

# ECE用のpfSenseコミュニティロードバランサの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[pfSenseのインストール](#)

[ソリューションの概要](#)

[準備](#)

[設置](#)

[ネットワーク構成](#)

[初期設定の完了](#)

[管理者の基本設定](#)

[必要なパッケージの追加](#)

[証明書の設定](#)

[仮想IPの追加](#)

[ファイアウォールの設定](#)

[HAProxyの設定](#)

[HAProxyの概念](#)

[HAProxyの初期設定](#)

[HAProxyバックエンドの設定](#)

[HAProxyフロントエンドの設定](#)

---

## はじめに

このドキュメントでは、エンタープライズチャットおよび電子メール(ECE)のロードバランサとしてpfSense Community Editionを設定する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ECE 12.x
- pfSenseコミュニティ版

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## pfSenseのインストール

### ソリューションの概要

pfSense Community Editionは、ファイアウォール、ロードバランサ、セキュリティスキャナなど、多くのサービスを1つのサーバで提供する多機能の製品です。pfSenseはFree BSD上に構築されており、ハードウェア要件は最小限です。ロードバランサはHAProxyの実装であり、製品を設定するための使いやすいGUIが提供されます。

このロードバランサは、ECEとContact Center Management Portal(CCMP)の両方で使用できます。このドキュメントでは、ECEのpfSenseを設定する手順について説明します。

### 準備

ステップ 1 : pfSenseソフトウェアのダウンロード

[pfSense webサイト](#)を使用して、isoインストーライメージをダウンロードします。

ステップ 2 : VMの設定

VMを最小要件で設定します。

- 64ビットamd64(x86-64)互換CPU
- 1 GB以上のRAM
- 8 GB以上のディスクドライブ ( SSD、HDDなど )
- 1つ以上の互換性のあるネットワークインターフェイスカード
- ブータブルUSBドライブまたは大容量オプティカルドライブ ( DVDまたはBD ) による初期インストール

ラボのインストールでは、ネットワークインターフェイス(NIC)が1つだけ必要です。アプライアンスを実行する方法はいくつかありますが、最も簡単な方法は、ワンアームモードとも呼ばれる単一のNICを使用することです。ワンアームモードでは、ネットワークと通信する単一のインターフェイスがあります。これはラボにとっては簡単で適切な方法ですが、最も安全な方法ではありません。

アプライアンスをより安全に設定するには、少なくとも2つのNICを使用します。1つのNICはWANインターフェイスであり、パブリックインターネットと直接通信します。2番目のNICはLANインターフェイスで、社内ネットワークと通信します。また、セキュリティやファイアウォールのルールが異なるネットワークのさまざまな部分と通信するためのインターフェイスを追加することもできます。たとえば、パブリックインターネットに接続するNICを1つ、外部からアクセス可能なすべてのWebサーバがあるDMZネットワークに接続するNICを1つ、企業ネットワークに接続する3つ目のNICを持つことができます。これにより、内部ユーザと外部ユーザが、DMZに保持されているのと同じWebサーバのセットに安全にアクセスできます。実装前に、設計がセキュリティに及ぼす影響を理解しておく必要があります。特定の实装のベストプラクティスに従っていることをセキュリティエンジニアに確認します。

## 設置

ステップ 1 : VMへのISOのマウント


ステップ 2 : VMの電源をオンにし、プロンプトに従ってインストールします。

手順については、この[ドキュメント](#)を参照してください。

## ネットワーク構成

設定を続行するには、アプライアンスにIPアドレスを割り当てる必要があります。

---

 注：このドキュメントでは、ワンアームモードに設定されたアプライアンスについて説明します。

---

ステップ 1 : VLAN の設定

VLANのサポートが必要な場合は、最初の質問にyと答えてください。それ以外の場合は、nと答えます。

ステップ 2 : WANインターフェイスの割り当て

WANインターフェイスは、2アームモードのアプライアンスの非セキュア側であり、1アームモードの唯一のインターフェイスです。プロンプトが表示されたら、インターフェイス名を入力します。

ステップ 3 : LANインターフェイスの割り当て

LANインターフェイスは、2アームモードのアプライアンスのセキュア側です。プロンプトが表示されたら、必要に応じてインターフェイス名を入力します。

ステップ 4 : その他のインターフェイスの割り当て

特定のインストールに必要なその他のインターフェイスを設定します。これらはオプションであ

り、一般的ではありません。

## ステップ 5：管理インターフェイスへのIPアドレスの割り当て

ネットワークがDHCPをサポートしている場合、割り当てられたIPアドレスがコンソール画面に表示されます。

```
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コンソール

アドレスが割り当てられていない場合、または特定のアドレスを割り当てる場合は、次の手順を実行します。

1. コンソールメニューからオプション2を選択します。
2. nと答えてDHCPを無効にします。
3. WANインターフェイスのIPv4アドレスを入力します。
4. ビットカウントでネットマスクを入力します。(24 = 255.255.255.0、16 = 255.255.0.0、8 = 255.0.0.0)
5. WANインターフェイスのゲートウェイアドレスを入力します。
6. このゲートウェイをアプライアンスのデフォルトゲートウェイにする場合は、ゲートウェイプロンプトに対してyと答え、そうでない場合はnと答えます。
7. 必要に応じて、NICをIPv6用に設定します。
8. インターフェイスでDHCPサーバを無効にします。
9. yと答えて、webConfiguratorプロトコルでHTTPを有効にします。これは次の手順で使用します。

設定が更新されたことを示す確認メッセージが表示されます。

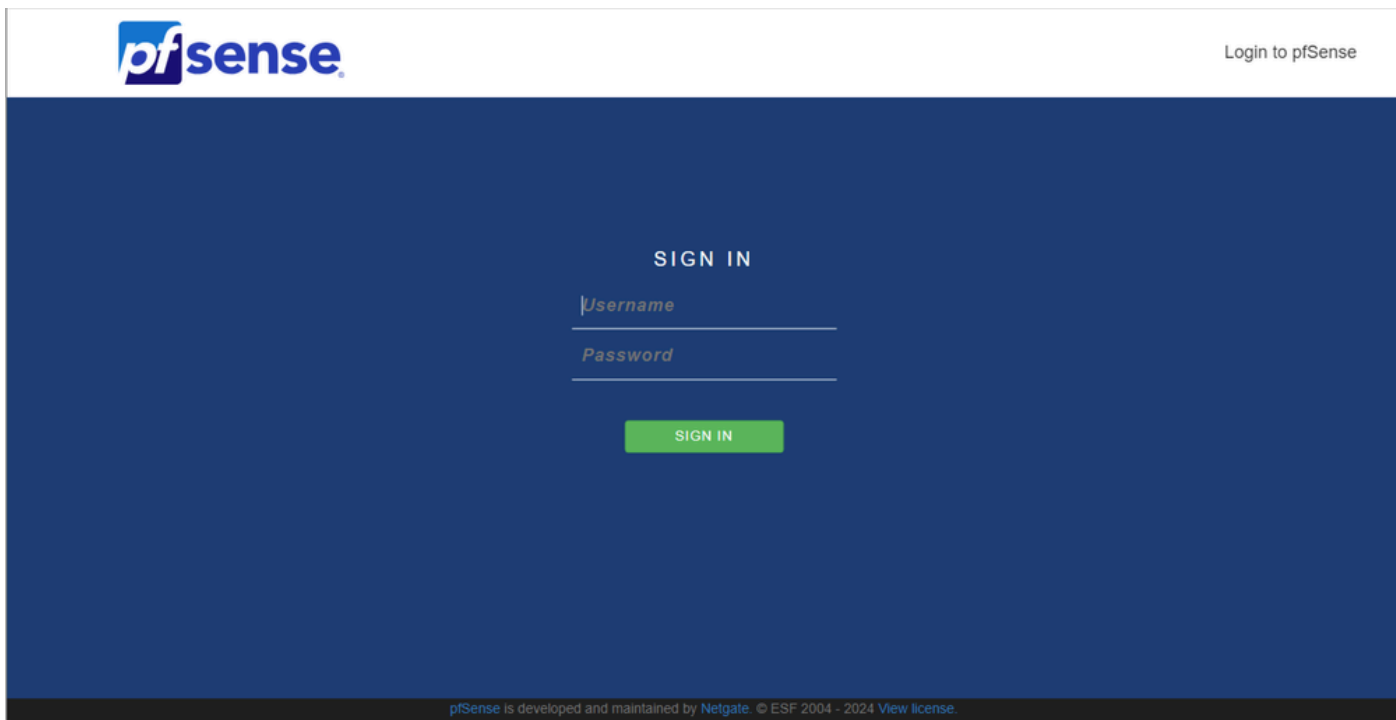
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://14.10.172.250/

Press <ENTER> to continue. █
```

