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

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。特定の実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。

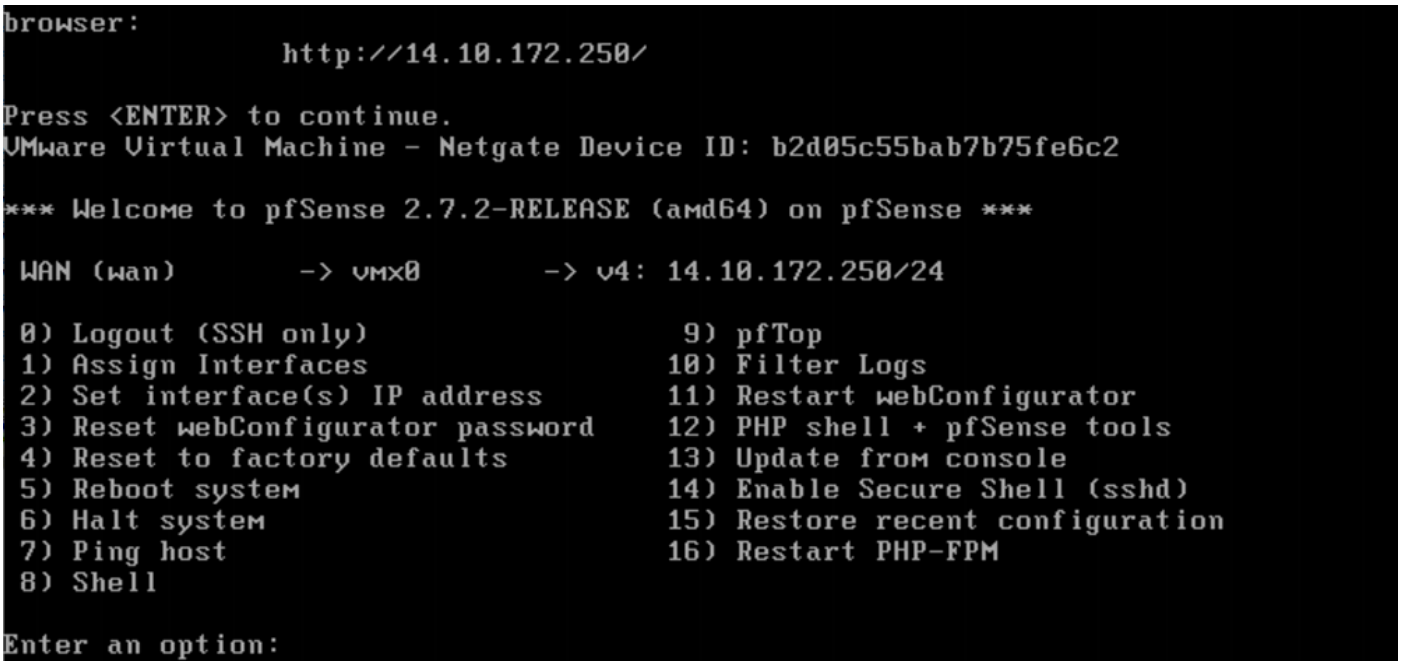
ステップ 4：その他のインターフェイスの割り当て

