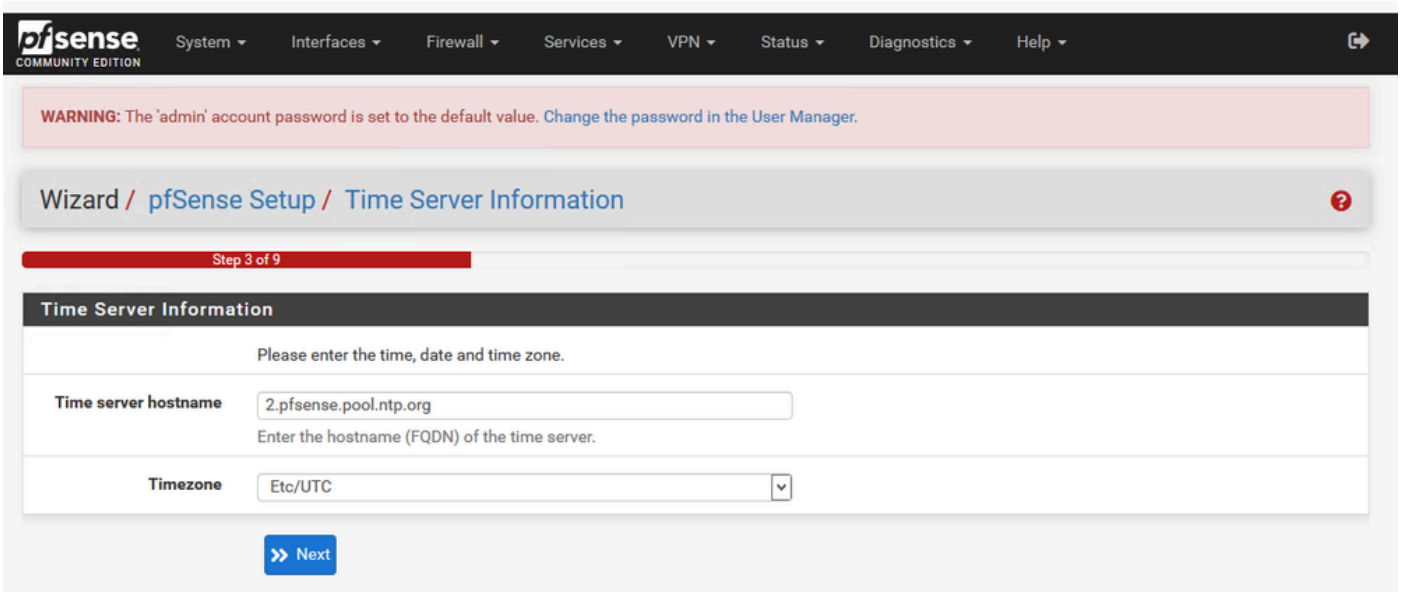
Geef de hostnaam, domeinnaam en DNS-serverinformatie op.



Wizard PFSense instellen - 2

Valideer de IP-adresinformatie. Als u aanvankelijk DHCP koos, kunt u dit nu veranderen.

Geef de NTP-tijdserver hostnaam en selecteer de juiste tijdzone in de vervolgkeuzelijst.



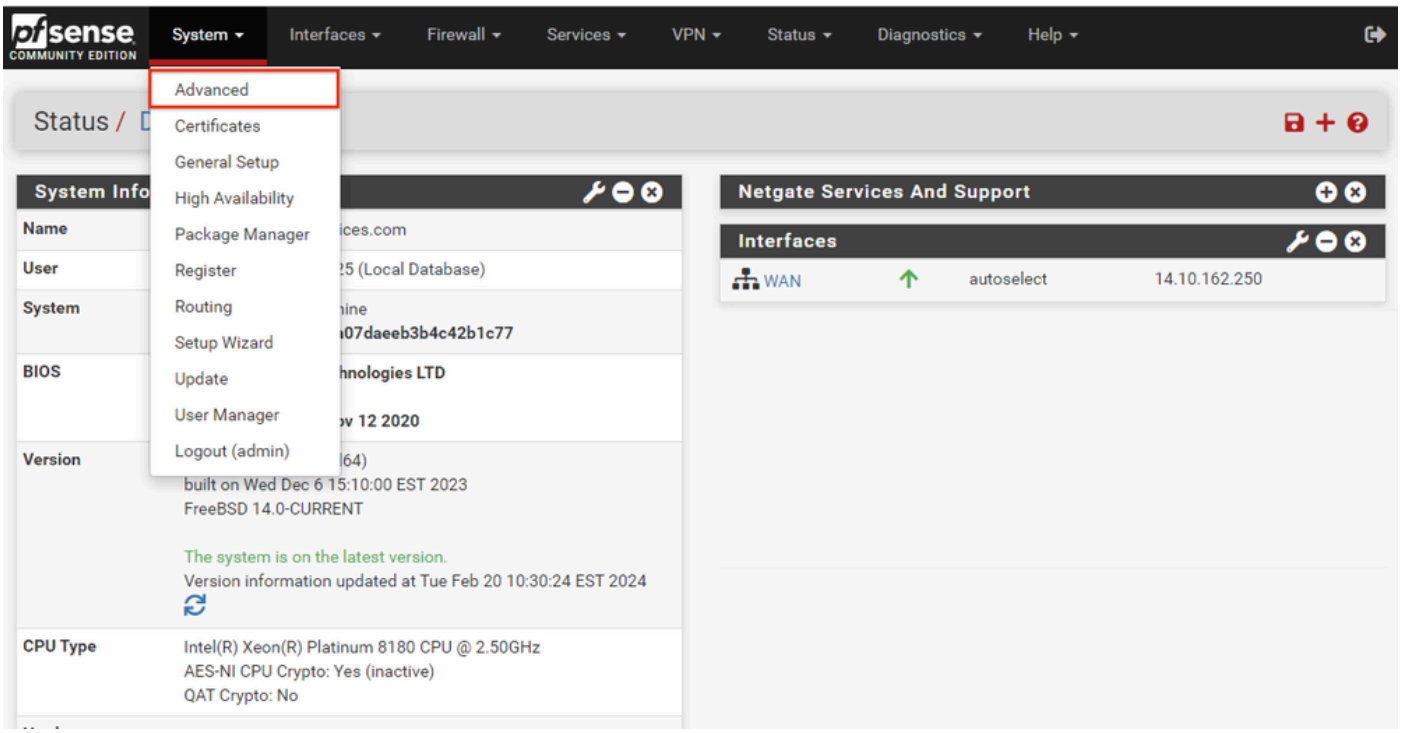
Wizard PFSense instellen - 3

Ga door met de installatiewizard tot het einde. De interface GUI wordt opnieuw opgestart en u wordt doorgestuurd naar de nieuwe URL zodra deze is voltooid.

Basisbeheerinstellingen configureren

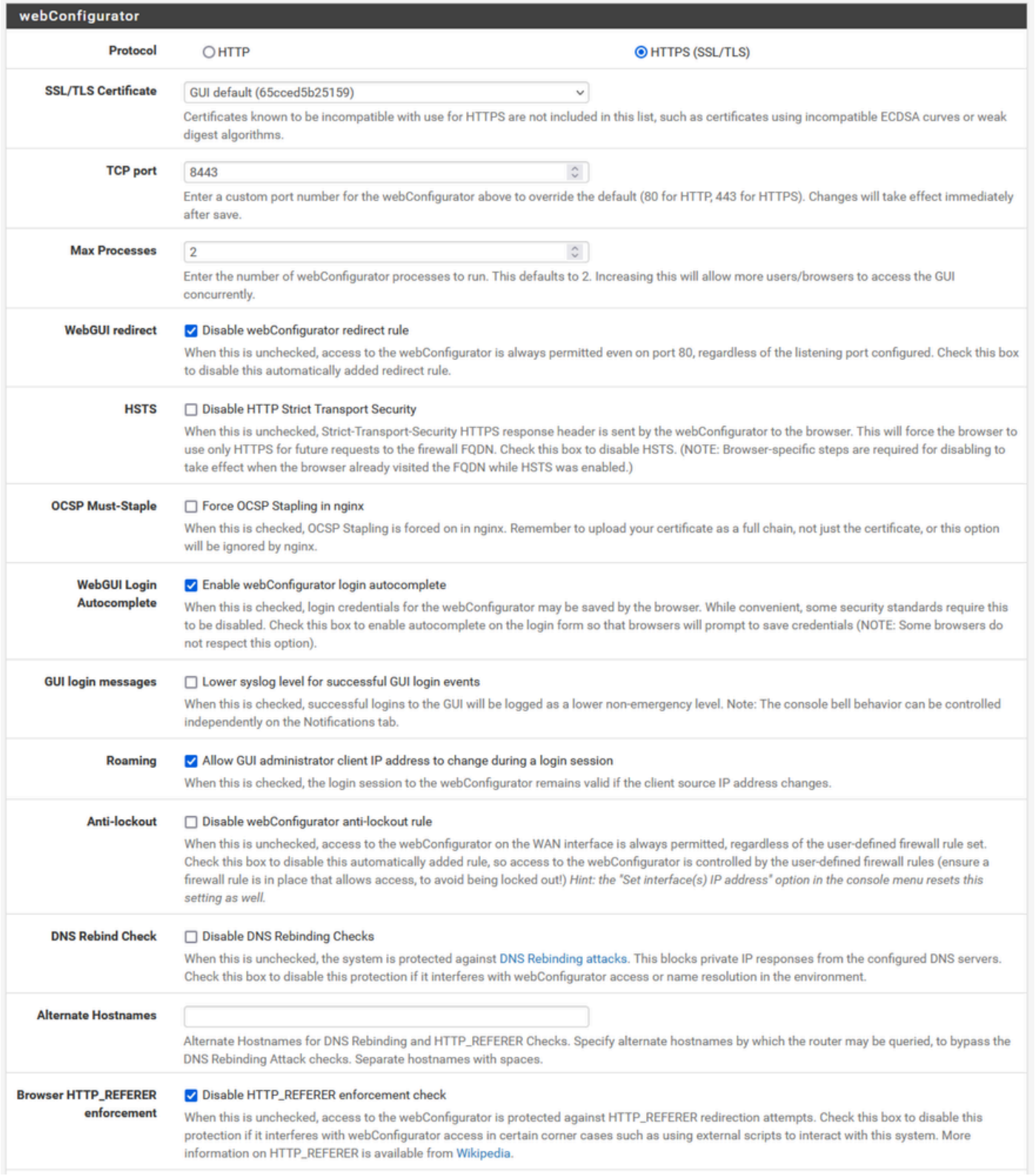
Stap 1. Aanmelden bij de beheerinterface

Stap 2. Selecteer Geavanceerd in het vervolgkeuzemenu Systeem



PFSense GUI - Admin Dropdown

Stap 3. WebConfigurator-instellingen bijwerken



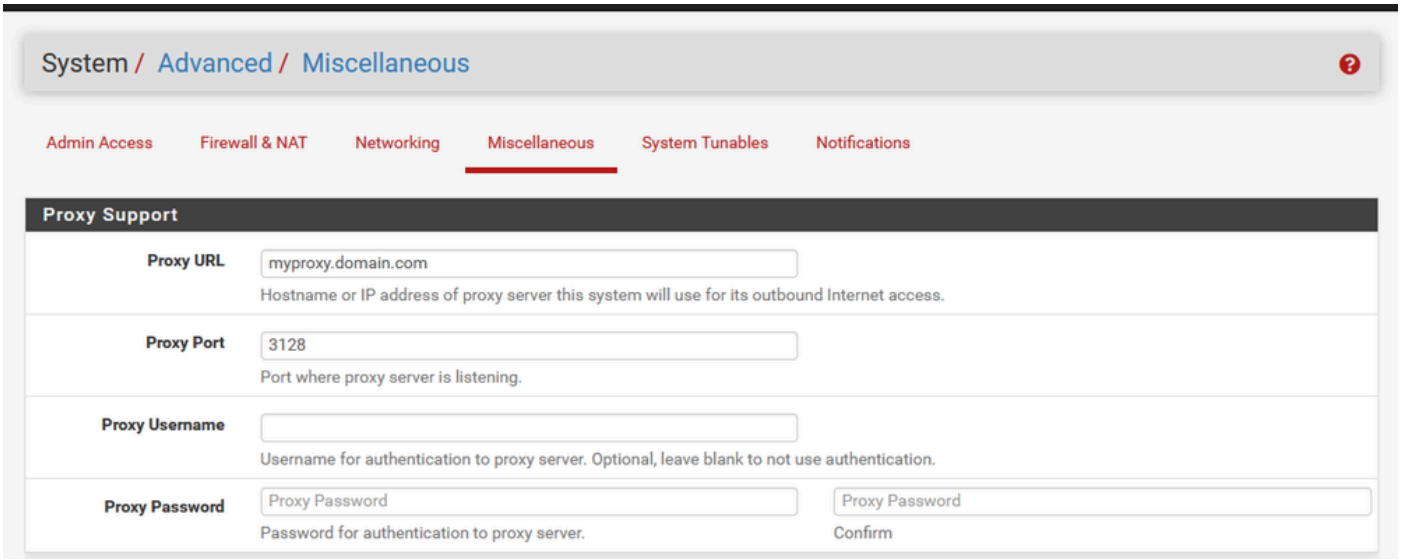
PFSense GUI - Admin-configuratie

1. Selecteer het HTTPS-protocol (SSL/TLS).
2. Laat het SSL/TLS-certificaat op dit moment over aan het zelfondertekende certificaat.
3. Verander de TCP-poort in een andere poort dan 443 om de interface beter te beveiligen en problemen met poortoverlap te voorkomen.
4. Selecteer de optie WebGUI redirect om de beheerinterface op poort 80 uit te schakelen.
5. Selecteer de Browser HTTP_REFERER handhavingsoptie.
6. Schakel Secure Shell in door de optie Secure Shell inschakelen te selecteren.

Opmerking: Zorg ervoor dat u de knop Opslaan selecteert voordat u doorgaat. Je wordt dan doorgestuurd naar de nieuwe https link.

Stap 4. Proxyserver configureren, indien nodig

Indien nodig kunt u de proxy-informatie op het tabblad Diversen configureren. Om de installatie en configuratie te voltooien, moet het apparaat toegang tot internet hebben.



PFSense GUI - Proxy-configuratie

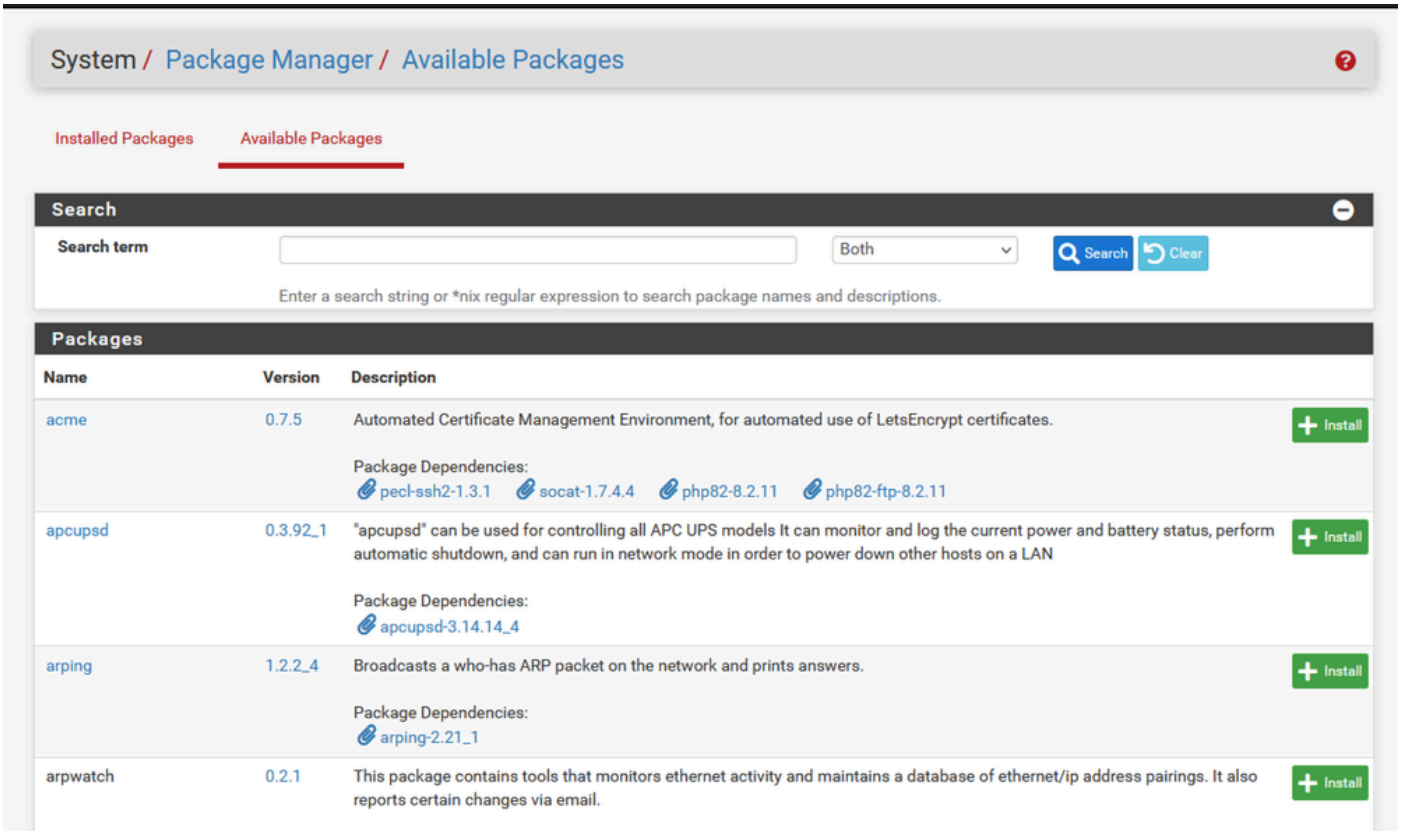
Opmerking: Zorg ervoor dat u de knop Opslaan selecteert nadat u de wijzigingen hebt aangebracht.

Vereiste pakketten toevoegen

Stap 1. Selecteer Systeem > Packet Manager

Stap 2. Beschikbare pakketten selecteren

Opmerking: het kan een paar minuten duren om alle beschikbare pakketten te laden. Als dit keer uit, verifieer dat de DNS servers correct worden gevormd. Vaak verhelpt een herstart van het apparaat de internetverbinding.



PFSense GUI - pakketlijst

Stap 3. Vereiste pakketten zoeken en installeren

1. proxy
2. Open-VM-tools

✎ Opmerking: selecteer het haproxy-devel pakket niet.