## 初期設定の完了

ステップ 1 : Webブラウザを開き、<http://<ip address of appliance>>に移動します。

 注 : 最初はHTTPSではなくHTTPを使用する必要があります。

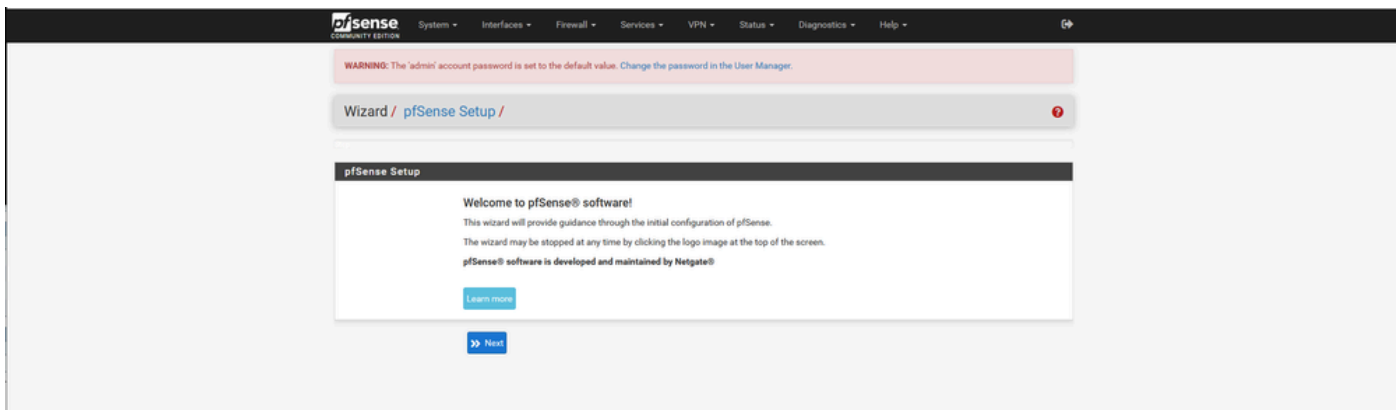


### pfSense管理ログイン

ステップ 2 : admin/pfSenseのデフォルトログインでログインします。

ステップ 3 : 初期設定を完了する

最初の2つの画面でnextをクリックします。



### pfSenseセットアップウィザード - 1

ホスト名、ドメイン名、およびDNSサーバ情報を入力します。

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

**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**   
Name of the firewall host, without domain part.  
Examples: pfsense, firewall, edgefw

**Domain**   
Domain name for the firewall.  
Examples: home.arpa, example.com

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**   
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

pfSenseセットアップウィザード - 2

IPアドレス情報を確認します。最初にDHCPを選択した場合は、ここで変更できます。

NTPタイムサーバのホスト名を入力し、ドロップダウンで正しいタイムゾーンを選択します。

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

**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**   
Enter the hostname (FQDN) of the time server.

**Timezone**

[» Next](#)

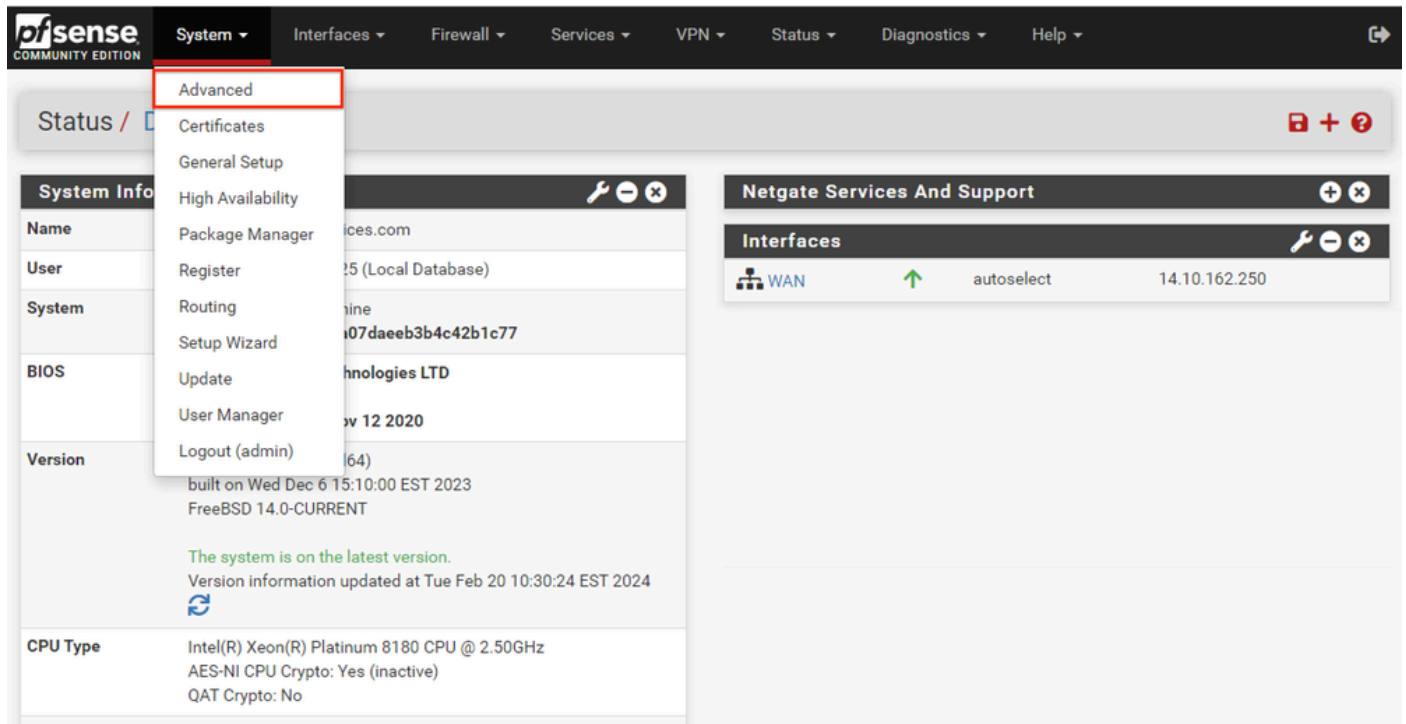
pfSenseセットアップウィザード - 3

最後までセットアップウィザードを続行します。インターフェイスGUIが再起動し、完了すると新しいURLにリダイレクトされます。

## 管理者の基本設定

ステップ 1：管理インターフェイスにログインします。

ステップ 2：SystemドロップダウンメニューからAdvancedを選択します



pfSense GUI – 管理ドロップダウン

ステップ 3：WebConfigurator設定の更新


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

pfSense GUI : 管理設定

1. HTTPS(SSL/TLS)プロトコルを選択します。
2. この時点では、SSL/TLS証明書を自己署名証明書のままにしておきます。
3. TCPポートを443以外のポートに変更して、インターフェイスのセキュリティを強化し、ポートのオーバーラップの問題を防止します。
4. WebGUIリダイレクトオプションを選択して、ポート80の管理インターフェイスを無効にします。
5. Browser HTTP\_REFERERエンフォースメントオプションを選択します。

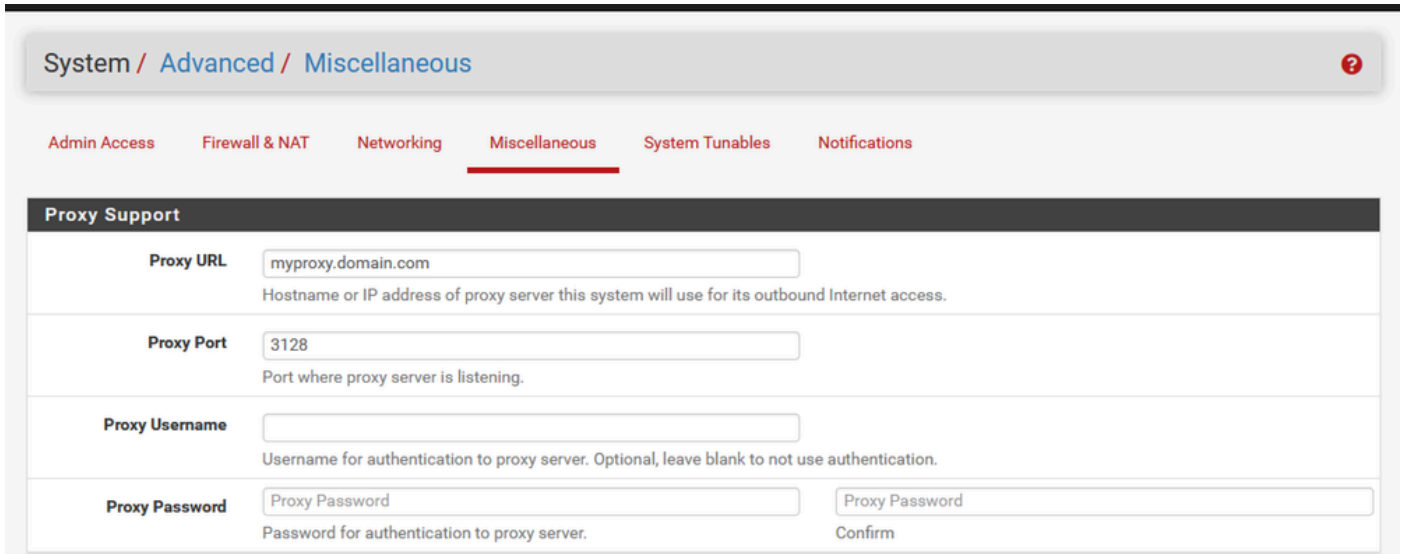


6. Enable Secure Shellオプションを選択して、セキュアシェルを有効にします。

 注：先に進む前に、必ずSaveボタンを選択してください。新しいHTTPSリンクにリダイレクトされます。

ステップ 4：必要に応じてプロキシサーバを設定する


必要に応じて、[その他]タブでプロキシ情報を設定します。セットアップと設定を完了するには、アプライアンスがインターネットにアクセスできる必要があります。



The screenshot shows the pfSense GUI configuration page for Proxy Support. The breadcrumb trail is System / Advanced / Miscellaneous. The Miscellaneous tab is selected. The Proxy Support section contains the following fields:

| Proxy Support  |  |
|----------------|--|
| Proxy URL      | <input type="text" value="myproxy.domain.com"/><br><small>Hostname or IP address of proxy server this system will use for its outbound Internet access.</small>        |
| Proxy Port     | <input type="text" value="3128"/><br><small>Port where proxy server is listening.</small>  |
| Proxy Username | <input type="text"/><br><small>Username for authentication to proxy server. Optional, leave blank to not use authentication.</small>                                   |
| Proxy Password | <input type="password" value="Proxy Password"/> <input type="password" value="Proxy Password"/><br><small>Password for authentication to proxy server. Confirm</small> |


pfSense GUI：プロキシ設定

 注：変更を加えた後は、必ずSaveボタンを選択してください。

必要なパッケージの追加

ステップ 1：System > Package Managerを選択します。

ステップ 2：利用可能なパッケージの選択

 注：利用可能なすべてのパッケージをロードするには数分かかることがあります。タイムアウトした場合は、DNSサーバが正しく設定されていることを確認します。多くの場合、アプライアンスをリブートするとインターネット接続が修復されます。