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。

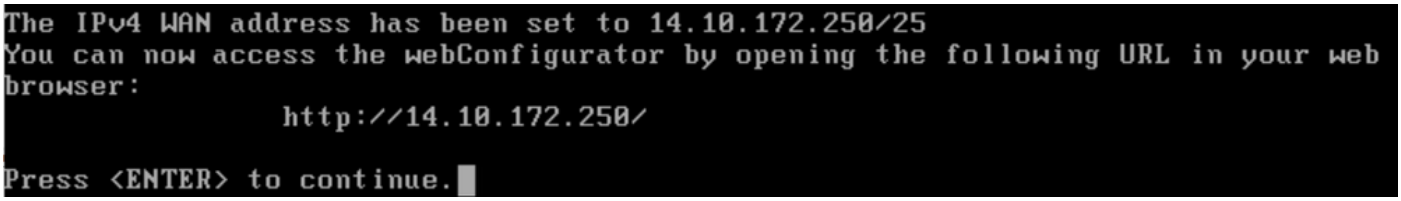


pfSenseコンソール

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。

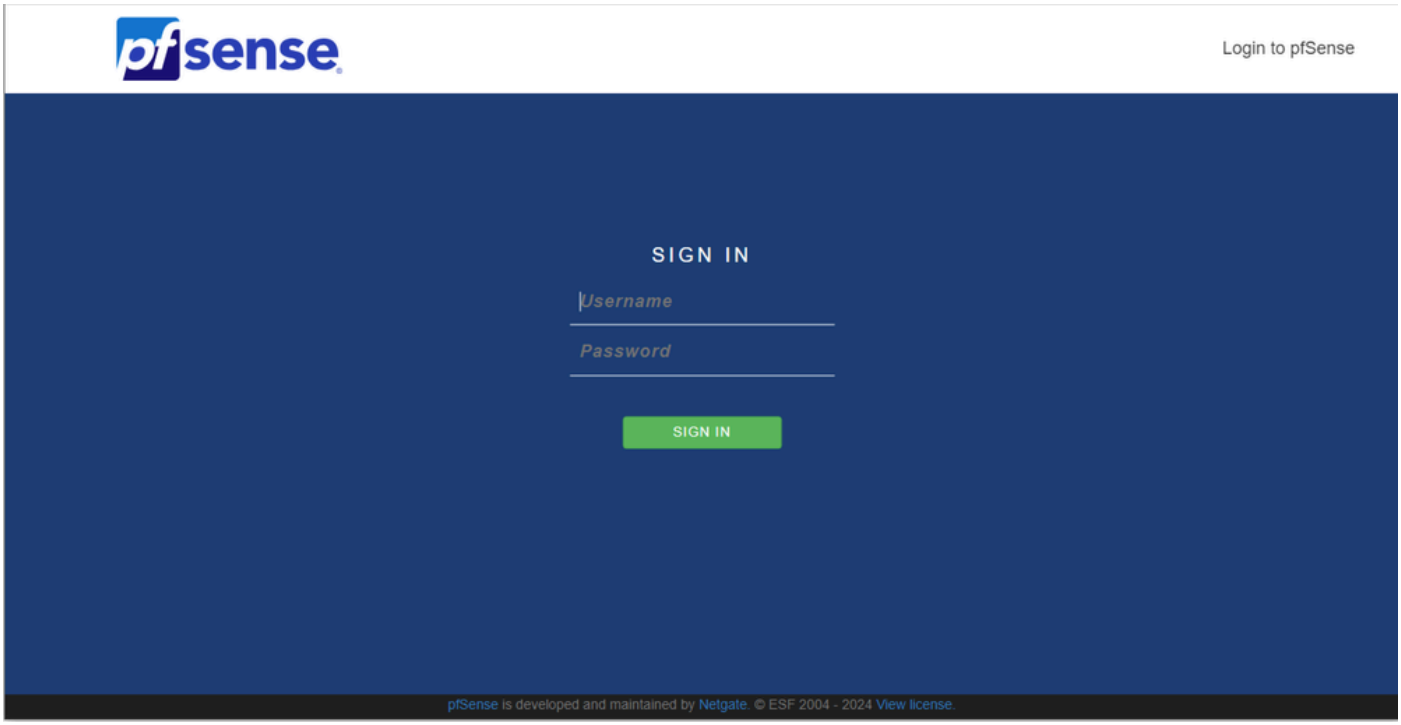


pfSenseの確認

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。