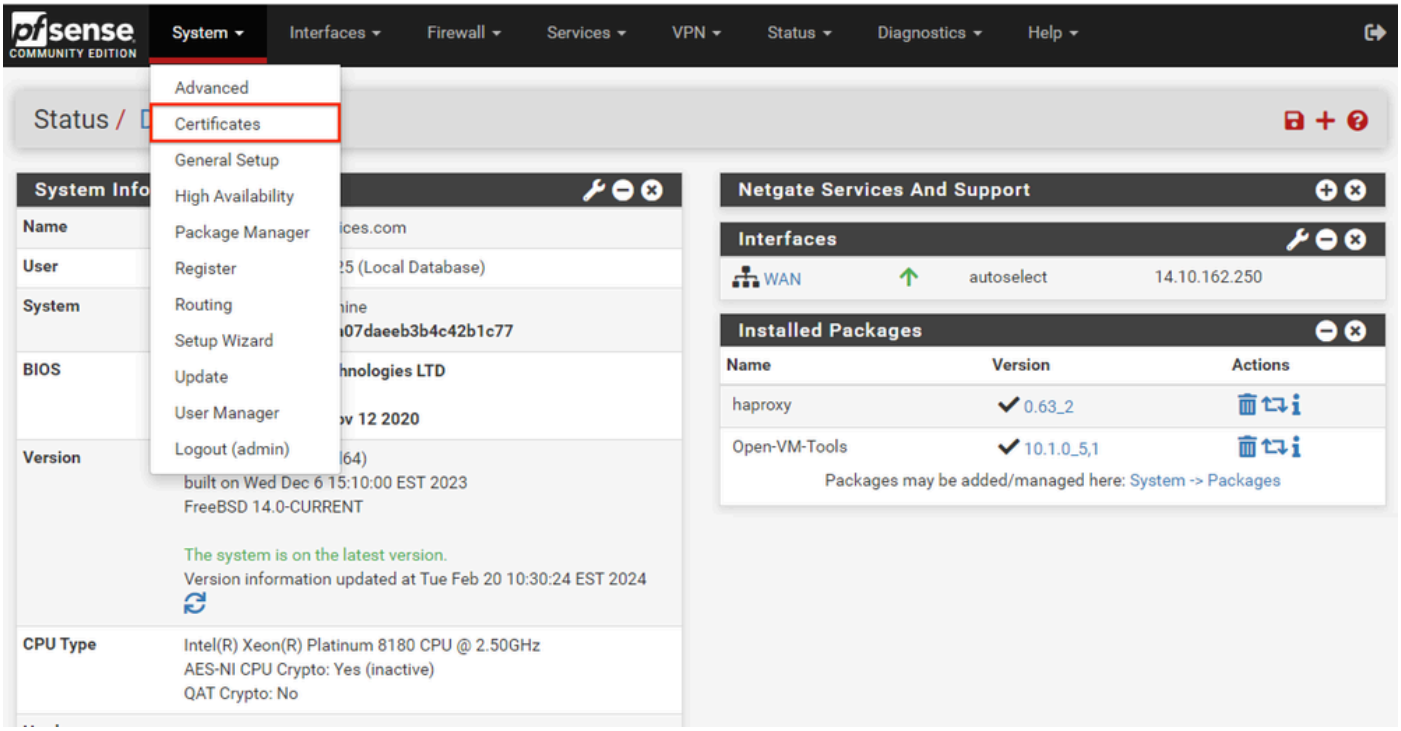
Certificaten configureren

pfSense kan zelfondertekend certificaat maken of het kan integreren met een openbare CA, een interne CA, of kan optreden als een CA en CA-ondertekende certificaten uitgeven. Deze handleiding bevat de stappen die u kunt integreren met een interne CA.

Zorg ervoor dat deze items beschikbaar zijn voordat u met deze sectie begint.

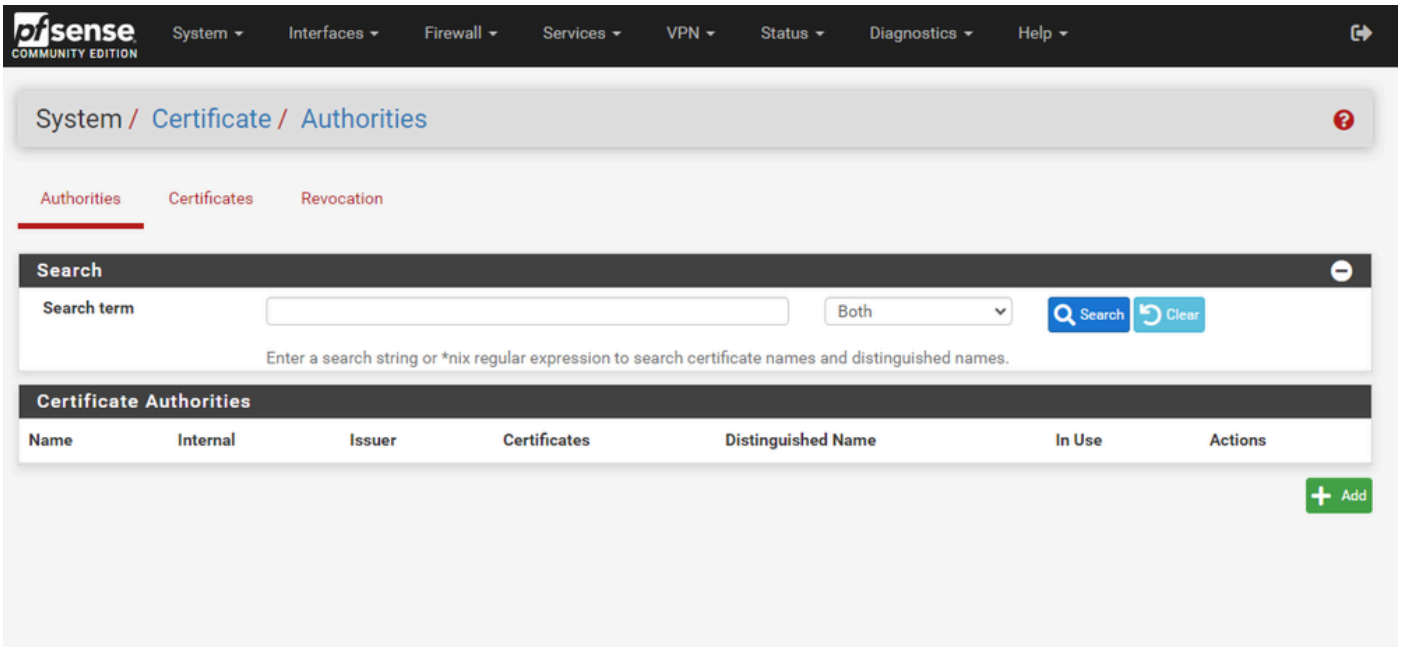
1. basiscertificaat voor CA opgeslagen als PEM- of Base-64-gecodeerd formaat.
2. Alle intermediaire (soms afgevende) certificaten voor CA die zijn opgeslagen als een PEM- of Base-64-gecodeerd formaat

Stap 1. Selecteer Certificaten in het vervolgkeuzemenu Systeem



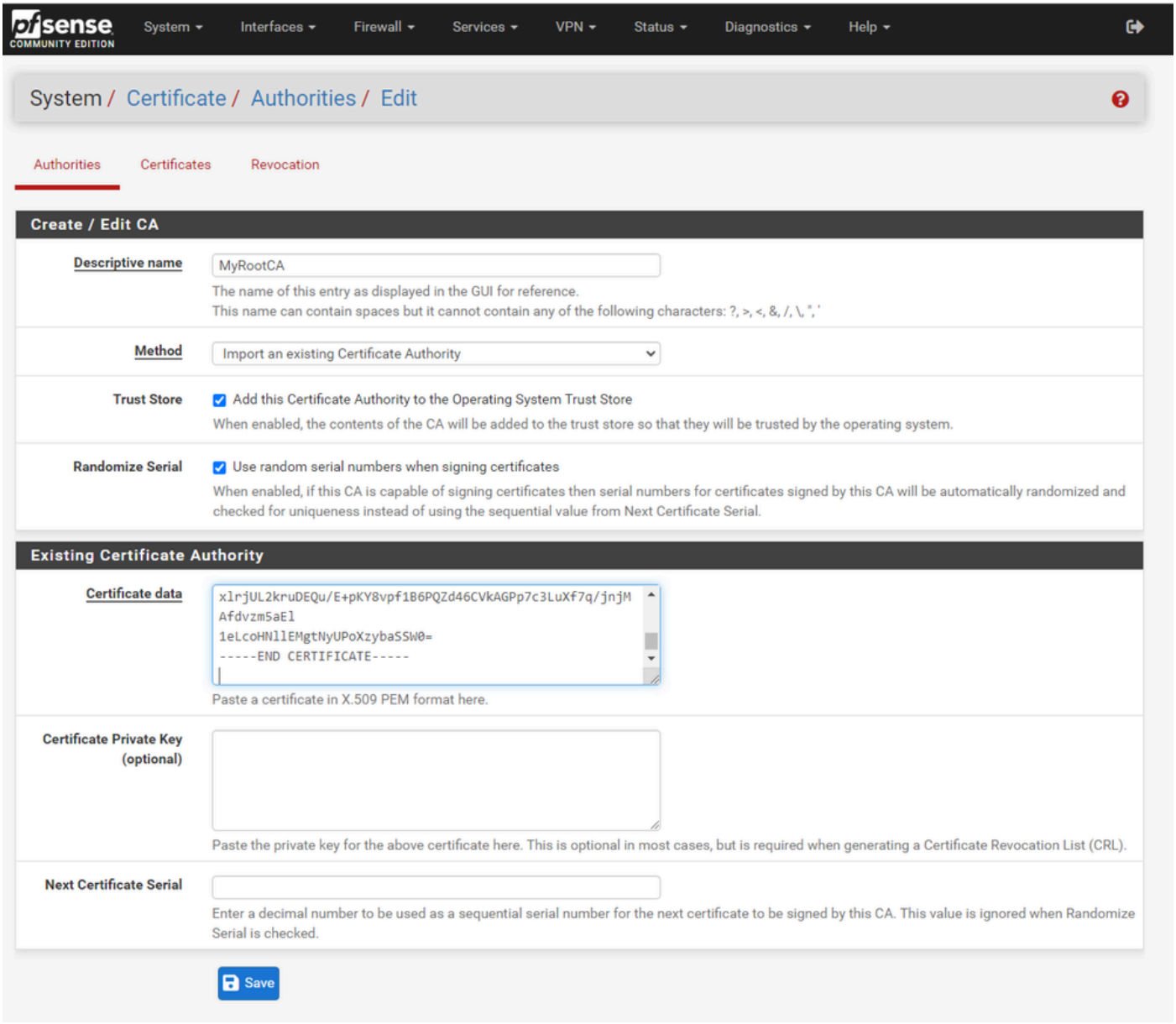
PfSense GUI - vervolgkeuzelijst Certificaten

Stap 2. Het CA Root Certificate importeren



SFSense GUI - CA-certificaatlijst

Selecteer de knop Toevoegen.



PFSense GUI - CA-import

Zoals in het beeld:

1. Verstrek een unieke, beschrijvende naam

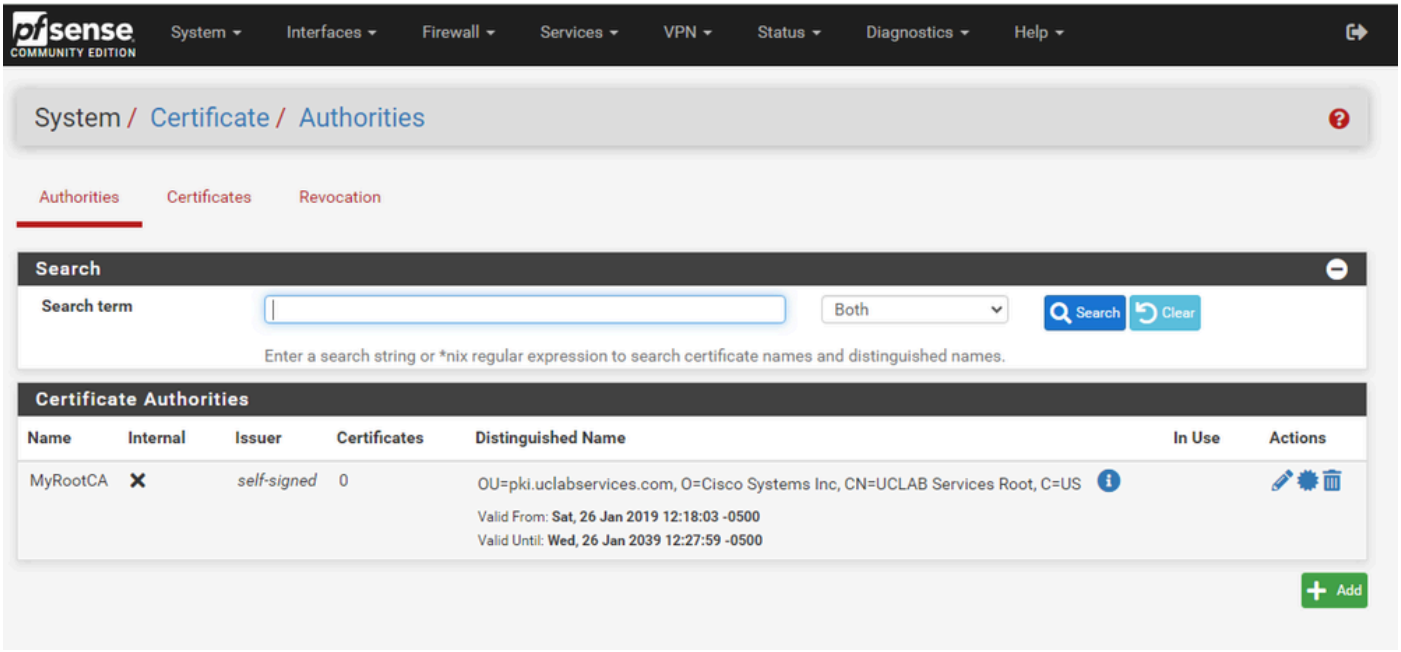
2. Selecteer Importeren van een bestaande certificeringsinstantie in de vervolgkeuzelijst Methode.

3. Controleer of de selectievakjes Trust Store en Randomize Serial zijn geselecteerd.

4. Plakt het gehele certificaat in het tekstvak Certificaatgegevens. Zorg ervoor dat u van de -----BEGIN CERTIFICAAT----- en -----END CERTIFICAAT----- lijnen omvat.

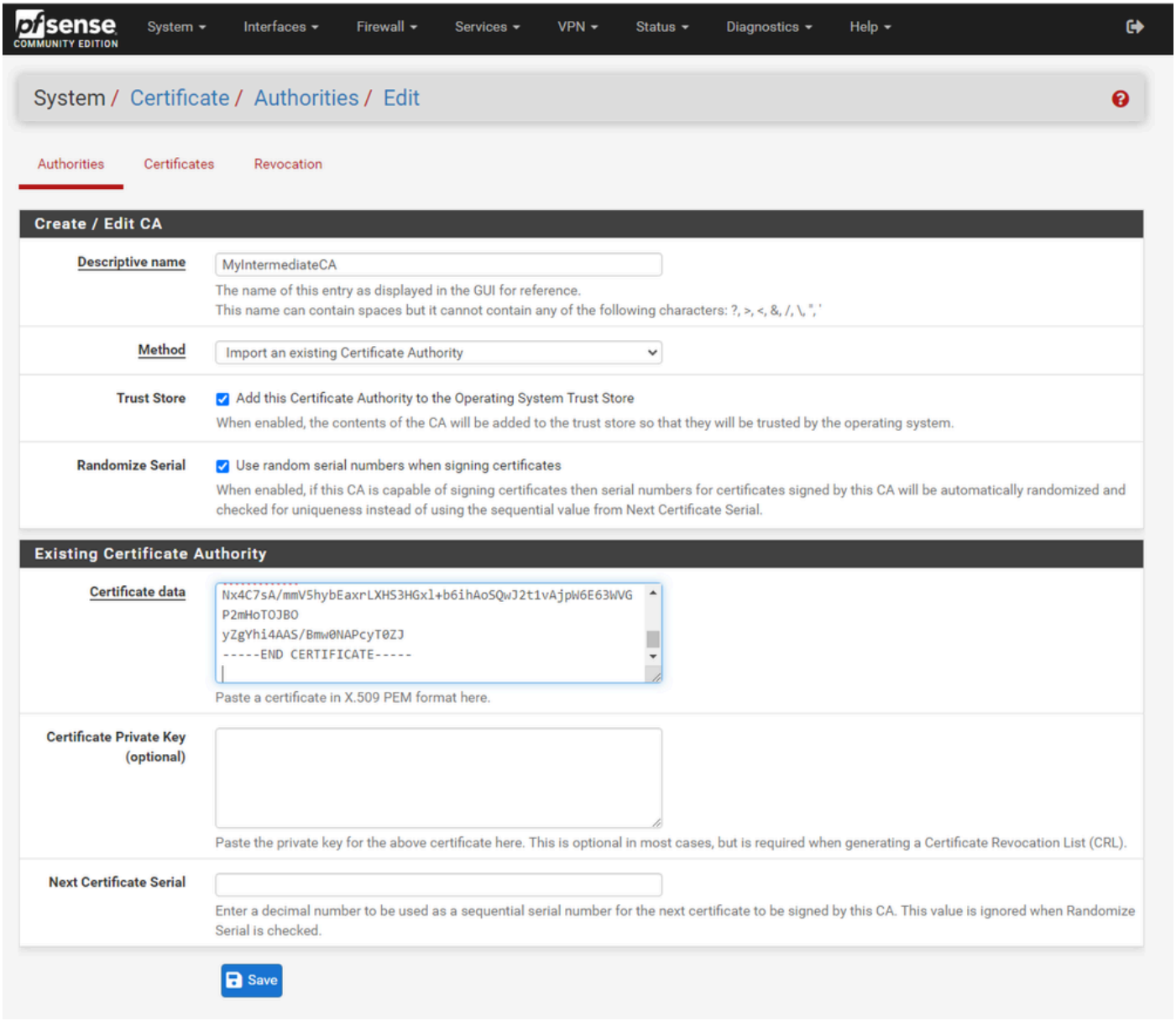
5. Selecteer Opslaan.