Installed Packages

Available Packages

## Search

Search term

Both

▼



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

## Packages

| Name     | Version  | Description   |                           |
|----------|----------|---|---------------------------|
| acme     | 0.7.5    | Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.<br>Package Dependencies:<br><a href="#">pecl-ssh2-1.3.1</a> <a href="#">socat-1.7.4.4</a> <a href="#">php82-8.2.11</a> <a href="#">php82-ftp-8.2.11</a>                                    | <a href="#">+ Install</a> |
| 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><a href="#">apcupsd-3.14.14_4</a> | <a href="#">+ Install</a> |
| arping   | 1.2.2_4  | Broadcasts a who-has ARP packet on the network and prints answers.<br>Package Dependencies:<br><a href="#">arping-2.21_1</a>  | <a href="#">+ Install</a> |
| 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.  | <a href="#">+ Install</a> |

pfSense GUI : パッケージリスト

## ステップ 3 : 必要なパッケージの検索とインストール

1. プロキシ
2. オープンVMツール



注:haproxy-develパッケージは選択しないでください。

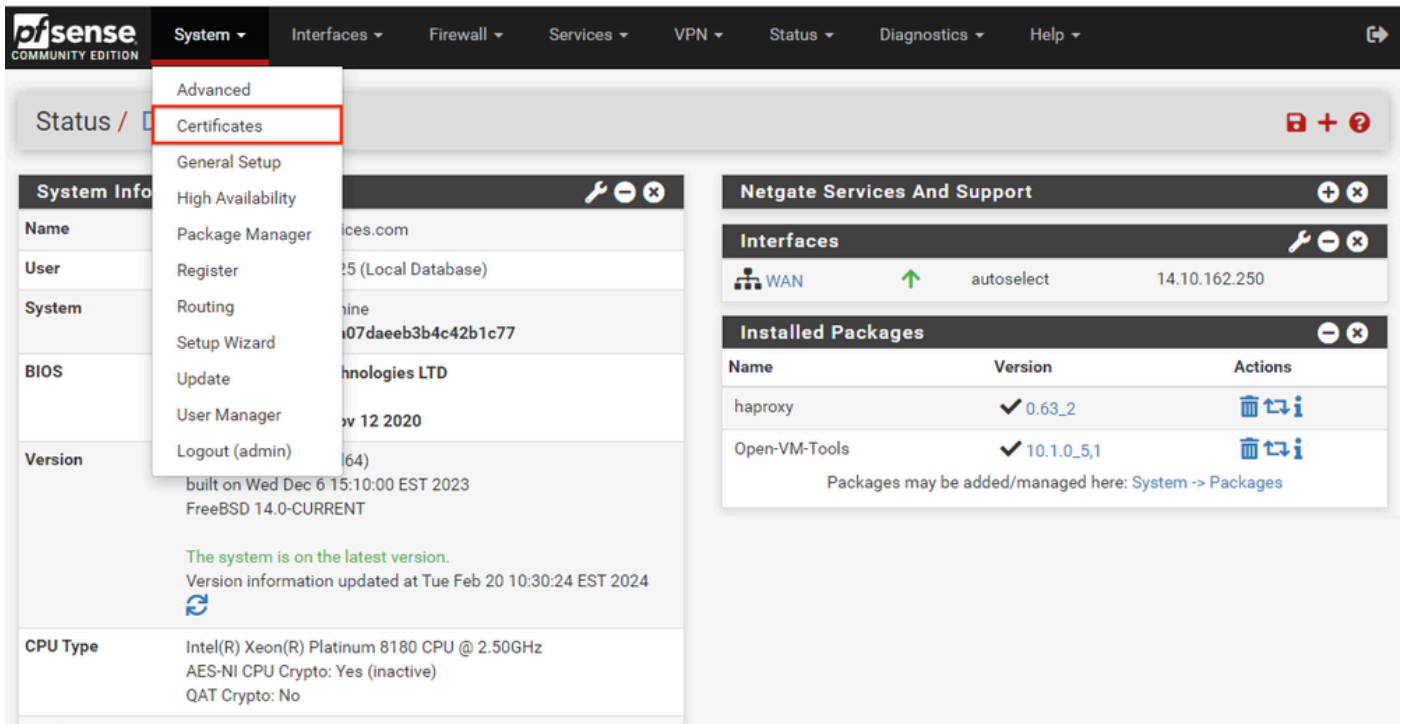
## 証明書の設定

pfSenseは、自己署名証明書を作成することも、パブリックCAや内部CAと統合することも、CAとして機能してCA署名付き証明書を発行することもできます。このガイドでは、内部CAと統合する手順について説明します。

このセクションを開始する前に、次の項目が使用可能であることを確認してください。

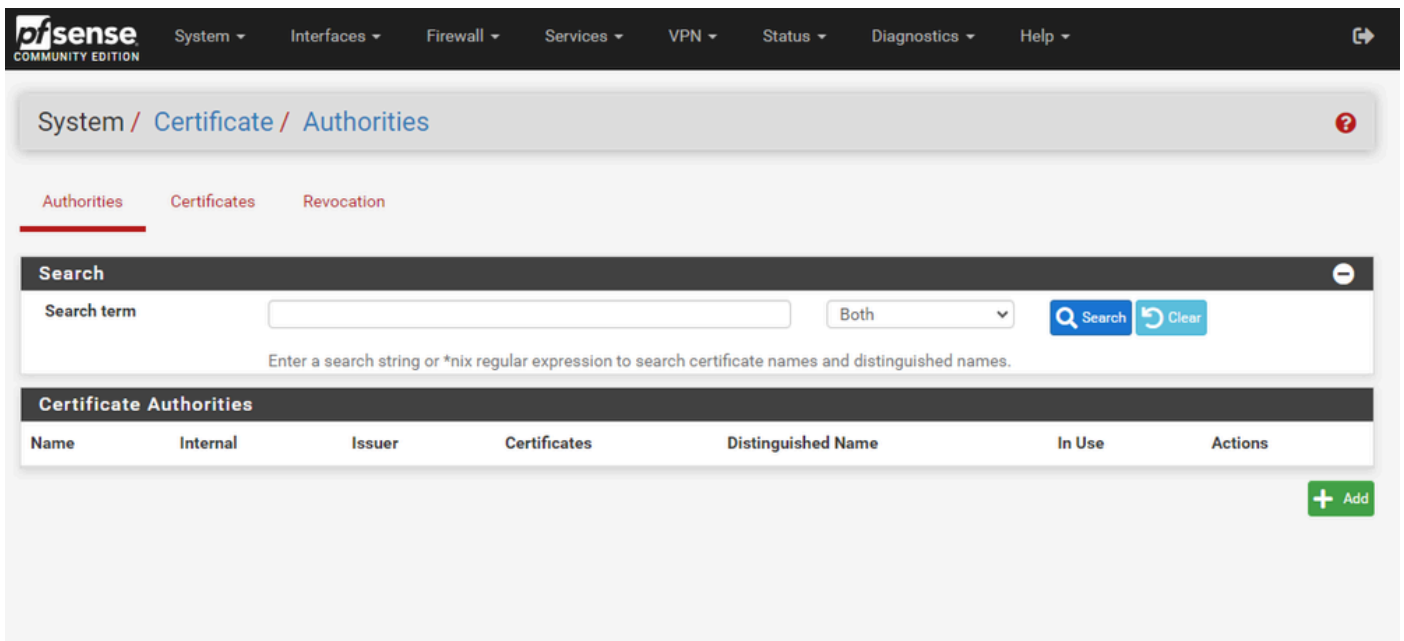
1. PEMまたはBase-64エンコード形式で保存されたCAのルート証明書。
2. PEMまたはBase-64エンコード形式で保存されるCAのすべての中間 (発行側と呼ばれることもあります) 証明書。

ステップ 1 : SystemドロップダウンメニューからCertificatesを選択します



pfSense GUI – 証明書ドロップダウン

## ステップ 2 : CAルート証明書のインポート



pfSense GUI:CA証明書リスト

Addボタンを選択します。

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

### Create / Edit CA

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

**Method**

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

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

### Existing Certificate Authority

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

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

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

pfSense GUI - CAインポート

図に示すように：

1. 一意の説明的な名前を指定します
2. 「方法」ドロップダウンから「既存の認証局のインポート」を選択します。
3. 「信頼ストア」および「シリアルランダム化」チェック・ボックスが選択されていることを確認します。
4. [証明書データ]テキストボックスに証明書全体を貼り付けます。-----BEGIN CERTIFICATE-----および-----END CERTIFICATE-----行からを含めていることを確認します。
5. Saveを選択します。
6. 図に示すように、証明書がインポートされていることを確認します。

pfSense  
COMMUNITY EDITION

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

System / Certificate / Authorities ?