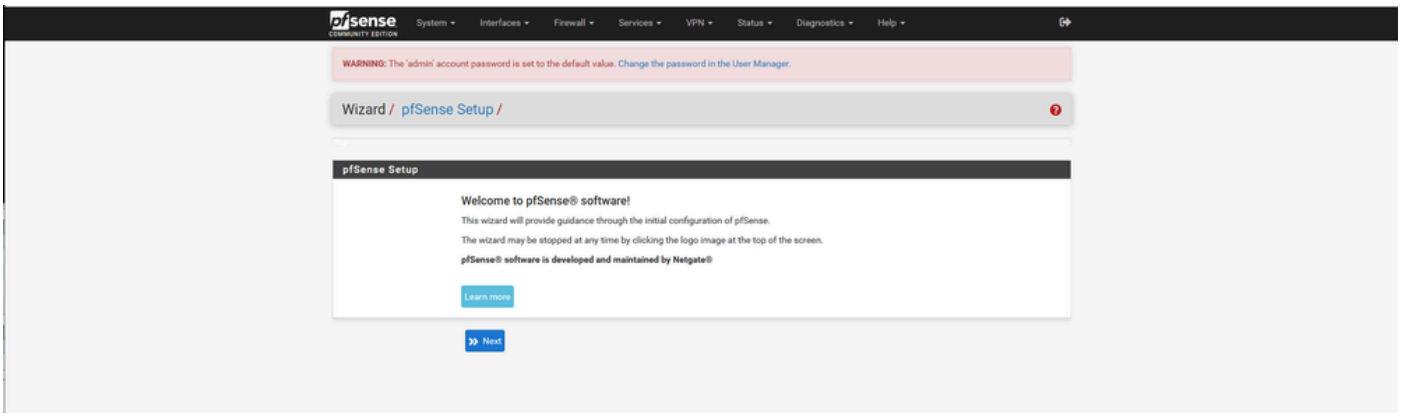


pfSense管理ログイン

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。

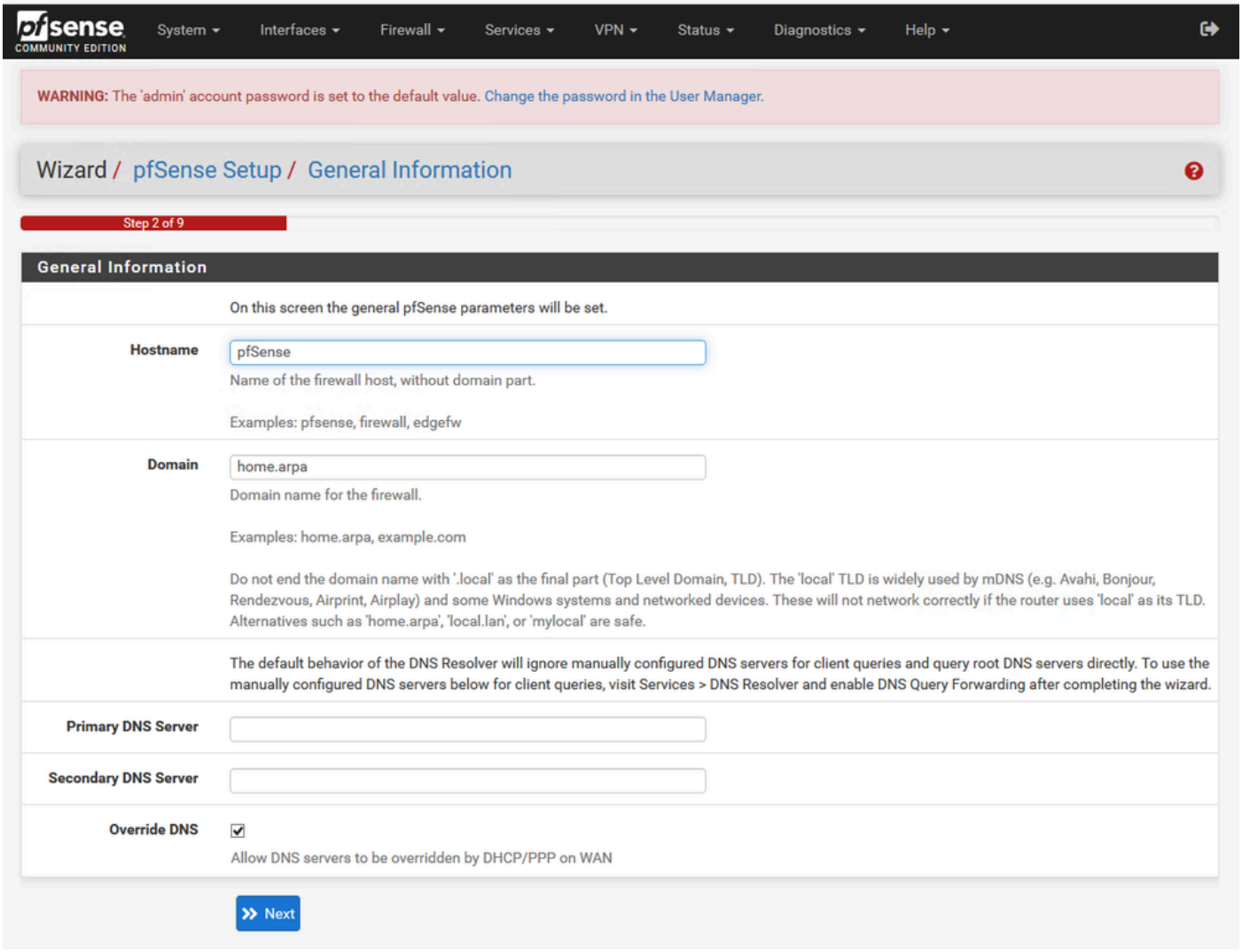
ステップ 3：初期設定を完了する

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

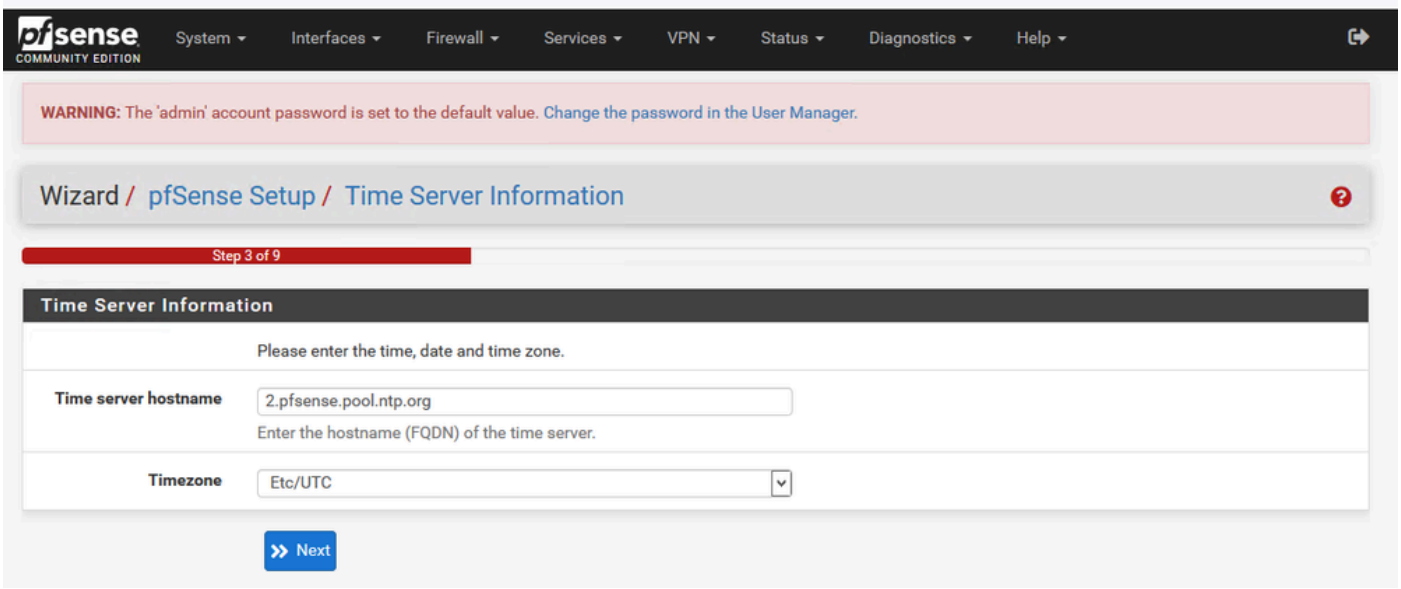
