# Configure pfSense Community Load Balancer for ECE

## Contents

## Introduction

This document describes the steps to setup and configure pfSense Community Edition as a Load Balancer for Enterprise Chat and Email (ECE).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- ECE 12.x
- pfSense Community Edition

### Components Used

The information in this document is based on these software versions:

- ECE 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. If your network is live, ensure that you understand the potential impact of any command.

# Install pfSense

## Solution Overview

pfSense Community Edition is a multi-function product that provides a Firewall, Load Balancer, Security Scanner, and many other services in a single server. pfSense is built on Free BSD and has minimal hardware requirements. The Load Balancer is an implementation of HAProxy and an easy to use GUI is provided to configure the product.

You can use this load balancer with both ECE and Contact Center Management Portal (CCMP). This document gives the steps to configure pfSense for ECE.

## Preparation

### Step 1. Download pfSense Software

Use the pfSense website to download the iso installer image.

### Step 2. Configure VM

Configure a VM with the minimum requirements:

• 64-bit amd64 (x86-64) compatible CPU

• 1GB or more RAM

• 8 GB or larger disk drive (SSD, HDD, etc)

• One or more compatible network interface cards

• Bootable USB drive or high capacity optical drive (DVD or BD) for initial installation

For a lab install, only one network interface (NIC) is required. There are several ways of running the appliance, but the easiest is with a single NIC, also called one-arm mode. In one-arm mode, there is a single interface that communicates to the network. While this is an easy way and adequate for a lab, it is not the most secure way.

A more secure way of configuring the appliance is to have at least two NICs. One NIC is the WAN interface and communicates directly with the public internet. The second NIC is the LAN interface, and communicates with the internal corporate network. You can also add additional interfaces to communicate with various parts of the network that have different security and firewall rules. For example, you can have one NIC connect to the public internet, one connect to the DMZ network where all the externally accessible web servers are, and a third NIC connect to the corporate network. This allows you to have internal and external users securely access the same set of web servers that are kept in a DMZ. Ensure that understand the security implications of any design before implementation. Consult with a security engineer to ensure best practices are followed for your specific implementation.

## Installation

### Step 1. Mount the ISO to the VM

### Step 2. Power on the VM and follow the prompts to install.

Refer to this document for step-by-step instructions.

## Network Setup

You must assign IP addresses to the appliance to continue configuration.

**Note**: This document shows an appliance configured in one-arm mode.

### Step 1. Configure VLANs

If you require VLAN support, answer y to the first question. Otherwise, answer n.

### Step 2. Assign WAN Interface

The WAN interface is the non-secure side of the appliance in two-arm mode and the only interface in one-arm mode. Enter the interface name when prompted.

### Step 3. Assign the LAN Interface

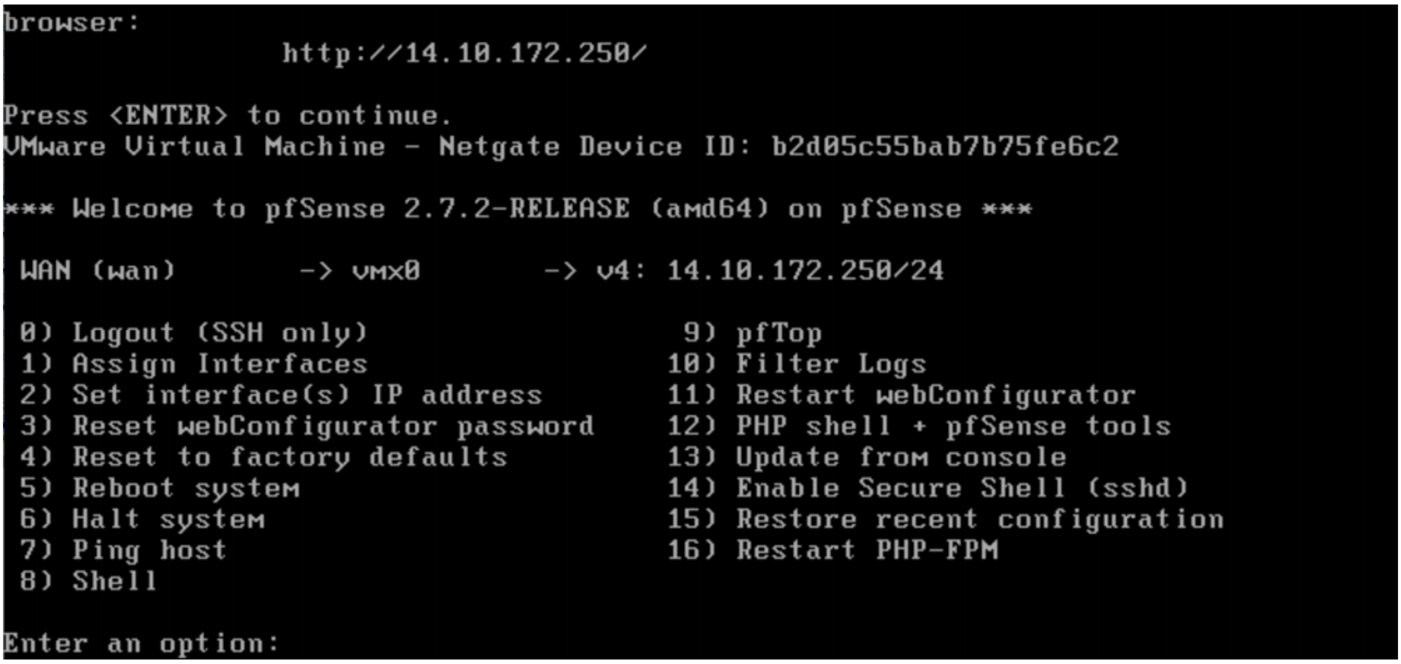
The LAN interface is the secure side of the appliance in two-arm mode. If required, enter the interface name when prompted.

### Step 4. Assign any other Interfaces

Configure any other interfaces you require for your specific install. These are optional and not common.

### Step 5. Assign IP Address to management interface

If your network supports DHCP, then the assigned IP address is shown in the console screen.



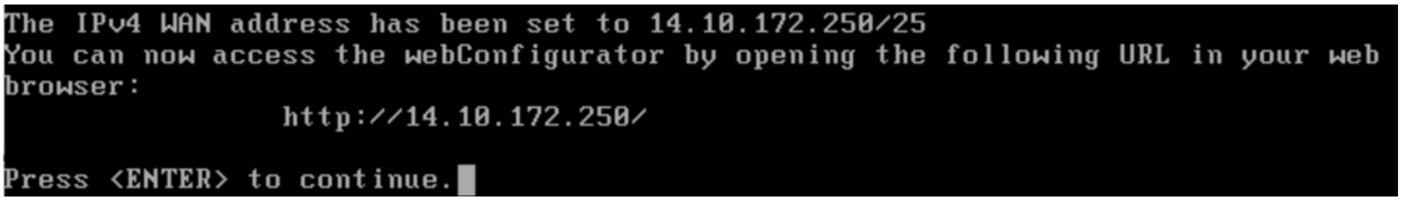
```
browser:
                http://14.10.172.250/

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:
```

*pfSense Console*

If there is no address assigned, or if you wish to assign a specific address perform these steps.

1. Choose option 2 from the console menu.
2. Answer n to disable DHCP.
3. Enter the IPv4 address for the WAN interface.
4. Enter the netmask in bit counts. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Enter the gateway address for the WAN interface.
6. If you would like this gateway to be the default gateway for the appliance, answer y to the gateway prompt, otherwise answer n.
7. Configure the NIC for IPv6 if desired.
8. Disable DHCP Server on the interface.
9. Answer y to enable HTTP on the webConfigurator protocol. This is used in the next steps.

You then receive confirmation that the settings have been updated.



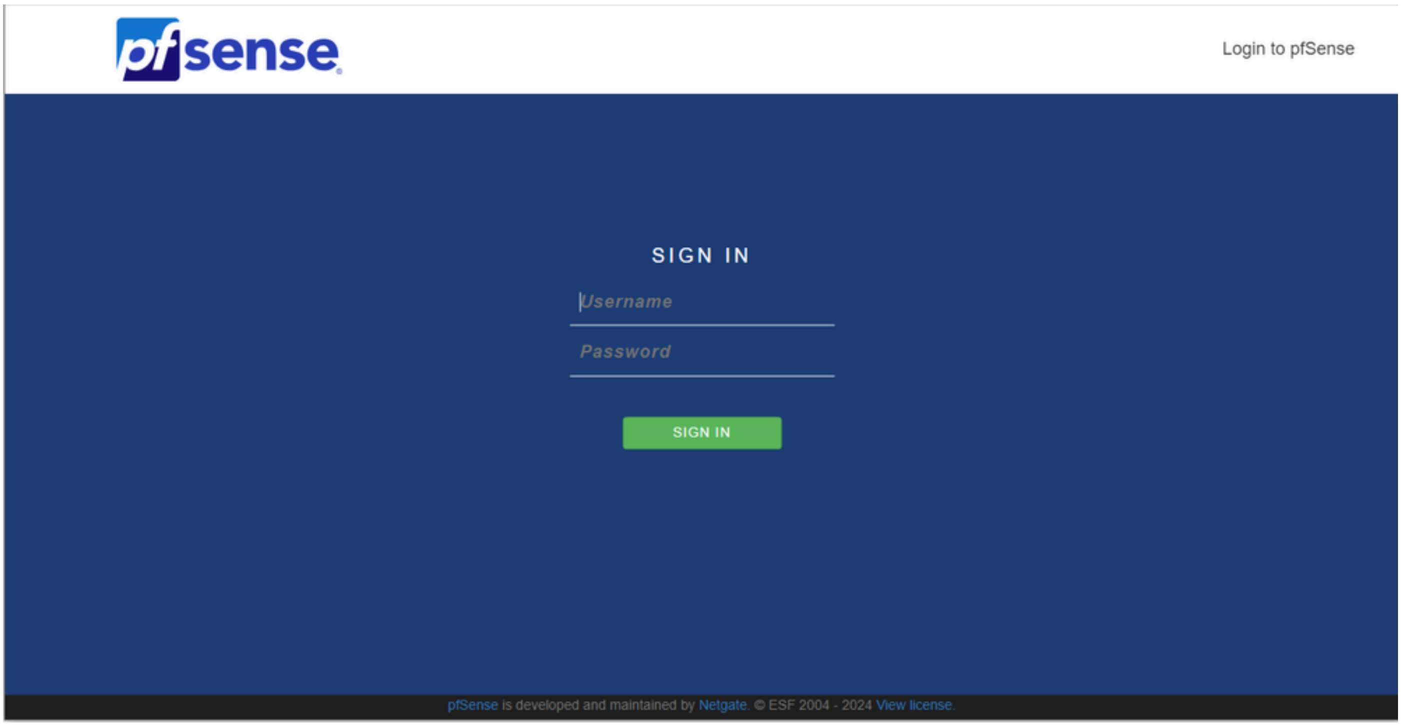
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://14.10.172.250/