Authorities Certificates Revocation

**Search** ⊖

Search term  Both Q Search ↺ Clear

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

**Certificate Authorities**

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

+ Add

pfSense GUI:CAリスト

ステップ 3 : CA中間証明書のインポート

pfSense  
COMMUNITY EDITION

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

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

### Create / Edit CA

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

**Method**

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

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

### Existing Certificate Authority

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

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

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

pfSense GUI - CA中間インポート

手順を繰り返してルートCA証明書をインポートし、中間CA証明書をインポートします。

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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

**Certificate Authorities**

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

pfSense GUI:CAリンク

図に示すように、中間証明書がルート証明書に正しくチェーンされていることを確認するために認証局を確認します。

#### ステップ 4 : ロードバランスされたWebサイトのCSRの作成とエクスポート

ここでは、CSRの作成、CSRのエクスポート、署名付き証明書のインポートの手順について説明します。PFX形式の既存の証明書がある場合は、この証明書をインポートできます。これらの手順については、pfSenseのドキュメントを参照してください。

1. 「証明書」メニューを選択し、「追加/署名」ボタンを選択します。

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

**Certificates**

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

## 2.証明書署名要求フォームに記入します。

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の作成

- 方法：ドロップダウンから[証明書署名要求の作成]を選択します
- 記述名：証明書の名前を指定します
- キータイプとダイジェストアルゴリズム：要件に一致していることを確認します。
- 共通名：完全修飾ドメイン名Webサイトを指定します
- ご使用の環境に応じて、残りの証明書情報を入力します



**Certificate Attributes**

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

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

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


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

**Alternative Names**     
 Type Value

**Add SAN Row**

pfSense GUI:CSR上級

- Certificate Type : ドロップダウンでServer Certificateを選択します。
- 代替名 : 実装に必要なサブジェクト代替名(SAN)を指定します。

 注 : 共通名はSANフィールドに自動的に追加されます。必要な名前を追加するだけで済みます。

すべてのフィールドが正しい場合は、Saveを選択します。

3. CSRをファイルにエクスポートします。

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

System / Certificates / Certificates









Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

| Name  | Issuer                          | Distinguished Name   | In Use          | Actions   |
|---|---------------------------------|--|-----------------|---|
| GUI default<br>(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<br>pending | ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US   |                 |     |

pfSense GUI:CSRのエクスポート

[エクスポート]ボタンを選択してCSRを保存し、CAで署名します。署名付き証明書を取得したら、これをPEMまたはBase-64ファイルとして保存し、プロセスを完了します。

4.署名付き証明書をインポートします。

System / Certificates / Certificates

Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

| Name  | Issuer                          | Distinguished Name   | In Use          | Actions |
|---|---------------------------------|--|-----------------|---------|
| GUI default<br>(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<br>pending | ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US   |                 |         |

pfSense GUI – 証明書のインポート

署名された証明書をインポートするには、鉛筆アイコンを選択します。

5.フォームに証明書データを貼り付けます。

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

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

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

**Descriptive name**

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

**Signing request data**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDvDCCAqQCAQAwZcHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
MAkGA1UEBHMCMVVMxZjZAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUCm1hbmdsZSBQYXJrMRowGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
YzESMBAGA1UECzMjQ2LzY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

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

**Final certificate data**

```
GBSAPwQWkas305JkKISY/pYEI2EW/7EZcDmHRUrnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yIz3IT4TJwDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5Mnuqx1PN97EPQngO/1IgXo4xDz6Dg+Iwt9pyrRZdxpmy
-----END CERTIFICATE-----
```

Paste the certificate received from the certificate authority here.

pfSense GUI – 証明書のインポート

Updateを選択して証明書を保存します。

6.証明書データが正しいことを確認します。

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

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

**Certificates**

| Name  | Issuer           | Distinguished Name  | In Use          | Actions |
|---|------------------|---|-----------------|---------|
| GUI default<br>(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 |                 |         |

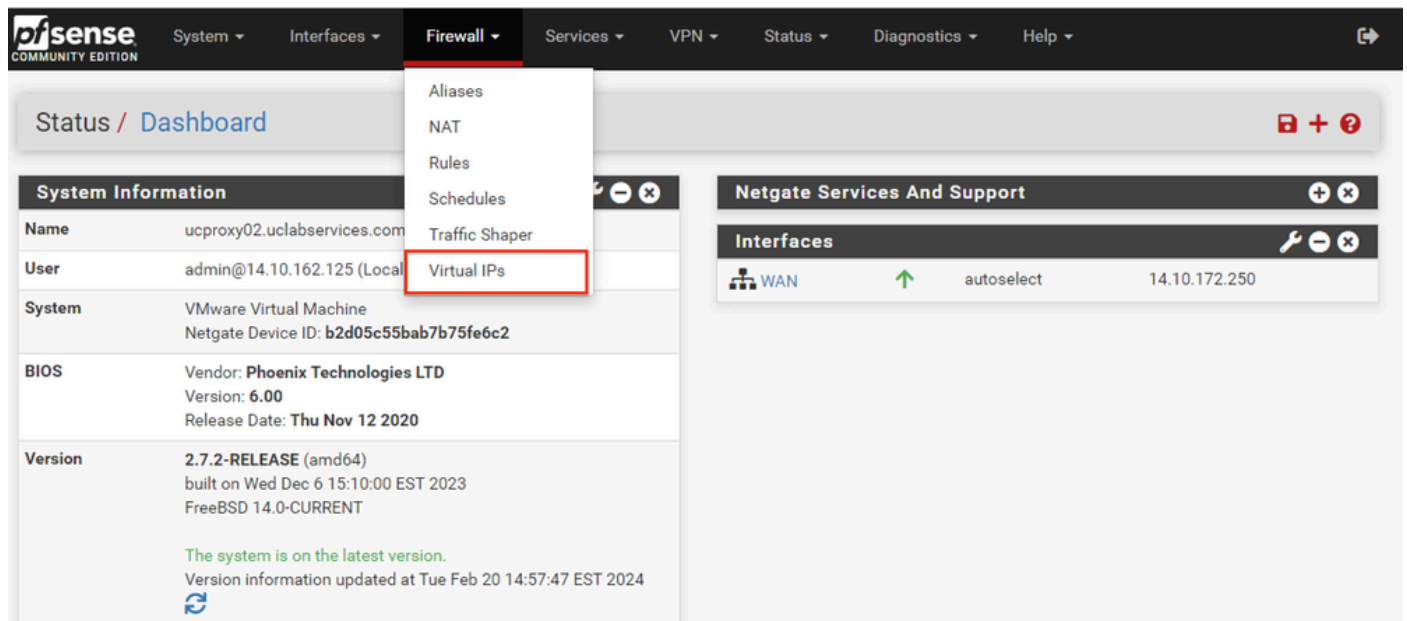
pfSense GUI : 証明書リスト

7.このpfSenseで複数のサイトをホストする場合は、このプロセスを繰り返します。

## 仮想IPの追加

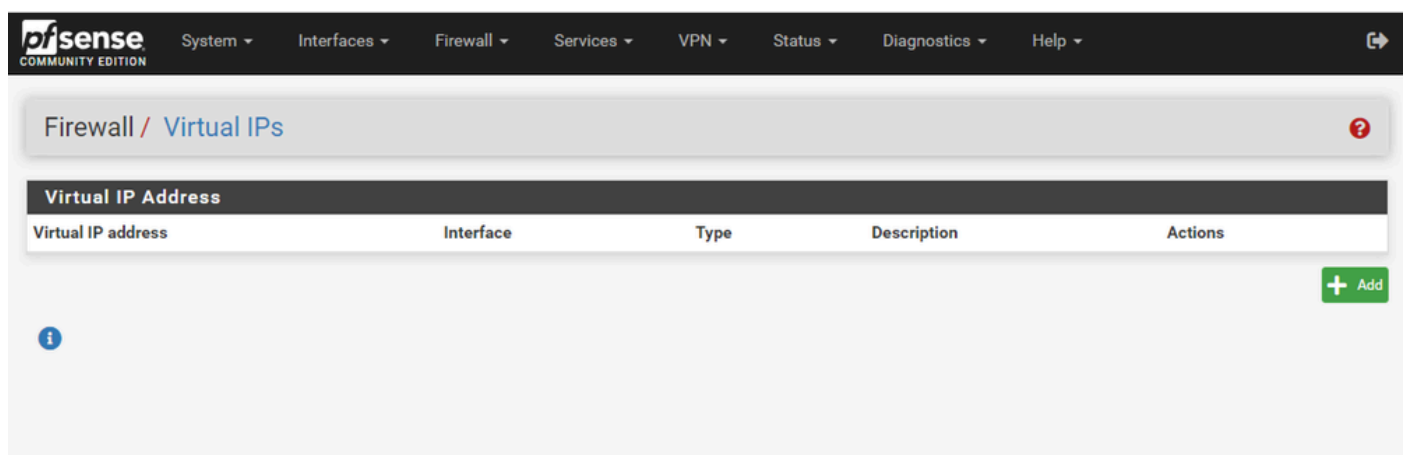
pfSenseでWebサイトをホストするには、少なくとも1つのIPが必要です。pfSenseでは、これは仮想IP(VIP)で実行されます。

ステップ 1 : FirewallドロップダウンからVirtual IPsを選択します



pfSense GUI:VIPドロップダウン

ステップ 2 : 「追加」 ボタンを選択します



pfSense GUI:VIPランディングページ

ステップ 3 : 住所情報の入力

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

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

Virtual IP Password: Virtual IP Password (Enter the VHID group password.) / Virtual IP Password (Confirm)

VHID Group: 1  
Enter the VHID group that the machines will share.