ホスト名、ドメイン名、およびDNSサーバ情報を入力します。



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。



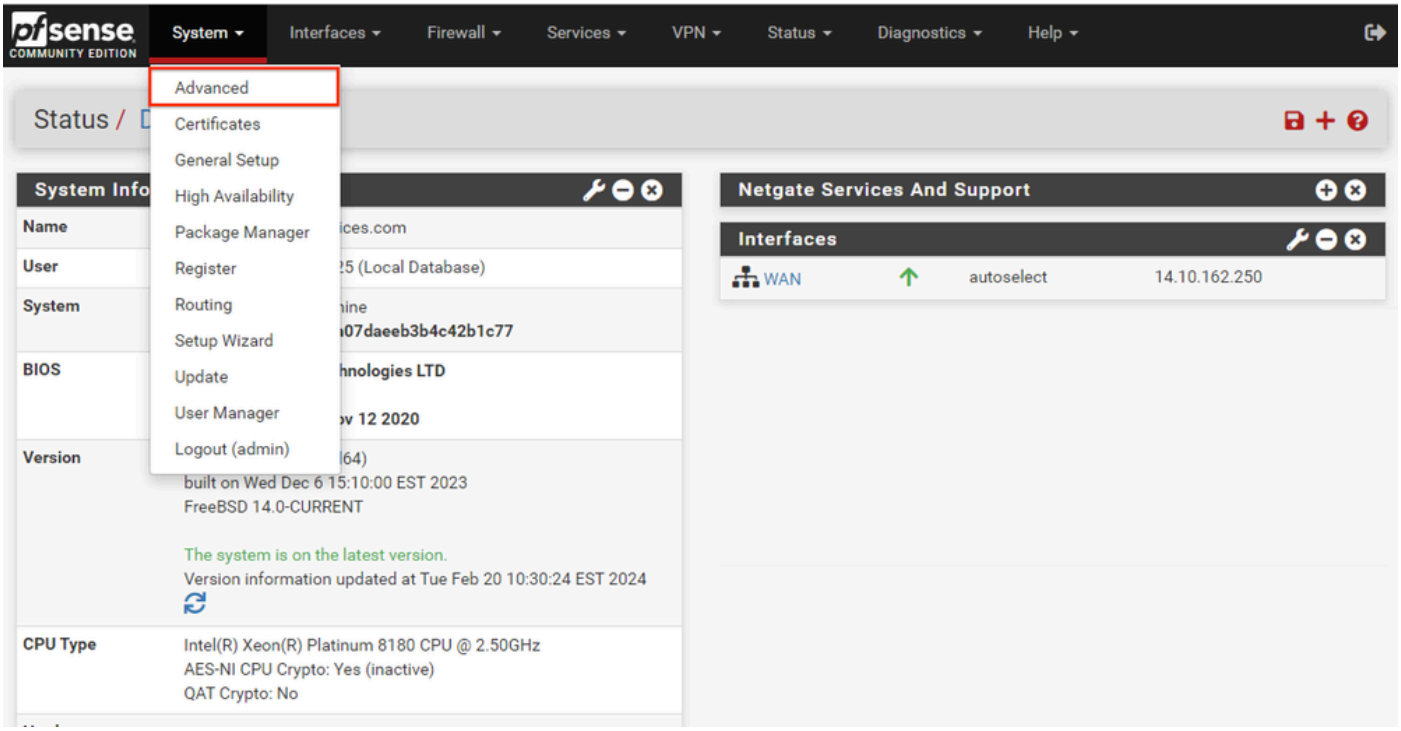
pfSenseセットアップウィザード – 3

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

pfSense GUI：管理設定