6. Controleer dat het certificaat wordt geïmporteerd zoals in de afbeelding.



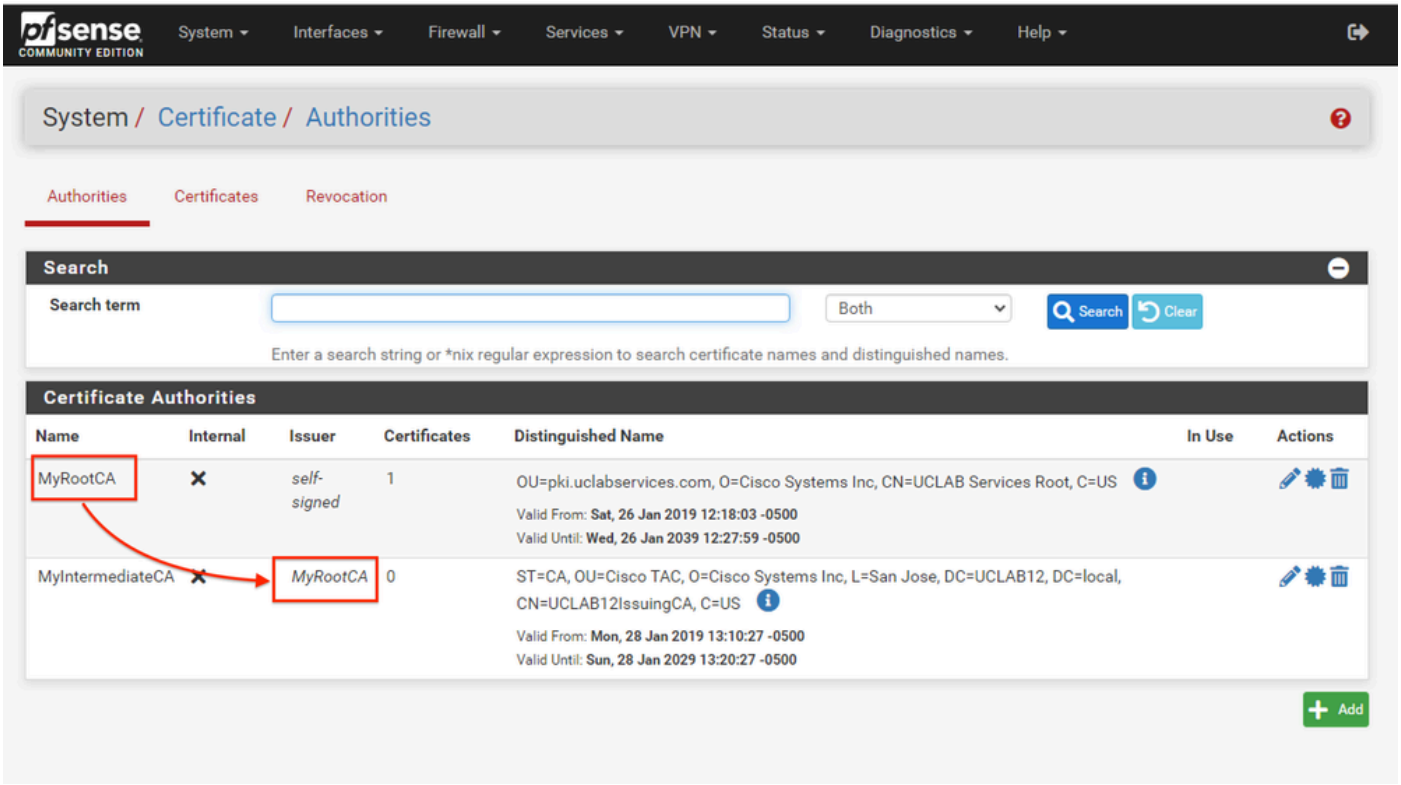
RFSense GUI - CA-lijst

Stap 3. Het CA-tussencertificaat importeren



SFSense GUI - CA tussenproducten importeren

Herhaal de stappen om het basis CA certificaat te importeren om het tussenliggende CA certificaat te importeren.



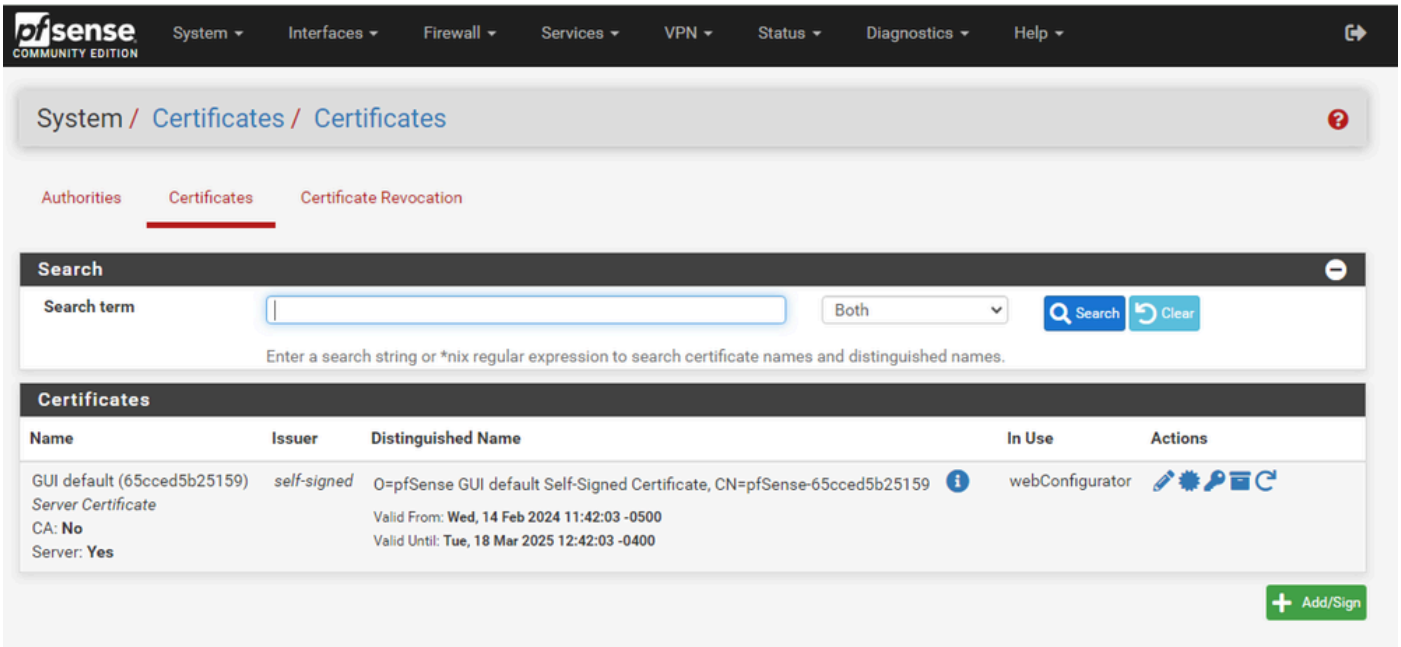
RFSense GUI - CA-links

Controleer de certificeringsinstanties om te controleren of het tussenproduct correct is gekoppeld aan het basiscertificaat zoals wordt aangegeven in de afbeelding.

Stap 4. Maak en exporteer een CSR voor de website met taakverdeling

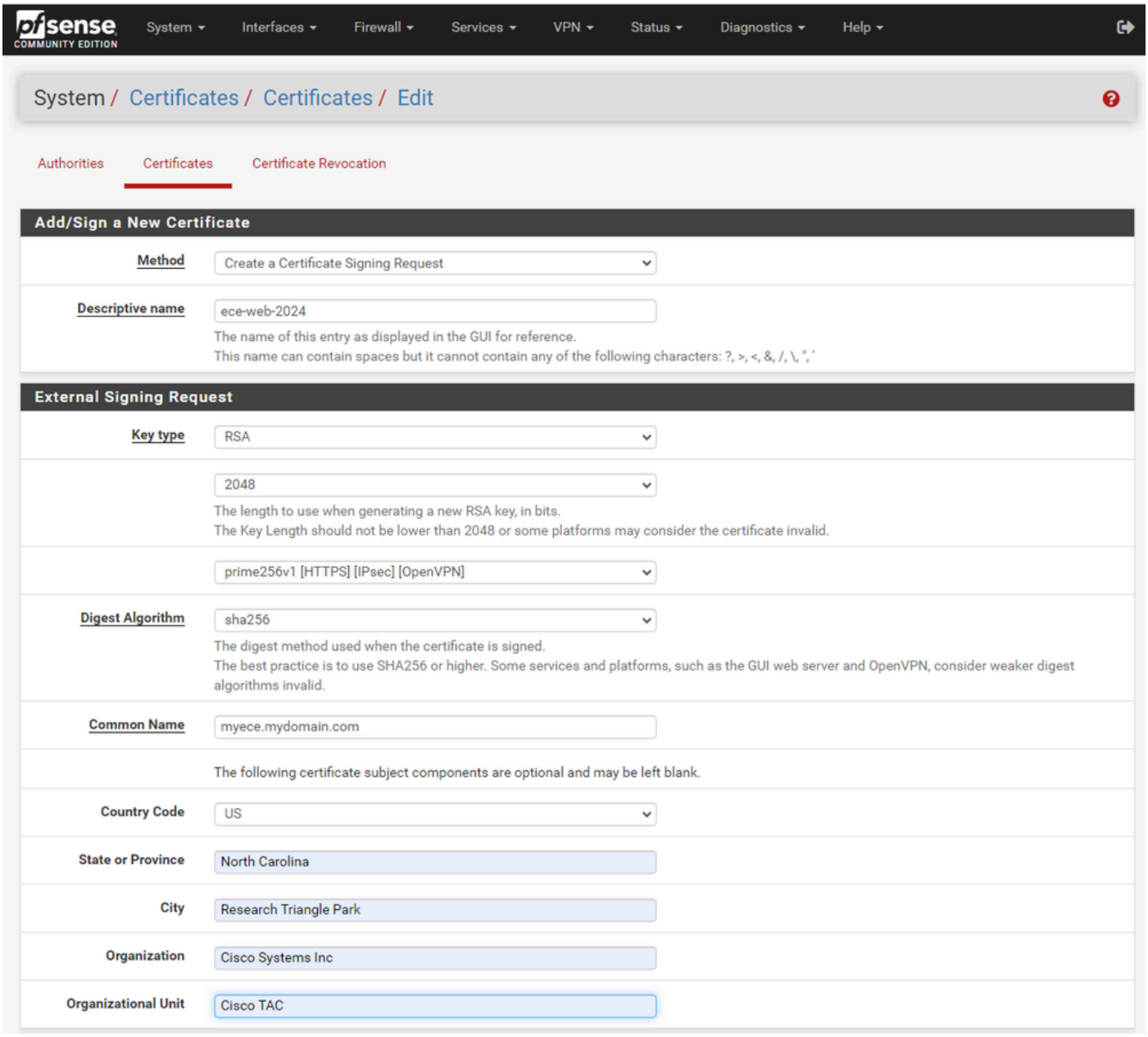
Dit beschrijft de stappen om een MVO te creëren, MVO uit te voeren, dan het ondertekende certificaat in te voeren. Als u al een bestaand certificaat in een PFX-indeling hebt, kunt u dit certificaat importeren. Raadpleeg de documentatie bij pfSense voor deze stappen.

1. Selecteer het menu Certificaten en selecteer vervolgens de knop Toevoegen/ondertekenen.



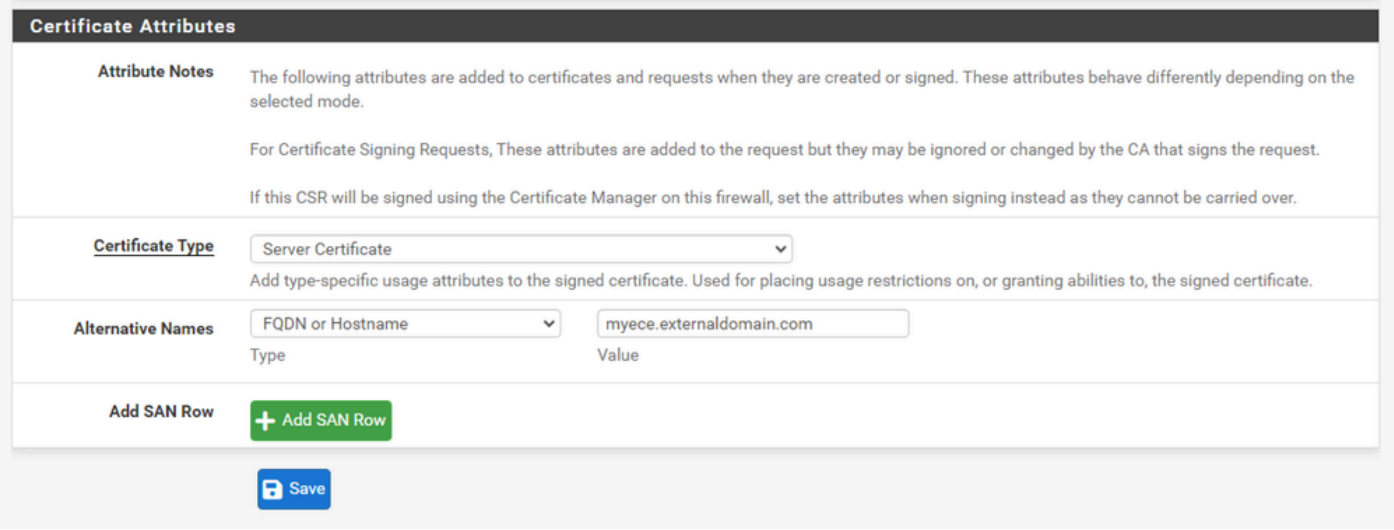
PfSense GUI - certificaatlijst

2. Vul het aanvraagformulier voor de ondertekening van het certificaat in.



PFSense GUI - CRS-creatie

- Methode: Selecteer Aanvraag voor certificaatondertekening maken in de vervolgkeuzelijst
- Beschrijvende naam: geef een naam voor het certificaat
- Key type en Digest Algoritme: Controleer of ze overeenkomen met uw vereisten
- Veelvoorkomende naam: Geef de volledig gekwalificeerde domeinnaam website
- Geef de resterende certificaatinformatie zoals vereist voor uw omgeving



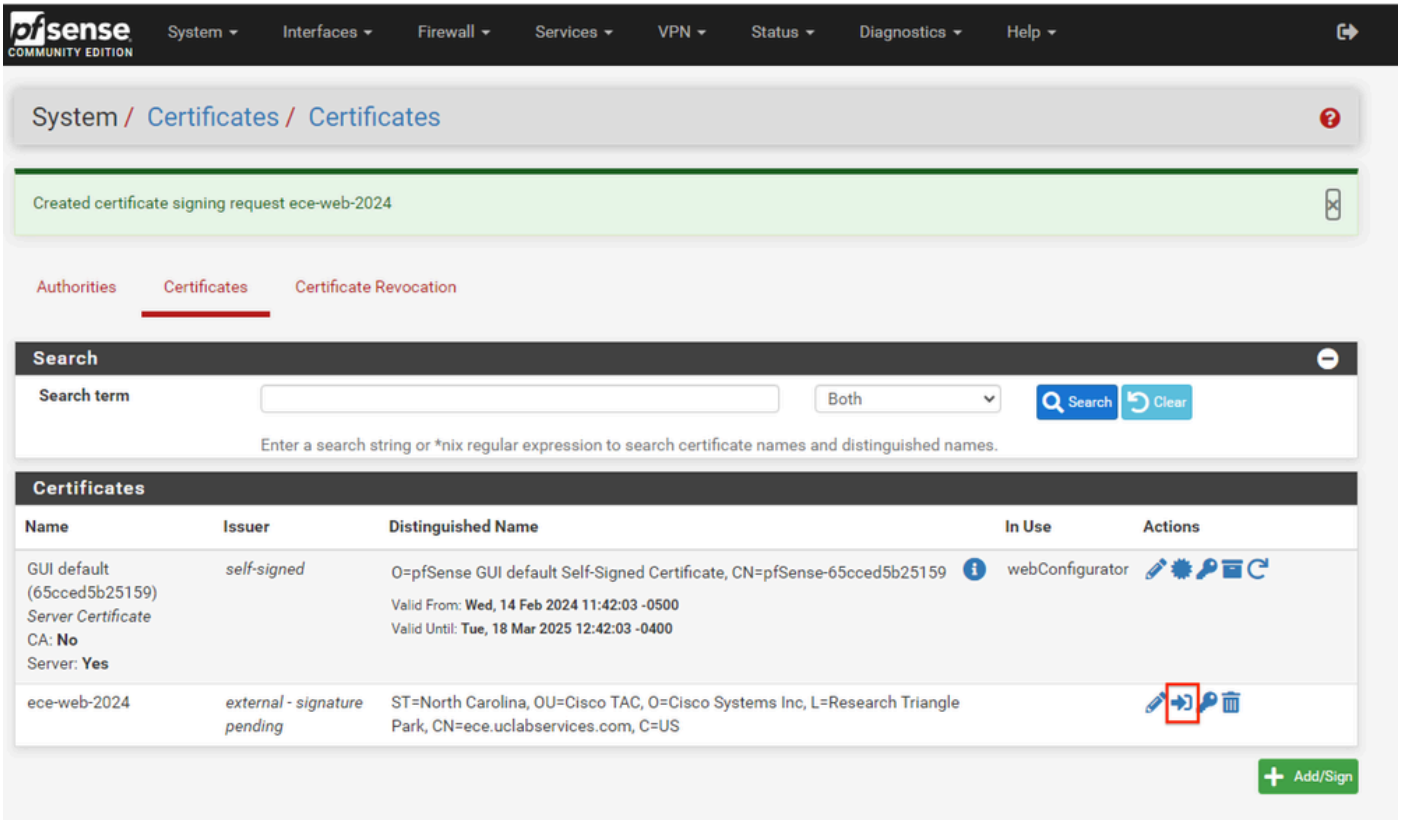
PFSense GUI - CSR geavanceerde security

- Certificaattype: Selecteer Servercertificaat in de vervolgkeuzelijst.
- Alternatieve namen: Geef elk onderwerp alternatieve namen (SAN) die nodig zijn voor uw implementatie.

Opmerking: de algemene naam wordt automatisch toegevoegd aan het SAN-veld. U hoeft alleen extra namen toe te voegen.

Selecteer Opslaan als alle velden juist zijn.

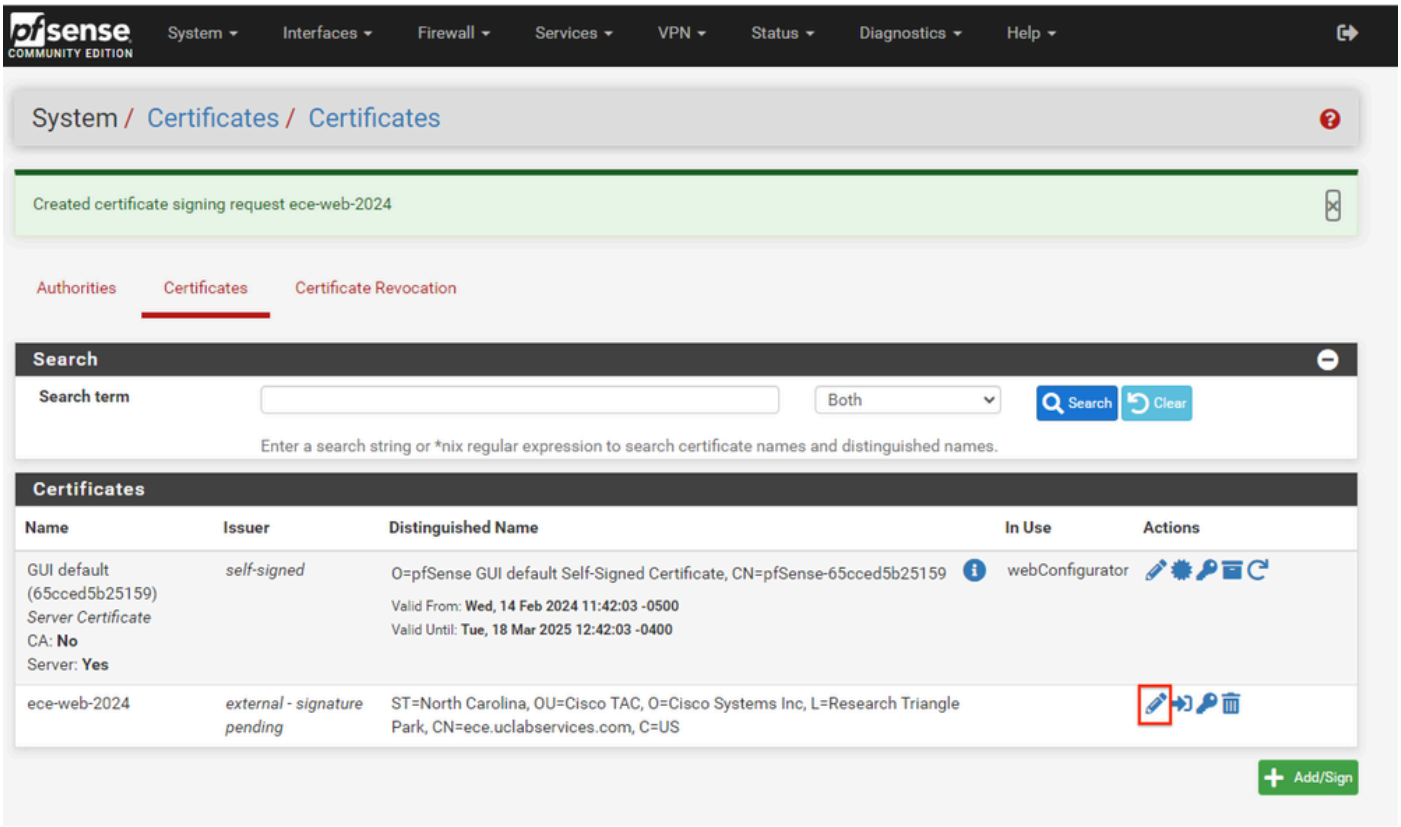
3. Exporteer de MVO naar een bestand.