Advertising frequency: 1 (Base) / 0 (Skew)  
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: ece-VIP  
A description may be entered here for administrative reference (not parsed).

pfSense GUI:VIPの設定

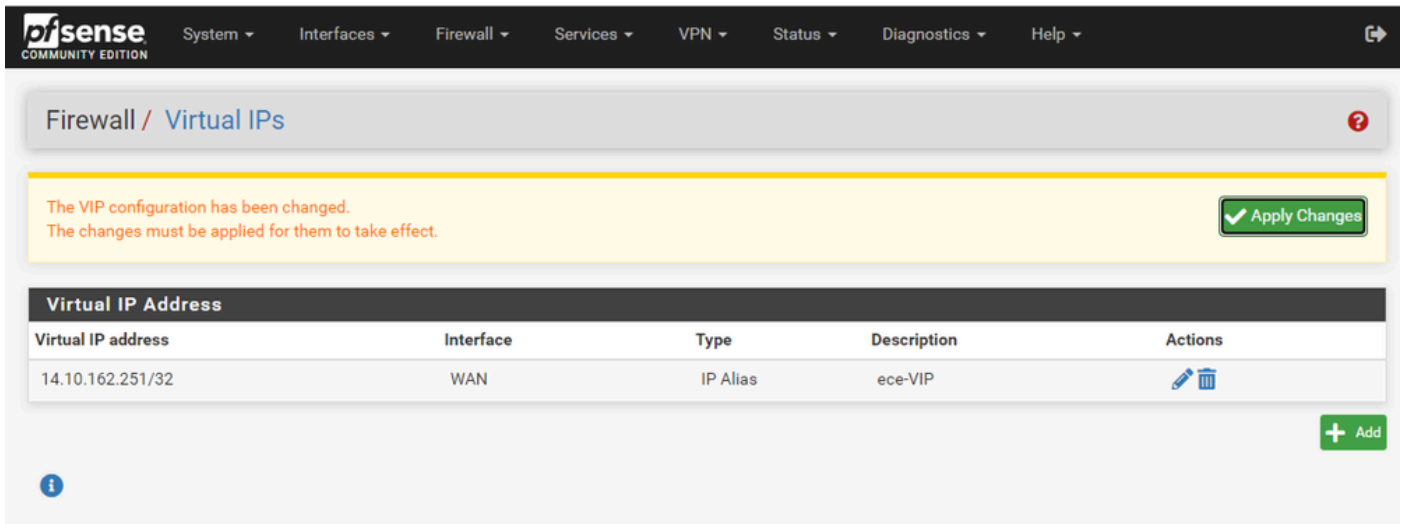
この情報を使用して、VIPを追加します。

- タイプ：IPエイリアスの選択
- Interface：このIPアドレスをブロードキャストするインターフェイスを選択します
- アドレス：IPアドレスを入力します。
- アドレスマスク：ロードバランシングに使用するIPアドレスの場合、マスクは/32である必要があります
- 説明：後で設定を理解しやすくするために、短いテキストを入力します

Saveを選択して、変更を確定します。

設定に必要なIPアドレスごとにこれを繰り返します。

ステップ 4：設定の適用



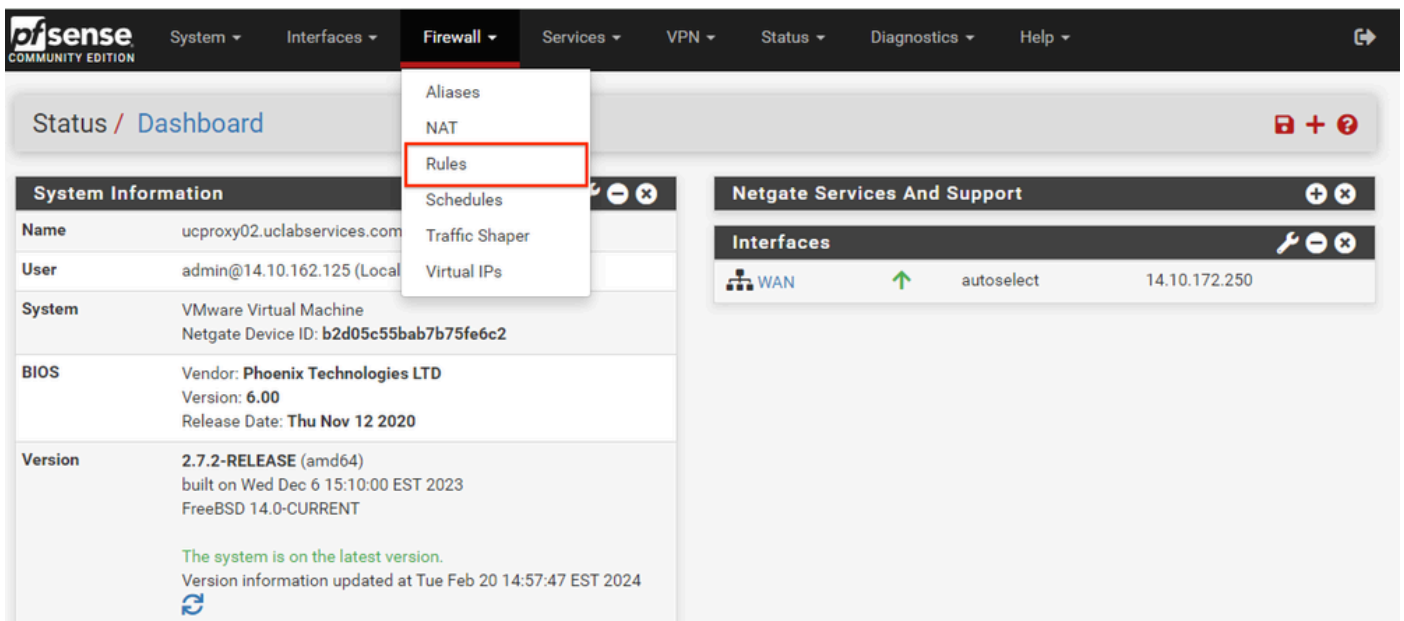
pfSense GUI:VIPリスト

すべてのVIPを追加したら、Apply Changesボタンを選択します。

## ファイアウォールの設定

pfSenseにはファイアウォールが組み込まれています。デフォルトのルールセットは非常に制限されています。アプライアンスを実稼働環境に移行する前に、包括的なファイアウォールポリシーを構築する必要があります。

ステップ 1 : FirewallドロップダウンからRulesを選択します



pfSense GUI:Firewall Rulesドロップダウン

ステップ 2 : いずれかの追加ボタンを選択します

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

Firewall / Rules / WAN 📊 📄 ?

Floating WAN

Rules (Drag to Change Order)

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

⬆️ Add ⬆️ Add 🗑️ Delete 🔄 Toggle 📄 Copy 💾 Save ➕ Separator

ℹ️

pfSense GUI : ファイアウォール規則リスト

1つのボタンをクリックすると、選択した行の上に新しいルールが追加され、もう1つのボタンをクリックすると、選択したルールの下にルールが追加されます。どちらのボタンも最初のルールに使用できます。

ステップ 3 : IPアドレスのポート443へのトラフィックを許可するファイアウォールルールを作成します

pfSense  
COMMUNITY EDITION

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

Firewall / Rules / Edit

### Edit Firewall Rule

**Action**

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

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

**Interface**

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

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

### Source

**Source**  Invert match   /

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

### Destination

**Destination**  Invert match   /

**Destination Port Range**

From Custom To Custom

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

### Extra Options

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

**Description**

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

**Advanced Options**

pfSense GUI : ファイアウォールパスルールの設定

この情報を使用してルールを作成します。

- アクション : [パス]を選択します
- Interface : ルールが適用されるインターフェイスを選択します。
- アドレスファミリとプロトコル : 必要に応じて選択
- ソース : 「任意」として選択したままにします。
- Destination: DestinationドロップダウンからAddressまたはAliasを選択し、ルールが適用されるIPアドレスを入力します
- Destination Port Range:FromとToの両方のドロップダウンでHTTPS(443)を選択します。
- ログ : このルールに一致するパケットをアカウントティング用としてログに記録するには、チェックボックスをオンにします



- ・ 説明：後でルールを参照するテキストを入力します

[Save] を選択します。

ステップ 4：他のすべてのトラフィックをpfSenseにドロップするファイアウォールルールを作成します

「追加」ボタンを選択して、新しく作成した規則の下に規則を挿入します。

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

- Action:** Set to 'Block'. A hint explains the difference between block and reject.
- Disabled:** 'Disable this rule' is unchecked.
- Interface:** Set to 'WAN'.
- Address Family:** Set to 'IPv4'.
- Protocol:** Set to 'TCP'.
- Source:** 'Source' is 'Any', 'Invert match' is unchecked. A 'Display Advanced' button is present.
- Destination:** 'Destination' is 'Any', 'Invert match' is unchecked. 'Destination Port Range' is set to '(other)' for both 'From' and 'To' fields.
- Extra Options:** 'Log' is checked. 'Description' is 'Drop all other inbound traffic'.
- Advanced Options:** A 'Display Advanced' button is present.
- Save:** A blue 'Save' button is at the bottom.

pfSense GUI：ファイアウォールドロップルールの設定

- アクション：ブロックを選択
- Interface：ルールが適用されるインターフェイスを選択します。
- アドレスファミリとプロトコル：必要に応じて選択
- ソース：「任意」として選択したままにします。
- 宛先：「任意」として選択したままにします
- ログ：このルールに一致するパケットをアカウントリング用としてログに記録するには、チェックボックスをオンにします
- 説明：後でルールを参照するテキストを入力します

[Save] を選択します。

ステップ 5：ルールを確認し、ブロックルールが一番下にあることを確認します

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The page displays a list of rules with the following columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The rules are ordered as follows:

| 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 | 📌✎📄🗑️   |

At the bottom of the table, there are several action buttons: Add (up arrow), Add (down arrow), Delete, Toggle, Copy, Save, and Separator.