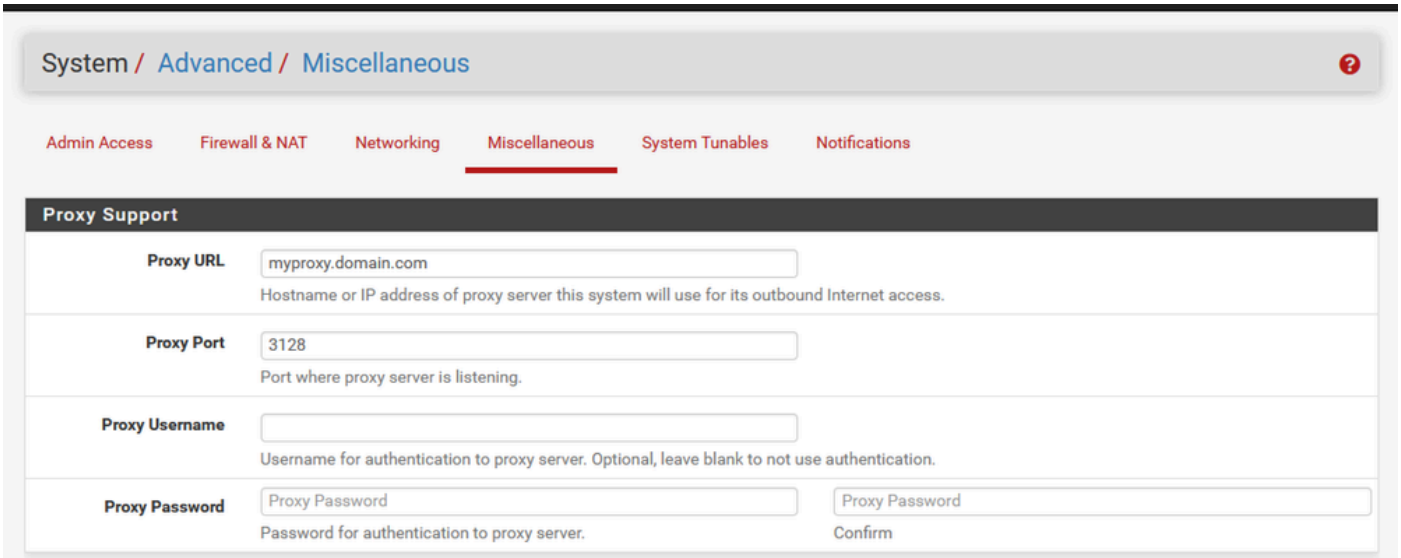
1. HTTPS(SSL/TLS)プロトコルを選択します。
2. この時点では、SSL/TLS証明書を自己署名証明書のままにしておきます。
3. TCPポートを443以外のポートに変更して、インターフェイスのセキュリティを強化し、ポートのオーバーラップの問題を防止します。
4. WebGUIリダイレクトオプションを選択して、ポート80の管理インターフェイスを無効にします。
5. Browser HTTP_REFERERエンフォースメントオプションを選択します。