Press <ENTER> to continue.
```

*pfSense Confirmation*

## Complete Initial Setup

**Step 1. Open a web browser and navigate to: http://<ip_address_of_appliance>**

**Note**: You must use HTTP and not HTTPS initially.



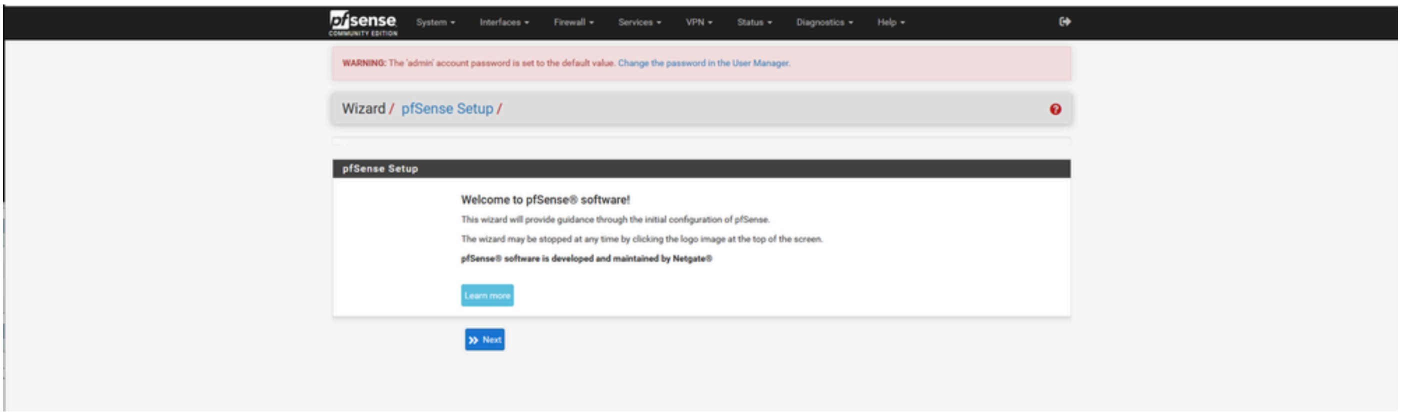
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

*pfSense Admin Login*

### Step 2. Login with the default login of admin / pfSense

### Step 3. Complete the initial setup

Click next through the first two screens.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup /

pfSense Setup

Welcome to pfSense® software!

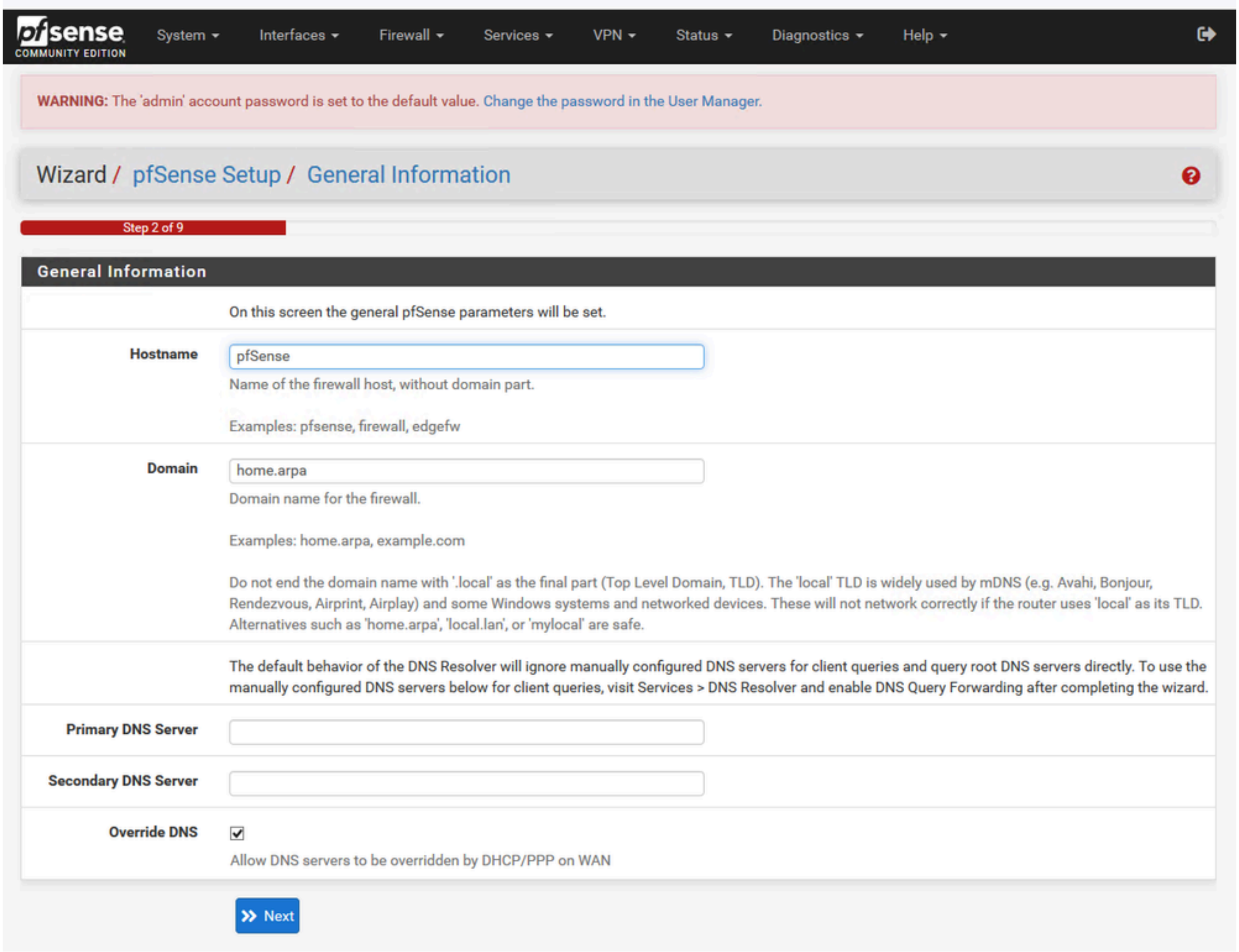
This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

**pfSense® software is developed and maintained by Netgate®**

*pfSense Setup Wizard - 1*

Provide the host name, domain name, and DNS server information.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

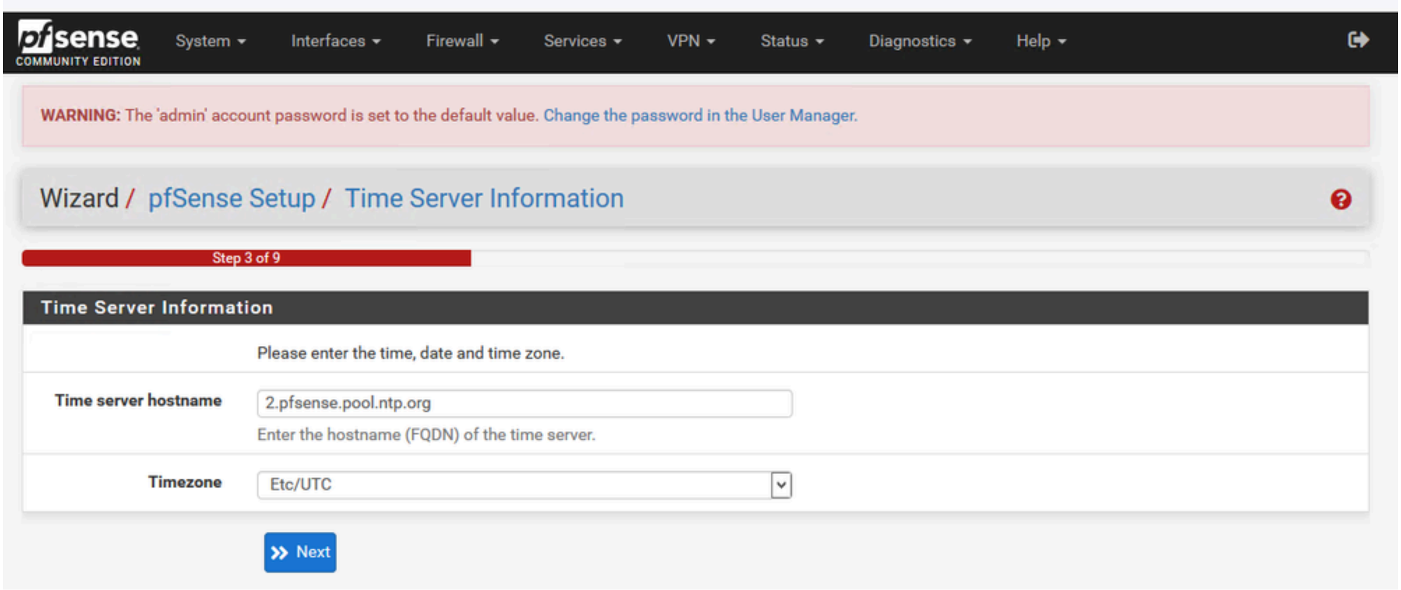
On this screen the general pfSense parameters will be set.

| | |
|---|---|
| Hostname | pfSense<br>Name of the firewall host, without domain part.<br>Examples: pfsense, firewall, edgefw |
| Domain | home.arpa<br>Domain name for the firewall.<br>Examples: home.arpa, example.com<br>Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe. |
| | The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard. |
| Primary DNS Server | |
| Secondary DNS Server | |
| Override DNS | ☑<br>Allow DNS servers to be overridden by DHCP/PPP on WAN |

*pfSense Setup Wizard - 2*

Validate the IP Address information. If you initially chose DHCP, you can change this now.

Provide the NTP Time server hostname and select the correct Timezone in the drop-down.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

| | |
|---|---|
| Time server hostname | 2.pfsense.pool.ntp.org<br>Enter the hostname (FQDN) of the time server. |
| Timezone | Etc/UTC |

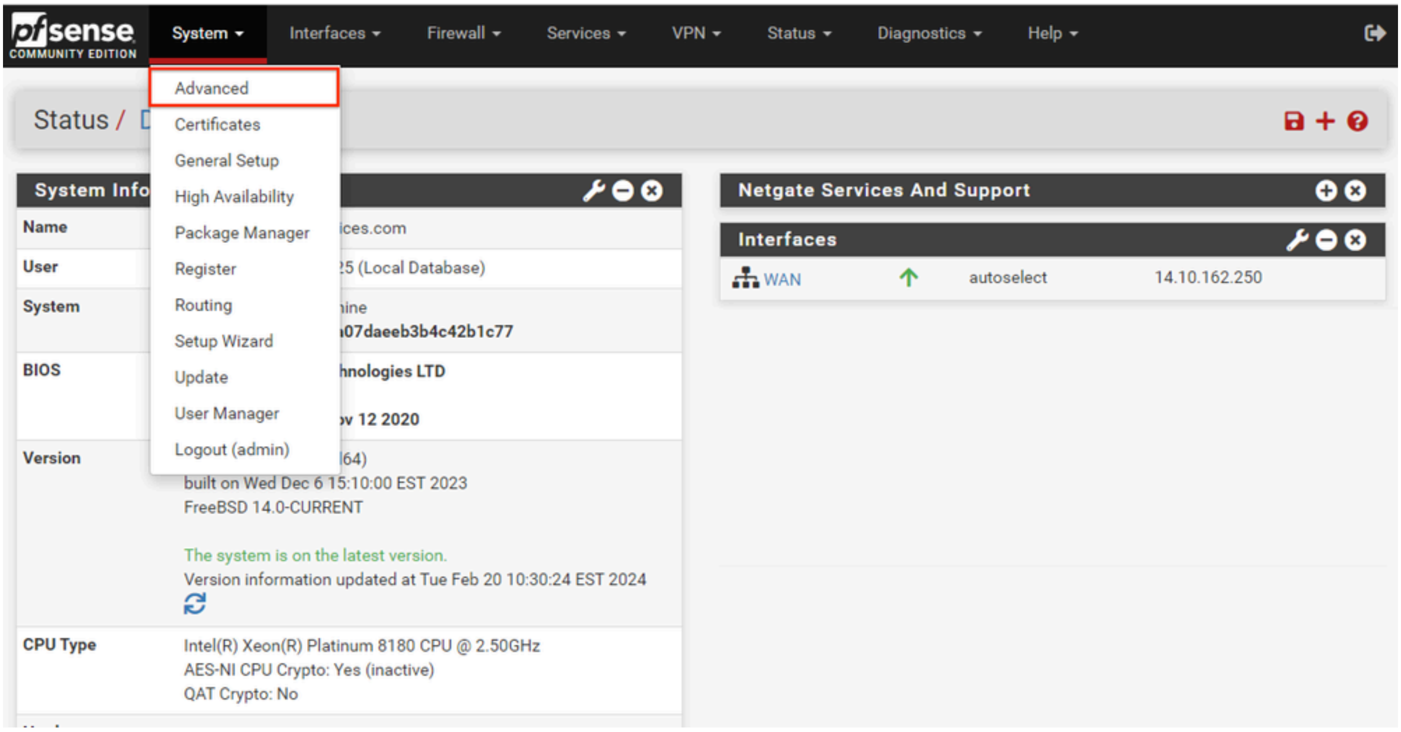
*pfSense Setup Wizard - 3*

Continue through the setup wizard until the end. The interface GUI restarts and you are redirected to the new URL once complete.

## Configure Basic Admin Settings

### Step 1. Login to the admin interface

### Step 2. Select Advanced from the System drop-down menu

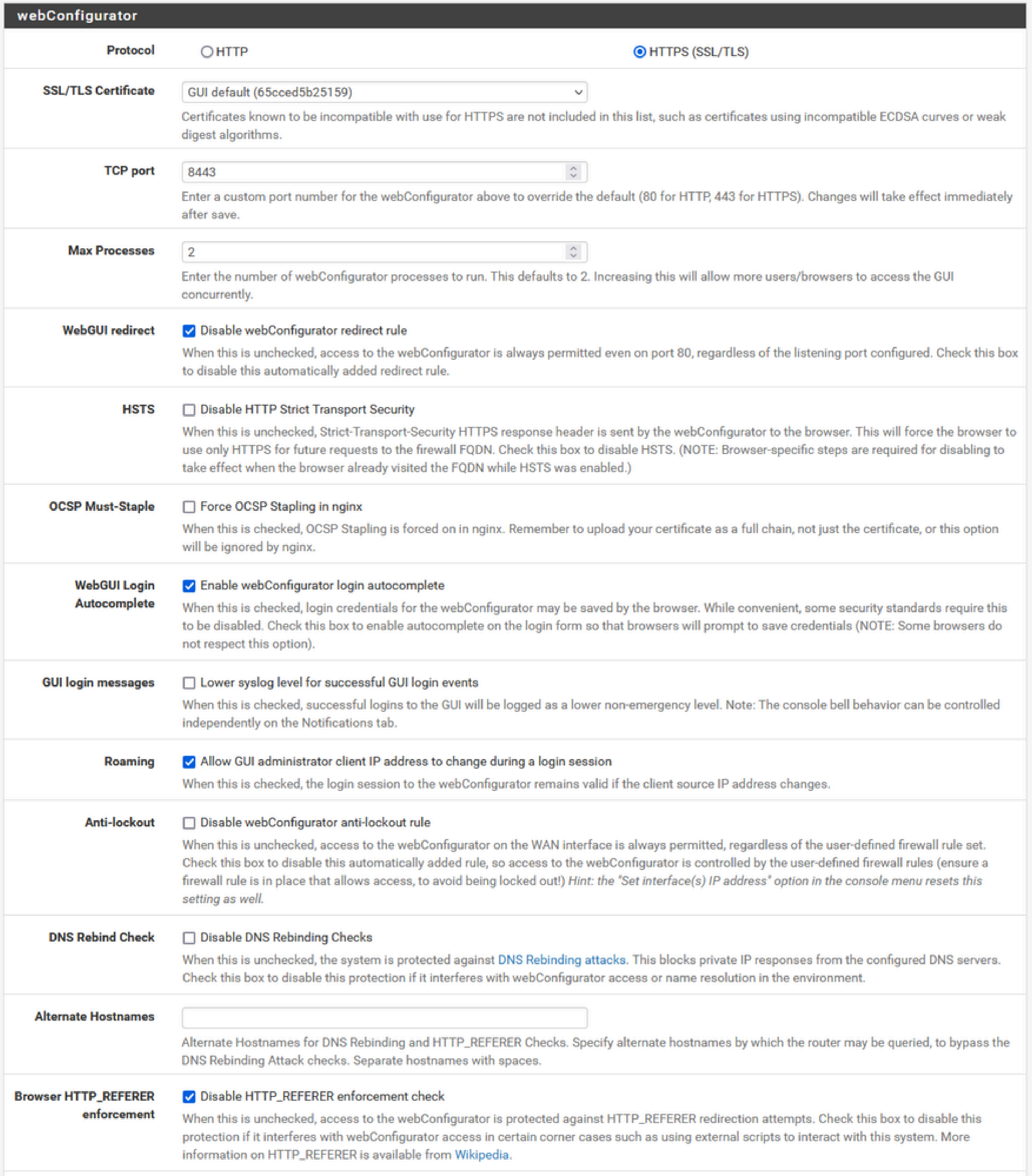


| | |
|---|---|
| Name | ices.com |
| User | 5 (Local Database) |
| System | ine<br>07daeeb3b4c42b1c77 |
| BIOS | hnologies LTD<br>v 12 2020 |
| Version | 64)<br>built on Wed Dec 6 15:10:00 EST 2023<br>FreeBSD 14.0-CURRENT<br>The system is on the latest version.<br>Version information updated at Tue Feb 20 10:30:24 EST 2024 |
| CPU Type | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz<br>AES-NI CPU Crypto: Yes (inactive)<br>QAT Crypto: No |

| | | |
|---|---|---|
| WAN | autoselect | 14.10.162.250 |

*pfSense GUI - Admin Dropdown*

### Step 3. Update webConfigurator settings



webConfigurator

Protocol ○ HTTP ● HTTPS (SSL/TLS)

SSL/TLS Certificate: GUI default (65cced5b25159)

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.

TCP port: 8443

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.

Max Processes: 2

Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect ☑ Disable webConfigurator redirect rule

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.

HSTS □ Disable HTTP Strict Transport Security

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.)

OCSP Must-Staple □ Force OCSP Stapling in nginx

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.

WebGUI Login Autocomplete ☑ Enable webConfigurator login autocomplete

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).

GUI login messages □ Lower syslog level for successful GUI login events

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.

Roaming ☑ Allow GUI administrator client IP address to change during a login session

When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes.

Anti-lockout □ Disable webConfigurator anti-lockout rule

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!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

DNS Rebind Check □ Disable DNS Rebinding Checks

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.

Alternate Hostnames:

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.

Browser HTTP_REFERER enforcement ☑ Disable HTTP_REFERER enforcement check

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.

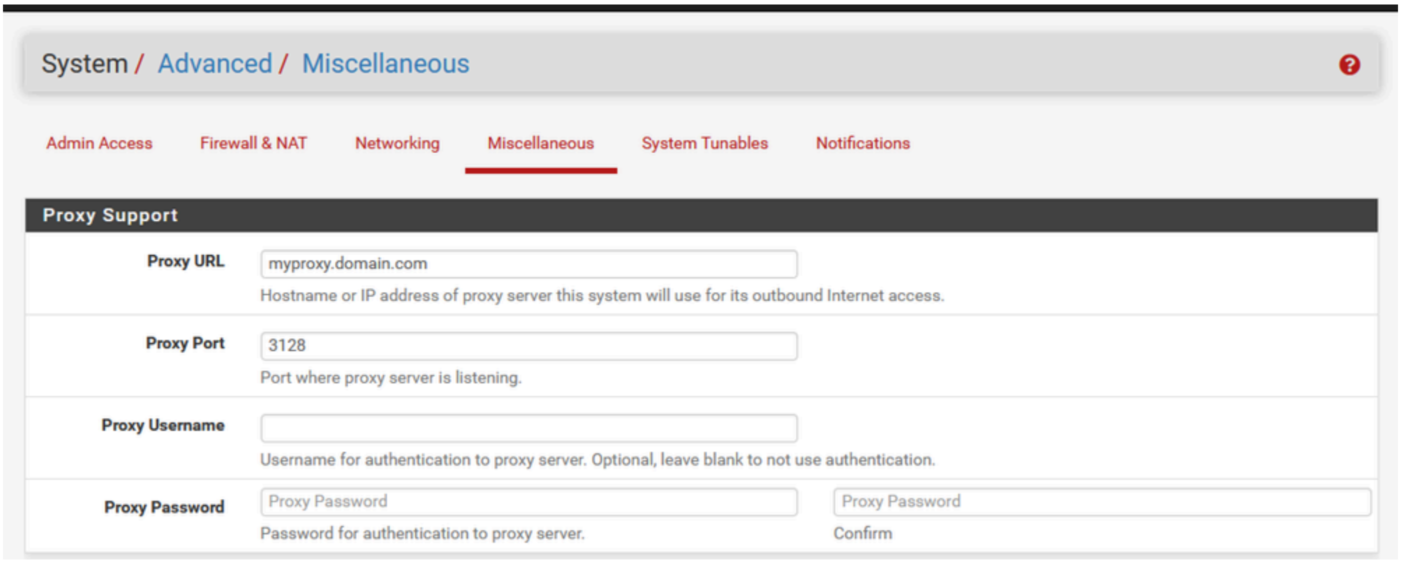
*pfSense GUI - Admin Configuration*

1. Select the HTTPS (SSL/TLS) protocol.
2. Leave the SSL/TLS Certificate to the self-signed certificate at this time.
3. Change the TCP Port to a port other than 443 to better secure the interface and prevent issues with port overlap.
4. Select the WebGUI redirect option to disable the admin interface on port 80.
5. Select the Browser HTTP_REFERER enforcement option.
6. Enable Secure Shell by selecting the Enable Secure Shell option.

**Note**: Ensure that you select the **Save** button before you proceed. You are then redirected to the new https link.

### Step 4. Configure Proxy Server if needed

If required, configure the proxy information on the Miscellaneous tab. To complete the setup and configuration, the appliance must have internet access.



Proxy Support

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

Proxy Port: 3128
Port where proxy server is listening.

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

Proxy Password: Proxy Password
Password for authentication to proxy server.
Proxy Password
Confirm

*pfSense GUI - Proxy Configuration*

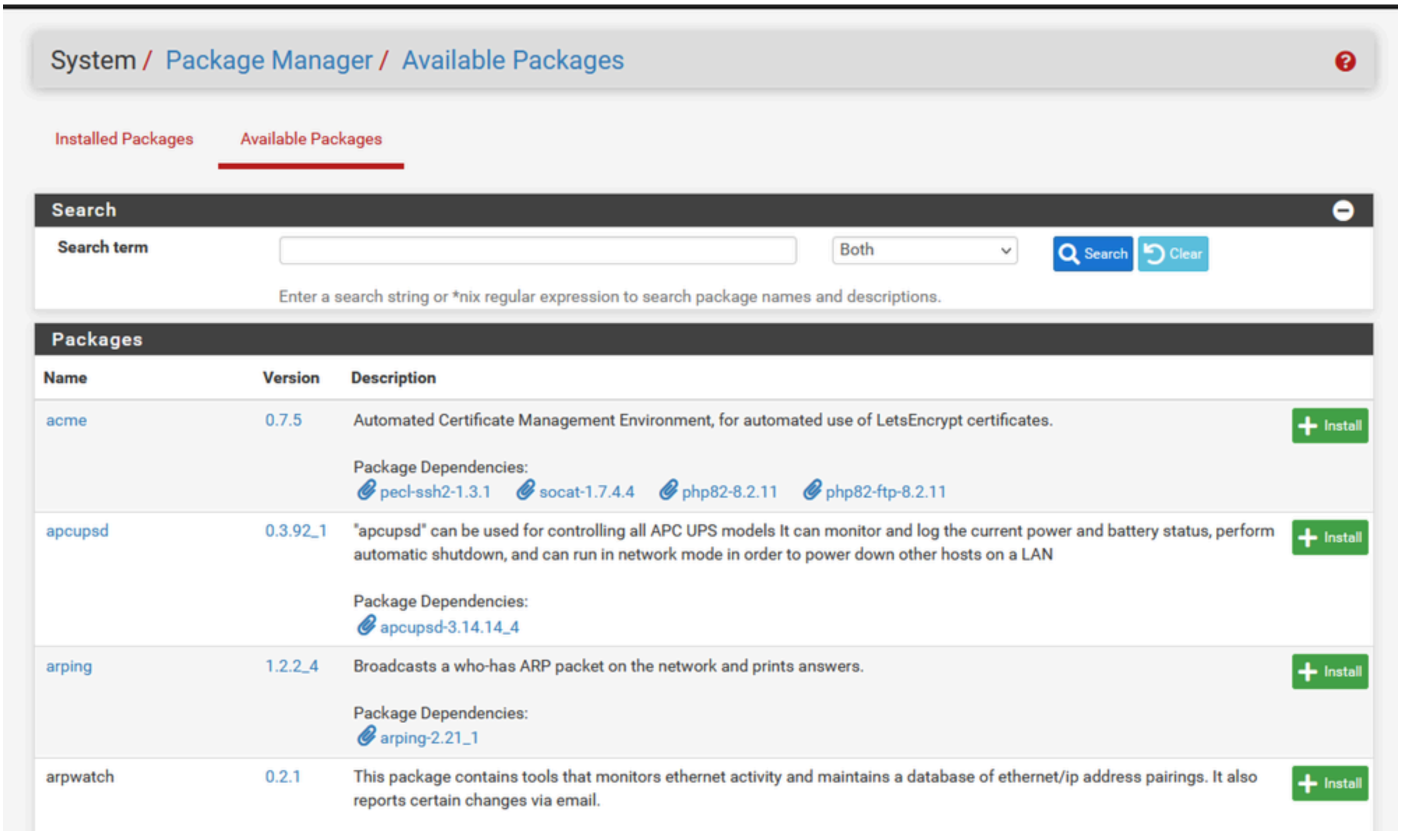
**Note**: Ensure that you select the **Save** button after making changes.

## Add Required Packages

### Step 1. Select System > Package Manager

### Step 2. Select Available Packages

**Note**: It can take a few minutes to load all of the packages that are available. If this times out, verify that the DNS servers are configured correctly. Often, a reboot of the appliance fixes the internet connectivity.



System / Package Manager / Available Packages

Installed Packages | Available Packages

**Search**

Search term [ ] Both Search Clear

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.<br>Package Dependencies:<br>pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11 | 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<br>Package Dependencies:<br>apcupsd-3.14.14_4 | Install |
| arping | 1.2.2_4 | Broadcasts a who-has ARP packet on the network and prints answers.<br>Package Dependencies:<br>arping-2.21_1 | 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. | Install |

*pfSense GUI - Package List*

### Step 3. Find and Install required packages

1. haproxy
2. Open-VM-Tools

**Note**: Do not select the haproxy-devel package.

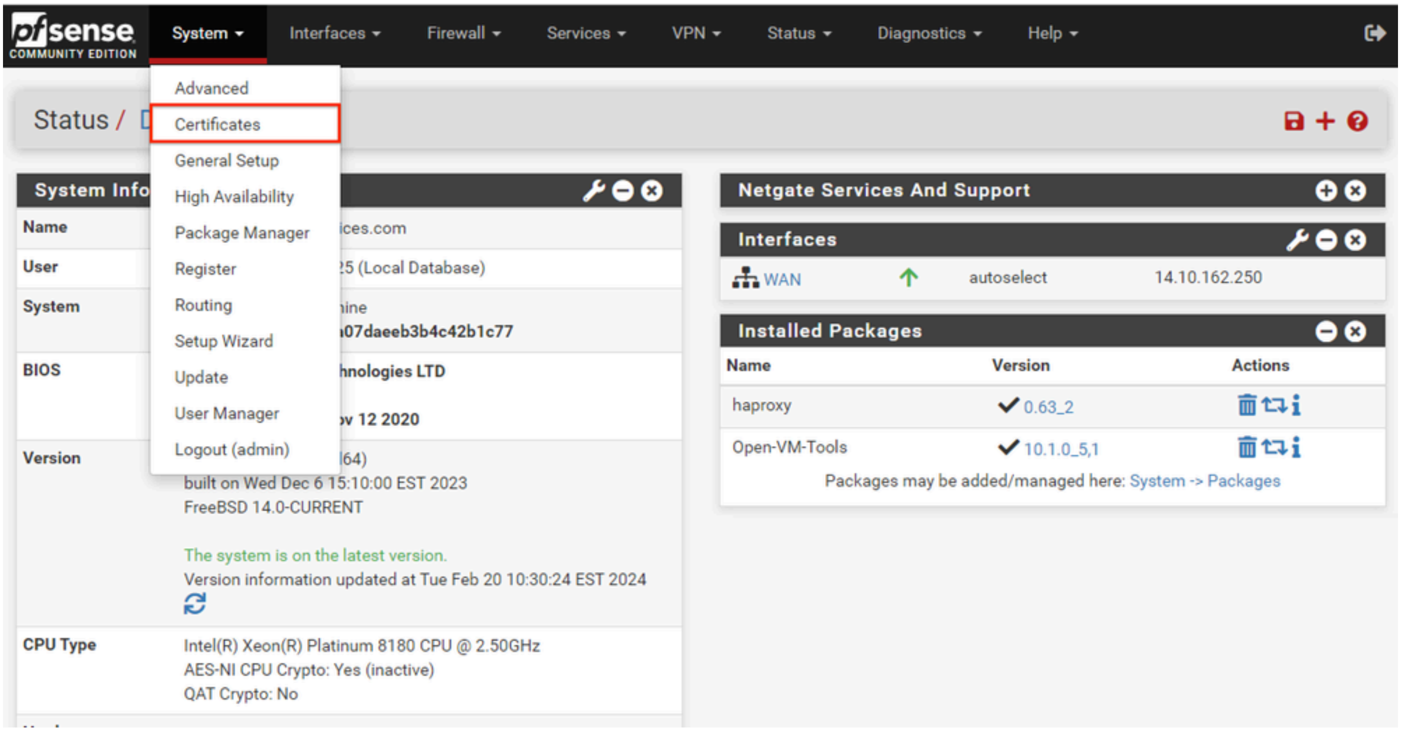
## Configure Certificates

pfSense can create self-signed certificate or it can integrate with a public CA, an internal CA, or can act as a CA and issue CA-signed certificates. This guide shows the steps to integrate with an internal CA.

Before you begin this section, ensure that you have these items available.

1. Root certificate for CA saved as either a PEM or Base-64 encoded format.
2. All intermediate (sometimes called issuing) certificates for CA saved as either a PEM or Base-64 encoded format.

### Step 1. Select Certificates from the System drop-down menu



System Info

| | |
|---|---|
| Name | ices.com |
| User | 25 (Local Database) |
| System | ine<br>07daeeb3b4c42b1c77 |
| BIOS | hnologies LTD<br>v 12 2020 |
| Version | 64)<br>built on Wed Dec 6 15:10:00 EST 2023<br>FreeBSD 14.0-CURRENT<br>The system is on the latest version.<br>Version information updated at Tue Feb 20 10:30:24 EST 2024 |
| CPU Type | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz<br>AES-NI CPU Crypto: Yes (inactive)<br>QAT Crypto: No |

Netgate Services And Support

Interfaces

| | | | |
|---|---|---|---|
| WAN | ↑ | autoselect | 14.10.162.250 |

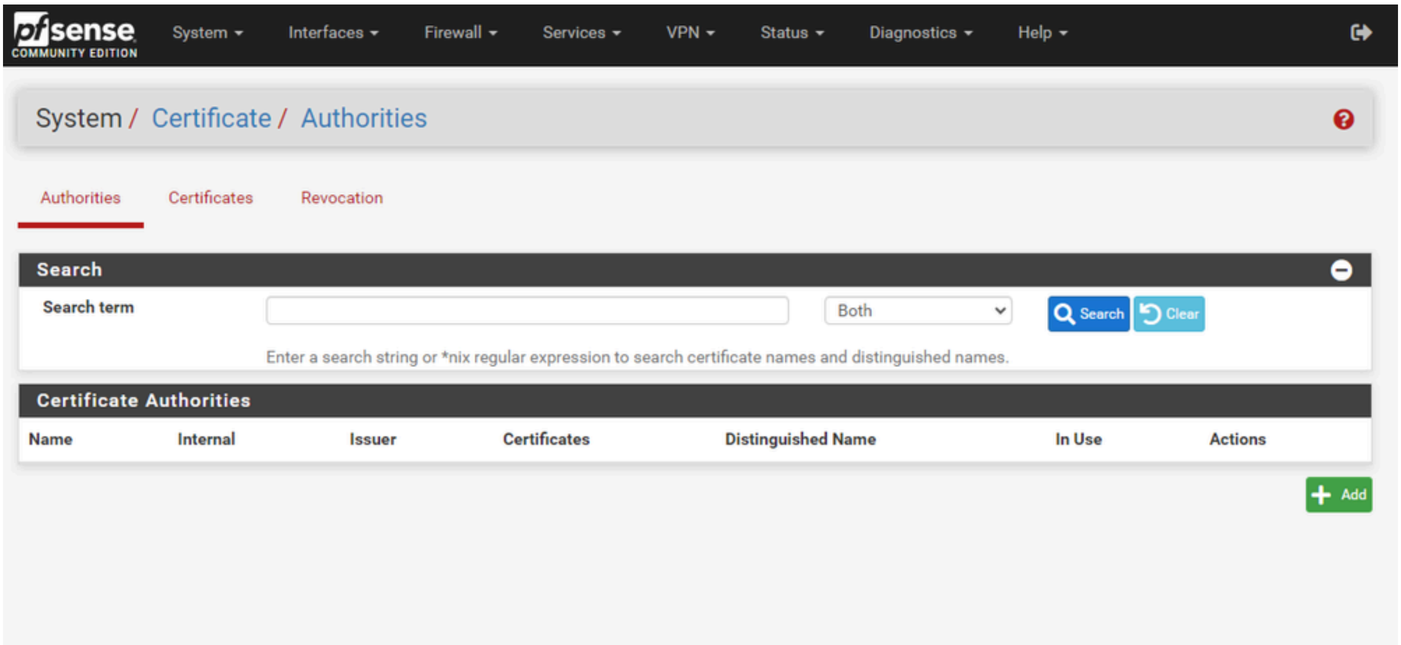
Installed Packages

| Name | Version | Actions |
|---|---|---|
| haproxy | ✓ 0.63_2 | |
| Open-VM-Tools | ✓ 10.1.0_5,1 | |

Packages may be added/managed here: System -> Packages

*pfSense GUI - Certificates Dropdown*

## Step 2. Import the CA Root Certificate



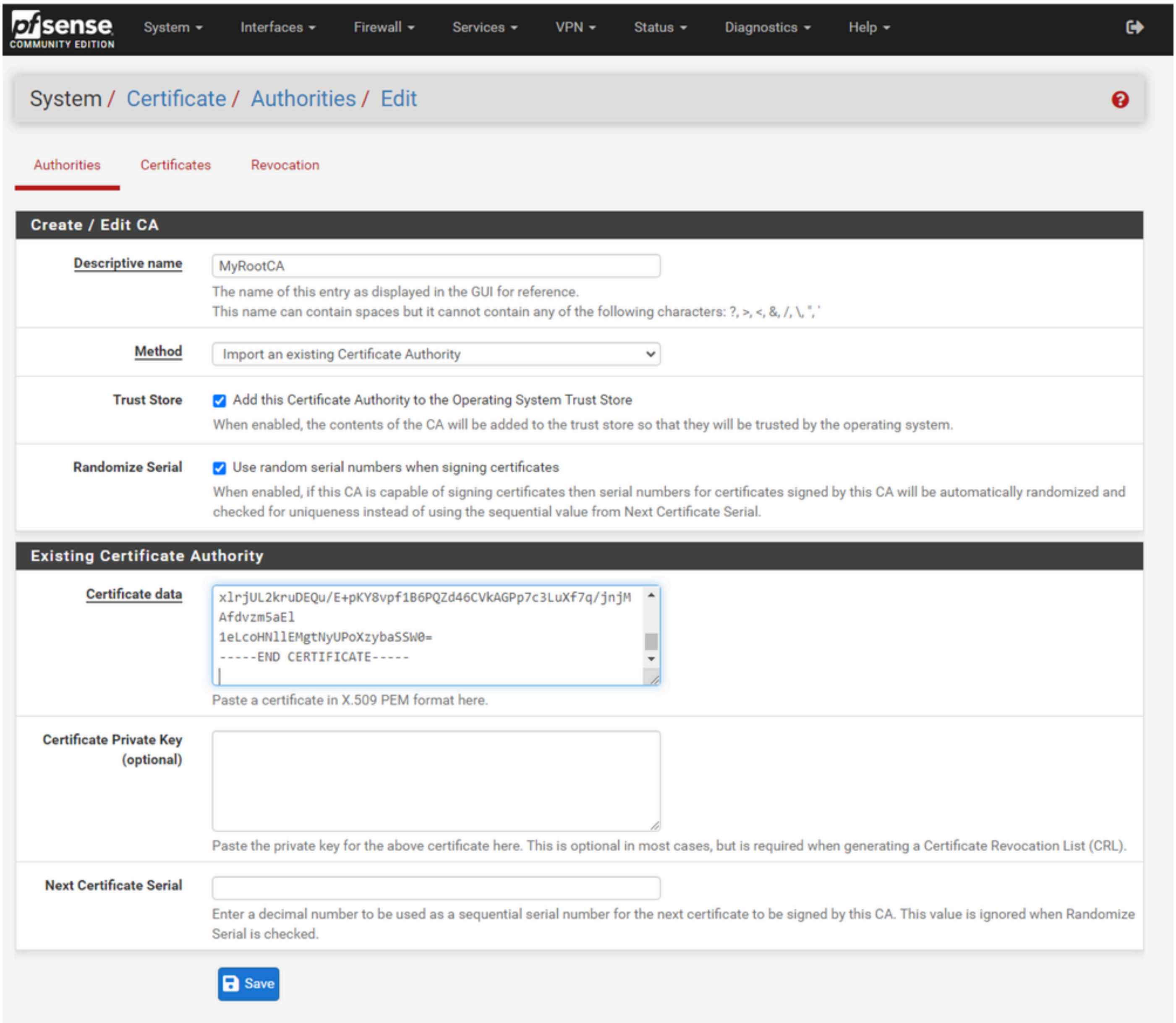
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

| Name | Internal | Issuer | Certificates | Distinguished Name | In Use | Actions |
|---|---|---|---|---|---|---|

*pfSense GUI - CA Certificates List*

Select the **Add** button.



System / Certificate / Authorities / Edit

**Create / Edit CA**

**Descriptive name**: MyRootCA

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**: Import an existing Certificate Authority

**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**:

```
xlrjUL2kruDEQu/E+pKY8vpf1B6PQZd46CVkAGPp7c3LuXf7q/jnjM
Afdvzm5aEl
1eLcoHNlIEMgtNyUPoXzybaSSW0=
-----END CERTIFICATE-----
```

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.

*pfSense GUI - CA Import*

As shown in the image:

1. Provide a unique, descriptive name

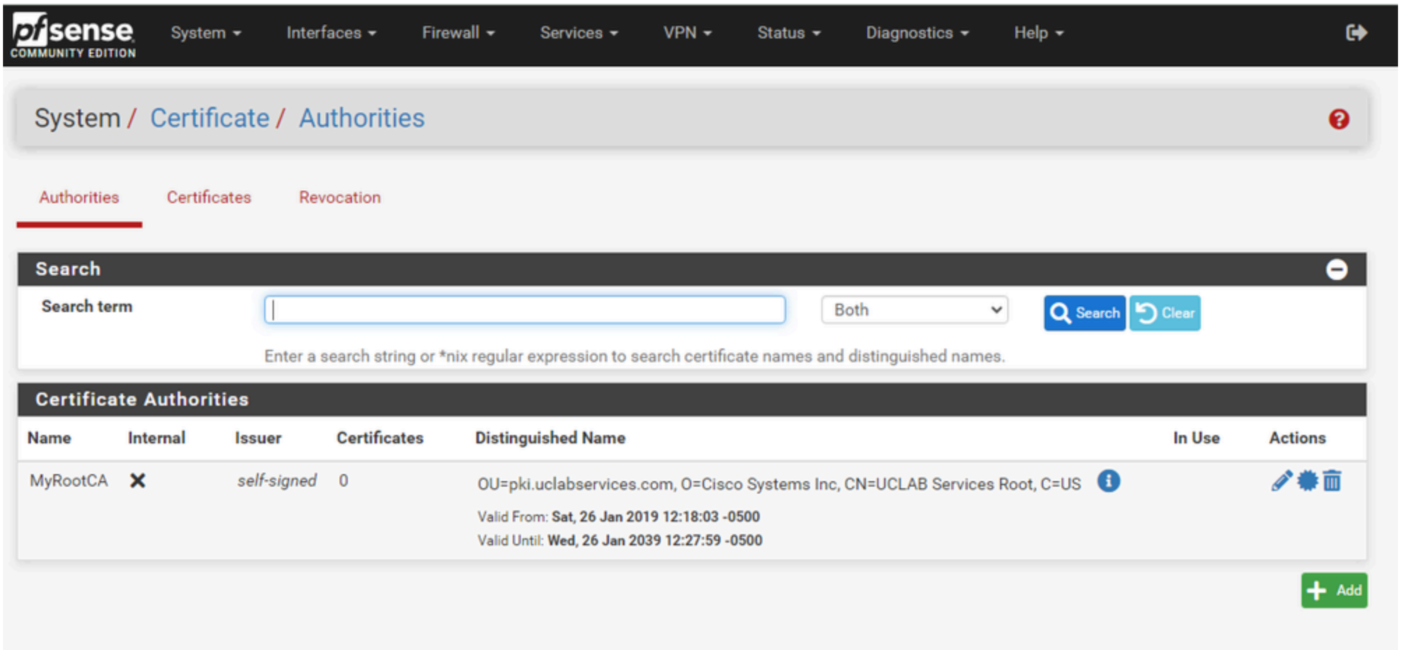
2. Select Import an existing Certificate Authority from the Method drop-down.

3. Ensure that the Trust Store and Randomize Serial check-boxes are selected.

4. Paste the entire certificate into the Certificate data text box. Ensure that you include from the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.

5. Select **Save**.

6. Verify that the Certificate is imported as shown in the image.



System / Certificate / Authorities

**Search**

Search term: Both

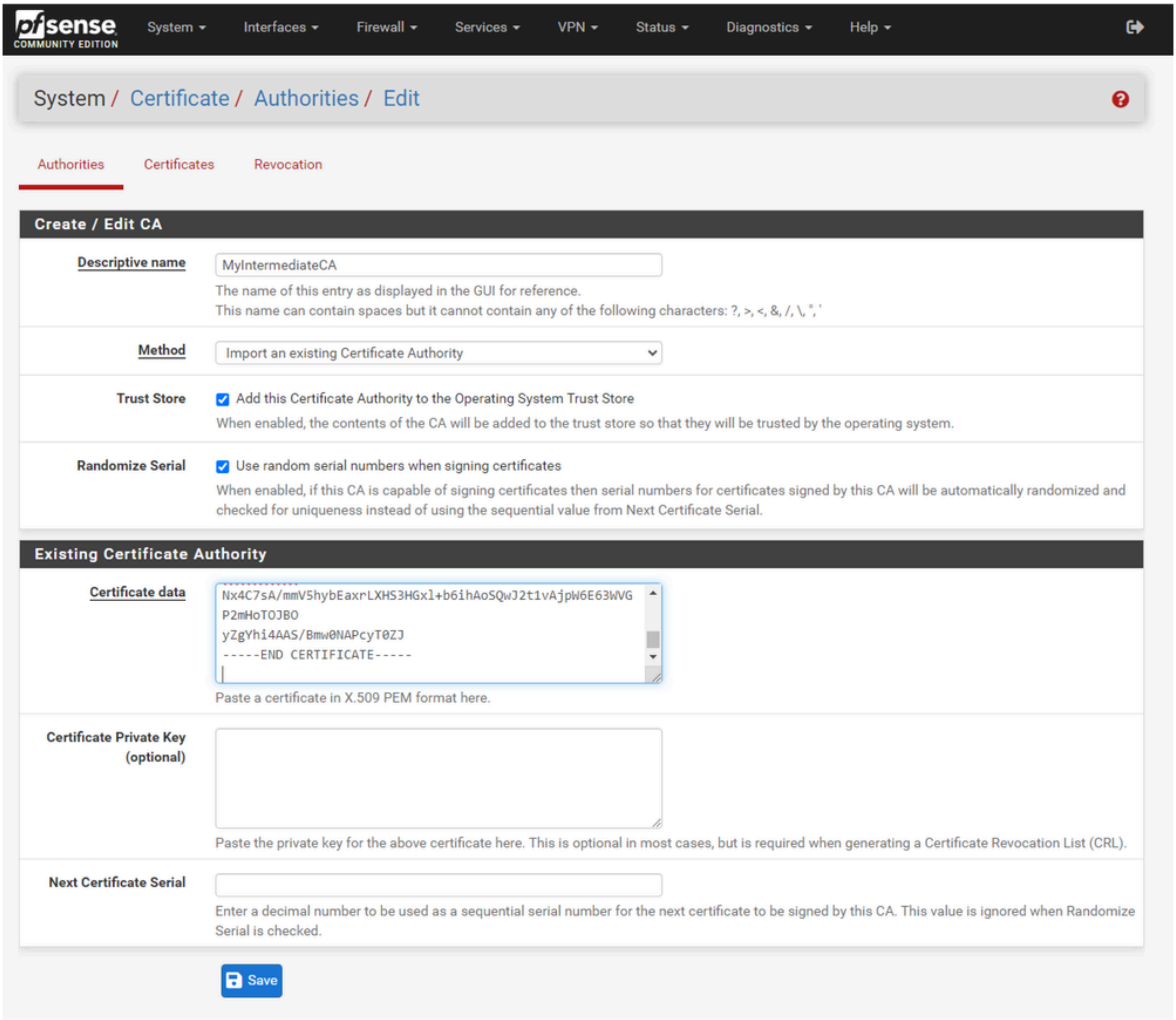
Enter a search string or *nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

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

*pfSense GUI - CA List*

## Step 3. Import the CA Intermediate Certificate



System / Certificate / Authorities / Edit

**Create / Edit CA**

**Descriptive name**: MyIntermediateCA

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**: Import an existing Certificate Authority

**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**:

```
Nx4C7sA/mmV5hybEaxrLXHS3HGxl+b6ihAoSQwJ2t1vAjpW6E63WVG
P2mHoTOJBO
yZgYhi4AAS/Bmw0NAPcyT0ZJ
-----END CERTIFICATE-----
```

Paste a certificate in X.509 PEM format here.

**Certificate Private Key (optional)**:

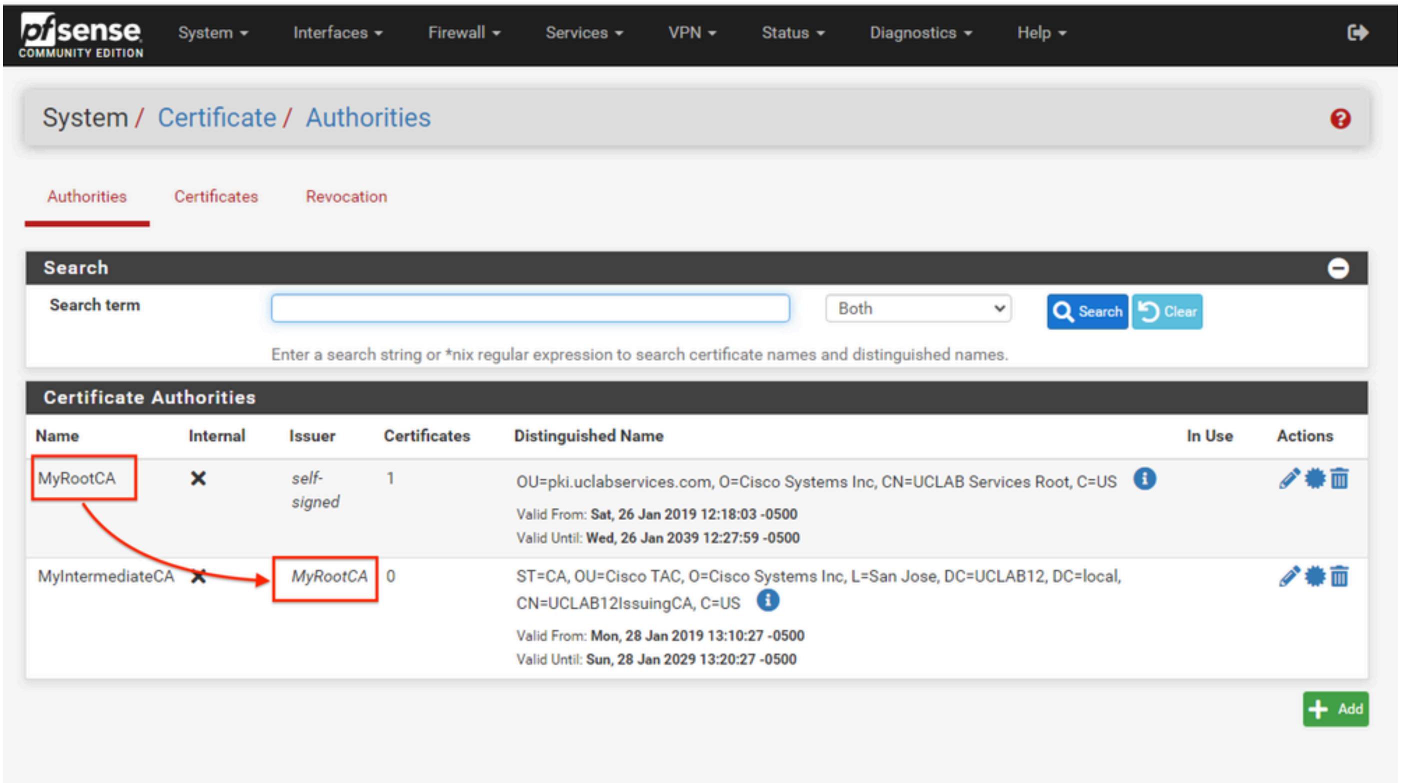
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

**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.

*pfSense GUI - CA Intermediate Import*

Repeat the steps to import the root CA certificate to import the intermediate CA certificate.



Search term

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 ℹ<br>Valid From: **Sat, 26 Jan 2019 12:18:03 -0500**<br>Valid Until: **Wed, 26 Jan 2039 12:27:59 -0500** | | ✎ ✹ 🗑 |
| MyIntermediateCA | ✗ | *MyRootCA* | 0 | ST=CA, OU=Cisco TAC, O=Cisco Systems Inc, L=San Jose, DC=UCLAB12, DC=local, CN=UCLAB12IssuingCA, C=US ℹ<br>Valid From: **Mon, 28 Jan 2019 13:10:27 -0500**<br>Valid Until: **Sun, 28 Jan 2029 13:20:27 -0500** | | ✎ ✹ 🗑 |

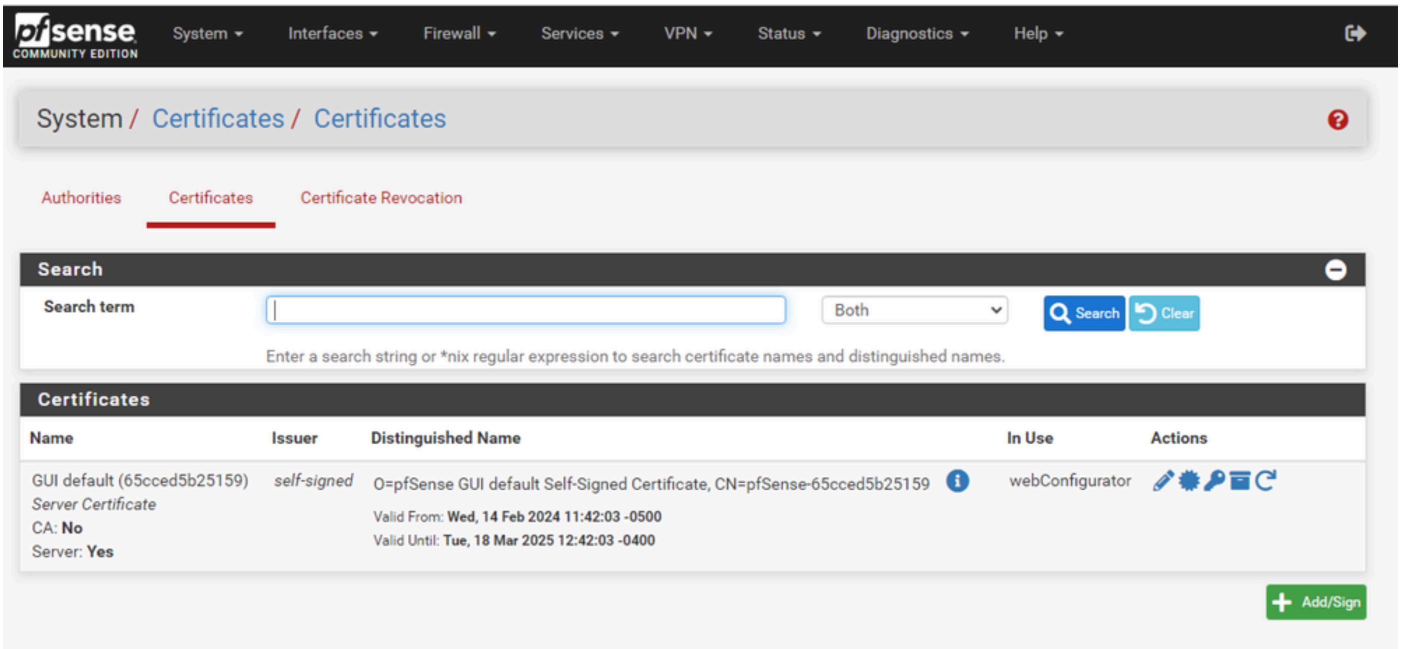
*pfSense GUI - CA Links*

Review the Certificate Authorities to ensure that the Intermediate is correctly chained to the root certificate as shown in the image.

### Step 4. Create and Export a CSR for the load-balanced web-site

This describes the steps to create a CSR, export the CSR, then import the signed certificate. If you already have an existing certificate in a PFX format, you can import this certificate. Consult the pfSense documentation for these steps.

1. Select the Certificates menu, then select the **Add/Sign** button.



Search term

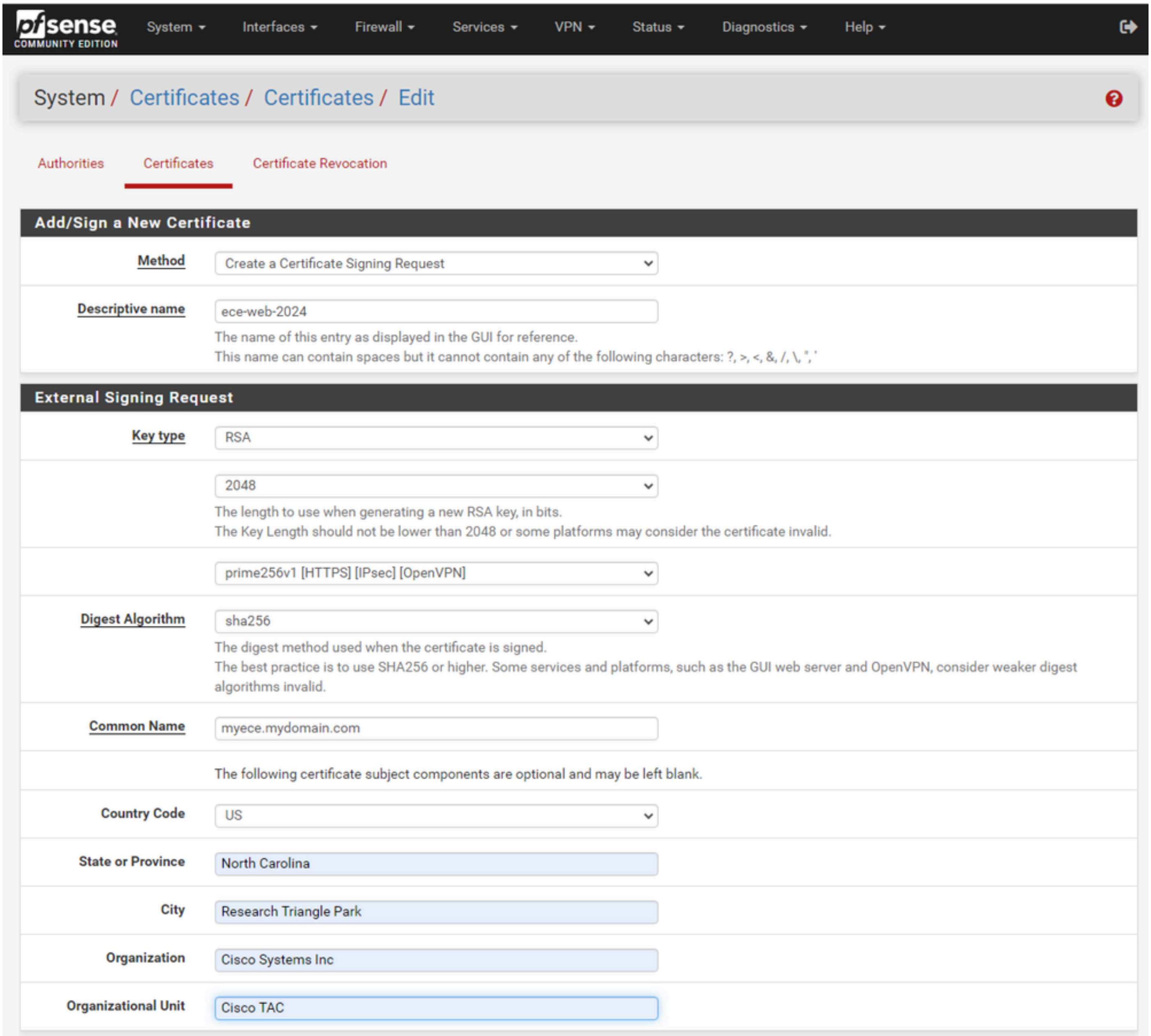
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|---|---|---|---|
| GUI default (65cced5b25159)<br>*Server Certificate*<br>CA: **No**<br>Server: **Yes** | *self-signed* | O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 ℹ<br>Valid From: **Wed, 14 Feb 2024 11:42:03 -0500**<br>Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400** | webConfigurator | ✎ ✹ 🔑 ▬ ↻ |

*pfSense GUI - Certificates List*

2. Complete the Certificate Signing Request form.



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

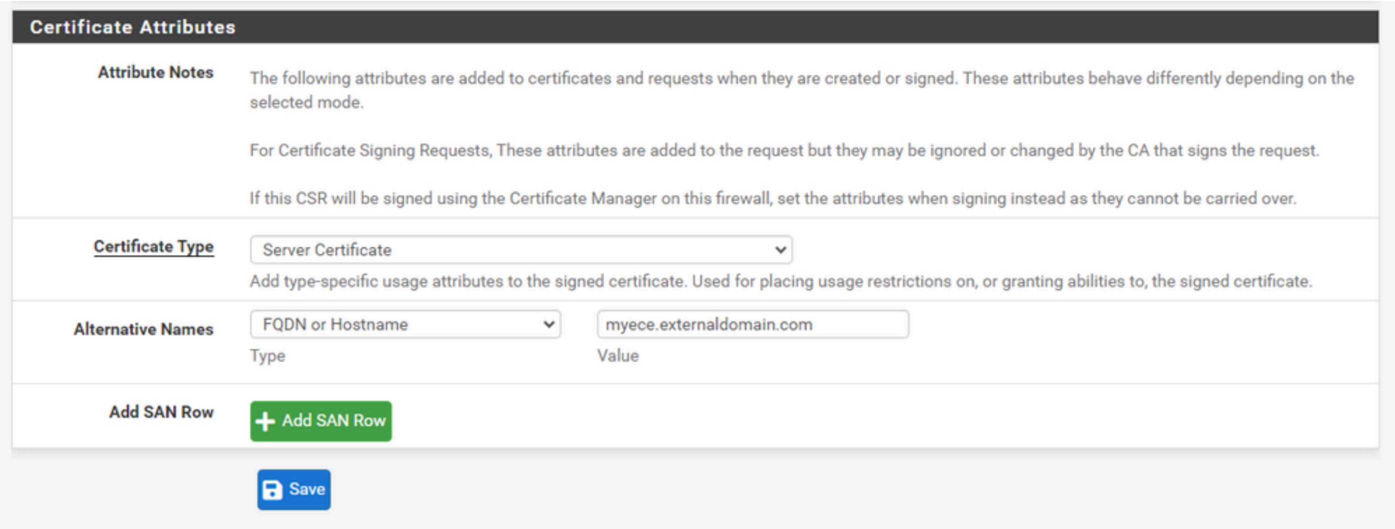
City: Research Triangle Park

Organization: Cisco Systems Inc

Organizational Unit: Cisco TAC

*pfSense GUI - CSR Creation*

- Method: Select Create a Certificate Signing Request from the drop-down
- Descriptive Name: Provide a name for the certificate
- Key type and Digest Algorithm: Review to ensure they match your requirements
- Common Name: Provide the fully qualified domain name web-site
- Provide the remaining certificate information as required for your environment



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

Alternative Names: FQDN or Hostname (Type) myece.externaldomain.com (Value)

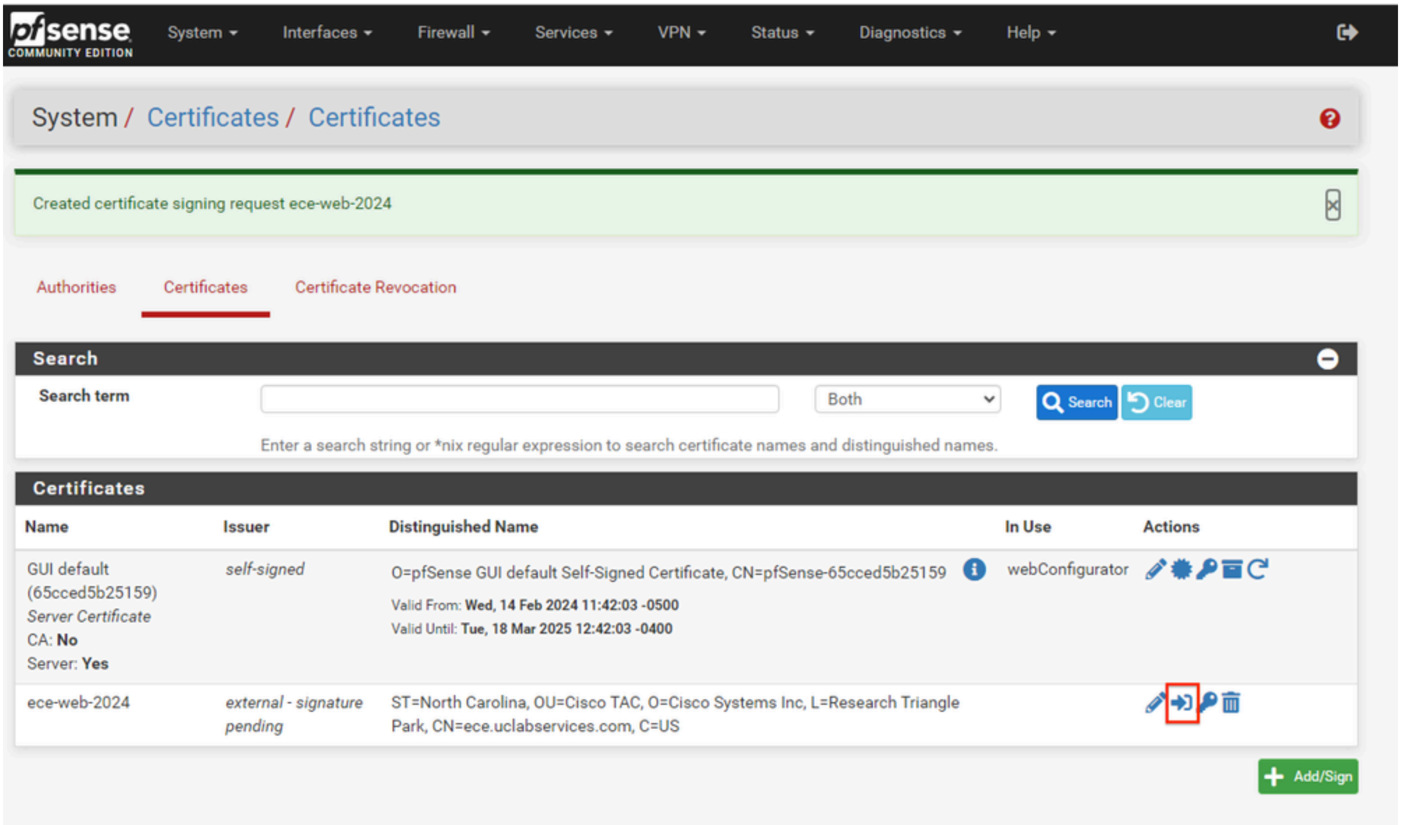
*pfSense GUI - CSR Advanced*

- Certificate Type: Select Server Certificate in the drop-down.
- Alternative Names: Provide any Subject Alternative Names (SAN) required for your implementation.

**Note**: The common name is automatically added to the SAN field. You only need to add additional names required.

Select **Save** once all fields are correct.

3. Export the CSR to a file.



System / Certificates / Certificates

Created certificate signing request ece-web-2024

**Search**

Search term: Both
Enter a search string or *nix regular expression to search certificate names and distinguished names.

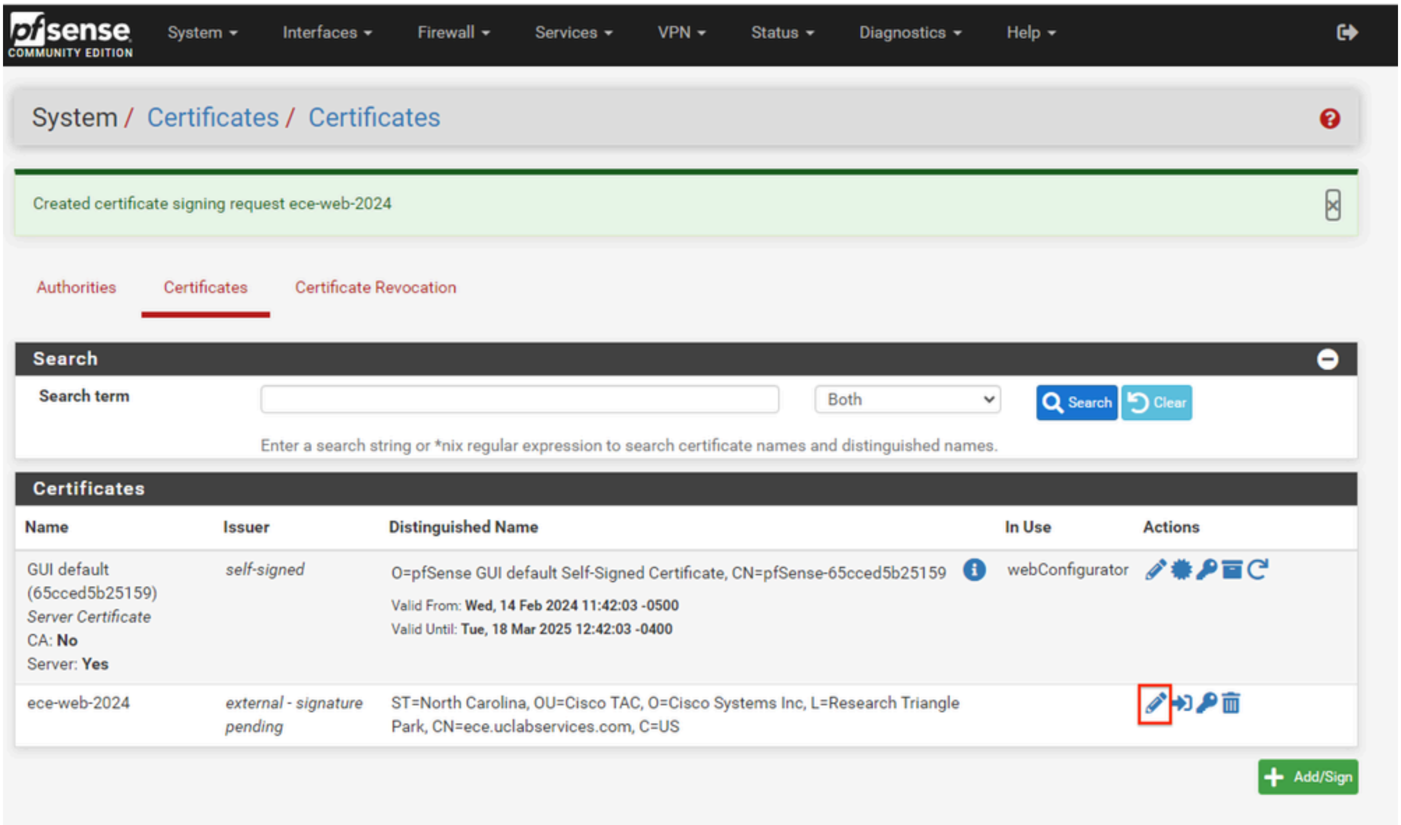
**Certificates**

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|---|---|---|---|
| GUI default (65cced5b25159)<br>*Server Certificate*<br>CA: **No**<br>Server: **Yes** | *self-signed* | O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159<br>Valid From: **Wed, 14 Feb 2024 11:42:03 -0500**<br>Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400** | 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 | | |

*pfSense GUI - CSR Export*

Select the Export button to save the CSR, then sign this with your CA. Once you have the signed certificate, save this as a PEM or Base-64 file to complete the process.

4. Import the signed certificate.



Created certificate signing request ece-web-2024

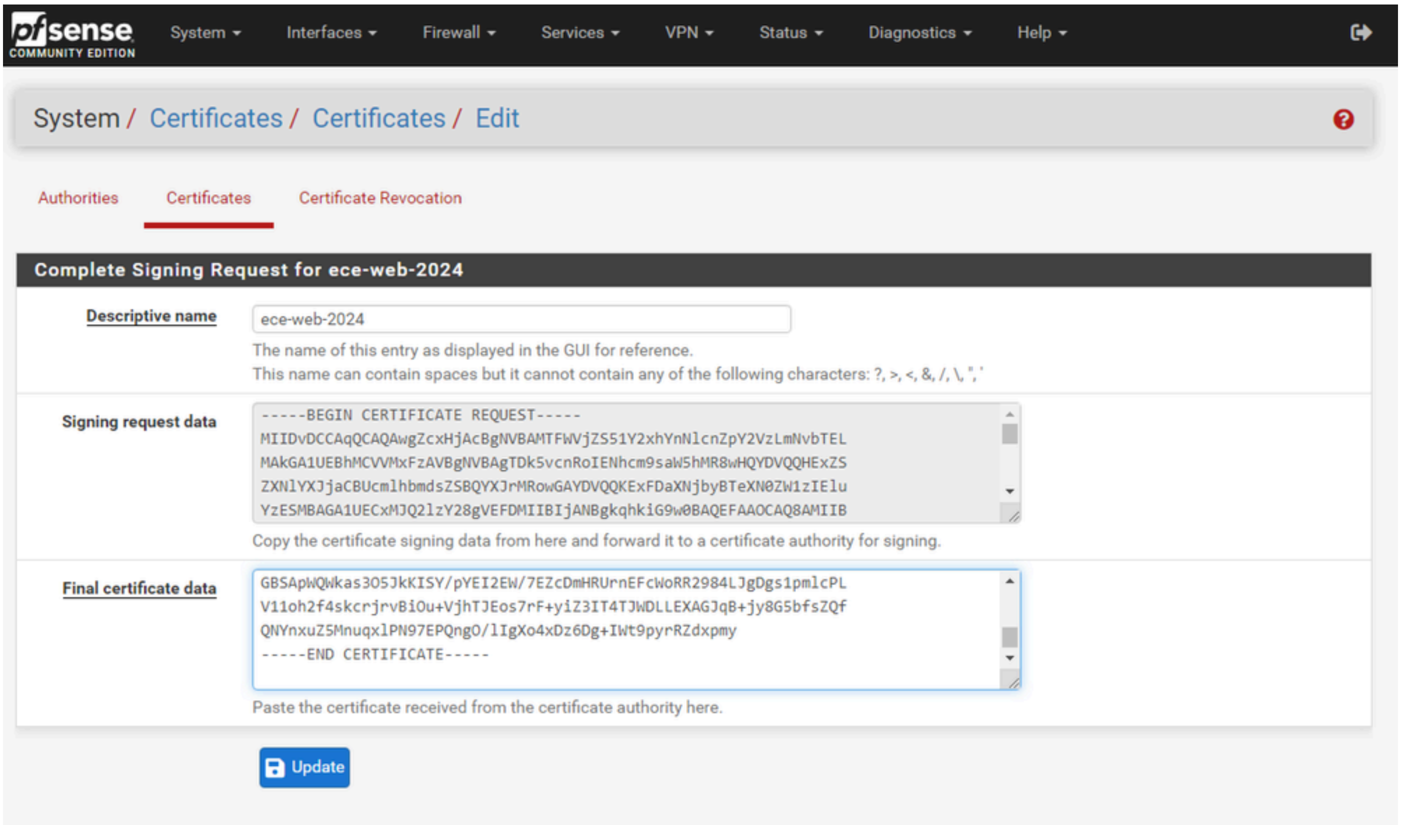
Enter a search string or *nix regular expression to search certificate names and distinguished names.

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|---|---|---|---|
| GUI default (65cced5b25159)<br>*Server Certificate*<br>CA: **No**<br>Server: **Yes** | *self-signed* | O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159<br>Valid From: **Wed, 14 Feb 2024 11:42:03 -0500**<br>Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400** | 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 | | |

*pfSense GUI - Certificate Import*

Select the Pencil icon to import the signed certificate.

5. Paste the certificate data in the form.



System / Certificates / Certificates / Edit

**Complete Signing Request for ece-web-2024**

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: ?, >, <, &, /, \, ", '

Signing request data:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDvDCCAqQCAQAwgZcxHjAcBgNVBAMTFWVjZS51Y2xhYnNlcnZpY2VzLmNvbTEL
MAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMR8wHQYDVQQHExZS
ZXNlYXJjaCBUcmlhbmdsZSBQYXJrMRowGAYDVQQKExFDaXNjbyBTeXN0ZW1zIElu
YzESMBAGA1UECxMJQ2lzY28gVEFDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

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

Final certificate data:

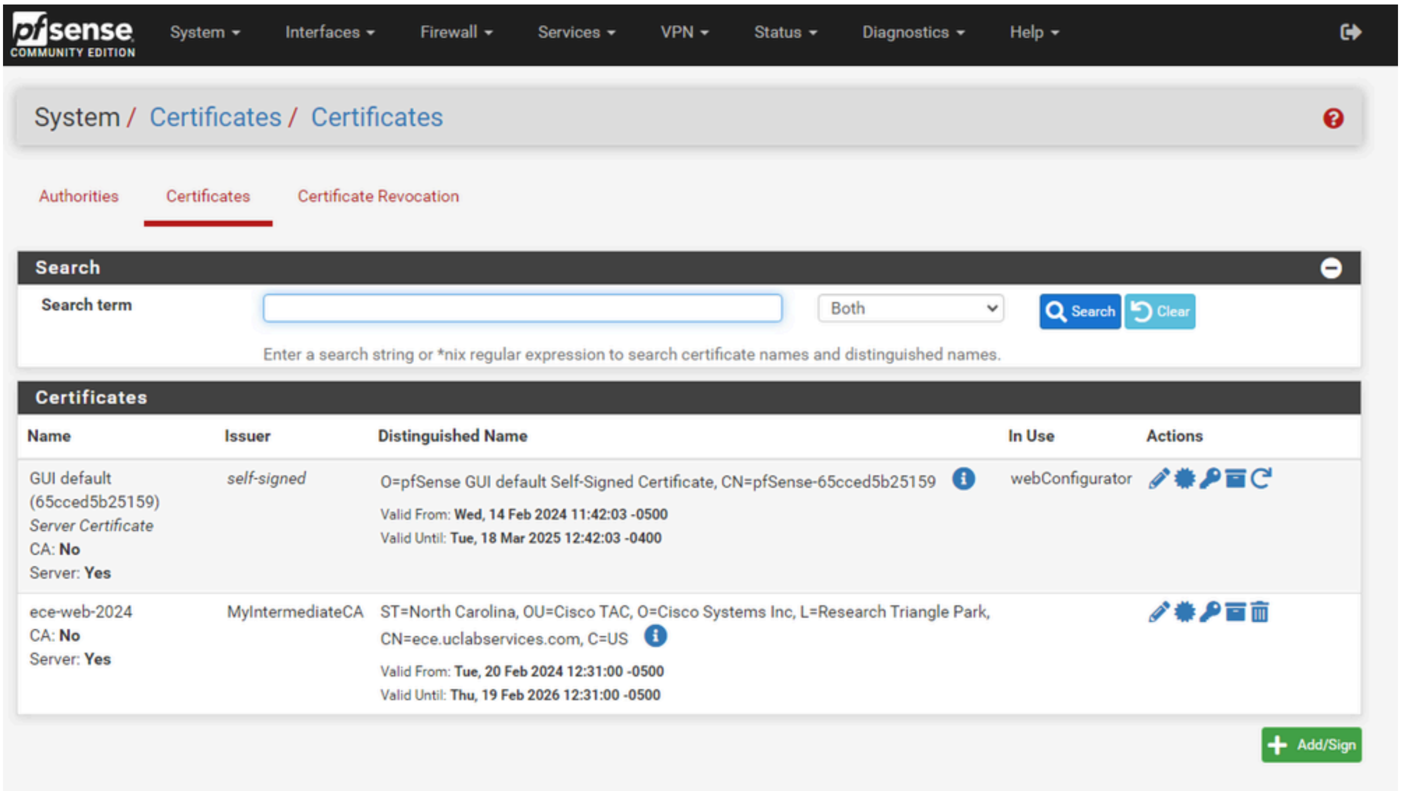
```
GBSApWQWkas3O5JkKISY/pYEI2EW/7EZcDmHRUrnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yiZ3IT4TJWDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5MnuqxlPN97EPQngO/lIgXo4xDz6Dg+IWt9pyrRZdxpmy
-----END CERTIFICATE-----
```

Paste the certificate received from the certificate authority here.