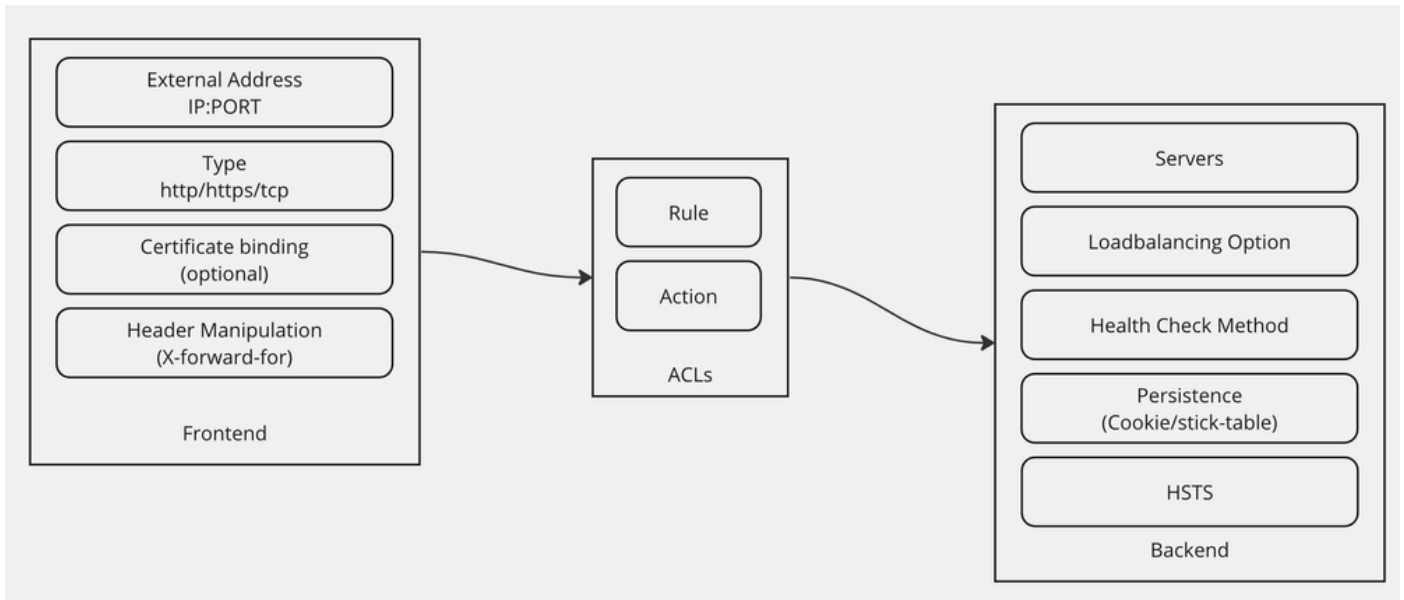
pfSense GUI：ファイアウォール規則リスト

必要に応じて、ルールをドラッグして並べ替えます。

環境に必要な順序にファイアウォールルールが並んだら、Apply Changesを選択します。

## HAProxyの設定

### HAProxyの概念



## HAProxyの概念

HAProxyは、フロントエンド/バックエンドモデルで実装されます。

フロントエンドは、顧客が通信するプロキシの側を定義します。

フロントエンドはIPとポートの組み合わせ、証明書のバインドで構成され、いくつかのヘッダー操作を実装できます。

バックエンドは、物理Webサーバと通信するプロキシの側を定義します。

バックエンドは、実際のサーバとポート、初期割り当て、ヘルスチェック、持続性のためのロードバランシング方式を定義します。

フロントエンドは、専用バックエンドまたはACLを使用して、どのバックエンドと通信すればよいかを認識します。

ACLはさまざまなルールを作成できるため、特定のフロントエンドがさまざまな要素に応じて異なるバックエンドと通信できます。

## HAProxyの初期設定

ステップ 1 : Services ドロップダウンからHAProxyを選択します

The screenshot shows the pfSense Community Edition interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Services' menu is open, listing various services such as Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, HAProxy (highlighted with a red box), IGMP Proxy, NTP, PPPoE Server, Router Advertisement, SNMP, and Wake-on-LAN. The main content area is divided into two sections: 'System Information' and 'Netgate Services And Support'. The 'System Information' section displays details like Name (ucproxy02.uclabservices.com), User (admin@14.10.162.125), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), Version (2.7.2-RELEASE), and CPU Type (Intel(R) Xeon(R) Platinum 8180 CPU). The 'Netgate Services And Support' section shows the contract type as 'Community Support' and provides links to 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES'.

pfSense GUI - HAProxy ドロップダウン

## ステップ 2 : 基本設定の構成

## General settings

 Enable HAProxy

**Installed version** 2.8.3-86e043a
**Maximum connections**


per process.

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

Current 'System Tunables' settings.

'kern.maxfiles': **30767**

'kern.maxfilesperproc': **27684**

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

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

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

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

**Number of threads to start per process**


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

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

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

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

**Reload stop behaviour**


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

**Carp monitor**


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

## Stats tab, 'internal' stats port

**Internal stats port**


EXAMPLE: 2200

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

**Internal stats refresh rate**


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

**Sticktable page refresh rate**


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

pfSense GUI:HAProxyのメイン設定

Enable HAProxyチェックボックスをオンにします。

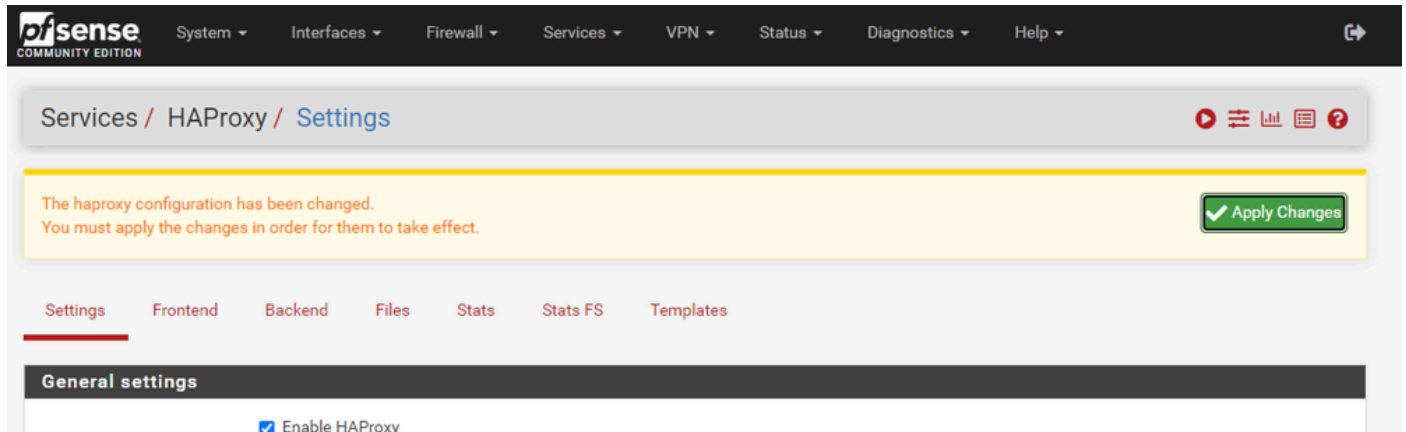
[最大接続数]に値を入力します。必要なメモリの詳細については、このセクションの表を参照してください。