PFSense GUI - CSR-export

Selecteer de knop Exporteren om de CSR op te slaan en onderteken dit vervolgens met uw CA. Zodra u het ondertekende certificaat hebt, slaat u dit op als een PEM- of Base-64-bestand om het proces te voltooien.

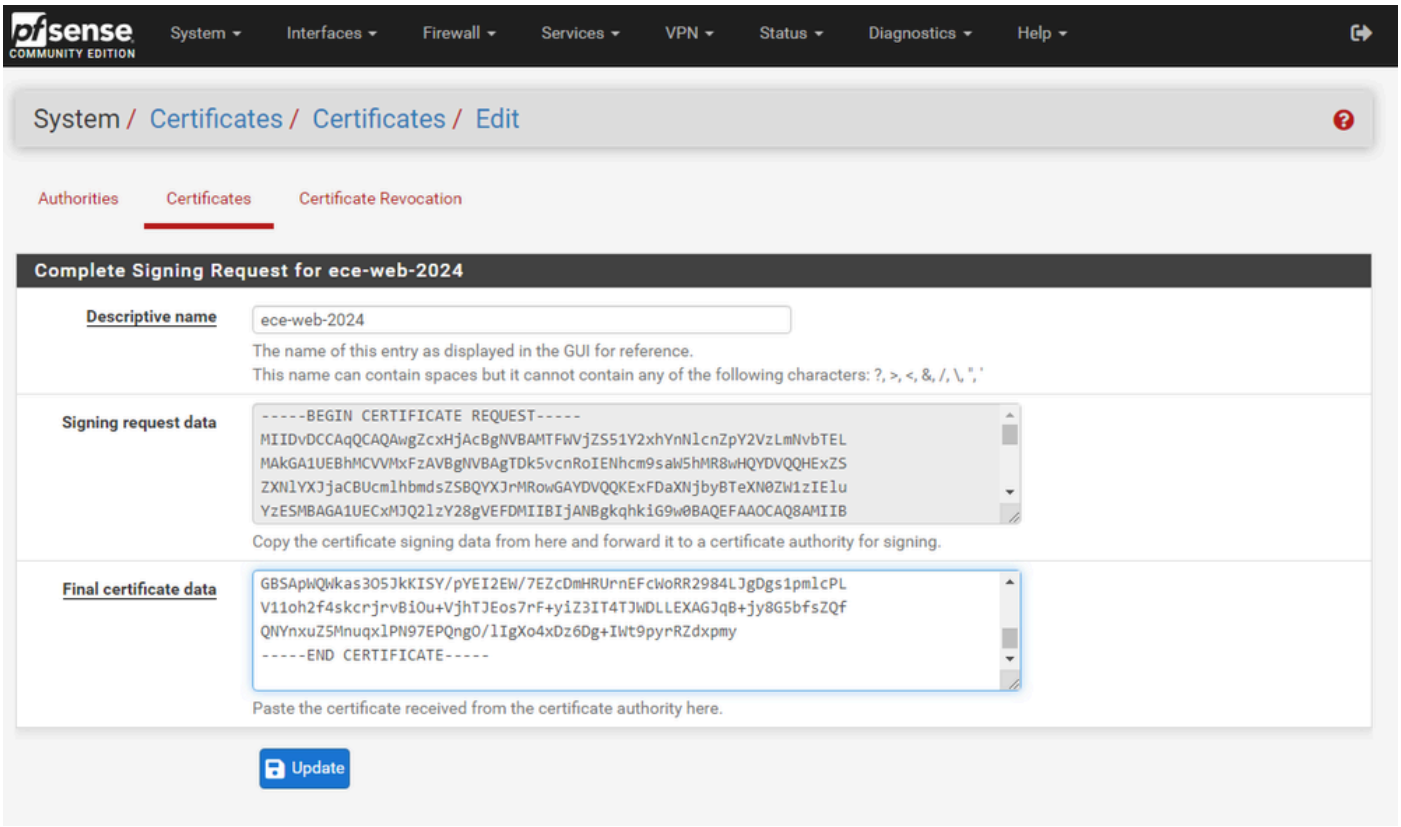
4. Voer het ondertekende certificaat in.



SFSense GUI - Certificaat importeren

Selecteer het pictogram Potlood om het ondertekende certificaat te importeren.

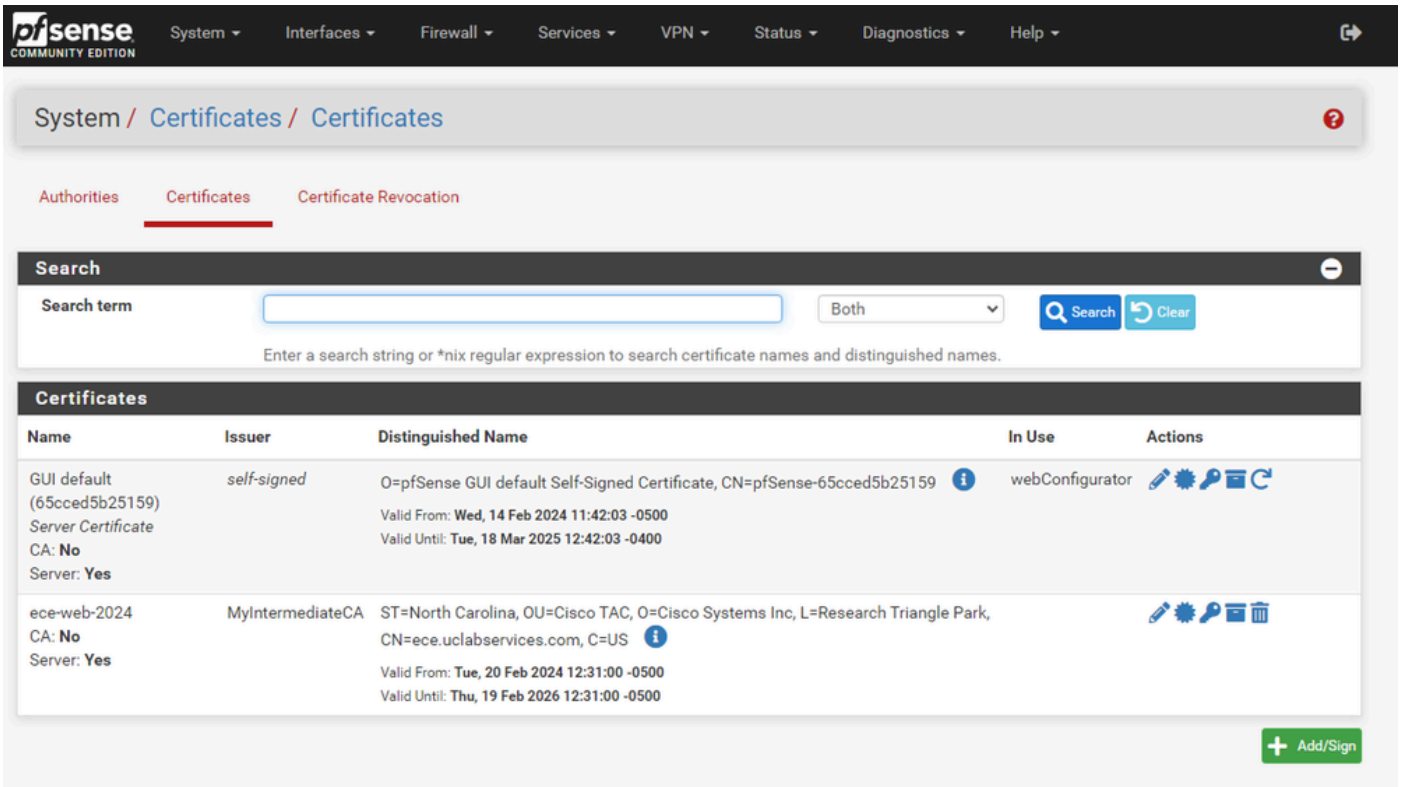
5. Plakt de certificaatgegevens in het formulier.



SFSense GUI - Certificaat importeren

Selecteer Bijwerken om het certificaat op te slaan.

6. Bekijk de certificaatgegevens om te controleren of deze correct zijn.



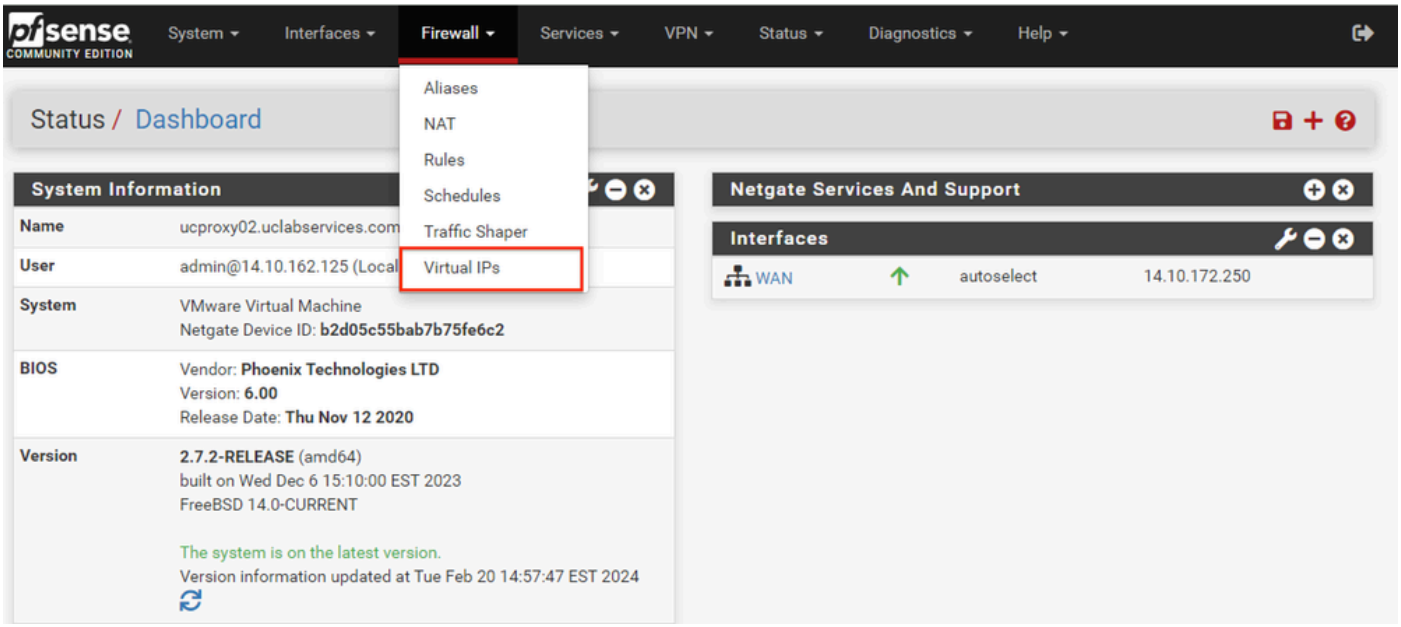
PfSense GUI - certificaatlijst

7. Herhaal dit proces als u meerdere sites op deze pcSense wilt hosten.

Virtuele IP’s toevoegen

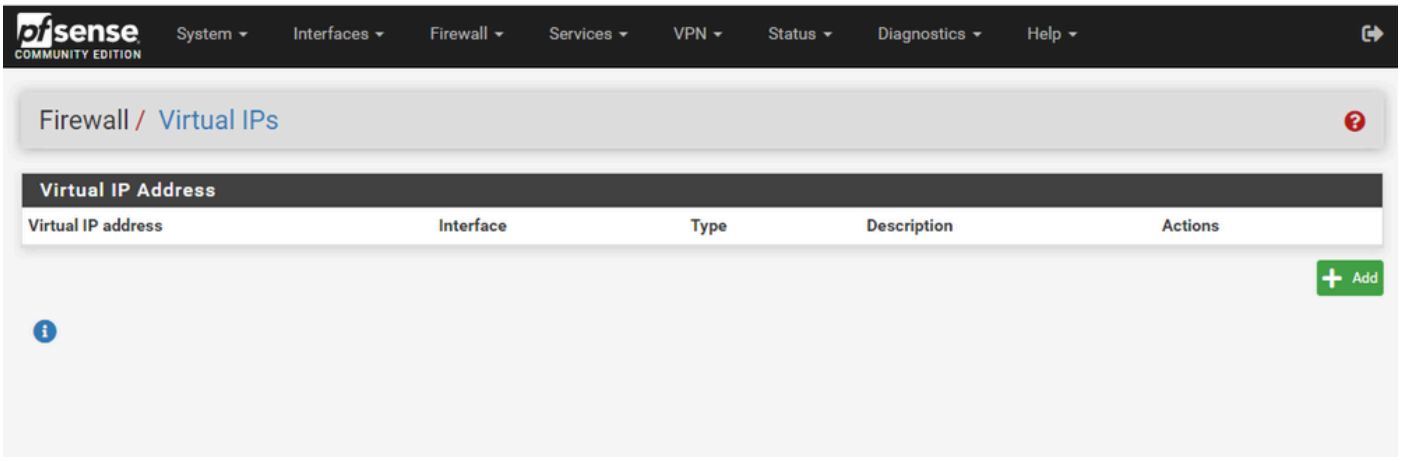
Minstens één IP is vereist om websites op de pfSense te hosten. In pfSense gebeurt dit met virtuele IP's (VIP's).

Stap 1. Selecteer virtuele IP's in de vervolgkeuzelijst Firewall



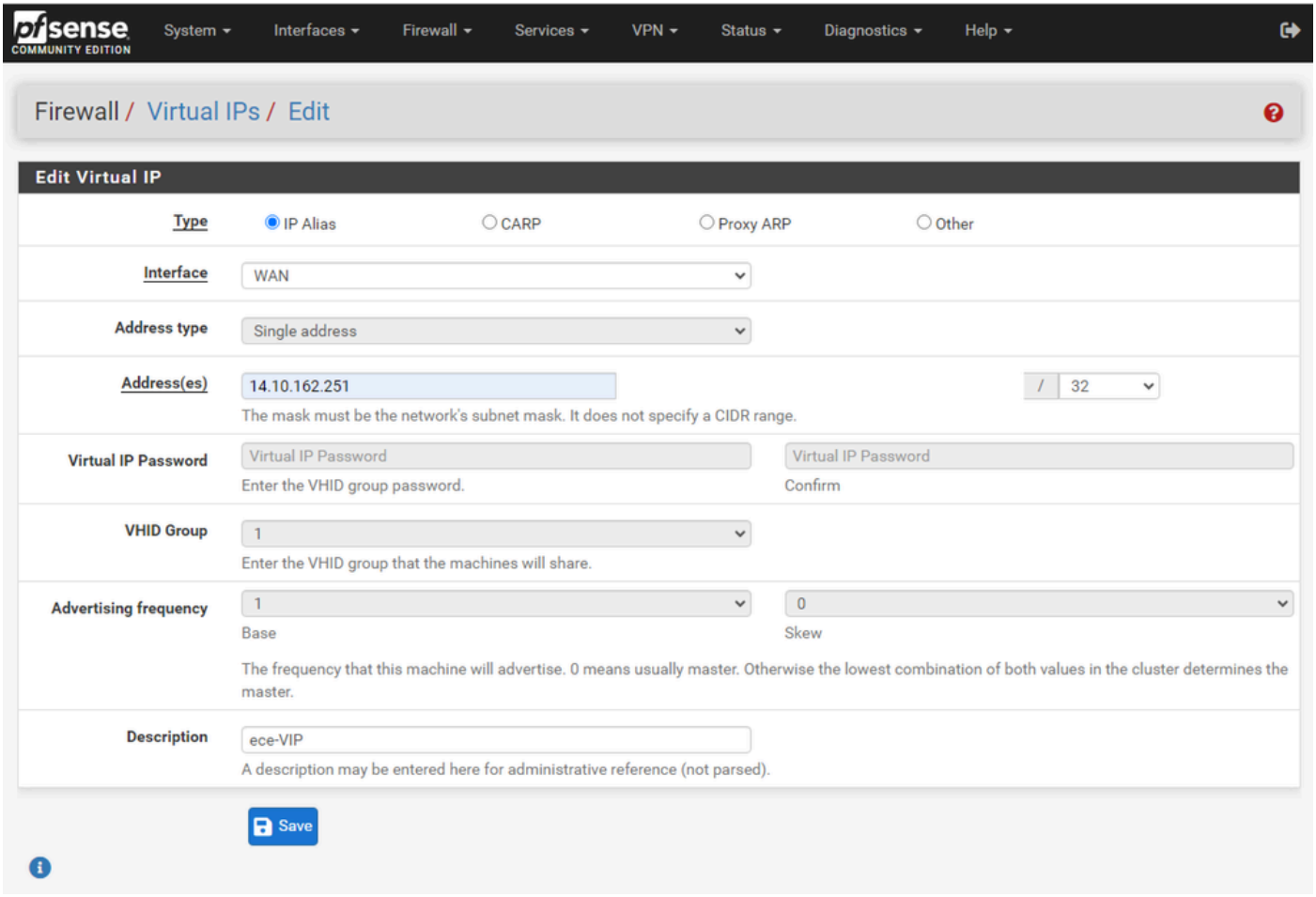
PfSense GUI - VIP-drop-down

Stap 2. Selecteer de knop Toevoegen



PfSense GUI - VIP-landingspagina

Stap 3. Adresinformatie opgeven



PFSense GUI - VIP-configuratie

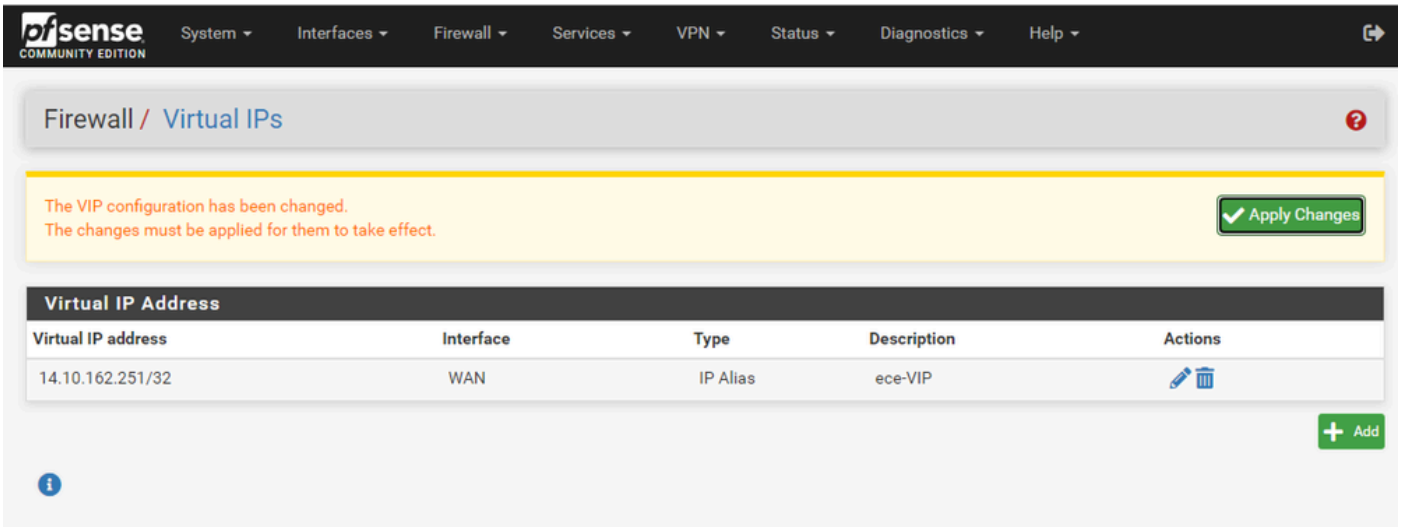
Gebruik de informatie om een VIP toe te voegen.