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。



pfSense GUI：プロキシ設定

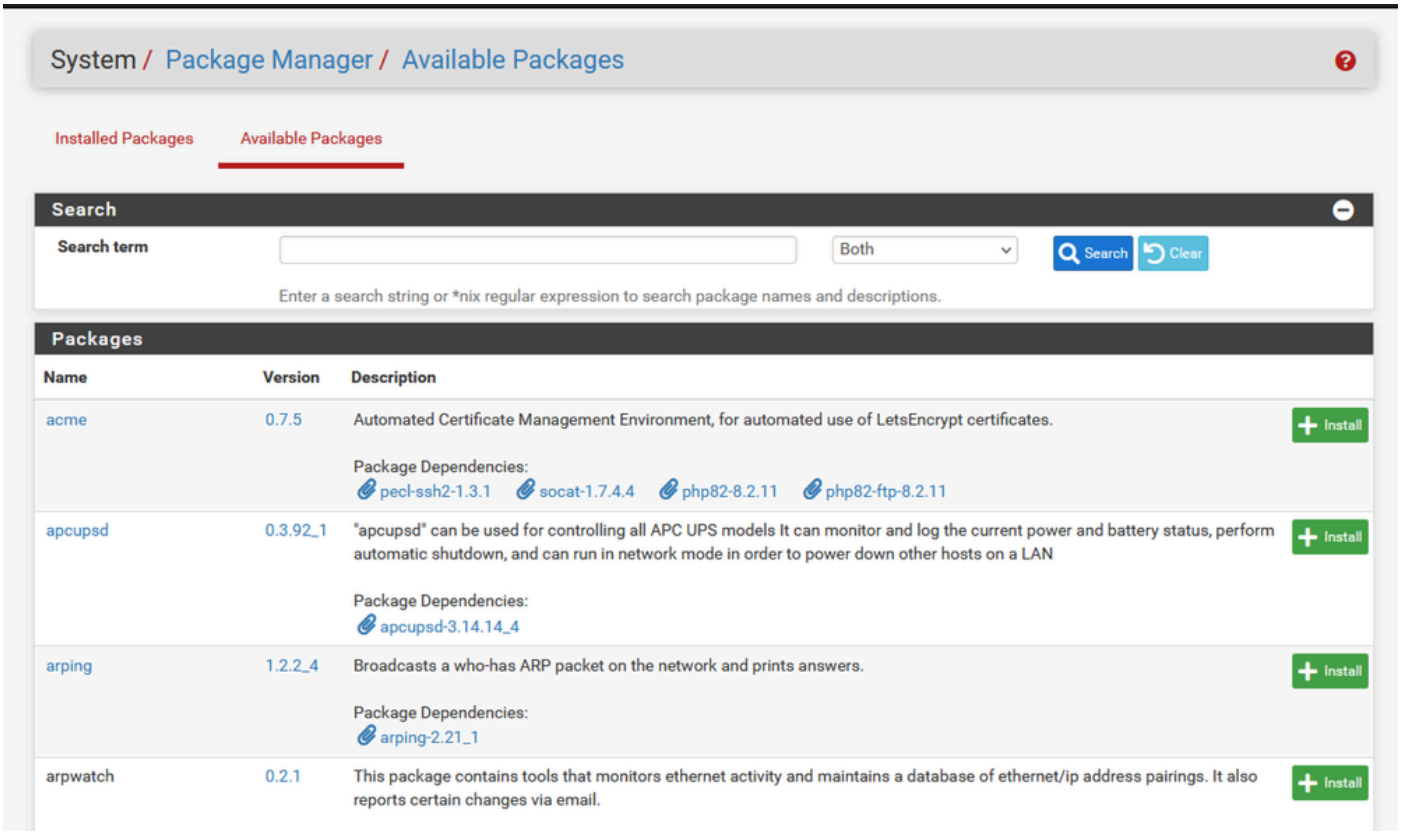
注：変更を加えた後は、必ずSaveボタンを選択してください。

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。



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。