内部統計ポートの値を入力します。このポートは、アプライアンスのHAProxy統計情報を表示するために使用されますが、アプライアンスの外部には公開されません。

[内部統計の更新間隔]に値を入力します。

残りの設定を確認し、必要に応じて環境を更新します。

[Save] を選択します。



Services / HAProxy / Settings

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


Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

General settings

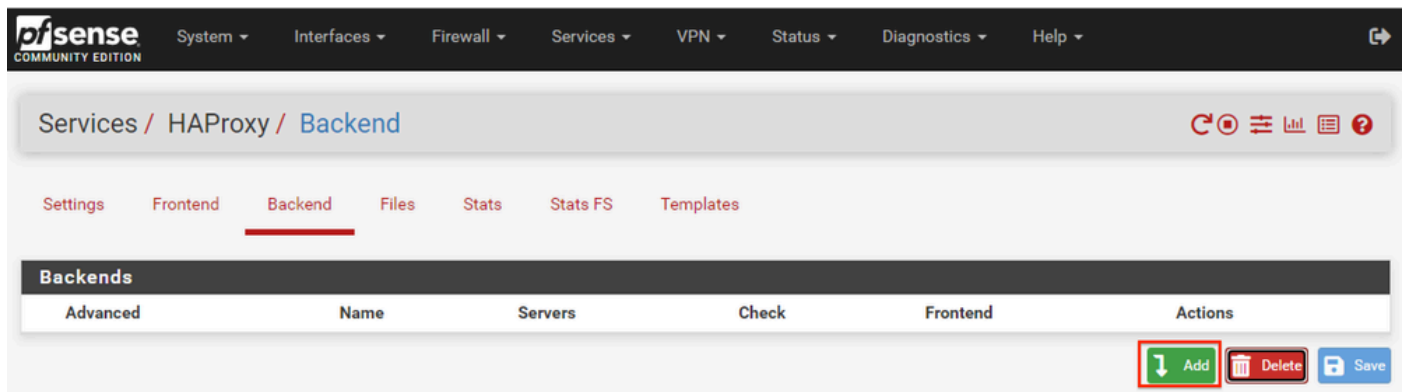
Enable HAProxy

pfSense GUI:HAProxyによる変更の適用

 注：設定変更は、[Apply Changes]ボタンを選択するまでアクティブになりません。複数の設定変更を行い、それらすべてを一度に適用できます。別のセクションで使用するために設定を適用する必要はありません。

## HAProxyバックエンドの設定




バックエンドから開始します。この理由は、フロントエンドがバックエンドを参照しなければならないからです。[バックエンド]メニューが選択されていることを確認します。



Services / HAProxy / Backend

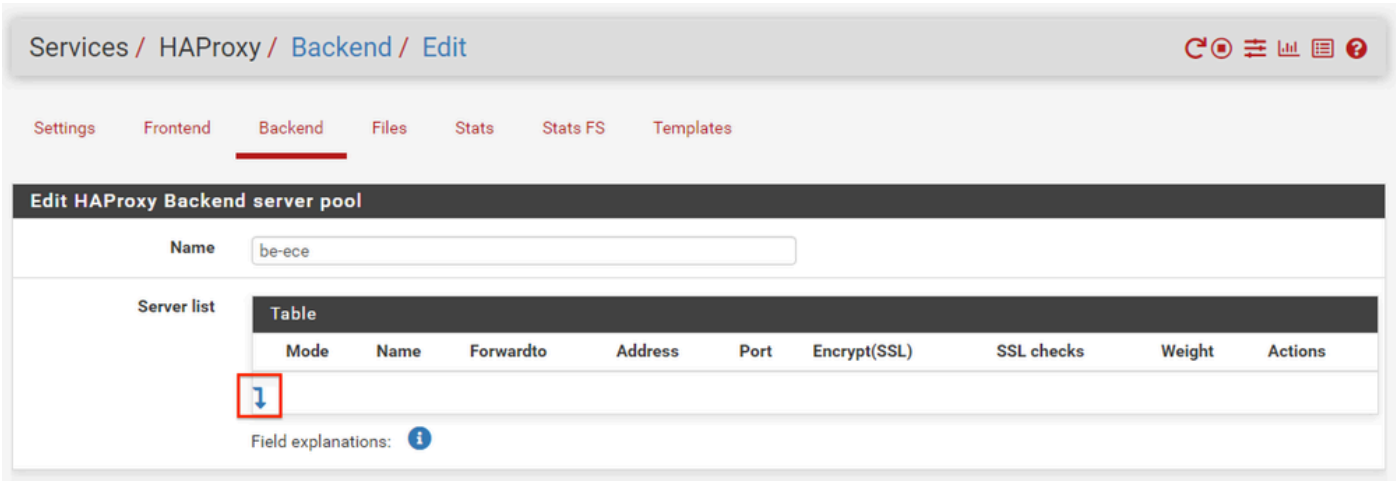
Settings Frontend Backend Files Stats Stats FS Templates

Backends

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

pfSense GUI:HAProxyによるバックエンドの追加

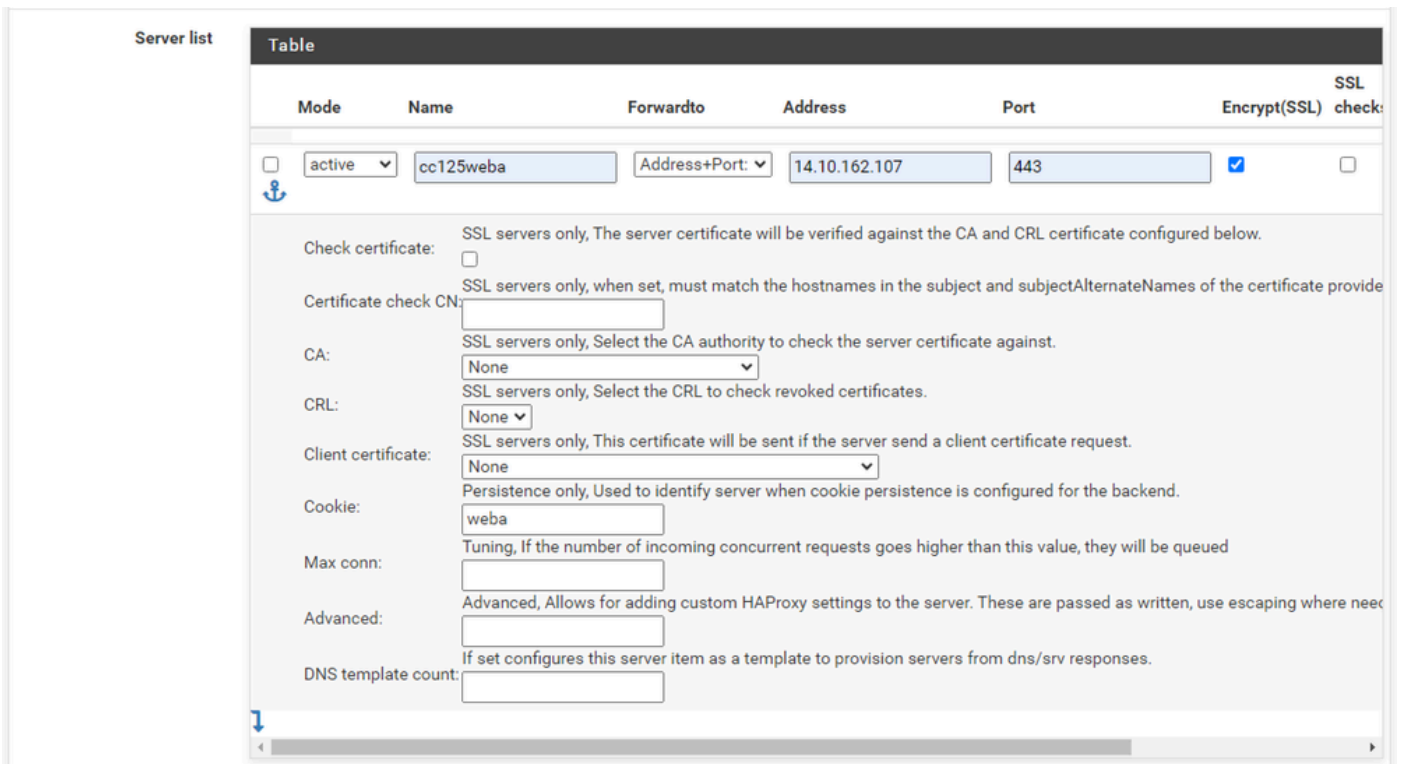
Addボタンを選択します。



pfSense GUI:HAProxyバックエンド開始

バックエンドの名前を指定します。

下矢印を選択して、最初のサーバをサーバリストに追加します



バックエンド - サーバリスト

サーバを参照する名前を指定します。これは、実際のサーバ名と一致する必要はありません。この名前が統計ページに表示されます。

サーバのアドレスを入力します。これは、FQDNのIPアドレスとして設定できます。

接続先のポートを指定します。ECEのポート443である必要があります。

「暗号化(SSL)」チェックボックスを選択します。

Cookieフィールドに値を入力します。これはセッションスティッキ性Cookieの内容であり、パッ

クエンド内で一意である必要があります。

最初のサーバを設定した後、下向き矢印を選択して、環境内の他のWebサーバを設定します。

**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バックエンド - ロードバランシング

ロードバランシングオプションを設定します。

ECEサーバーの場合は、「最小接続」に設定する必要があります。



| Access control lists and actions |   |
|----------------------------------|---|
| <b>Timeout / retry settings</b>  |   |
| Connection timeout               | 60000<br>The time (in milliseconds) we give up if the connection does not complete within (default 30000).  |
| Server timeout                   | 60000<br>The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).   |
| Retries                          | 2<br>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.  |
| <b>Health checking</b>           |   |
| Health check method              | HTTP<br><small>HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).</small>   |
| Check frequency                  | <br>milliseconds<br>For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.  |
| Log checks                       | <input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged.<br>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<br><small>OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the webserver and is less easy to filter out of its logs.</small>  |
| Url used by http check requests. | /system/web/view/platform/common/login/root.jsp?partitionId=1<br>Defaults to / if left blank.   |
| Http check version               | HTTP/1.1\r\nHost:\ ece125.uclabservices.com<br>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:<br><code>HTTP/1.1\r\nHost:\ www</code><br>Also some hosts might require an accept parameter like this:<br><code>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</code> |