- Type: IP-alias selecteren
- Interface: Selecteer de interface voor dit IP-adres dat moet worden uitgezonden
- Adres(sen): IP-adres invoeren
- Adresmasker: voor IP-adressen die worden gebruikt voor taakverdeling, moet het masker een /32 zijn
- Beschrijving: Geef een korte tekst om de configuratie later beter te begrijpen

Selecteer Opslaan om de wijziging toe te voegen.

Herhaal dit voor elk IP-adres dat vereist is voor de configuratie.

Stap 4. Configuratie toepassen



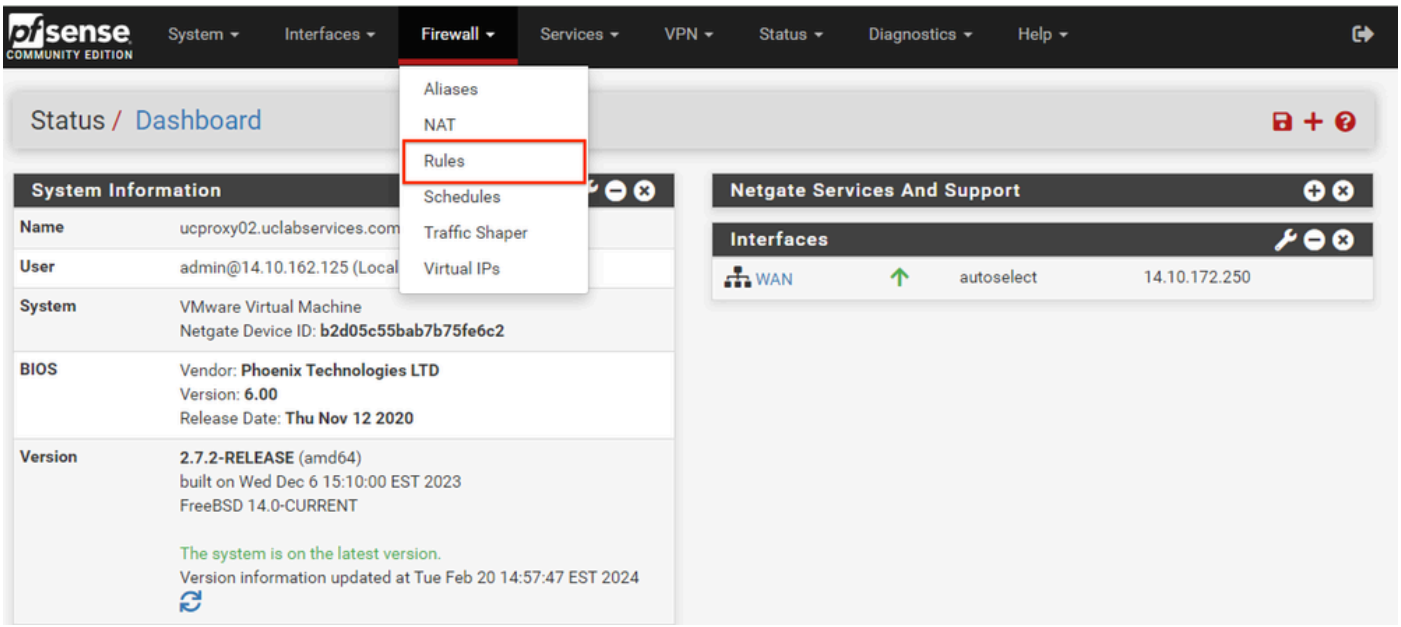
PfSense GUI - VIP-lijst

Selecteer de knop Wijzigingen toepassen nadat alle VIP's zijn toegevoegd.

Firewall configureren

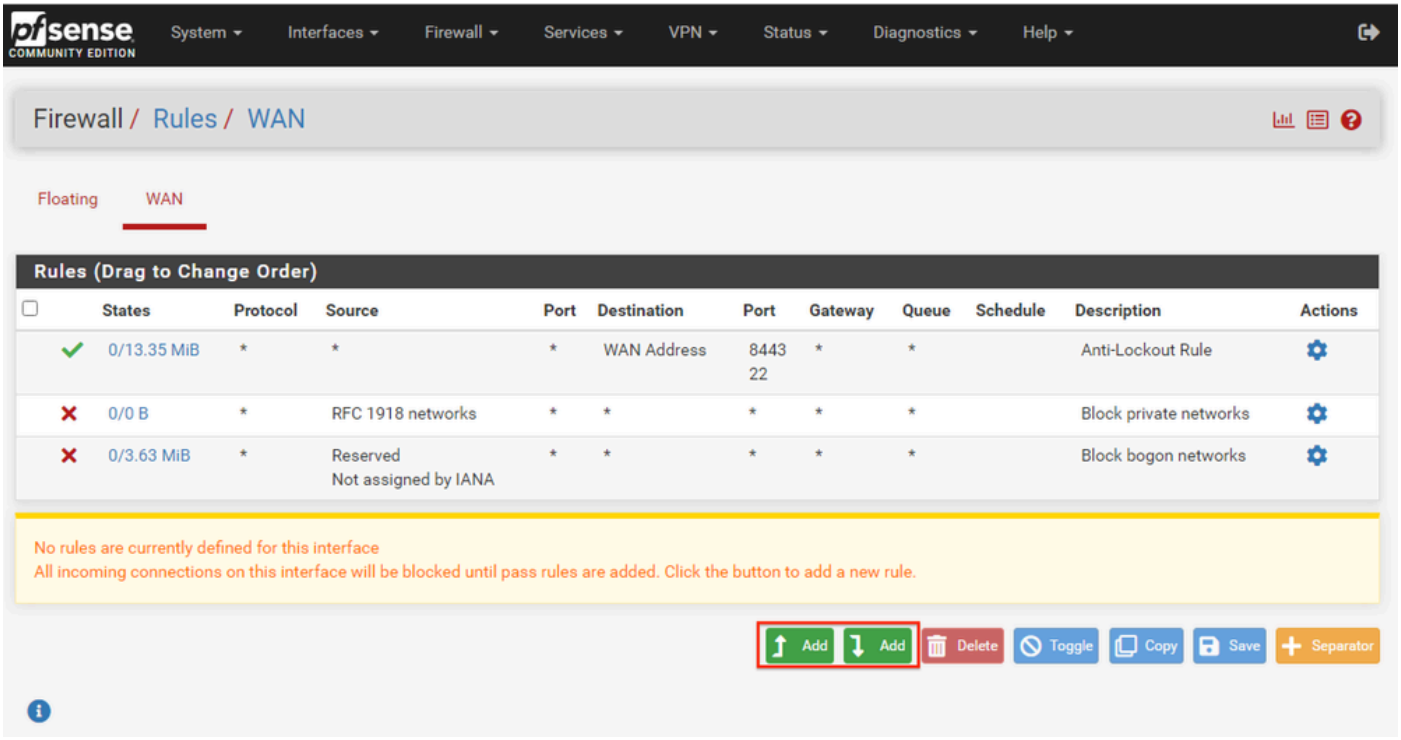
pfSense heeft een ingebouwde firewall. De standaardregel-set is zeer beperkt. Zorg ervoor dat u een uitgebreid firewallbeleid opstelt voordat het apparaat in productie wordt genomen.

Stap 1. Selecteer Regels in de vervolgkeuzelijst Firewall



RFSense GUI - vervolgkeuzelijst met firewallregels

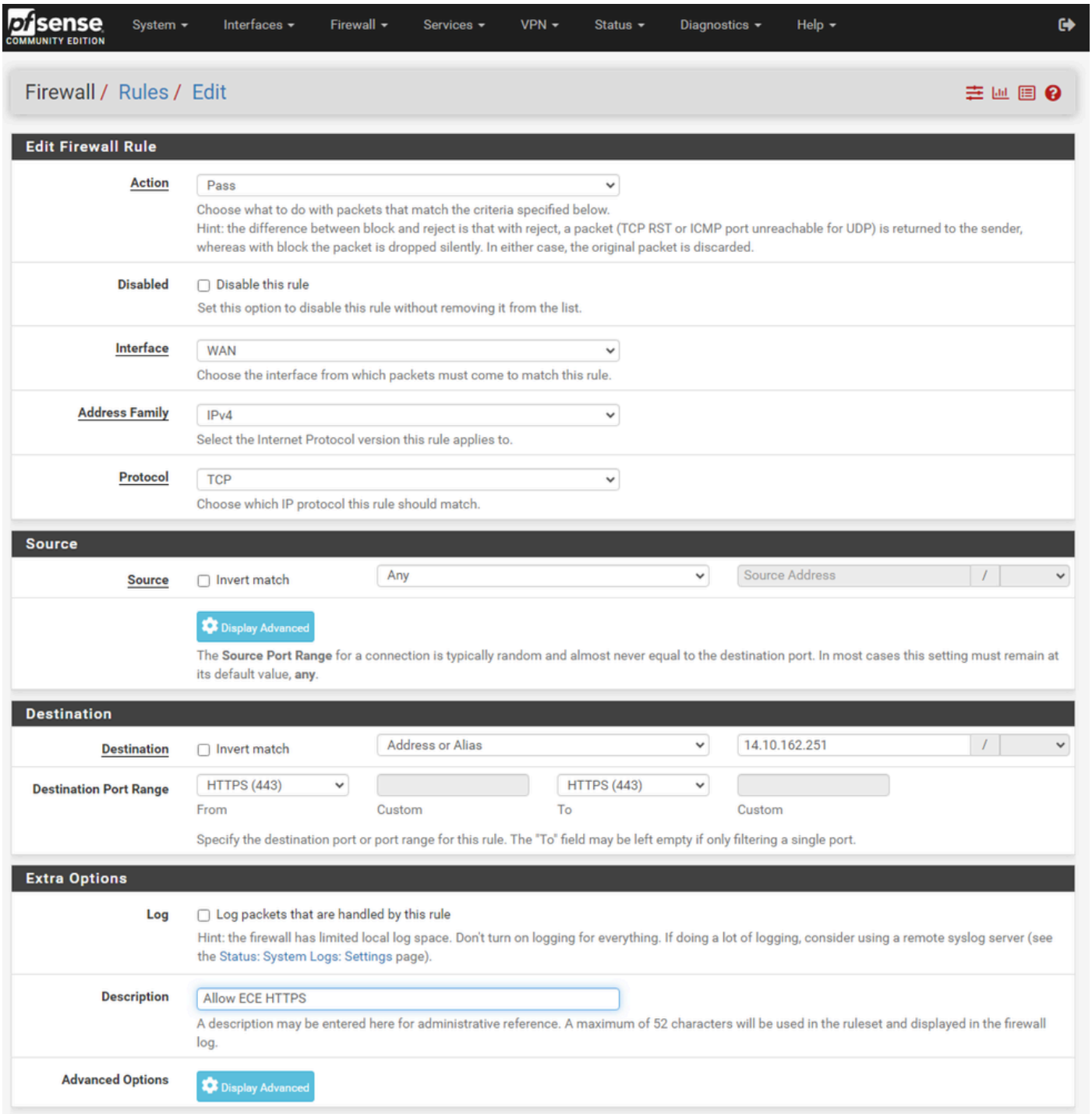
Stap 2. Selecteer een van de knoppen Toevoegen



RFSense GUI - lijst met firewallregels

Merk op dat de ene knop de nieuwe regel boven de geselecteerde regel toevoegt, terwijl de andere knop de regel onder de geselecteerde regel toevoegt. Beide knoppen kunnen voor de eerste regel worden gebruikt.

Stap 3. Firewallregel maken om verkeer toe te staan naar poort 443 voor het IP-adres



Configuratie van PFSense GUI - Firewall Pass-regel

Gebruik de informatie om de regel te maken.

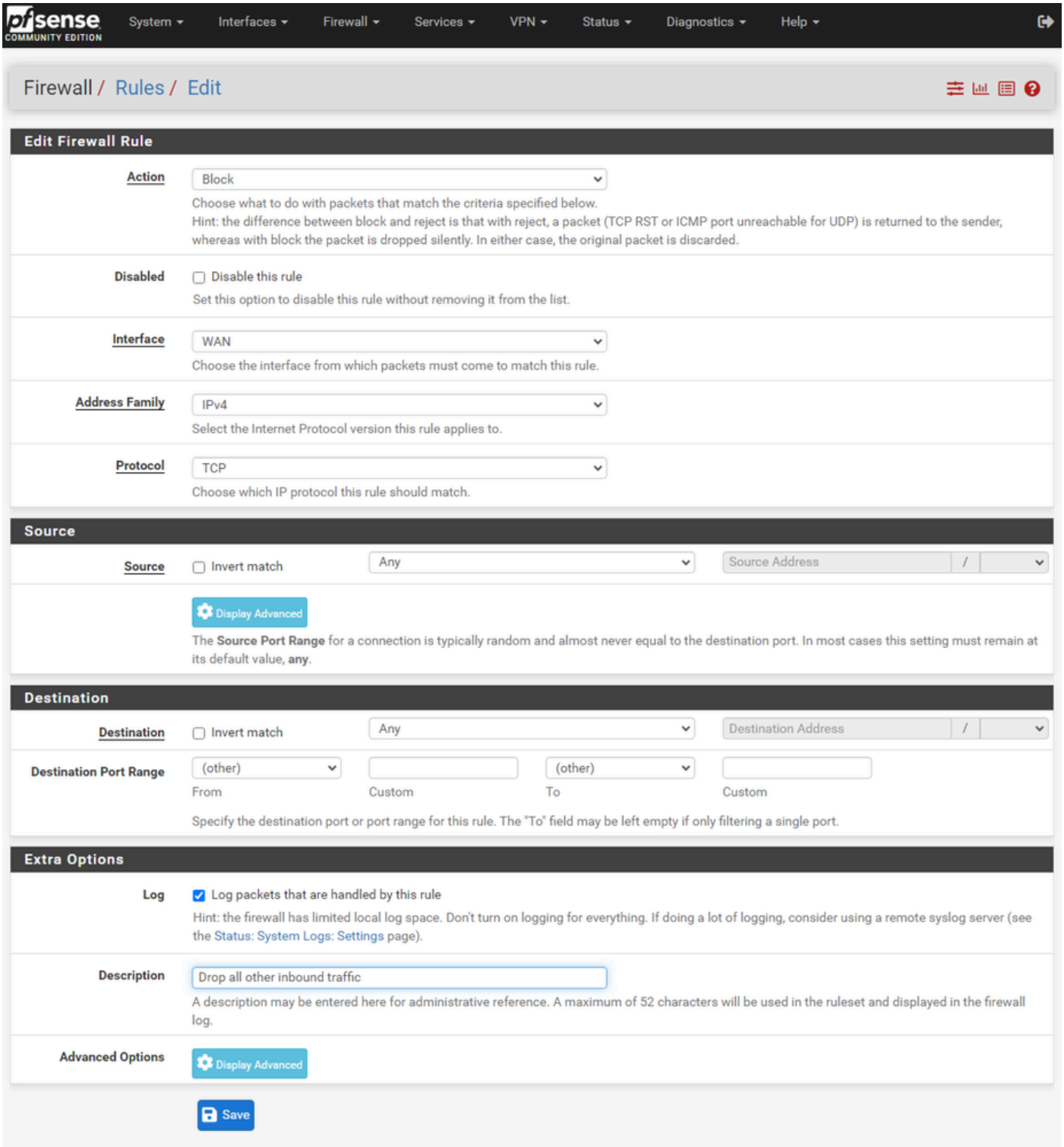
- Actie: kies Pass
- Interface: Kies de interface waarop de regel van toepassing is
- Adresfamilie en -protocol: kies de gewenste keuze
- Bron: Laat geselecteerd als Any
- Bestemming: Selecteer Adres of Alias uit de vervolgkeuzelijst Bestemming en voer vervolgens het IP-adres in waarop de regel van toepassing is
- Poortbereik bestemming: Selecteer HTTPS (443) in de vervolgkeuzelijst Van en Tot
- Log: Selecteer het aanvinkvakje om alle pakketten te registreren die aan deze regel voor accounting voldoen

- Beschrijving: Geef tekst om later naar de regel te verwijzen

Selecteer Opslaan.

Stap 4. Maak een firewallregel om al het andere verkeer naar de pfSense te laten vallen

Selecteer de knop Toevoegen om de regel onder de nieuwe regel in te voegen.