*pfSense GUI - Certificate Import*

Select **Update** to save the certificate.

6. Review the certificate data to ensure it is correct.



System / Certificates / Certificates

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

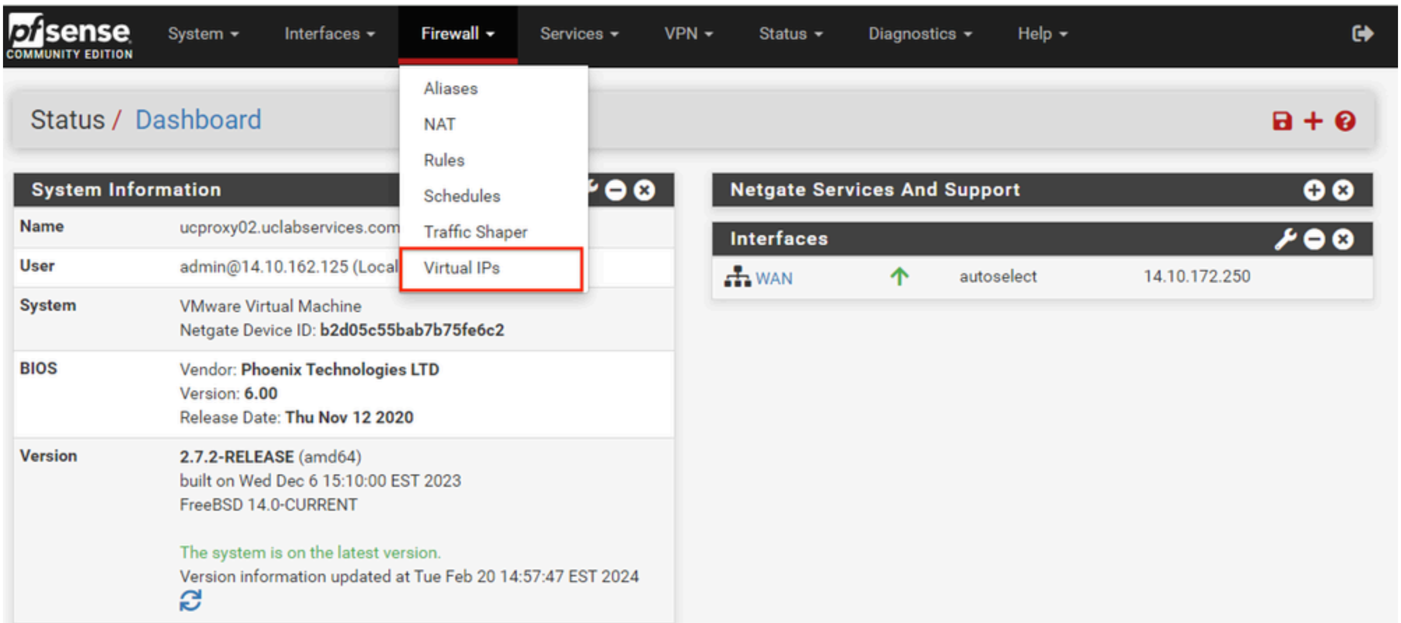
*pfSense GUI - Certificate List*

7. Repeat this process if you wish to host multiple sites on this pfSense.

## Add Virtual IPs

At least one IP is required to host websites on the pfSense. In pfSense this is done with Virtual IPs (VIPs).

### Step 1. Select Virtual IPs from the Firewall drop-down



Status / Dashboard

**System Information**

| | |
|---|---|
| Name | ucproxy02.uclabservices.com |
| User | admin@14.10.162.125 (Local |
| System | VMware Virtual Machine<br>Netgate Device ID: **b2d05c55bab7b75fe6c2** |
| BIOS | Vendor: **Phoenix Technologies LTD**<br>Version: **6.00**<br>Release Date: **Thu Nov 12 2020** |
| Version | **2.7.2-RELEASE** (amd64)<br>built on Wed Dec 6 15:10:00 EST 2023<br>FreeBSD 14.0-CURRENT<br>The system is on the latest version.<br>Version information updated at Tue Feb 20 14:57:47 EST 2024 |

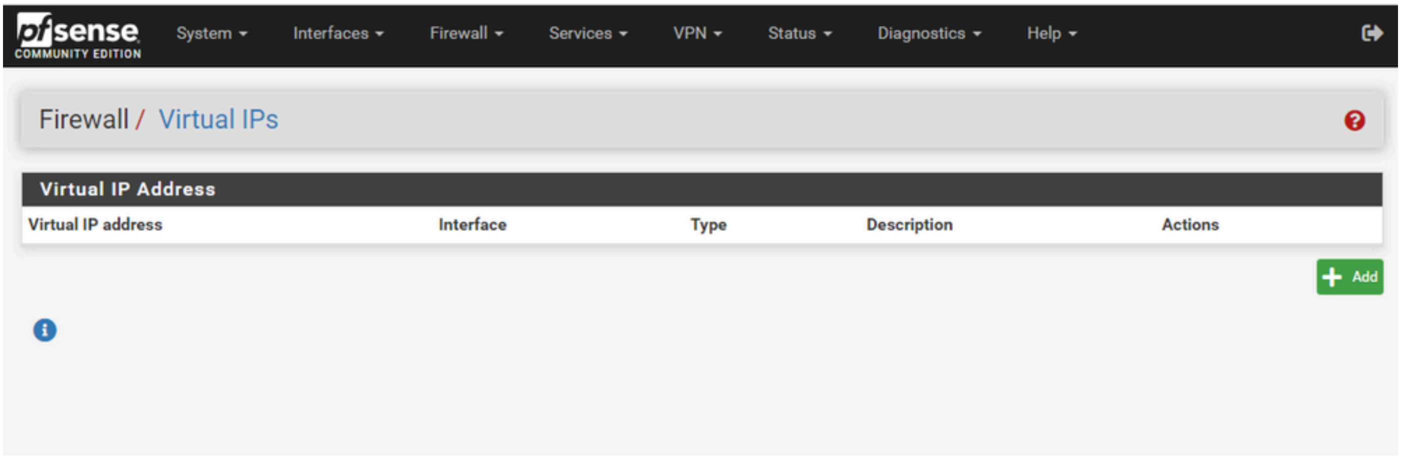
**Netgate Services And Support**

**Interfaces**

| | | |
|---|---|---|
| WAN | autoselect | 14.10.172.250 |

*pfSense GUI - VIP Dropdown*

### Step 2. Select the Add button



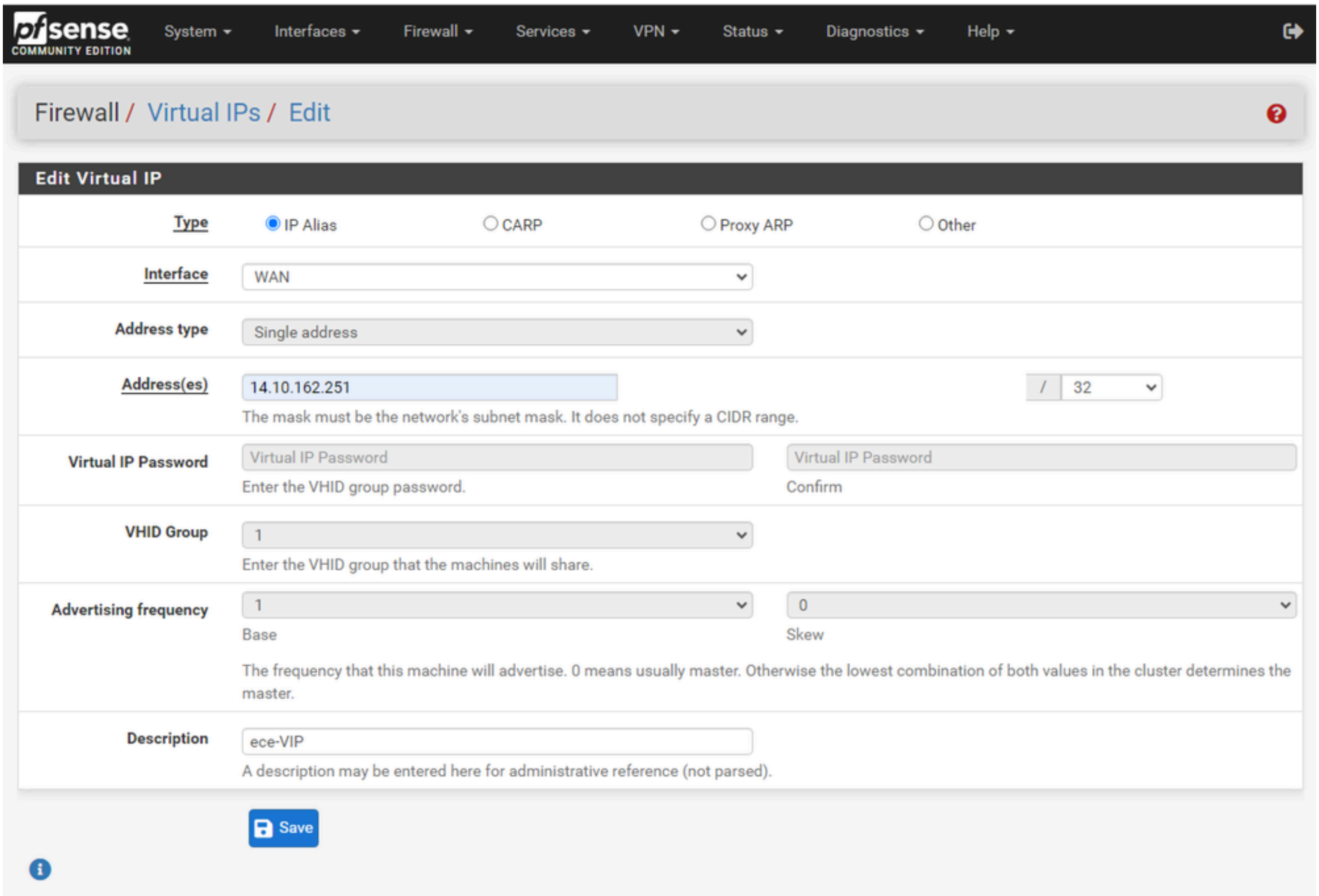
Firewall / Virtual IPs

**Virtual IP Address**

| Virtual IP address | Interface | Type | Description | Actions |
|---|---|---|---|---|

*pfSense GUI - VIP Landing Page*

### Step 3. Provide Address information



Firewall / Virtual IPs / Edit

Edit Virtual IP

| | |
|---|---|
| Type | ● IP Alias ○ CARP ○ Proxy ARP ○ Other |
| Interface | WAN |
| Address type | Single address |
| Address(es) | 14.10.162.251 / 32<br>The mask must be the network's subnet mask. It does not specify a CIDR range. |
| Virtual IP Password | Virtual IP Password<br>Enter the VHID group password.<br>Virtual IP Password<br>Confirm |
| VHID Group | 1<br>Enter the VHID group that the machines will share. |
| Advertising frequency | 1<br>Base<br>0<br>Skew<br>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 | ece-VIP<br>A description may be entered here for administrative reference (not parsed). |

*pfSense GUI - VIP Configuration*

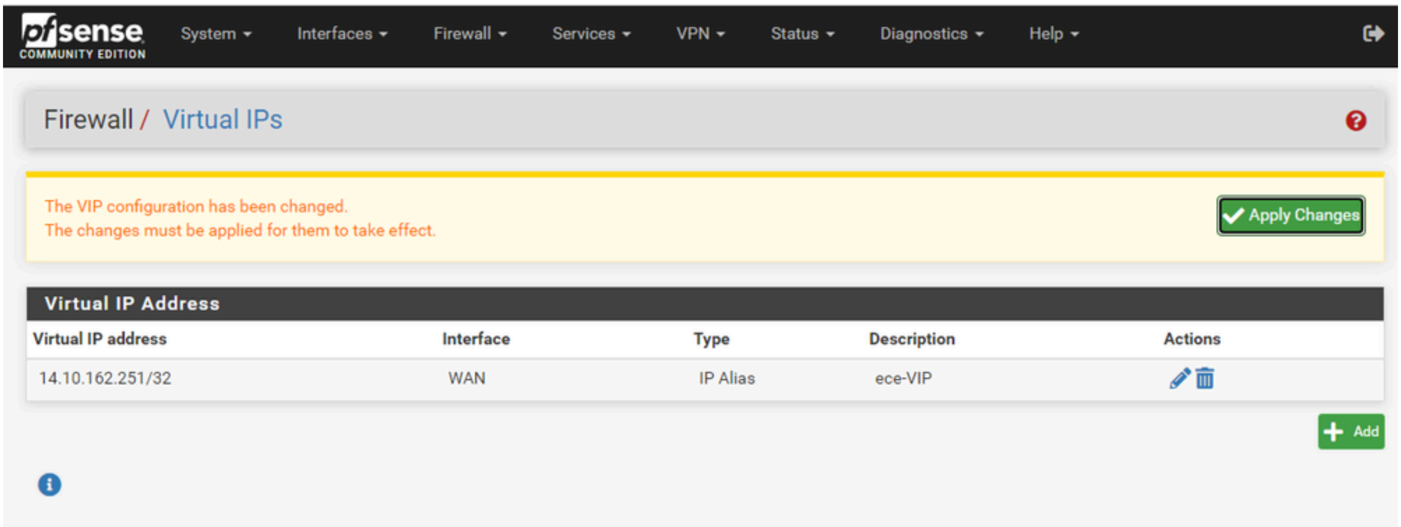
Use the information to add a VIP.

- Type: Select IP Alias
- Interface: Select the interface for this IP Address to be broadcast
- Address(es): Enter the IP Address
- Address Mask: For IP addresses used for load-balancing, the mask must be a /32
- Description: Provide a short text to make it easier to understand the configuration later

Select **Save** to commit the change.

Repeat this for each IP Address required for your configuration.

### Step 4. Apply Configuration



Firewall / Virtual IPs

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

Virtual IP Address

| Virtual IP address | Interface | Type | Description | Actions |
|---|---|---|---|---|
| 14.10.162.251/32 | WAN | IP Alias | ece-VIP | |

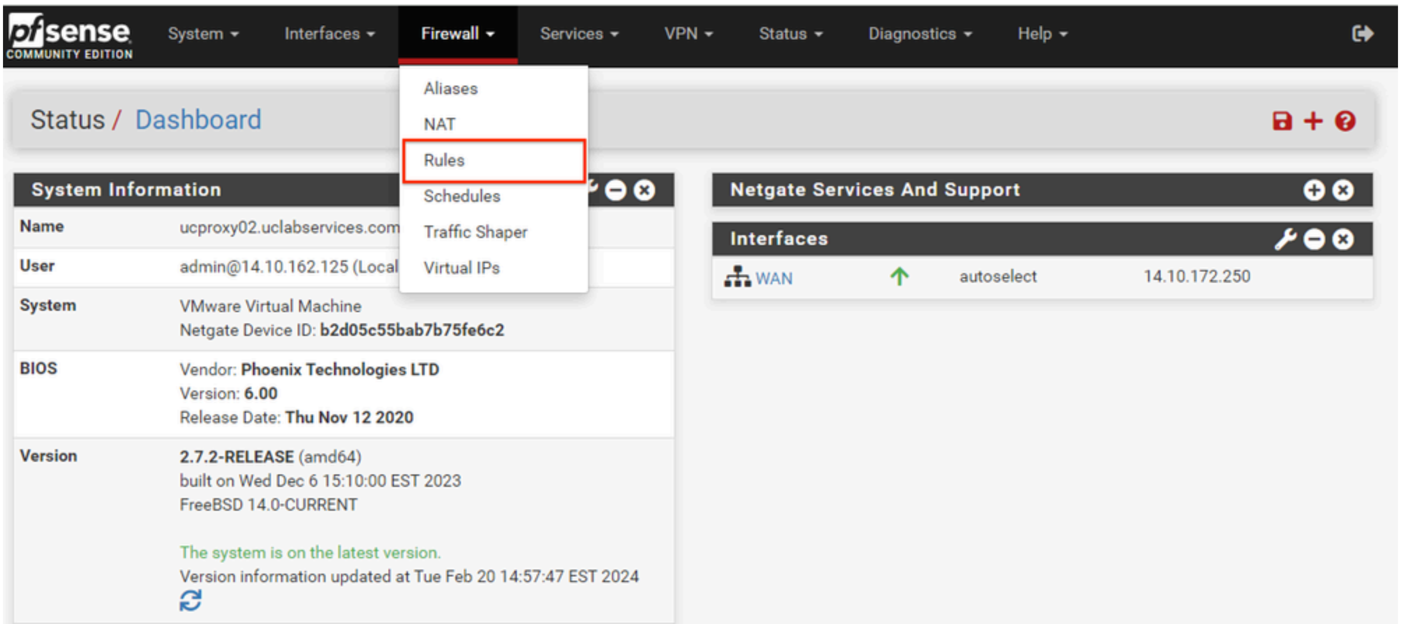
*pfSense GUI - VIP List*

Select the, **Apply Changes** button after all VIPs have been added.

## Configure Firewall

pfSense has a built-in firewall. The default rule-set is very limited. Before the appliance is put into production, ensure that you build a comprehensive firewall policy.

### Step 1. Select Rules from the Firewall drop-down



Status / Dashboard

System Information

| | |
|---|---|
| Name | ucproxy02.uclabservices.com |
| User | admin@14.10.162.125 (Local |
| System | VMware Virtual Machine<br>Netgate Device ID: **b2d05c55bab7b75fe6c2** |
| BIOS | Vendor: **Phoenix Technologies LTD**<br>Version: **6.00**<br>Release Date: **Thu Nov 12 2020** |
| Version | **2.7.2-RELEASE** (amd64)<br>built on Wed Dec 6 15:10:00 EST 2023<br>FreeBSD 14.0-CURRENT<br>The system is on the latest version.<br>Version information updated at Tue Feb 20 14:57:47 EST 2024 |

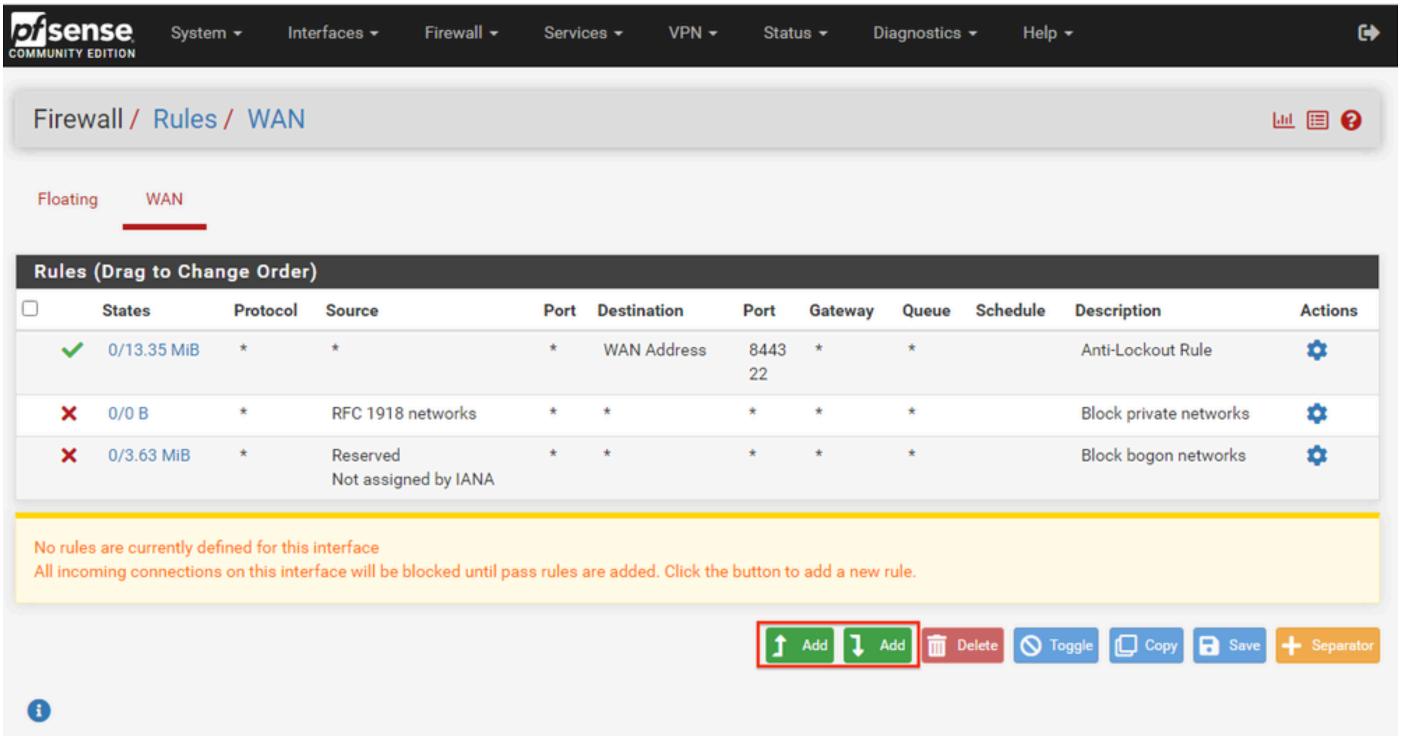
Netgate Services And Support

Interfaces

| | | | |
|---|---|---|---|
| WAN | ↑ | autoselect | 14.10.172.250 |

*pfSense GUI - Firewall Rules Dropdown*

### Step 2. Select one of the Add buttons



Firewall / Rules / WAN

Rules (Drag to Change Order)

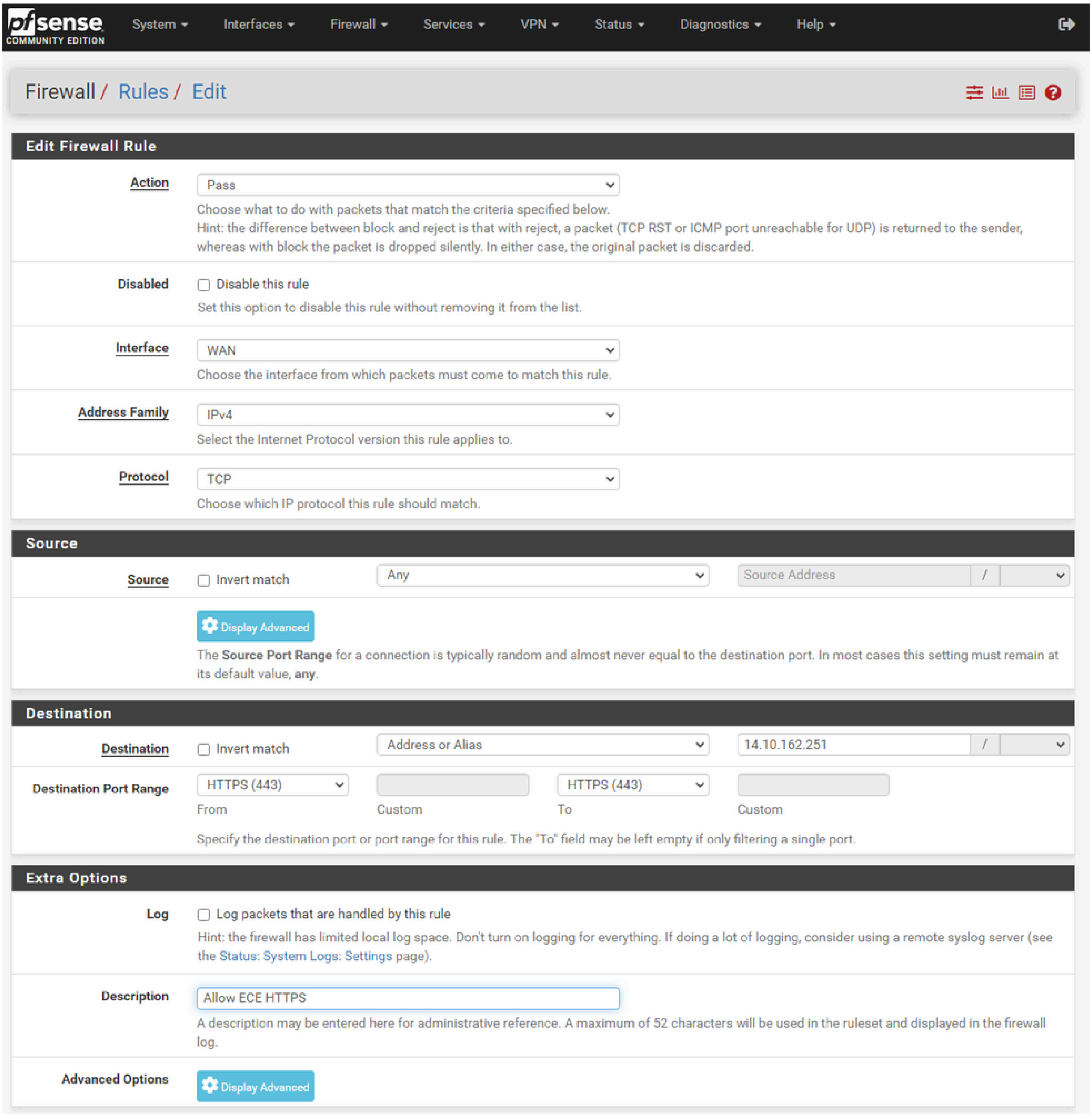
| ☐ | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 0/13.35 MiB | * | * | * | WAN Address | 8443<br>22 | * | * | | Anti-Lockout Rule | ⚙ |
| ✗ | 0/0 B | * | RFC 1918 networks | * | * | * | * | * | | Block private networks | ⚙ |
| ✗ | 0/3.63 MiB | * | Reserved<br>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.

*pfSense GUI - Firewall Rules List*

Note that one button adds the new rule above the selected line while the other adds the rule below the selected rule. Either button can be used for the first rule.

### Step 3. Create firewall rule to allow traffic to port 443 for the IP address



Firewall / Rules / Edit

**Edit Firewall Rule**

**Action**: Pass

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**: WAN

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

**Address Family**: IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**: TCP

Choose which IP protocol this rule should match.

**Source**

**Source**: □ Invert match | Any | Source Address /

Display Advanced

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 | Address or Alias | 14.10.162.251 /

**Destination Port Range**: HTTPS (443) From | Custom | HTTPS (443) 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**: Allow ECE HTTPS

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**: Display Advanced

*pfSense GUI - Firewall Pass Rule Configuration*

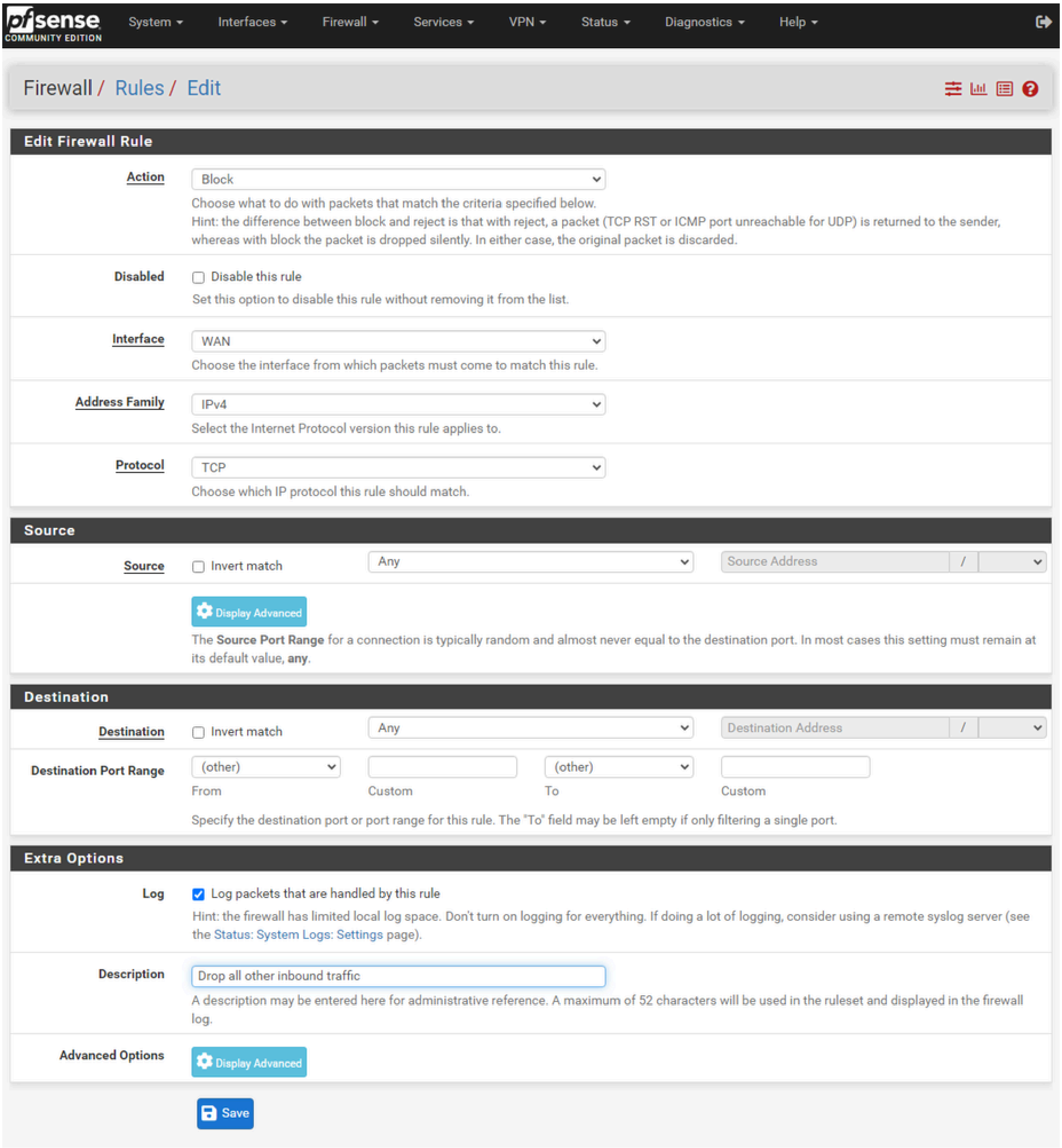
Use the information to create the rule.

- Action: Select Pass