## HAProxyバックエンド - ヘルスチェック

この設定では、アクセスコントロールリスト(ACL)は使用されません。

タイムアウト/再試行設定は、デフォルト設定のままにしておくことができます。

ヘルスチェックセクションを設定します。

- ヘルスチェック方法 : HTTP
- 頻度の確認 : 空白のままにして、1秒ごとのデフォルトを使用します。
- ログのチェック : このオプションを選択すると、ログに健全性の変更が書き込まれます。
- Httpチェック方法 : リストからGETを選択します。
- httpチェックリクエストで使用されるURL。 : ECEサーバーの場合は、  
/system/web/view/platform/common/login/root.jsp?partitionId=1と入力します。
- HTTPチェックバージョン : Enter、HTTP/1.1\r\nHost:\ {fqdn\_of\_server}

最後のバックスラッシュの後、サーバのFQDNの前にスペースを入れてください。

**Agent checks**

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

**Cookie persistence**

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

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

**Cookie Name**   
The string name to track in Set-Cookie and Cookie HTTP headers.  
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASPNET\_SessionId

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

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

**Cookie Cachable**  Allows shared caches to cache the server response.

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

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

**Cookie domains**   
Domains to set the cookie for, 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**   
Sticktables that are kept in memory, and when matched make sure the same server will be used.  
`No stick-table will be used`

**Email notifications**

**Mail level**   
Define the maximum loglevel to send emails for.

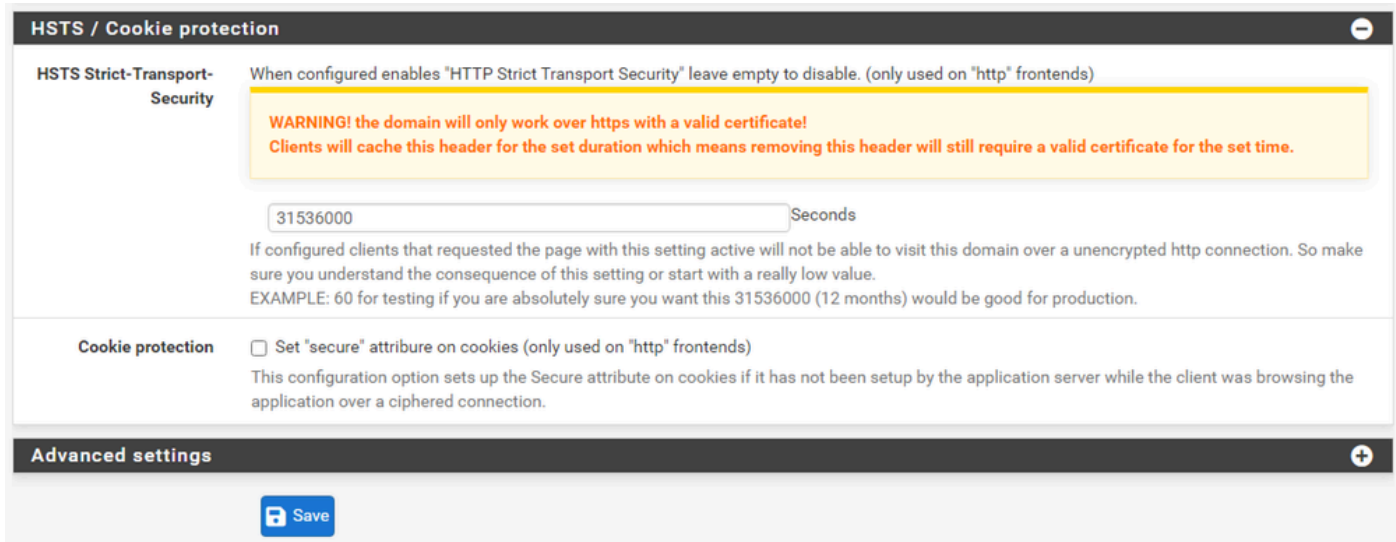
**Mail to**   
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

HAProxyバックエンド – クッキーの持続性

エージェントチェックは選択しないままにします。

クッキーの持続性を設定します。

1. Cookie Enabled : クッキーベースの持続性を有効にする場合に選択します。
2. Cookie名 : Cookieの名前を指定します。
3. クッキーモード : ドロップダウンボックスから[挿入]を選択します。
4. 残りのオプションは未設定のままにします。



HAProxyバックエンド – HSTS

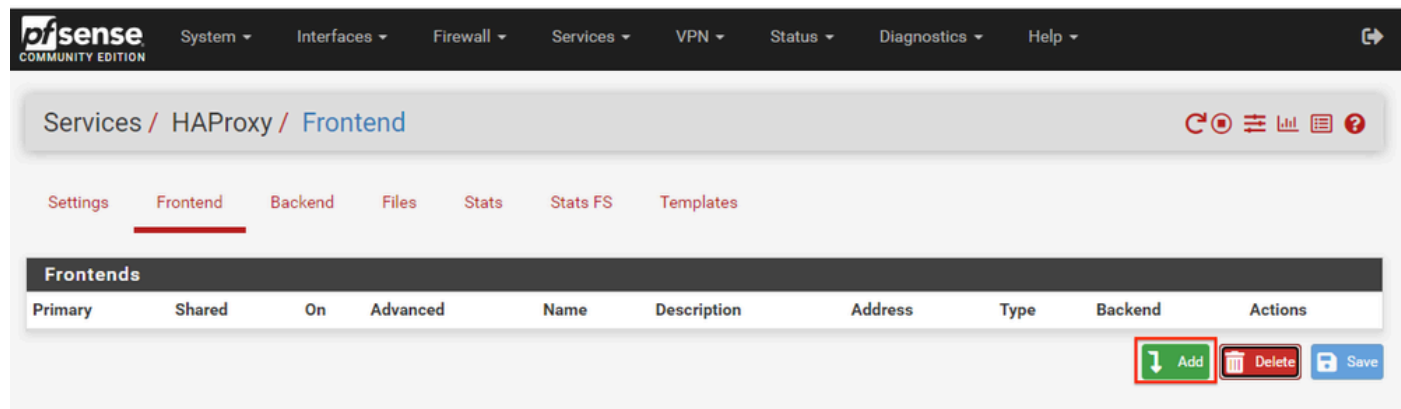
バックエンド構成フォームの残りのセクションは、デフォルト設定のままにしておくことができます。

HSTSを設定する場合は、このセクションでタイムアウト値を設定します。ECEはHSTSクッキーも挿入するため、この設定は冗長になります。

Saveを選択します。

## HAProxyフロントエンドの設定

フロントエンドメニューに変更します。



pfSense GUI - HAProxyフロントエンドの追加

Addボタンを選択します

Settings Frontend Backend Files Stats Stats FS Templates

### Edit HAProxy Frontend

**Name**

**Description**

**Status**

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

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

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

**Max connections**

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

**Type**

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

HAProxy – フロントエンドヘッダー

フロントエンドの名前を指定します。

フロントエンドを後で識別するのに役立つ説明を提供します。

外部アドレステーブルで次の操作を行います。

1. リッスンアドレス：このWebサイト用に作成したVIPを選択します。
2. ポート：443と入力します。
3. SSLオフロード：このオプションを選択すると、セッションCookieを挿入できます。

Max connectionsは空のままにします。

Typeにhttp/https(offloading)が選択されていることを確認します。

## 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 will not be the same as WWW.domain.TLD  
- 'Not' makes the match if the value given is not matched

Example:

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

acl's with the same name will be 'combined' using OR criteria.

For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

**NOTE Important change in behaviour, since package version 0.32**

-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.

-acl's alone no longer implicitly generate use\_backend configuration. Add 'actions' below to accomplish this behaviour.

### Actions

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

#### Table

| Action | Parameters | Condition acl names | Actions |
|--------|------------|---------------------|---------|
|        |            |                     |         |

Example:

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

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 – デフォルトのバックエンド選択

最も簡単な設定は、ドロップダウンからデフォルトバックエンドを選択することです。これは、VIPが単一のWebサイトをホストする場合に選択できます。

### Default backend, access control lists and actions

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

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

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

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

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

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

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

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

Example:  

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

**Default Backend**

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

#### HAProxyバックエンド – ACLアドバンスド

図に示すように、ACLを使用すると、条件に基づいて単一のフロントエンドを複数のバックエンドにリダイレクトできます。

要求のホストが名前とポート番号、または単に名前が始まるかどうかを確認するためにACLがチェックしていることがわかります。これに基づいて、特定のバックエンドが使用されます。

これはECEでは一般的ではありません。

**SSL Offloading**

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

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

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

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

**Additional certificates** Which of these certificate will be send will be determined by 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-ssl3, force-tls10 force-tls11 force-tls12 no-ssl3 no-tls10 no-tls11 no-tls12 no-tls-tickets  
Example: no-ssl3 ciphers ECDH+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 ECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecdhe secp256k1

#### HAProxyフロントエンド – 証明書バインド

[SSLオフロード]セクションで、このサイトで使用するために作成した証明書を選択します。この証明書はサーバ証明書である必要があります。

オプションのAdd ACL for certificate Subject Alternative Namesを選択します。

残りのオプションはデフォルト値のままにしておくことができます。

このフォームの最後にあるSaveを選択します。

Services / HAProxy / Frontend

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

Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

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

Add Delete Save

HAProxy – 設定の適用

Apply Changesを選択して、フロントエンドとバックエンドの変更を実行コンフィギュレーションにコミットします。

これで、pfSenseのセットアップと設定は完了です。



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。