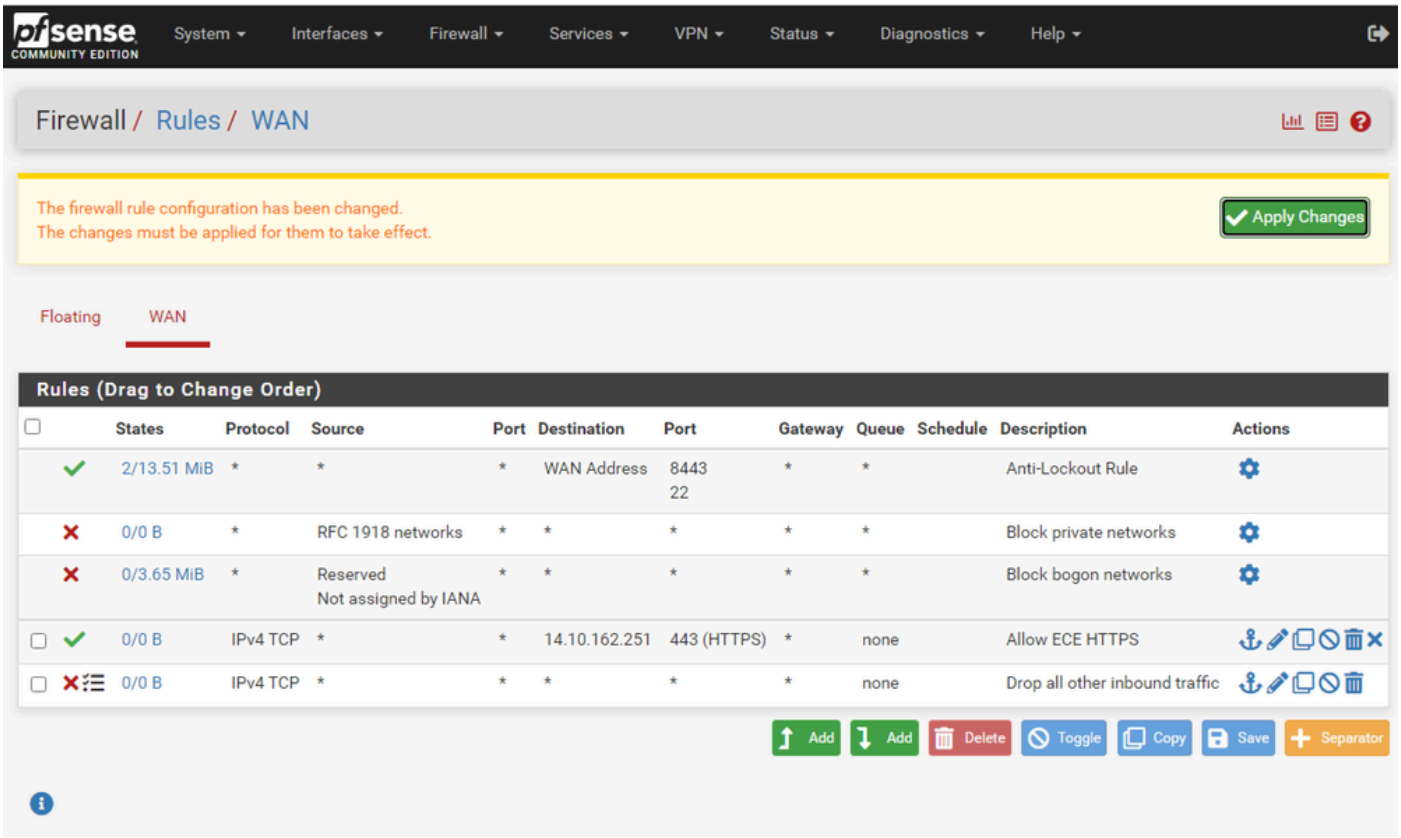
SFSense GUI - configuratie van drop-regels voor firewall

- Actie: Blok selecteren

- Interface: Kies de interface waarop de regel van toepassing is
- Adresfamilie en -protocol: kies de gewenste keuze
- Bron: Laat geselecteerd als Any
- Bestemming: als zodanig geselecteerd
- Log: Selecteer het aanvinkvakje om alle pakketten te registreren die aan deze regel voor accounting voldoen
- Beschrijving: Geef tekst om later naar de regel te verwijzen

Selecteer Opslaan.

Stap 5. Herzie de regels en zorg ervoor dat de blokregel onderaan is



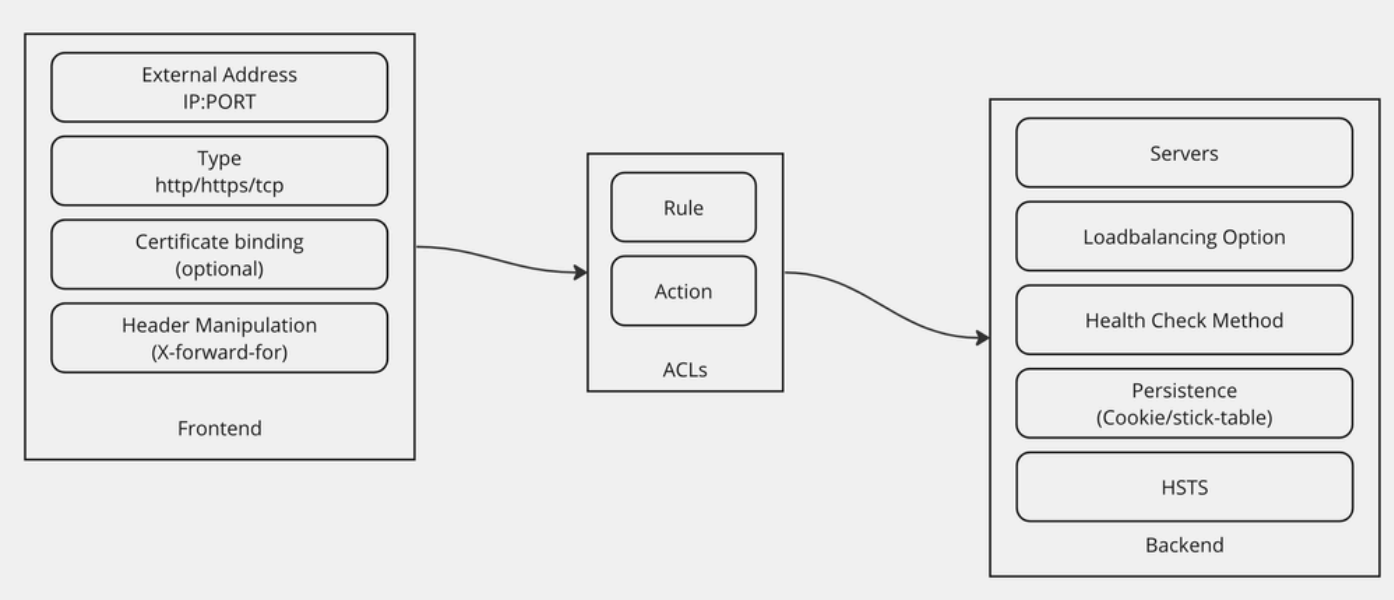
RFSense GUI - lijst met firewallregels

Indien nodig sleept u de regels om ze te sorteren.

Selecteer Wijzigingen toepassen als de firewallregels in de gewenste volgorde zijn geplaatst.

HAProxy configureren

HAProxy-concepten



HAProxy-concepten

HAProxy wordt geïmplementeerd met een Frontend/Backend-model.

Het Frontend definieert de kant van de proxy waarmee klanten communiceren.

Het Frontend bestaat uit een IP en poortcombinatie, certificaatbinding en kan enige headermanipulatie implementeren.

De Backend definieert de kant van de proxy die communiceert met de fysieke webservers.

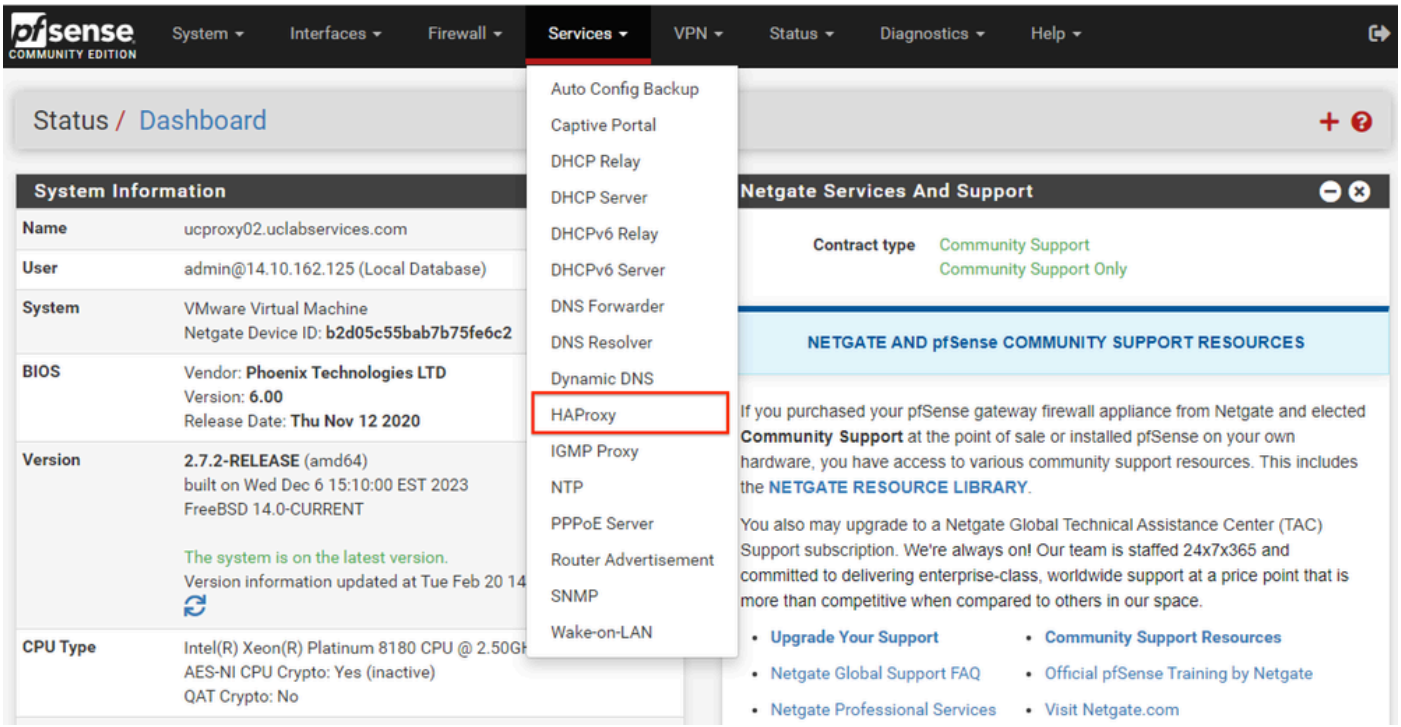
De Backend definieert de eigenlijke servers en poorten, de loadbalancing methode voor initiële toewijzing, gezondheidscontroles en persistentie.

Een Frontend weet met welke backend te communiceren door of een toegewijde backend of door ACLs te gebruiken.

ACL’s kunnen verschillende regels maken, zodat een gegeven frontend kan communiceren met verschillende backends, afhankelijk van verschillende dingen.

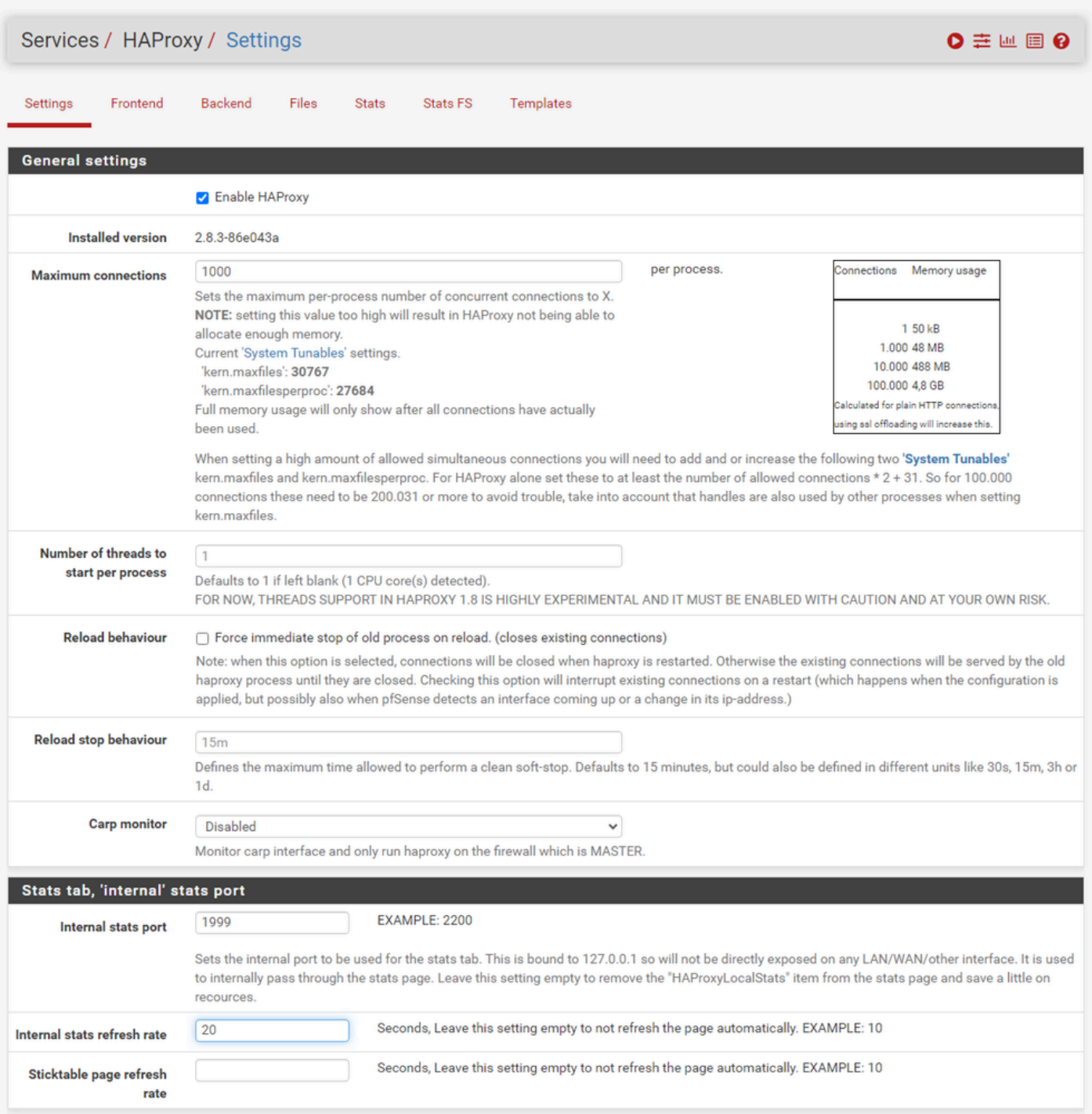
Eerste HAProxy-instellingen

Stap 1. Selecteer HAProxy in de vervolgkeuzelijst Services



PfSense GUI - HAProxy-vervolgkeuzelijst

Stap 2. Basisinstellingen configureren



PFSense GUI - HAProxy-hoofdinstellingen

Selecteer het aanvinkvakje Enable HAProxy.

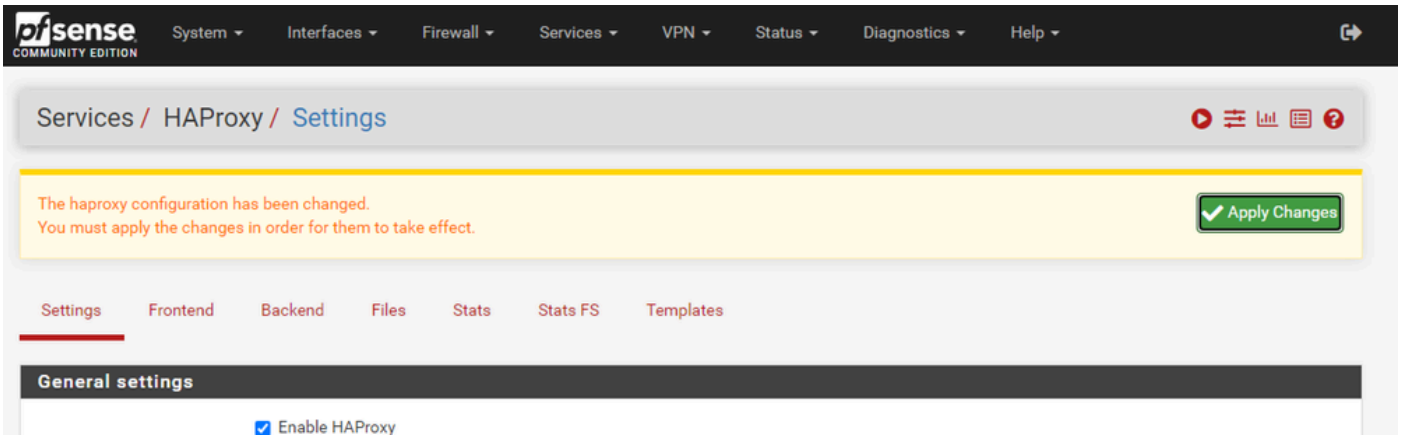
Voer een waarde in voor Maximum aantal verbindingen. Raadpleeg het diagram in deze sectie voor meer informatie over het benodigde geheugen.

Voer een waarde in voor de interne stats poort. Deze poort wordt gebruikt voor de weergave van HAProxy-statistieken van het apparaat, maar wordt niet buiten het apparaat weergegeven.

Voer een waarde in voor de verversingsfrequentie voor de interne status.

Bekijk de resterende configuratie en update zoals vereist voor uw omgeving.

Selecteer Opslaan.

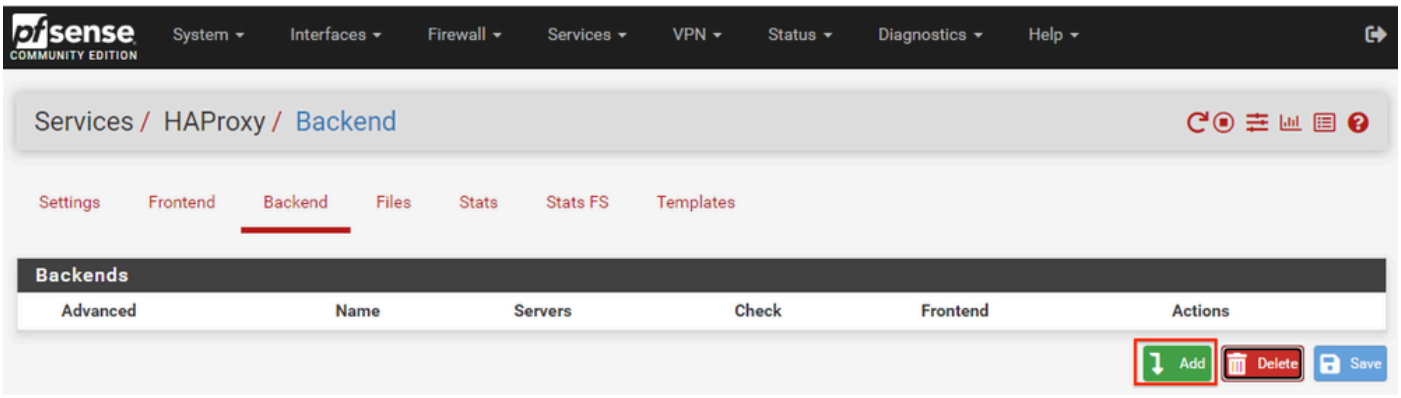


pfSense GUI - HAProxy Wijzigingen toepassen

Opmerking: de wijzigingen in de configuratie worden pas actief gemaakt als u de knop Wijzigingen toepassen selecteert. U kunt meerdere configuratiewijzigingen doorvoeren en ze allemaal tegelijk toepassen. De configuratie hoeft niet te worden toegepast om in een andere sectie te worden gebruikt.