- Interface: Choose the Interface the rule applies to
- Address Family and Protocol: Select as appropriate
- Source: Leave selected as Any
- Destination: Select Address or Alias from the Destination drop-down, then enter the IP address the rule applies to
- Destination Port Range: Select, HTTPS (443) in both the From and To drop-down
- Log: Select the check-box to log any packets which match this rule for accounting
- Description: Provide text to refer to the rule later

Select **Save**.

### Step 4. Create a firewall rule to drop all other traffic to the pfSense

Select the Add button to insert the rule below the newly created rule.



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

Firewall / Rules / Edit

**Edit Firewall Rule**

Action: Block

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: WAN

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

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

**Source**

Source: □ Invert match Any Source Address /

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 Any Destination Address /

Destination Port Range: (other) From, Custom, (other) 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: Drop all other inbound traffic

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:

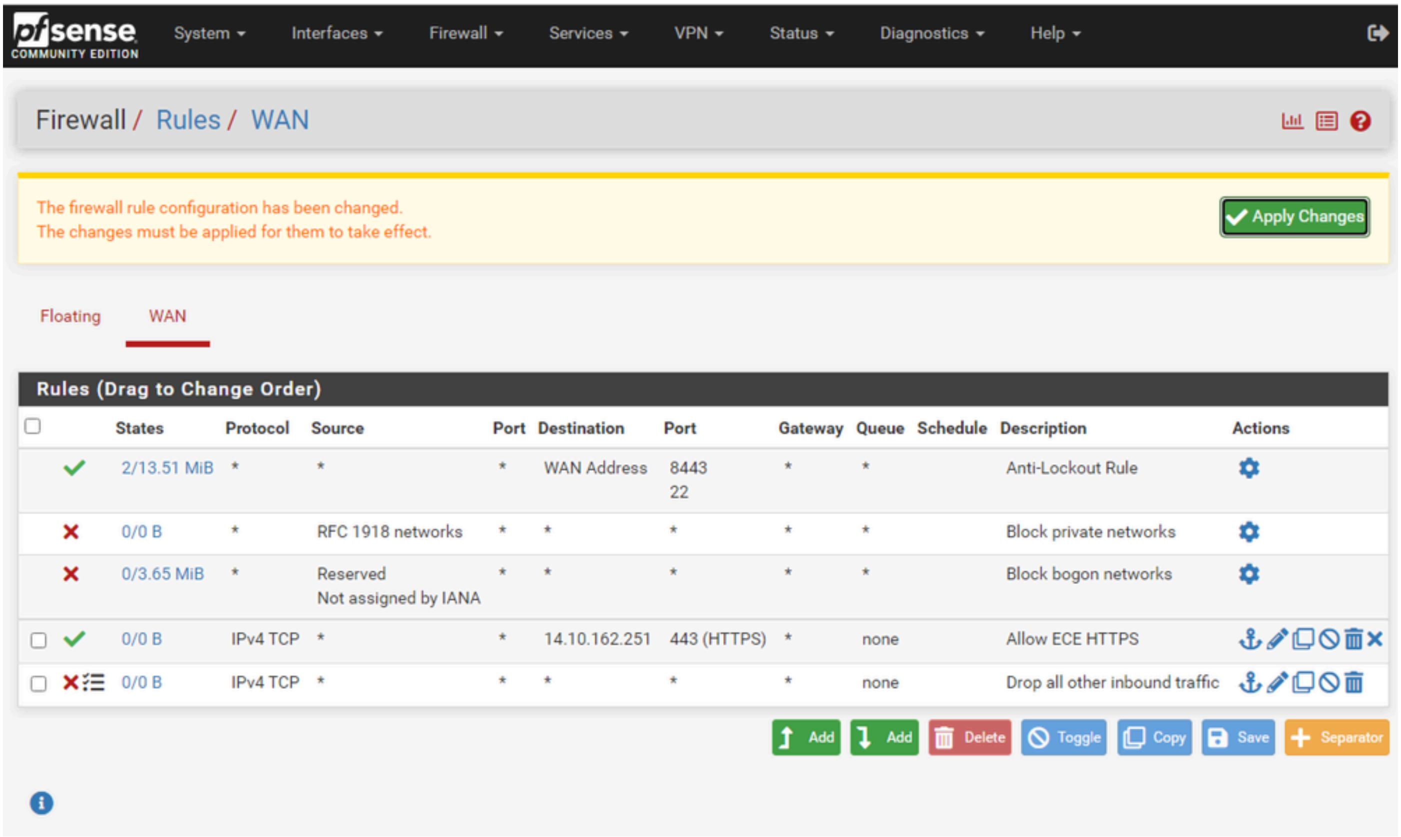
*pfSense GUI - Firewall Drop Rule Configuration*

- Action: Select Block
- Interface: Choose the Interface the rule applies to
- Address Family and Protocol: Select as appropriate
- Source: Leave selected as Any
- Destination: Leave selected as Any
- Log: Select the check-box to log any packets which match this rule for accounting

- Description: Provide text to refer to the rule later

Select **Save**.

### Step 5. Review the rules and ensure that the block rule is at the bottom



Firewall / Rules / WAN

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

Rules (Drag to Change Order)

| ☐ | | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ✓ | 2/13.51 MiB | * | * | * | WAN Address | 8443<br>22 | * | * | | Anti-Lockout Rule | ⚙ |
| | ✗ | 0/0 B | * | RFC 1918 networks | * | * | * | * | * | | Block private networks | ⚙ |
| | ✗ | 0/3.65 MiB | * | Reserved<br>Not assigned by IANA | * | * | * | * | * | | Block bogon networks | ⚙ |
| ☐ | ✓ | 0/0 B | IPv4 TCP | * | * | 14.10.162.251 | 443 (HTTPS) | * | none | | Allow ECE HTTPS | ⚓ ✎ ⧉ ⊘ 🗑 ✗ |
| ☐ | ✗ ☰ | 0/0 B | IPv4 TCP | * | * | * | * | * | none | | Drop all other inbound traffic | ⚓ ✎ ⧉ ⊘ 🗑 |

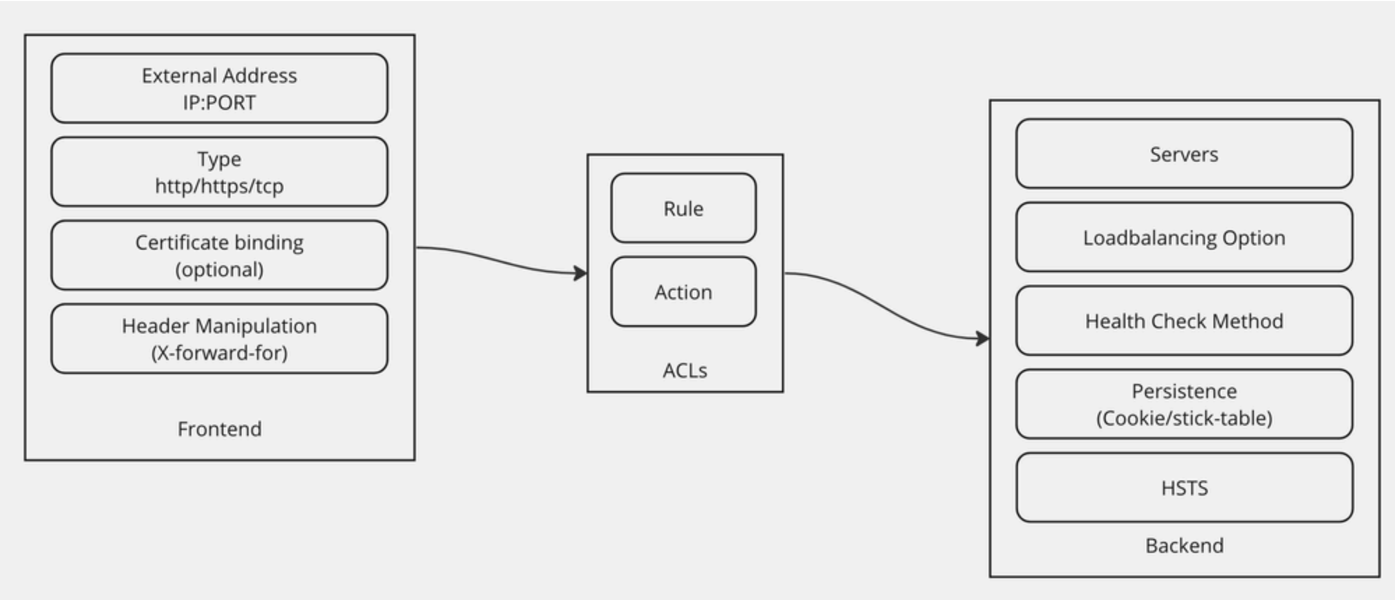
*pfSense GUI - Firewall Rules List*

If required, drag the rules to sort them.

Select, **Apply Changes** once the firewall rules are in the order required for your environment.

# Configure HAProxy

## HAProxy Concepts



*HAProxy Concepts*

HAProxy is implemented with a Frontend/Backend model.

The Frontend defines the side of the proxy that customers communicate with.

The Frontend consists of an IP and Port combination, certificate binding, and can implement some header manipulation.

The Backend defines the side of the proxy that communicates with the physical web servers.

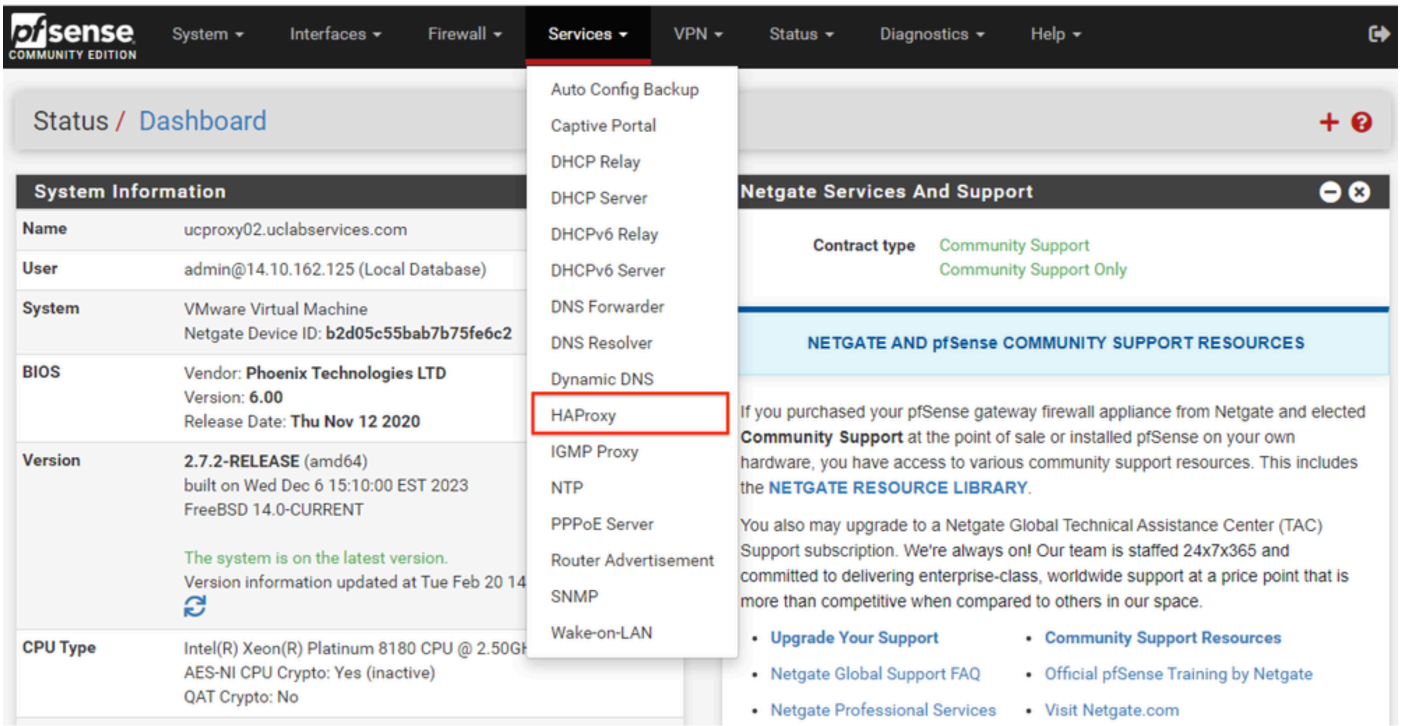
The Backend defines the actual servers and ports, the loadbalancing method for initial assignment, health checks, and persistence.

A Frontend knows what backend to communicate with by either a dedicated backend or by using ACLs.

ACLs can create different rules so that a given frontend can communicate with different backends depending on various things.

## Initial HAProxy Settings

### Step 1. Select HAProxy from the Services drop-down



Status / Dashboard

System Information

| | |
|---|---|
| Name | ucproxy02.uclabservices.com |
| User | admin@14.10.162.125 (Local Database) |
| System | VMware Virtual Machine<br>Netgate Device ID: **b2d05c55bab7b75fe6c2** |
| BIOS | Vendor: **Phoenix Technologies LTD**<br>Version: **6.00**<br>Release Date: **Thu Nov 12 2020** |
| Version | **2.7.2-RELEASE** (amd64)<br>built on Wed Dec 6 15:10:00 EST 2023<br>FreeBSD 14.0-CURRENT<br>The system is on the latest version.<br>Version information updated at Tue Feb 20 14 |
| CPU Type | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GH<br>AES-NI CPU Crypto: Yes (inactive)<br>QAT Crypto: No |

Netgate Services And Support

**Contract type** Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

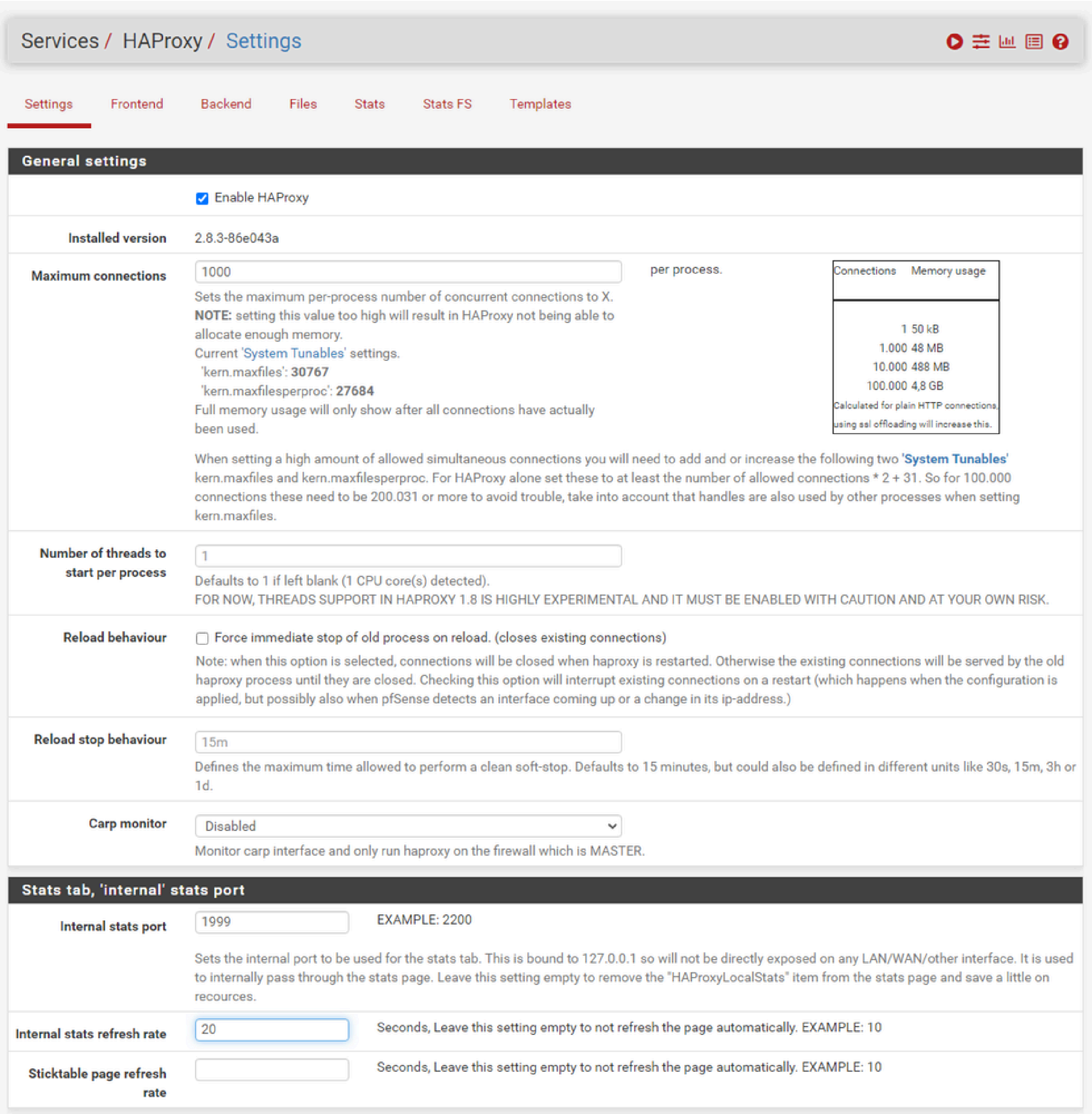
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team 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**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

*pfSense GUI - HAProxy Dropdown*

### Step 2. Configure basic settings



**General settings**

☑ Enable HAProxy

**Installed version** 2.8.3-86e043a

**Maximum connections** 1000 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.

| 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.

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.

**Number of threads to start per process** 1

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** 15m

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** Disabled

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

**Stats tab, 'internal' stats port**

**Internal stats port** 1999 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 recources.

**Internal stats refresh rate** 20 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

*pfSense GUI - HAProxy Main Settings*

Select the Enable HAProxy check-box.

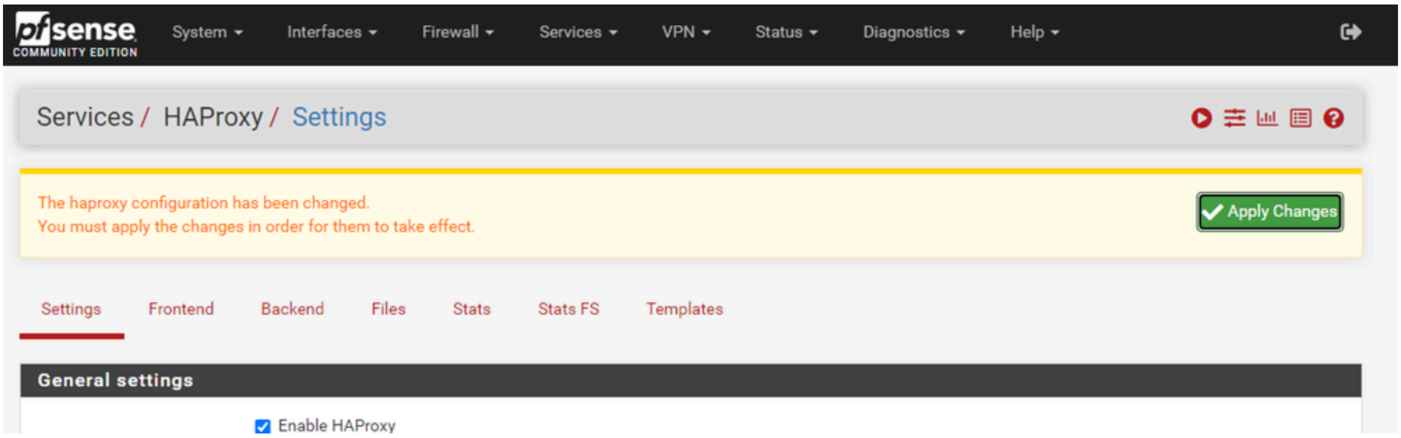
Enter a value for Maximum Connections. See the chart in this section for details on the memory required.

Enter a value for the Internal stats port. This port is used to show HAProxy statistics on the appliance but is not exposed outside of the appliance.

Enter a value for the Internal stats refresh rate.

Review the remaining configuration and update as required for your environment.