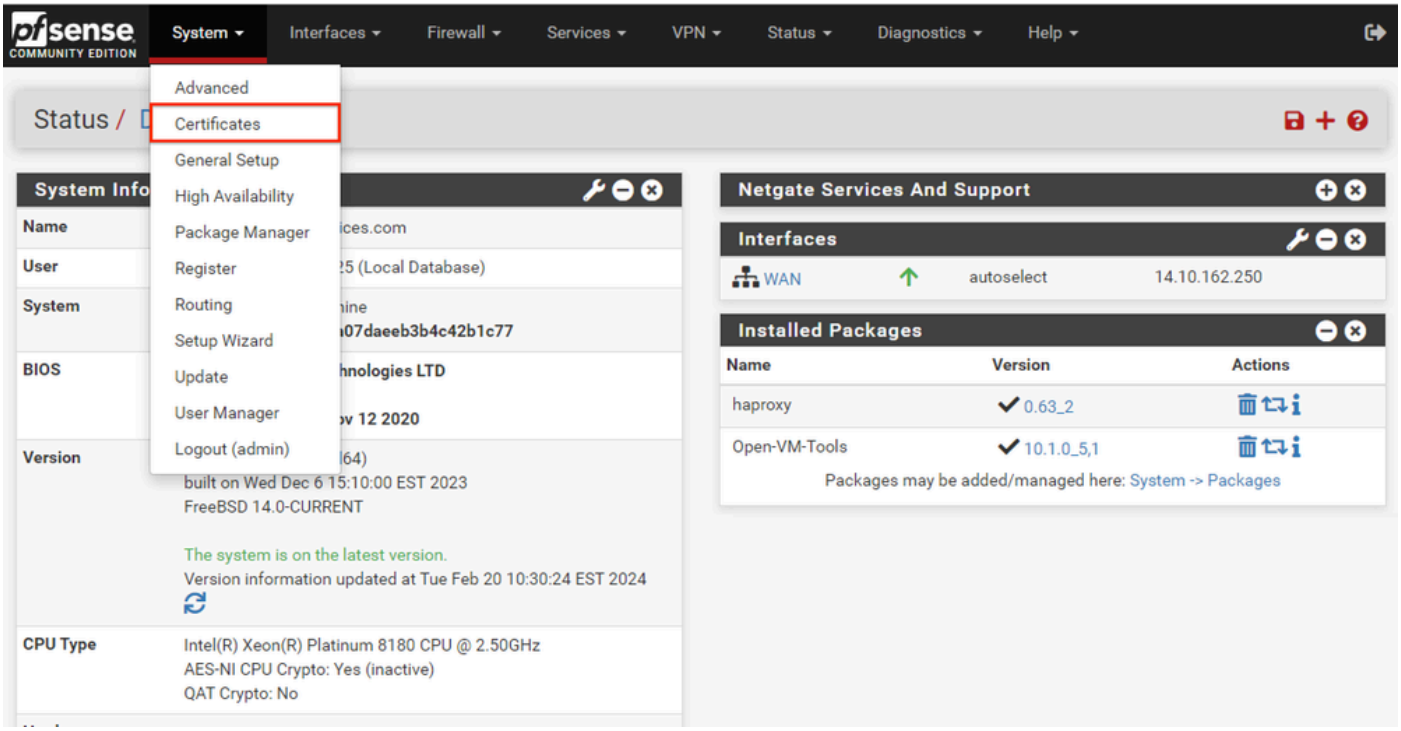
証明書の設定

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。

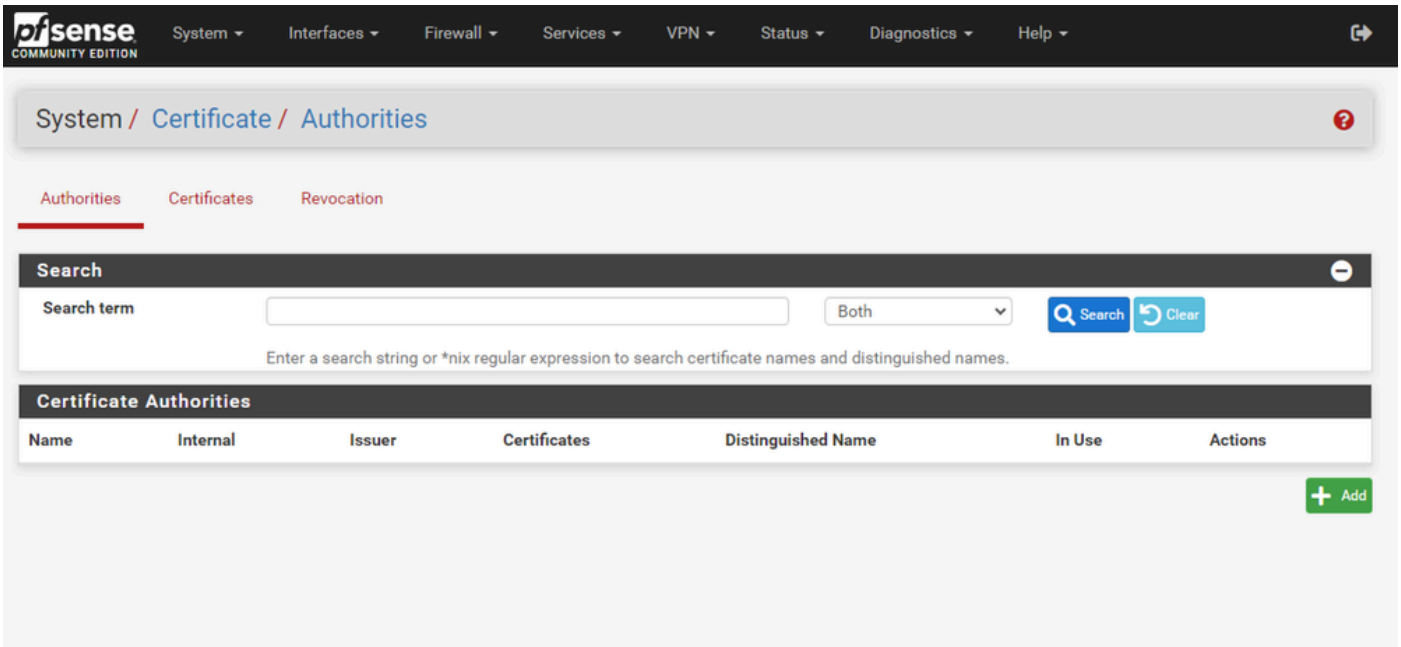
1. PEMまたはBase-64エンコード形式で保存されたCAのルート証明書。
2. PEMまたはBase-64エンコード形式で保存されるCAのすべての中間（発行側と呼ばれることもあります）証明書。