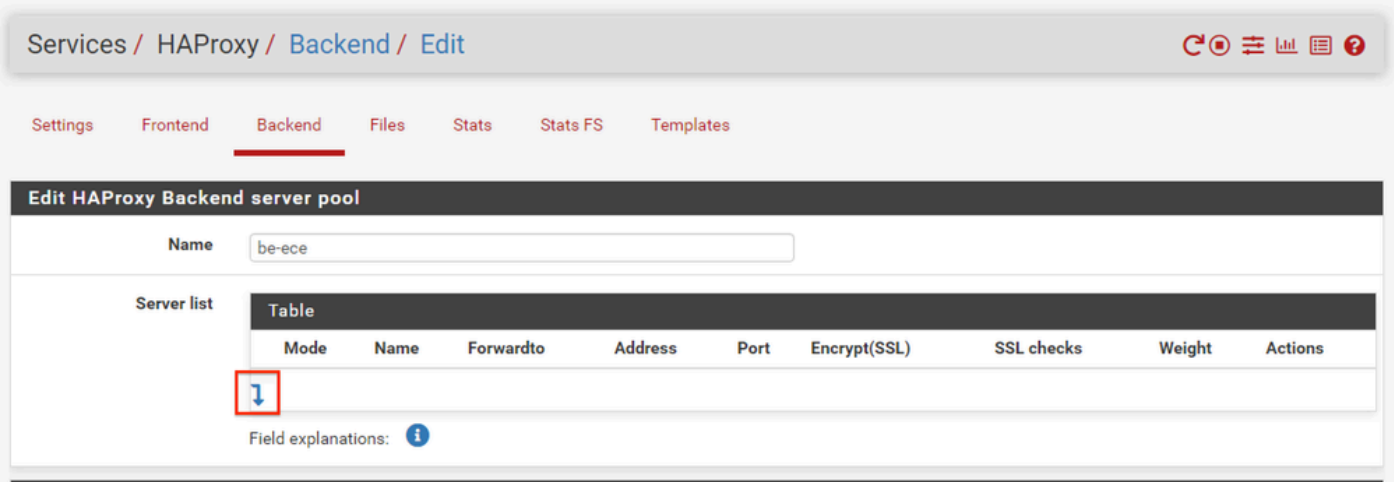
HAProxy-backkend configureren

Begin met het backend. De reden hiervoor is dat de frontend een backend moet noemen. Zorg ervoor dat u het Backend menu hebt geselecteerd.



pfSense GUI - HAProxy Toevoegen Backend

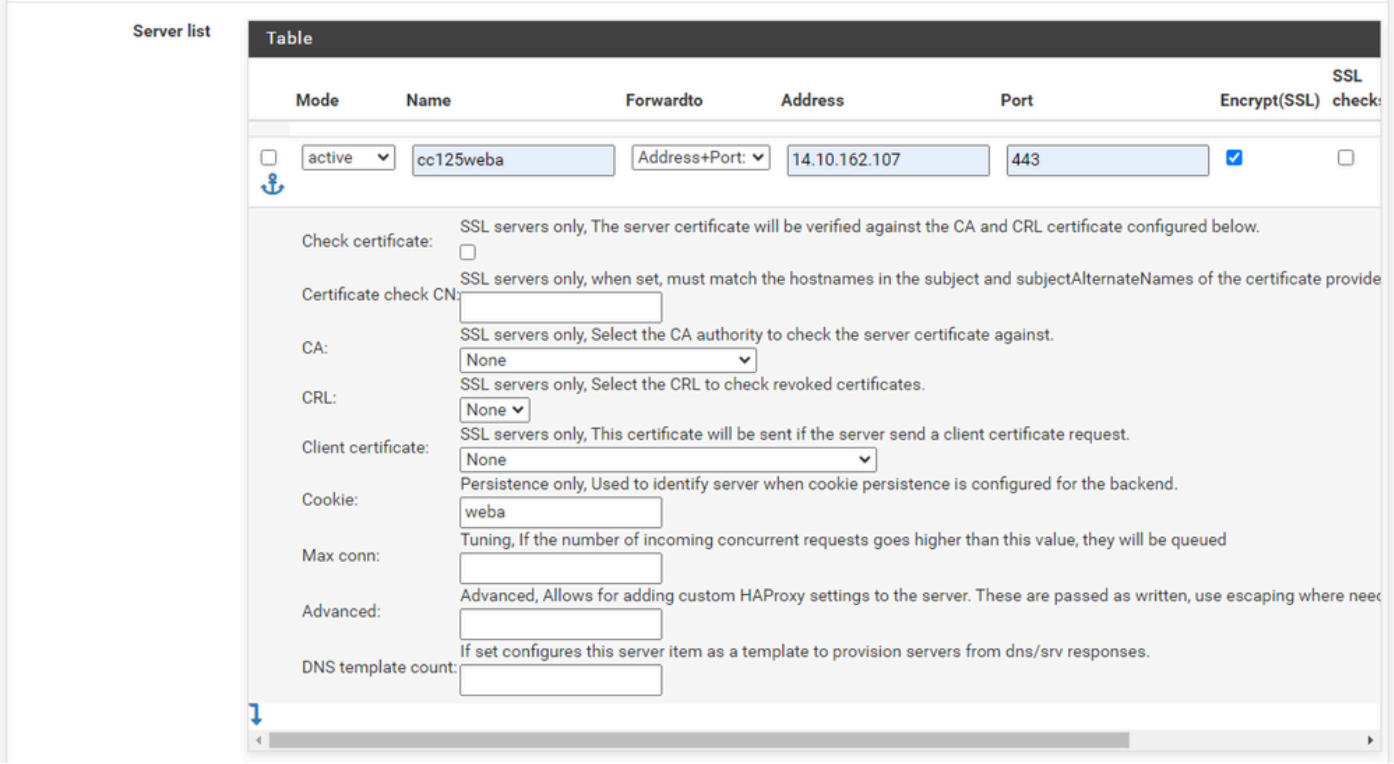
Selecteer de knop Toevoegen.



PfSense GUI - HAProxy backend start

Geef een naam voor het backend.

Selecteer de pijl-omlaag om de eerste server aan de lijst Server toe te voegen



Back-end - serverlijst

Geef een naam op die verwijst naar de server. Dit hoeft niet overeen te komen met de feitelijke servernaam. Dit is de naam die wordt weergegeven op de stats pagina.

Geef het adres van de server op. Dit kan worden geconfigureerd als een IP-adres voor FQDN.

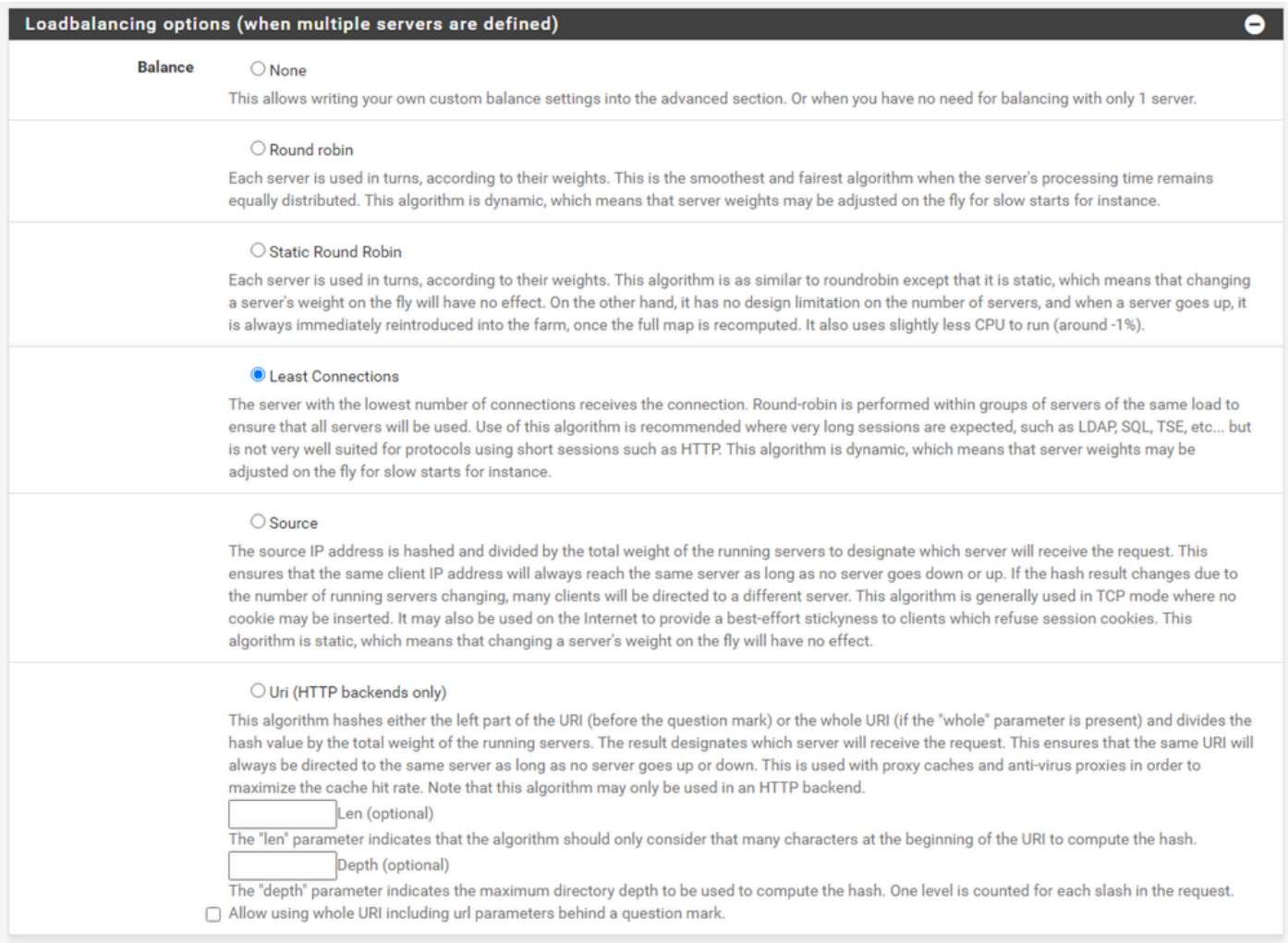
Geef de poort op waarop u verbinding wilt maken. Dit moet haven 443 voor ECE zijn.

Selecteer het selectievakje Encrypt (SSL).

Verstrek een waarde in het veld Cookie. Dit is de inhoud van de sessie stickiness cookie en moet

uniek zijn in het backend.

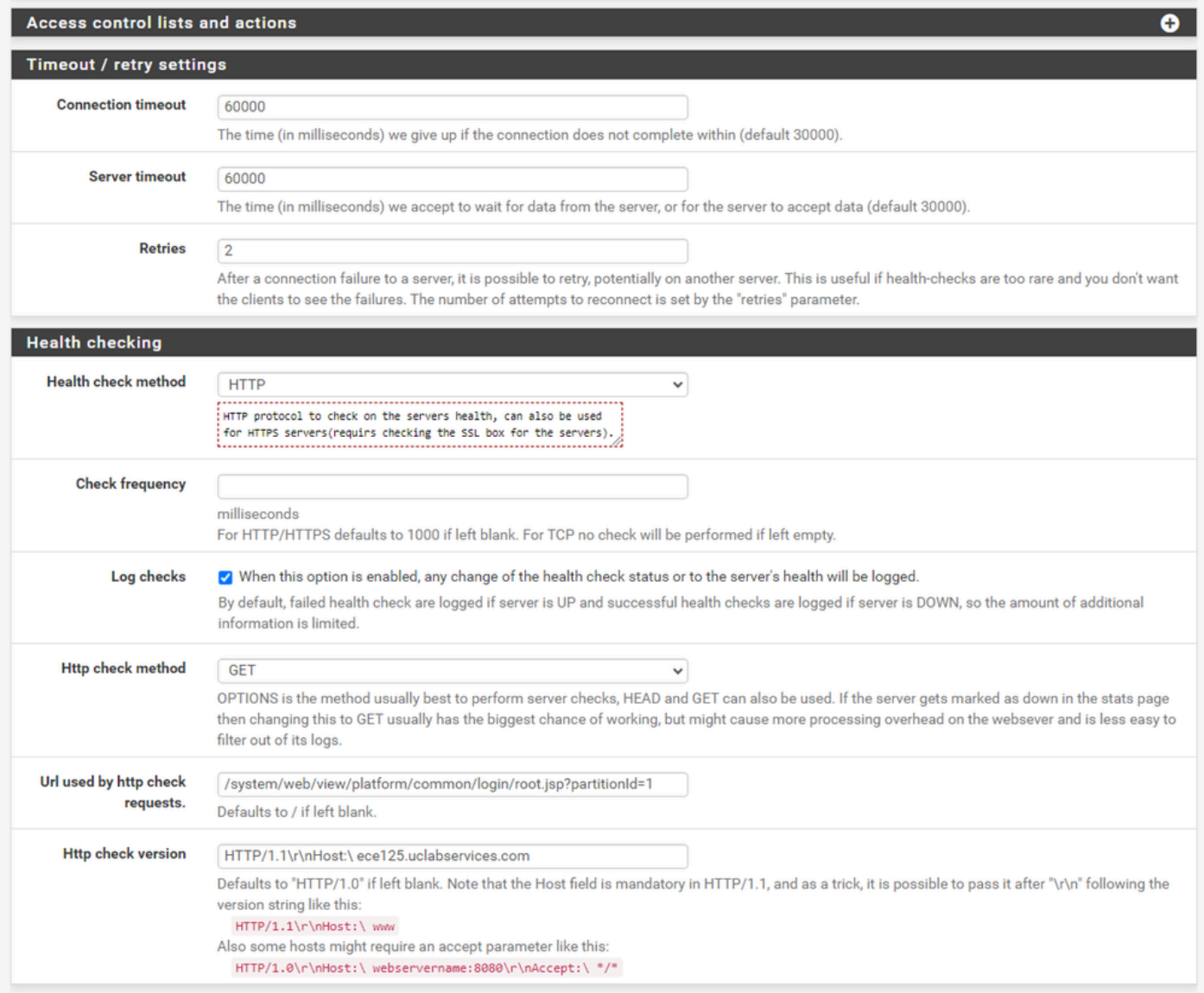
Nadat de eerste server is geconfigureerd, selecteert u de pijl-omlaag om andere webservers in de omgeving te configureren.



HAProxy Backend - Loadbalancing

Configureer de opties voor taakverdeling.

Voor ECE-servers moet dit worden ingesteld op Minst Connections.



HAProxy Backend - Health check

Toegangscontrolelijsten worden niet gebruikt in deze configuratie.

De instellingen voor time-out/opnieuw proberen kunnen bij hun standaardconfiguratie worden achtergelaten.

Configureer de sectie Gezondheidscontrole.

1. Health check methode: HTTP
2. Controleer frequentie: laat leeg om de standaardinstelling van elke 1 seconde te gebruiken.
3. Logcontroles: Selecteer deze optie om eventuele wijzigingen in de status van de logbestanden te schrijven.
4. HTTP-controlemethode: Selecteer GET in de lijst.
5. Url gebruikt door http check request.: Voor een ECE server enter, /system/web/view/platform/common/login/root.jsp?partitieId=1
6. HTTP-controleversie: Enter, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

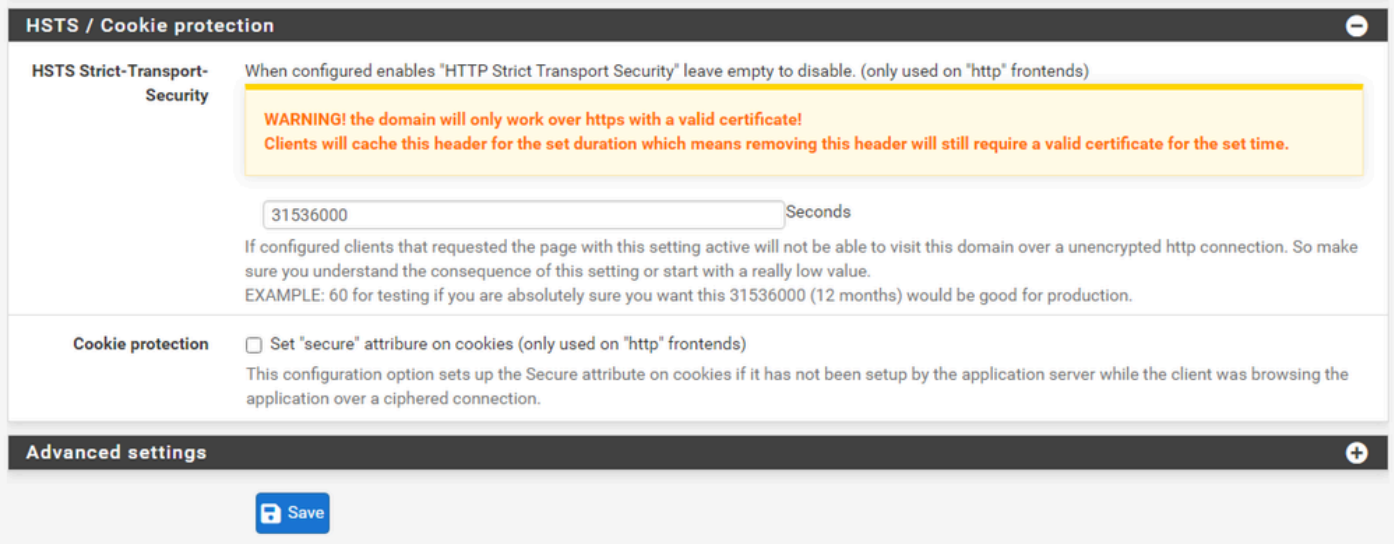
Zorg ervoor dat u een ruimte na de laatste backslash, maar vóór de FQDN van de server, opneemt.

HAProxy Backend - Cookie Persistence

Laat de Agent-controles uitgeschakeld.

Cookiepersistentie instellen:

1. Cookie Enabled: Selecteer deze optie om op cookies gebaseerde persistentie in te schakelen.
2. Cookienaam: Geef een naam voor de cookie.
3. Cookiemodus: Selecteer Invoegen in de vervolgkeuzelijst.
4. Laat de resterende opties los.



HAProxy Backend - HSTS

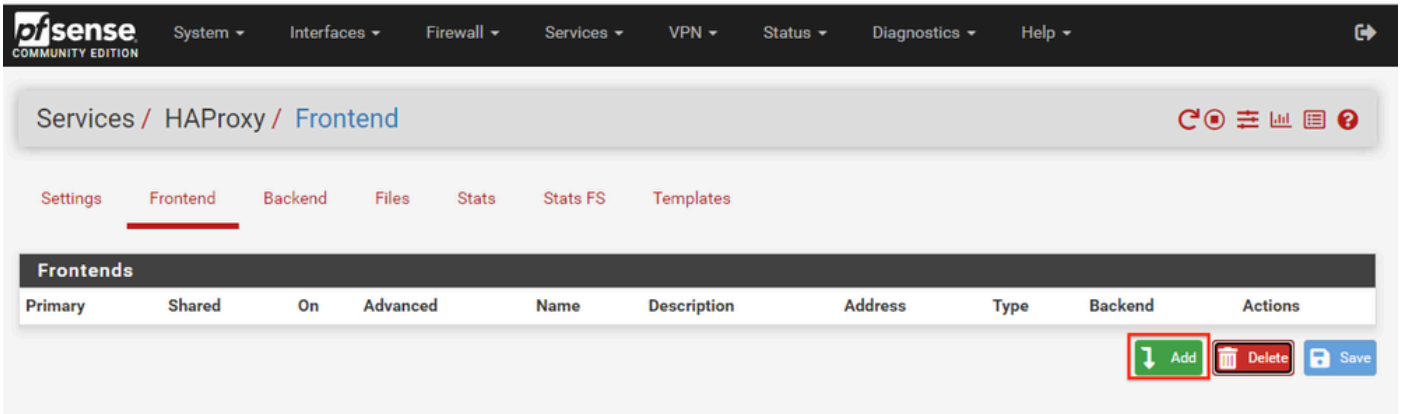
De resterende secties van het backend configuratieformulier kunnen bij hun standaardinstellingen worden achtergelaten.

Als u HSTS wilt configureren, configureer dan een tijdelijke waarde in deze sectie. ECE voegt ook een HSTS-cookie in, zodat deze configuratie overbodig is.

Selecteer Opslaan.