Select **Save.**



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

**General settings**

☑ Enable HAProxy

*pfSense GUI - HAProxy Apply Changes*

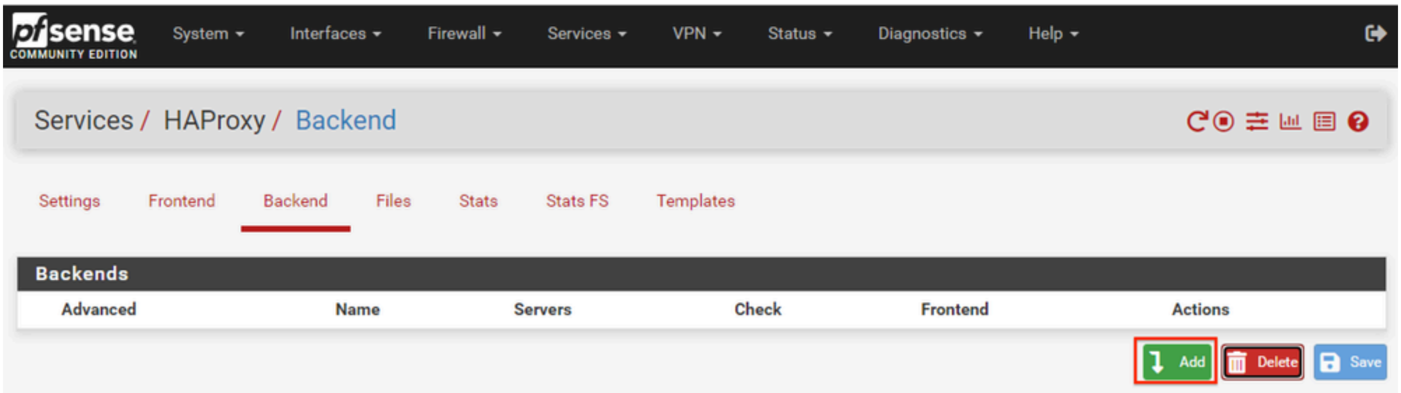
---

**Note**: Configuration changes are not made active until you select the, **Apply Changes** button. You can make multiple configuration changes and apply them all at one time. Configuration does not need to be applied to be used in another section.

---

## Configure HAProxy Backend

Start with the backend. The reason for this is that the frontend must reference a backend. Ensure that you have selected the Backend menu.

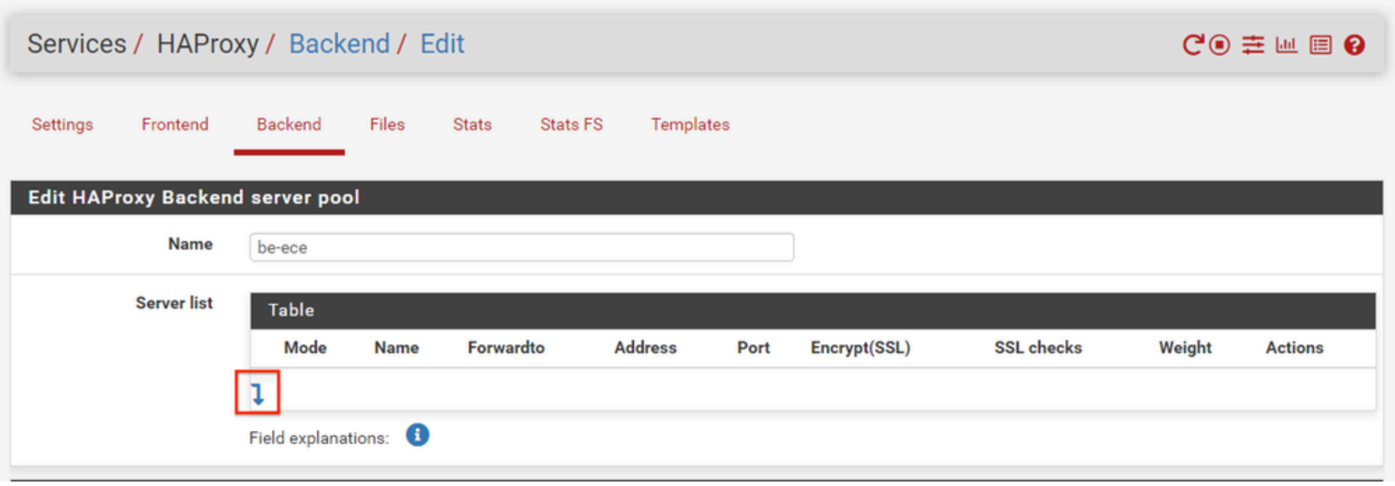


**Backends**

| Advanced | Name | Servers | Check | Frontend | Actions |
|---|---|---|---|---|---|

*pfSense GUI - HAProxy Add Backend*

Select the **Add** Button.



**Edit HAProxy Backend server pool**

Name: be-ece

Server list

Table

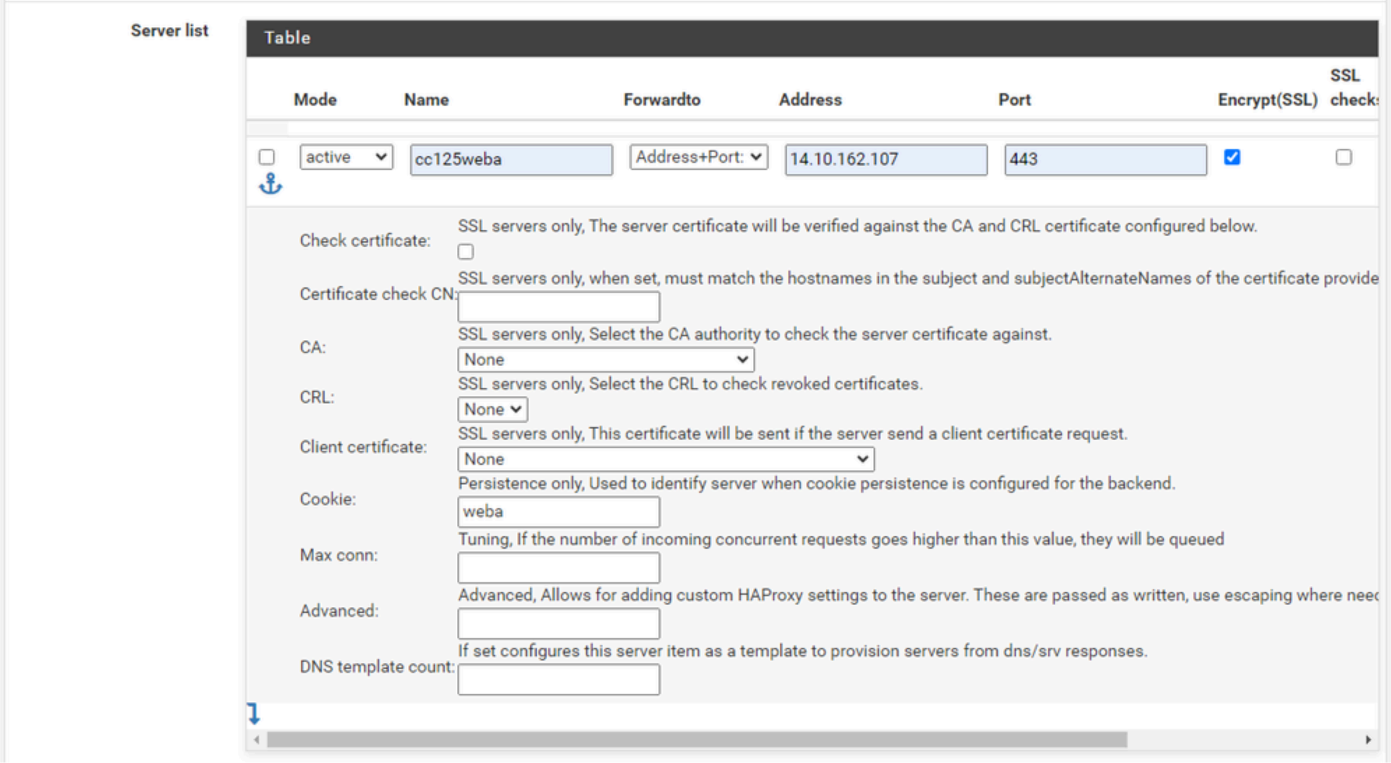
| Mode | Name | Forwardto | Address | Port | Encrypt(SSL) | SSL checks | Weight | Actions |
|---|---|---|---|---|---|---|---|---|

Field explanations:

*pfSense GUI - HAProxy Backend Start*

Provide a name for the backend.

Select the **down arrow** to add the first server to the Server list



Server list

Table

| | Mode | Name | Forwardto | Address | Port | Encrypt(SSL) | SSL check: |
|---|---|---|---|---|---|---|---|
| □ ⚓ | active | cc125weba | Address+Port: | 14.10.162.107 | 443 | ☑ | □ |

Check certificate: SSL servers only, The server certificate will be verified against the CA and CRL certificate configured below. □

Certificate check CN: SSL servers only, when set, must match the hostnames in the subject and subjectAlternateNames of the certificate provide

CA: SSL servers only, Select the CA authority to check the server certificate against. None

CRL: SSL servers only, Select the CRL to check revoked certificates. None

Client certificate: SSL servers only, This certificate will be sent if the server send a client certificate request. None

Cookie: Persistence only, Used to identify server when cookie persistence is configured for the backend. weba

Max conn: Tuning, If the number of incoming concurrent requests goes higher than this value, they will be queued

Advanced: Advanced, Allows for adding custom HAProxy settings to the server. These are passed as written, use escaping where neec

DNS template count: If set configures this server item as a template to provision servers from dns/srv responses.

*Backend - Server list*

Provide a name to reference the server. This does not need to match the actual server name. This is the name that is shown on the stats page.

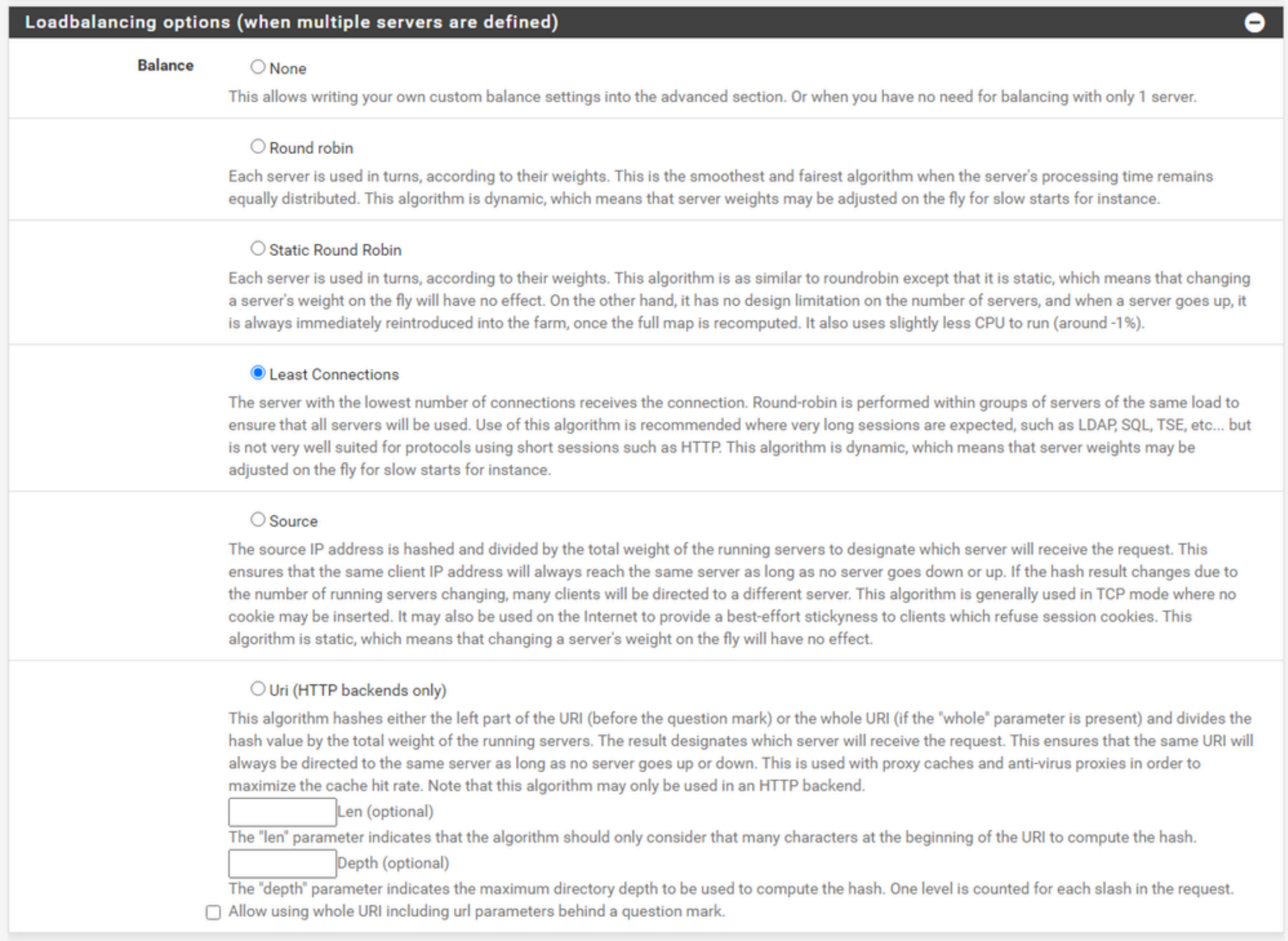
Provide the address for the server. This can be configured as either an IP Address for FQDN.

Provide the port to connect to. This must be port 443 for ECE.

Select the Encrypt(SSL) checkbox.

Provide a value in the Cookie field. This is the content of the session stickiness cookie and must be unique inside the backend.

After the first server has been configured, select the down arrow to configure any other web servers in the environment.



**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)

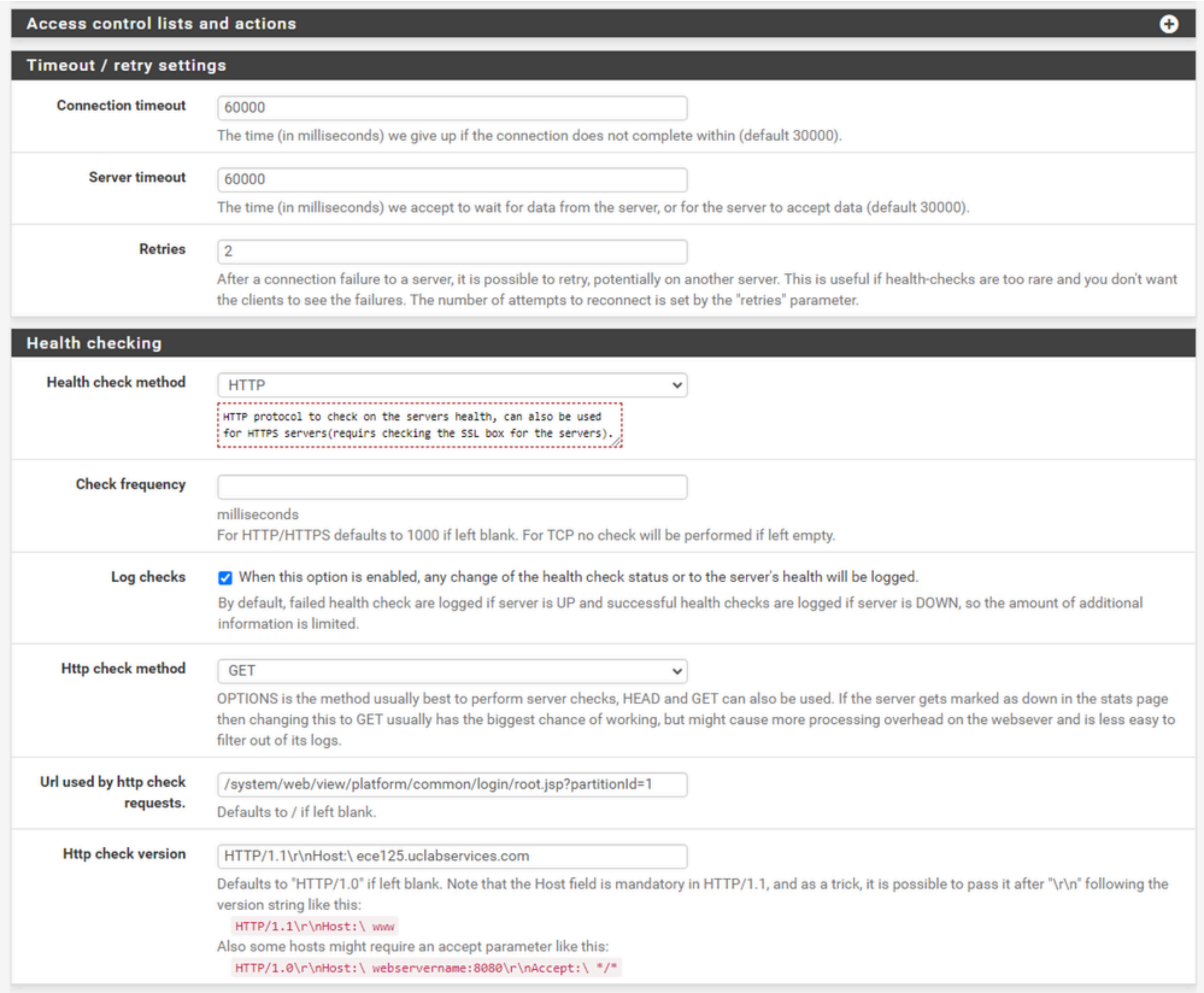
The "depth" parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request.

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

*HAProxy Backend - Loadbalancing*

Configure the Loadbalancing options.

For ECE servers, this must be set to Least Connections.



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
```
HTTP protocol to check on the servers health, can also be used
for HTTPS servers(requirs checking the SSL box for the servers).
```

Check frequency:
milliseconds
For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.

Log checks: ☑ 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
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 websever and is less easy to filter out of its logs.

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:
`HTTP/1.1\r\nHost:\ www`
Also some hosts might require an accept parameter like this:
`HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*`

*HAProxy Backend - Health checking*

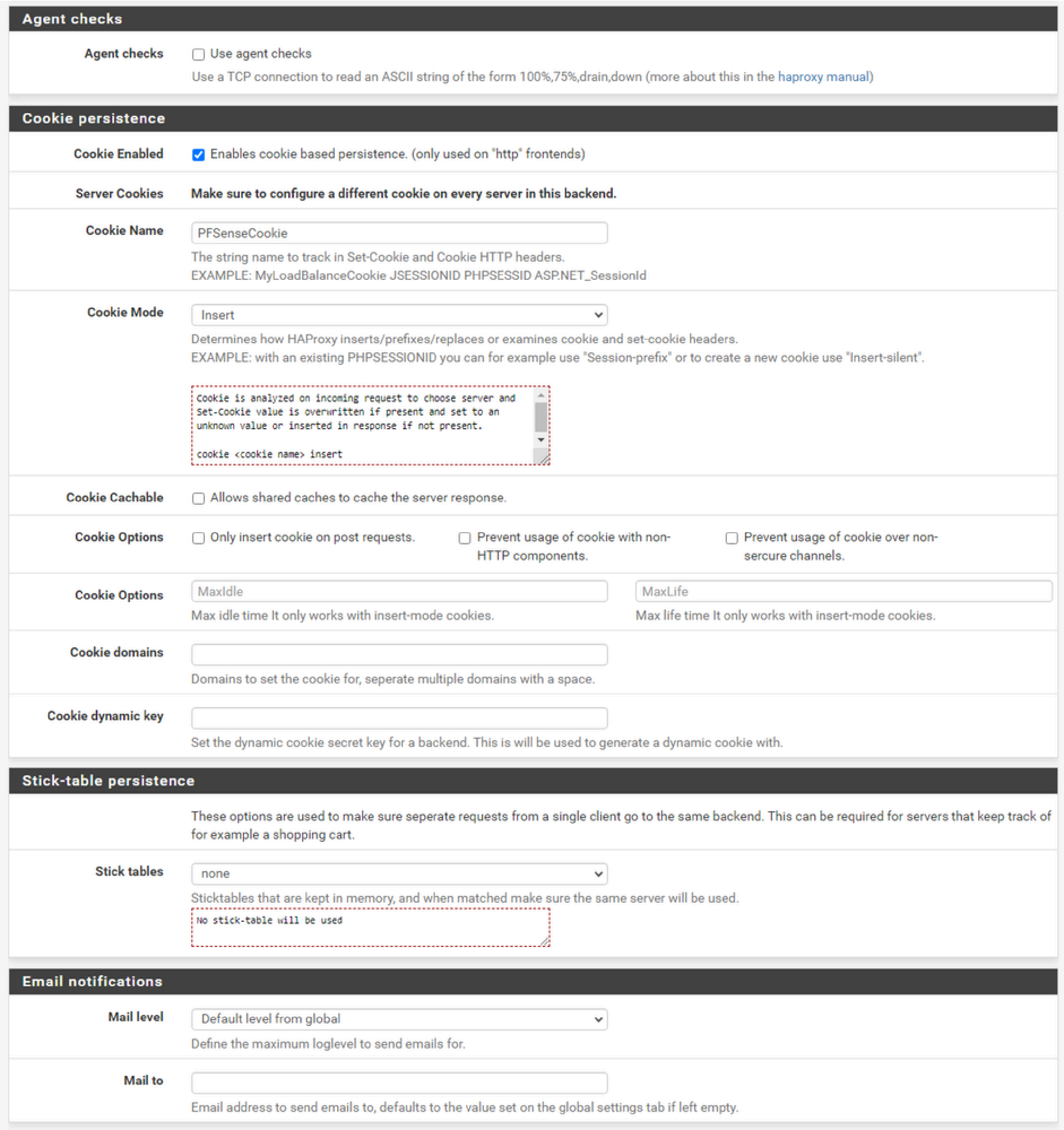
Access control lists are not used in this configuration.

Timeout / retry settings can be left at their default configuration.

Configure the Heath checking section.

1. Health check method: HTTP
2. Check frequency: Leave blank to use the default of every 1 second.
3. Log checks: Select this option to write any health changes to the logs.
4. Http check method: Select GET from the list.
5. Url used by http check requests.: For an ECE server enter, /system/web/view/platform/common/login/root.jsp?partitionId=1
6. HTTP check version: Enter, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

Ensure that you include a space after the final backslash but before the FQDN of the server.



**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** PFSenseCookie
The string name to track in Set-Cookie and Cookie HTTP headers.
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASP.NET_SessionId

**Cookie Mode** Insert
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-sercure channels.

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

**Cookie domains**
Domains to set the cookie for, seperate 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 seperate 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** none
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** Default level from global
Define the maximum loglevel to send emails for.

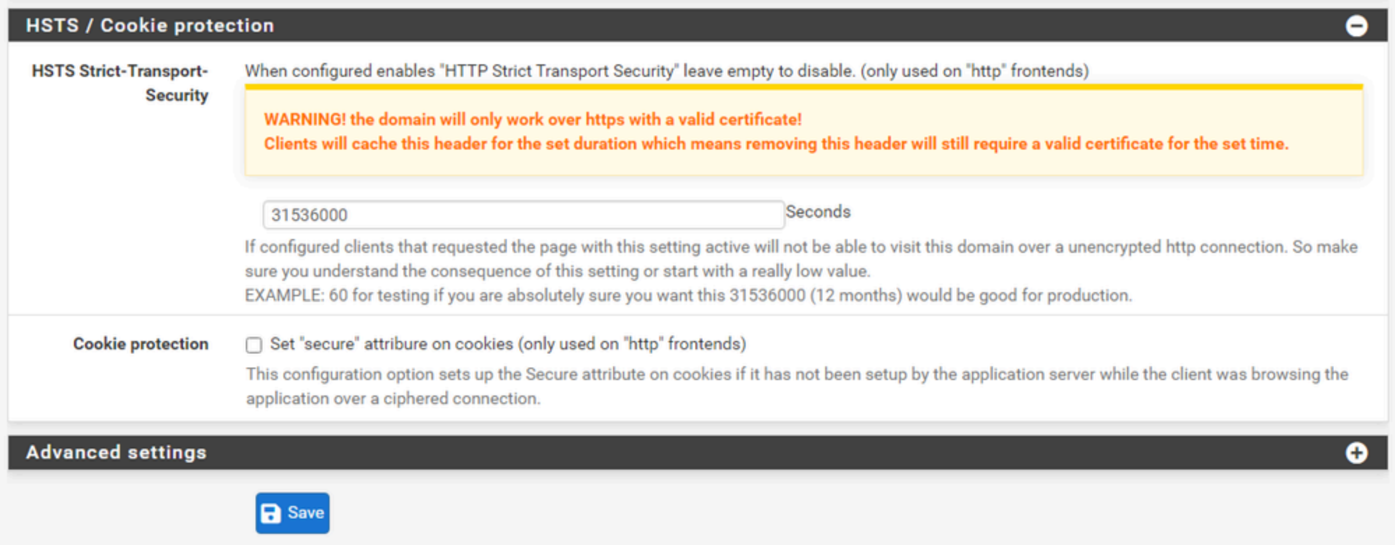
**Mail to**
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

*HAProxy Backend - Cookie Persistence*