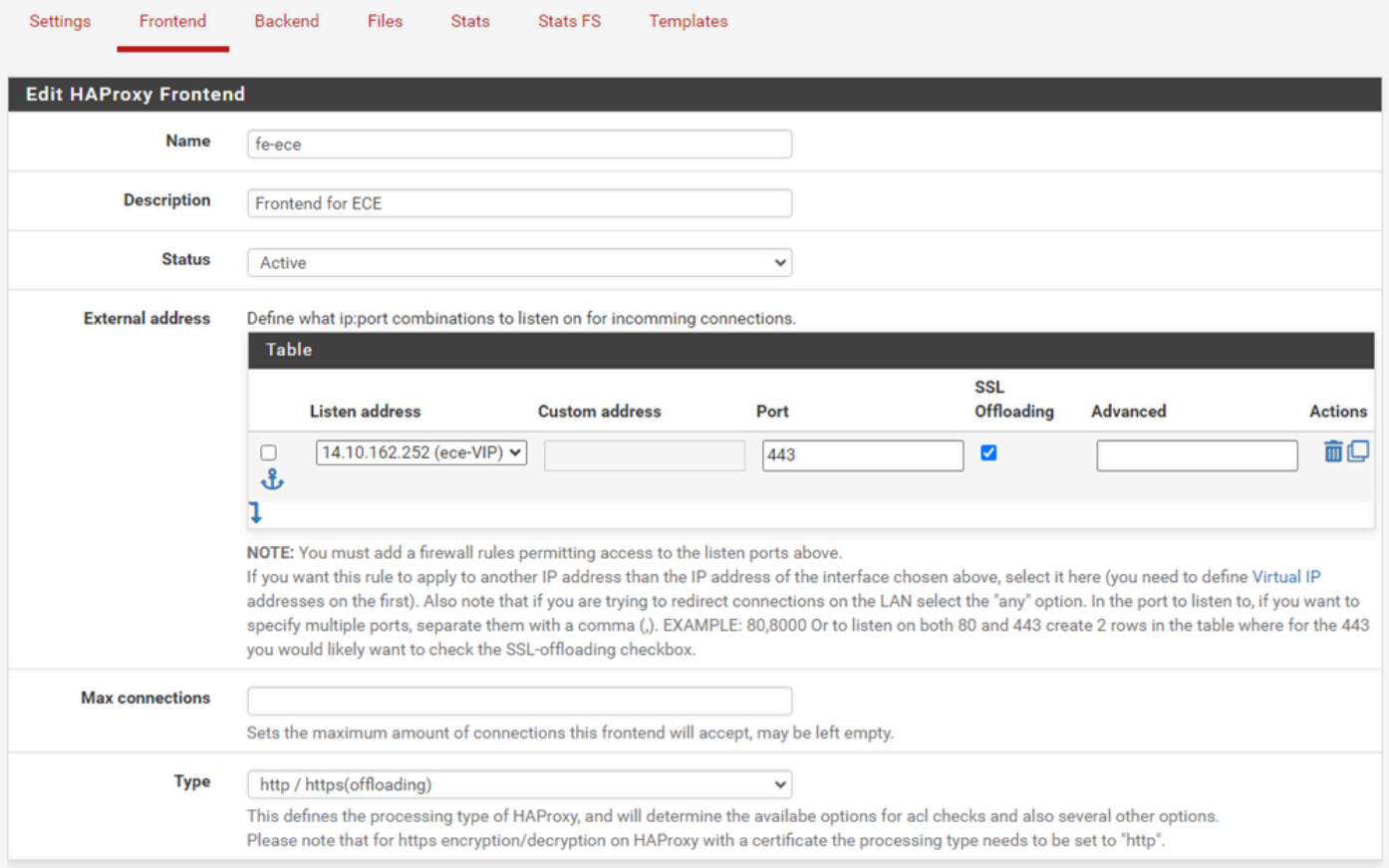
HAProxy-frontend configureren

Verandering in het menu Frontend.



pfSense GUI - HAProxy - Frontend toevoegen

Selecteer de knop Toevoegen



HAProxy - frontend header

Geef een naam op voor de voorzijde.

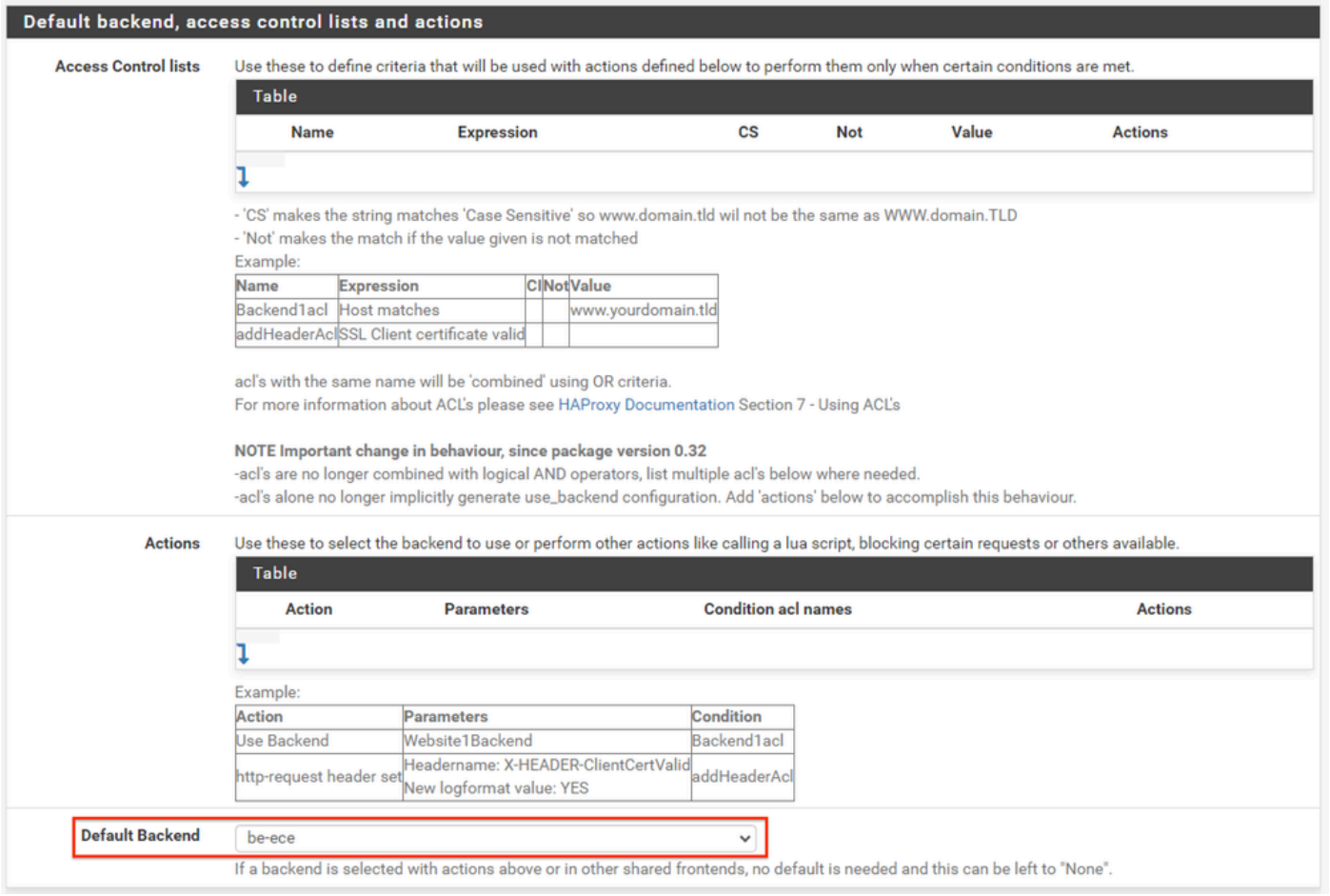
Geef een beschrijving om later de frontend te kunnen identificeren.

In de tabel Extern adres:

1. Luister adres: Selecteer de VIP die je voor deze website hebt gemaakt.
2. Poorten: Typ 443.
3. SSL Offloading: Selecteer deze optie zodat een sessiecookie kan worden ingevoegd.

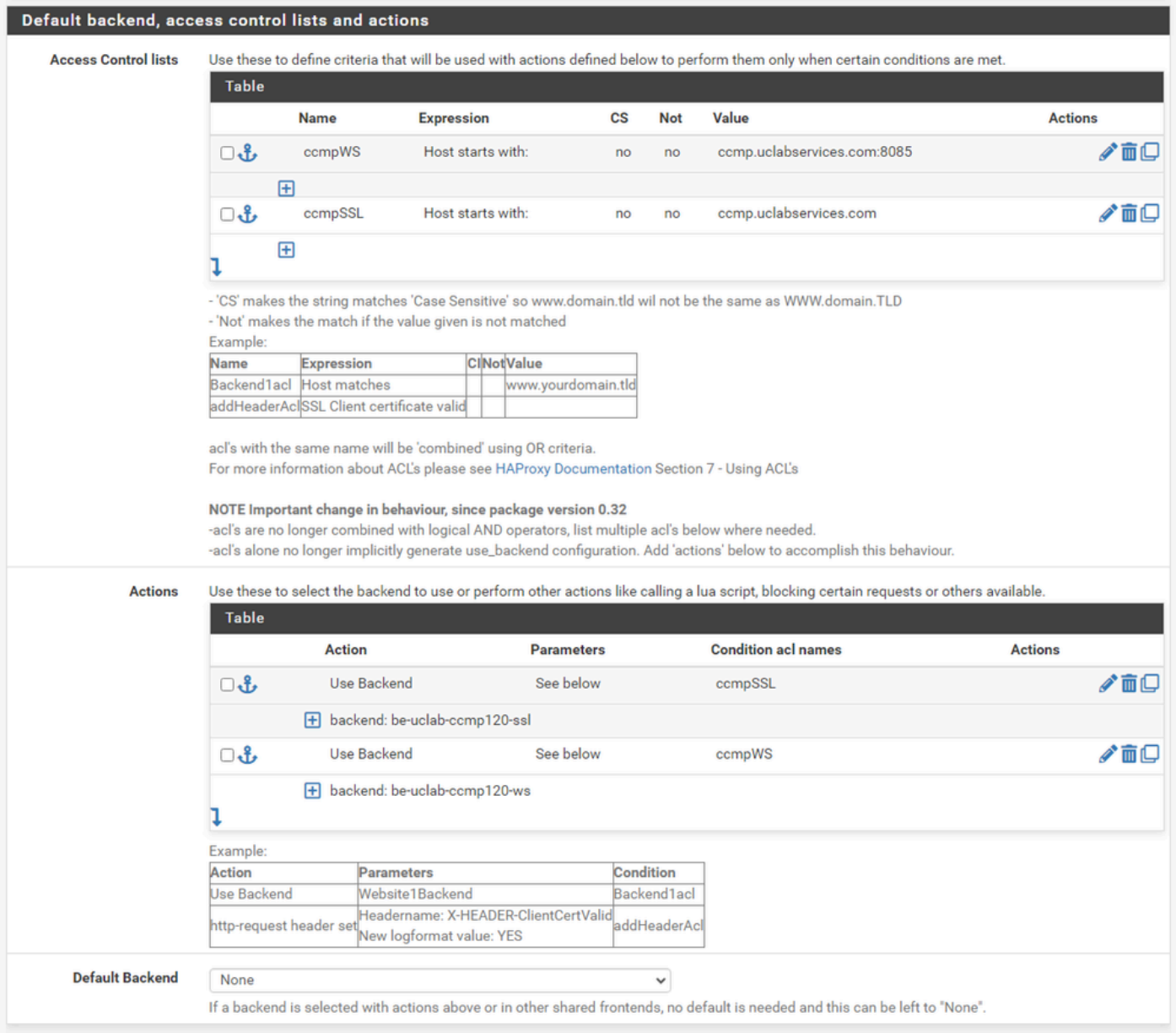
Laat de Max aansluitingen leeg.

Zorg ervoor dat het type is geselecteerd als http / https (offload).



HAProxy Backend - Standaard backend selectie

De eenvoudigste configuratie is om een Default Backend te kiezen uit de vervolgkeuzelijst. Dit kan worden geselecteerd wanneer de VIP een enkele website host.

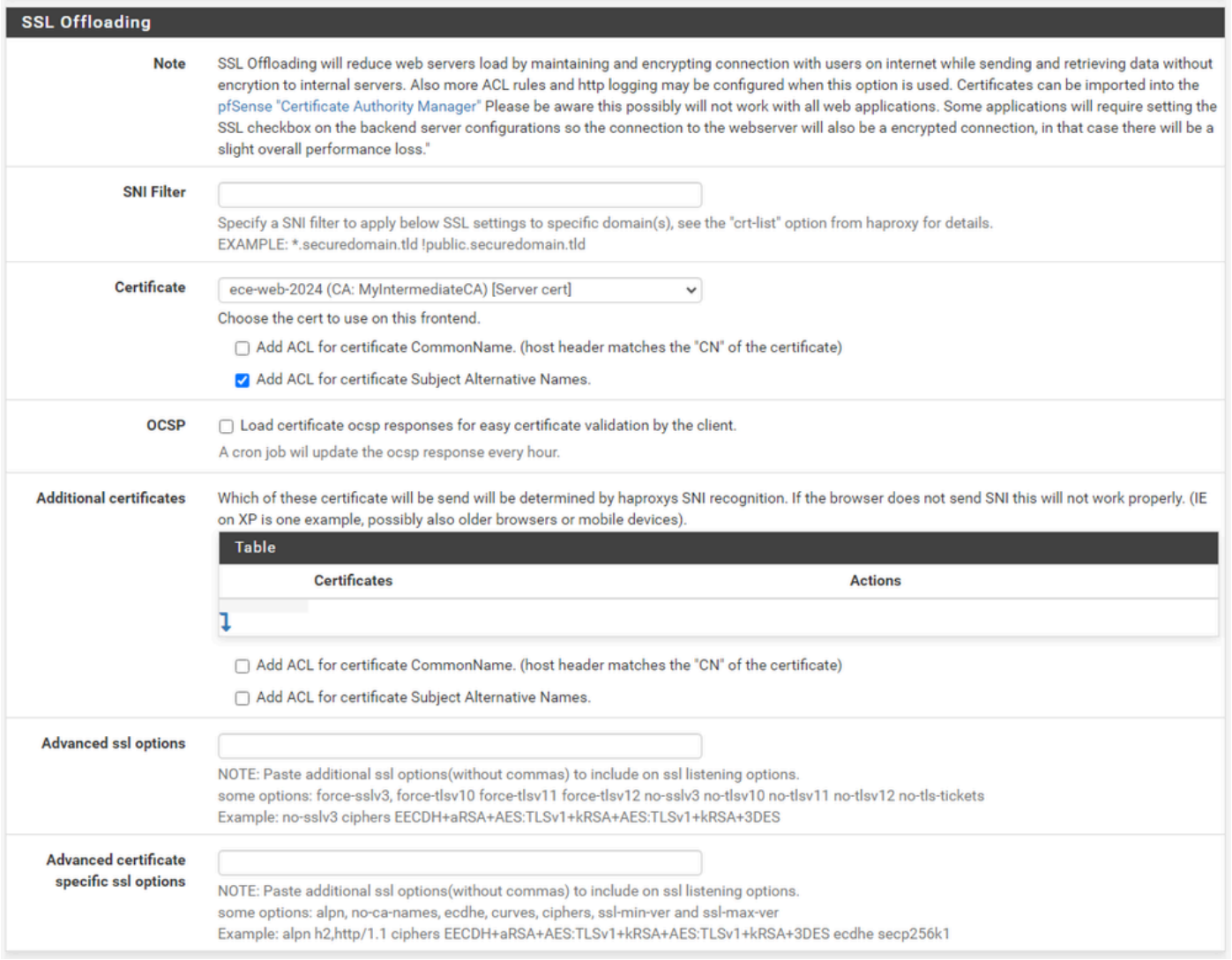


HAProxy-back-end - geavanceerde ACL

Zoals in het beeld wordt getoond, kunnen ACL's worden gebruikt om één frontend om te leiden naar meerdere backends op basis van voorwaarden.

U kunt zien dat de ACL controleert om te zien of de host in het verzoek begint met een naam en poortnummer. of gewoon de naam. Op basis hiervan wordt een specifiek backend gebruikt.

Dit is niet gebruikelijk bij ECE.



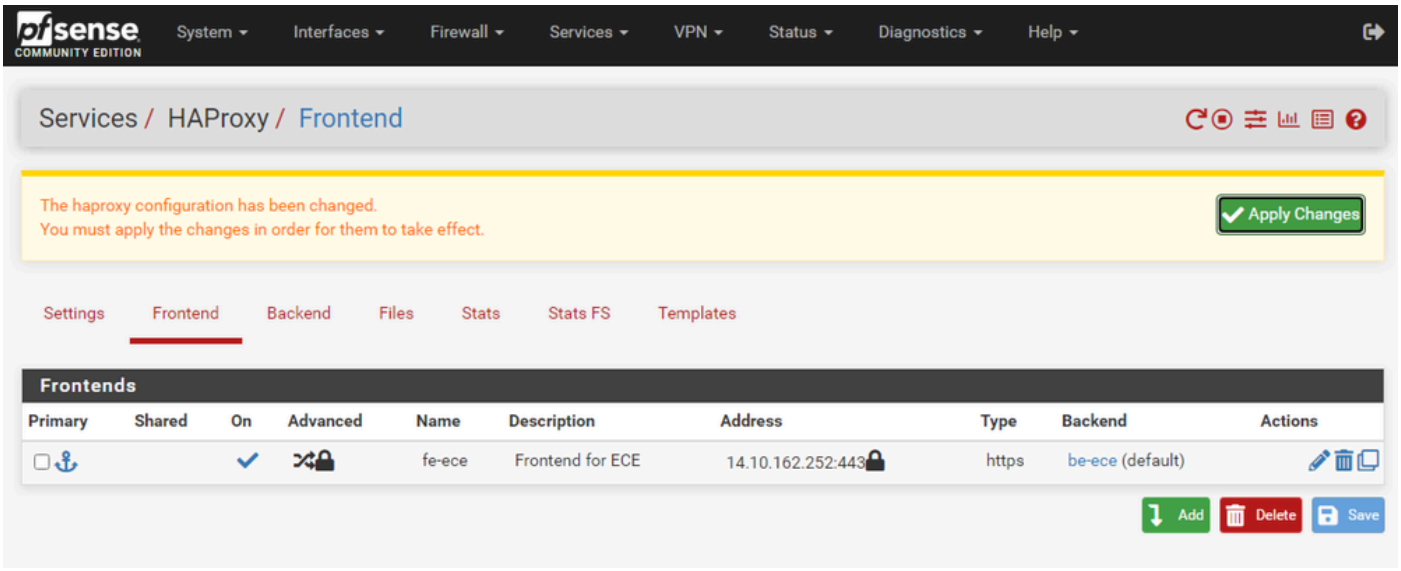
HAProxy Frontend - Certificaatbinding

Selecteer in het gedeelte SSL Offload het certificaat dat voor gebruik met deze site is gemaakt. Dit certificaat moet een servercertificaat zijn.

Selecteer de optie ACL toevoegen voor alternatieve namen van onderwerpcertificaten.

U kunt de resterende opties bij hun standaardwaarden laten staan.

Selecteer Opslaan aan het einde van dit formulier.



HAProxy - configuratie toepassen

Selecteer, pas Wijzigingen toe om de wijzigingen Frontend en Backend aan de lopende configuratie te verbinden.

Gefeliciteerd, u hebt de setup en configuratie van pfSense voltooid.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.