Leave the Agent checks unselected.

Configure Cookie persistence:

1. Cookie Enabled: Select to enable cookie based persistence.
2. Cookie Name: Provide a name for the cookie.
3. Cookie Mode: Select Insert from the drop-down box.
4. Leave the remaining options unset.



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" attribure 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.

*HAProxy Backend - HSTS*

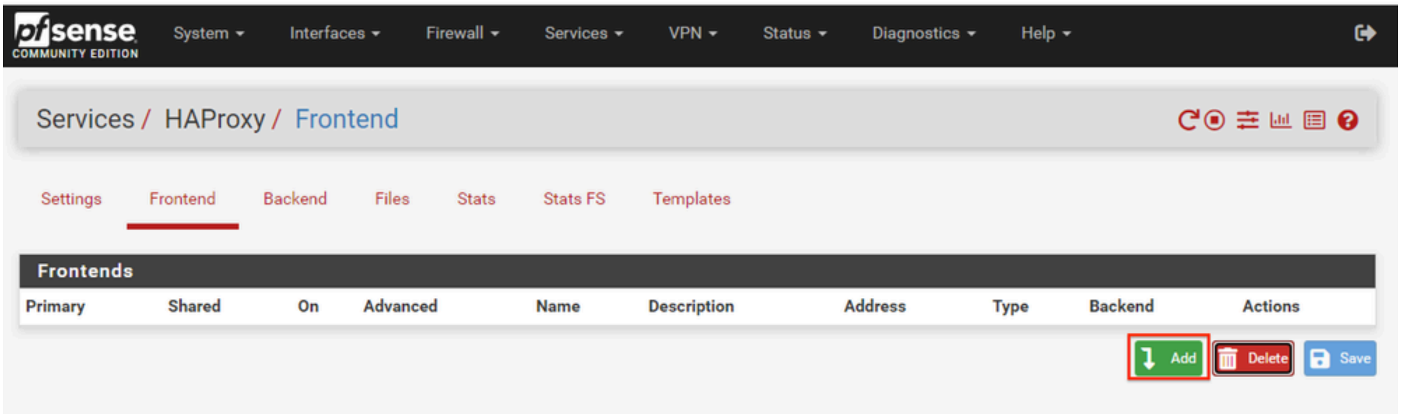
The remaining sections of the backend configuration form can be left at their default settings.

If you wish to configure HSTS, configure a timeout value in this section. ECE inserts an HSTS cookie as well so this configuration is redundant.

Select, **Save**.

## Configure HAProxy Frontend

Change to the Frontend menu.

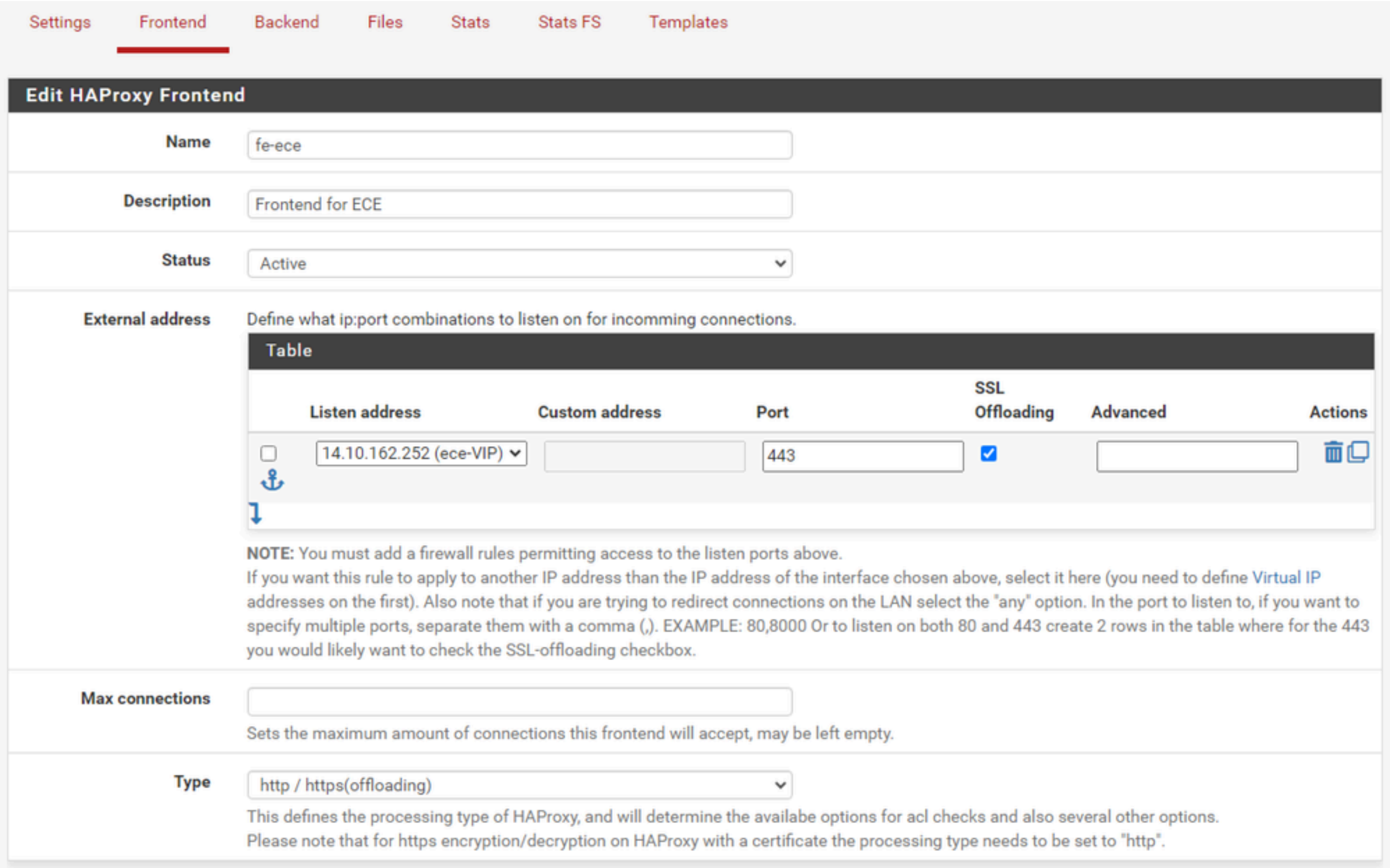


Frontends

| Primary | Shared | On | Advanced | Name | Description | Address | Type | Backend | Actions |
|---|---|---|---|---|---|---|---|---|---|

*pfSense GUI - HAProxy Add Frontend*

Select the, **Add** button



**Edit HAProxy Frontend**

| | |
|---|---|
| **Name** | fe-ece |
| **Description** | Frontend for ECE |
| **Status** | Active |

**External address**

Define what ip:port combinations to listen on for incomming connections.

Table

| | Listen address | Custom address | Port | SSL Offloading | Advanced | Actions |
|---|---|---|---|---|---|---|
| □ | 14.10.162.252 (ece-VIP) | | 443 | ☑ | | |

**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** http / https(offloading)

This defines the processing type of HAProxy, and will determine the availabe 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 - Frontend Header*

Provide a name for the Front end.

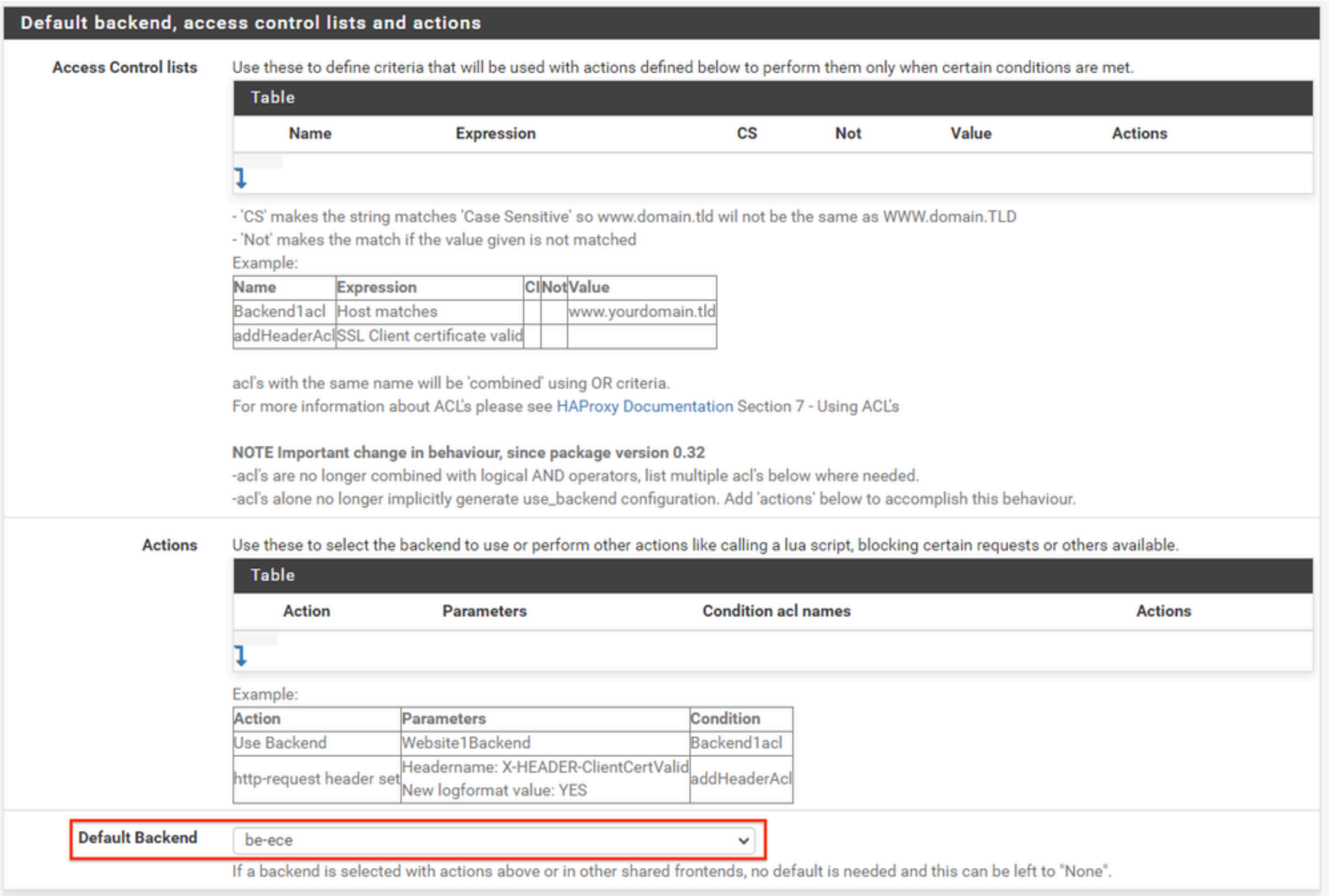
Provide a description to help identify the frontend later.

In the External address table:

1. Listen address: Select the VIP you created for this website.
2. Port: Enter 443.
3. SSL Offloading: Select this option so that a the session cookie can be inserted.

Leave the Max connections empty.

Ensure the Type is selected as 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 | CI | Not | Value |
|---|---|---|---|---|
| Backend1acl | Host matches | | | www.yourdomain.tld |
| addHeaderAcl | SSL Client certificate valid | | | |

acl's with the same name will be 'combined' using OR criteria.
For more information about ACL's 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 |
|---|---|---|---|

Example:

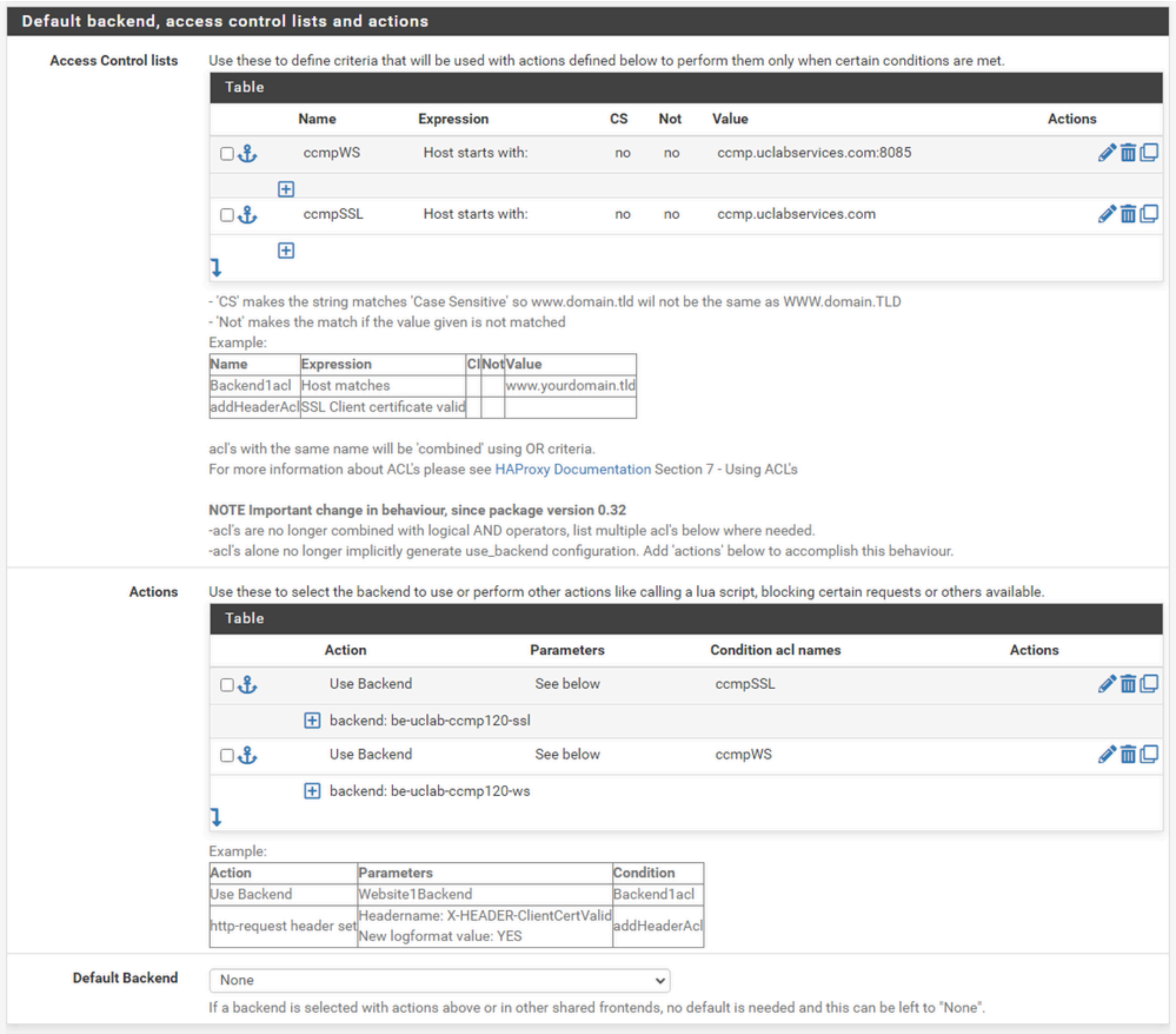
| Action | Parameters | Condition |
|---|---|---|
| Use Backend | Website1Backend | Backend1acl |
| http-request header set | Headername: X-HEADER-ClientCertValid<br>New logformat value: YES | addHeaderAcl |

**Default Backend** be-ece

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 Backend - Default backend selection*

The easiest configuration is to choose a Default Backend from the drop-down. This can be selected when the VIP hosts a single website.



**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 |
|---|---|---|---|---|---|---|
| □ ⚓ | ccmpWS | Host starts with: | no | no | ccmp.uclabservices.com:8085 | ✎ 🗑 ⧉ |
| ⊞ |  |  |  |  |  |  |
| □ ⚓ | 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 | CI | Not | Value |
|---|---|---|---|---|
| Backend1acl | Host matches |  |  | www.yourdomain.tld |
| addHeaderAcl | SSL Client certificate valid |  |  |  |

acl's with the same name will be 'combined' using OR criteria.
For more information about ACL's 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 |
|---|---|---|---|---|
| □ ⚓ | Use Backend | See below | ccmpSSL | ✎ 🗑 ⧉ |
|  | ⊞ backend: be-uclab-ccmp120-ssl |  |  |  |
| □ ⚓ | 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<br>New logformat value: YES | addHeaderAcl |

**Default Backend**

None

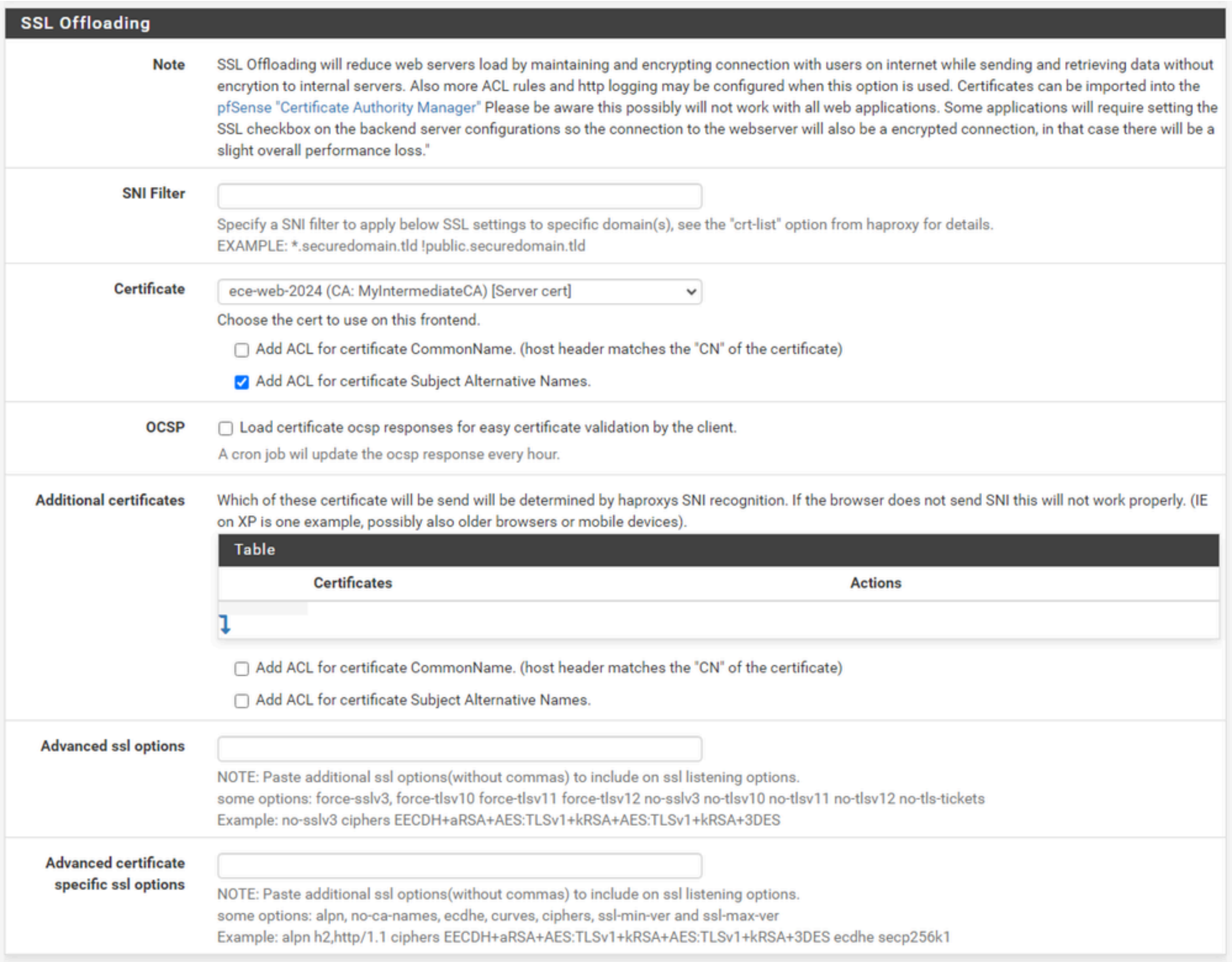
If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

*HAProxy Backend - ACL Advanced*

As shown in the image, ACLs can be used to redirect a single frontend to multiple backends based on conditions.

You can see that the ACL checks to see if the host in the request starts with a name and port number. or simply the name. Based on this a specific backend is used.

This is not common with 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 encrytion 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** ece-web-2024 (CA: MyIntermediateCA) [Server cert]

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 haproxys 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 |
|---|---|

□ Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)

□ 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-sslv3, force-tlsv10 force-tlsv11 force-tlsv12 no-sslv3 no-tlsv10 no-tlsv11 no-tlsv12 no-tls-tickets
Example: no-sslv3 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, ecdhe, 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 ecdhe secp256k1

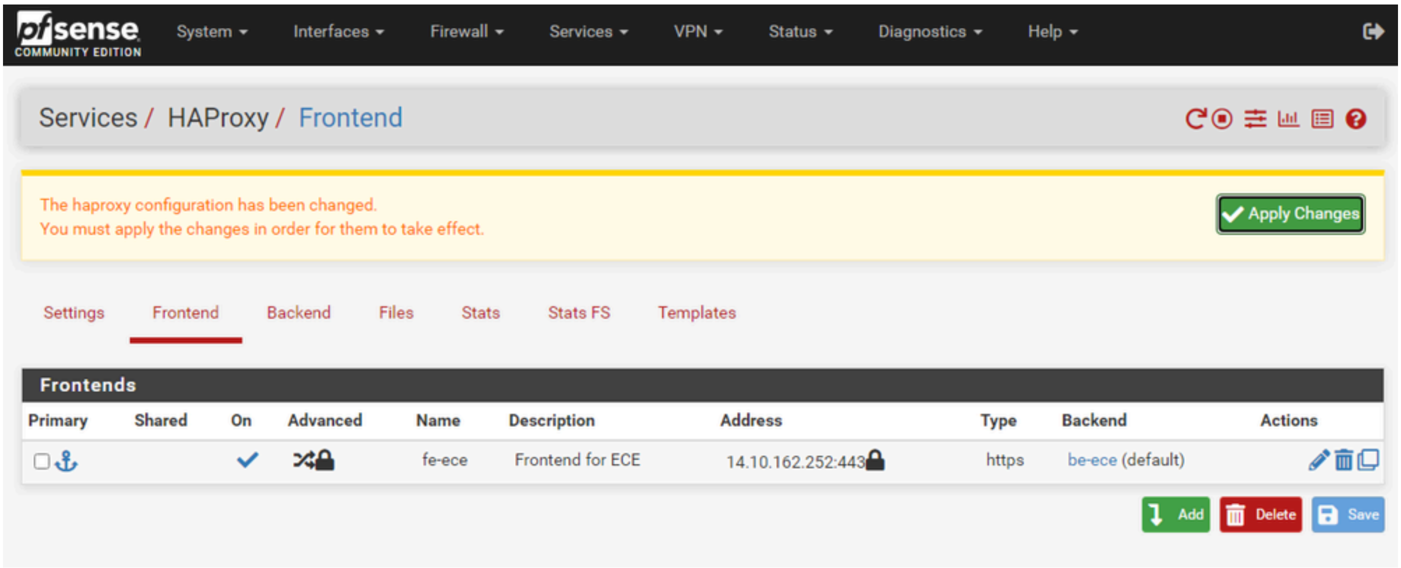
*HAProxy Frontend - Certificate binding*

In the SSL Offloading section, select the certificate created for use with this site. This certificate must be a server certificate.

Select the option, **Add ACL** for certificate Subject Alternative Names.

You can leave the remaining options at their default values.

Select, **Save** at the end of this form.



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

**Frontends**

| Primary | Shared | On | Advanced | Name | Description | Address | Type | Backend | Actions |
|---|---|---|---|---|---|---|---|---|---|
| ☐ ⚓ |  | ✓ | 🔀🔒 | fe-ece | Frontend for ECE | 14.10.162.252:443🔒 | https | be-ece (default) | ✎ 🗑 ❐ |

*HAProxy - Apply Configuration*

Select, **Apply Changes** to commit the Frontend and Backend changes to the running configuration.

Congratulations, you have completed the setup and configuration of pfSense.