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



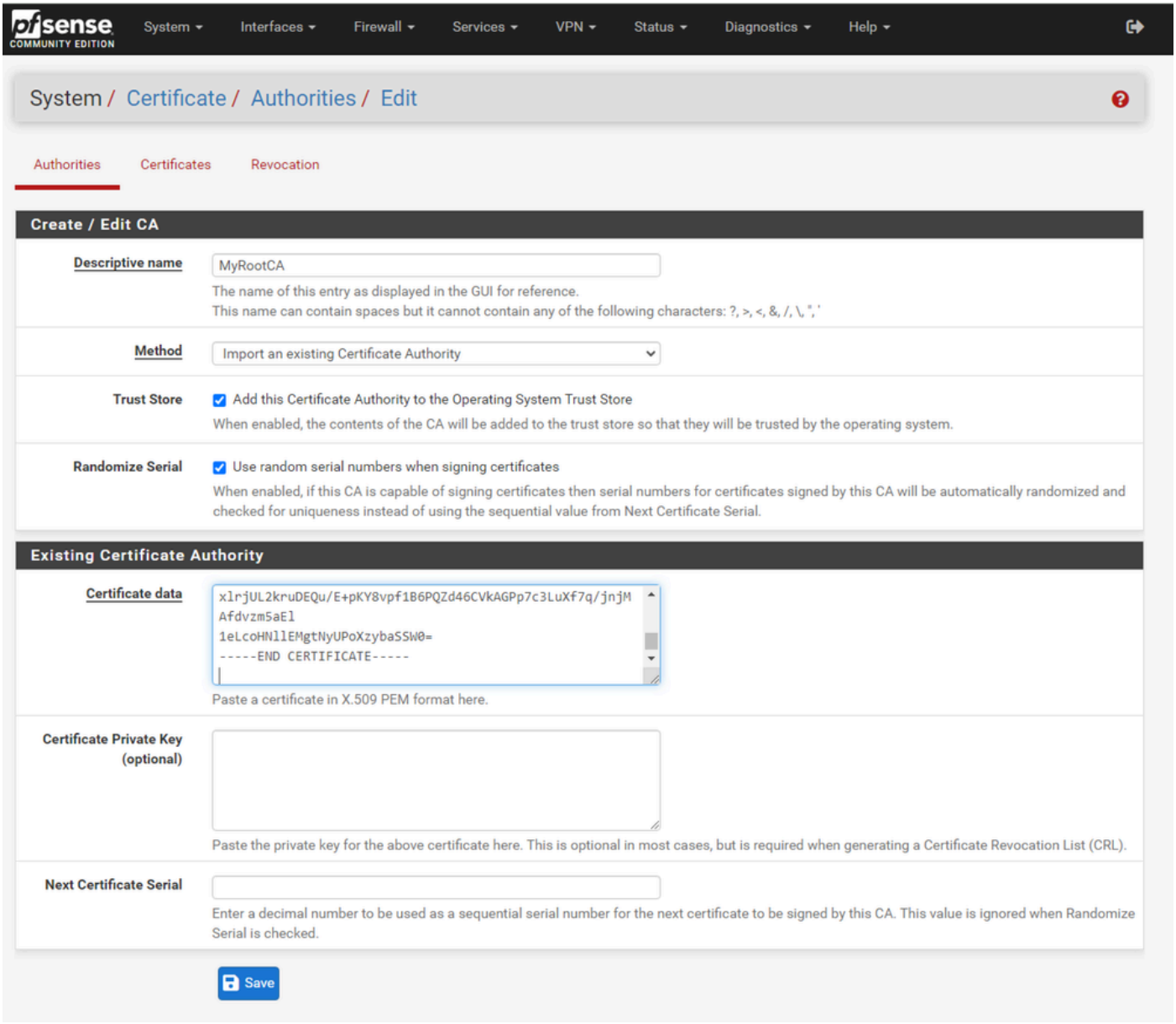
pfSense GUI – 証明書ドロップダウン

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。



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

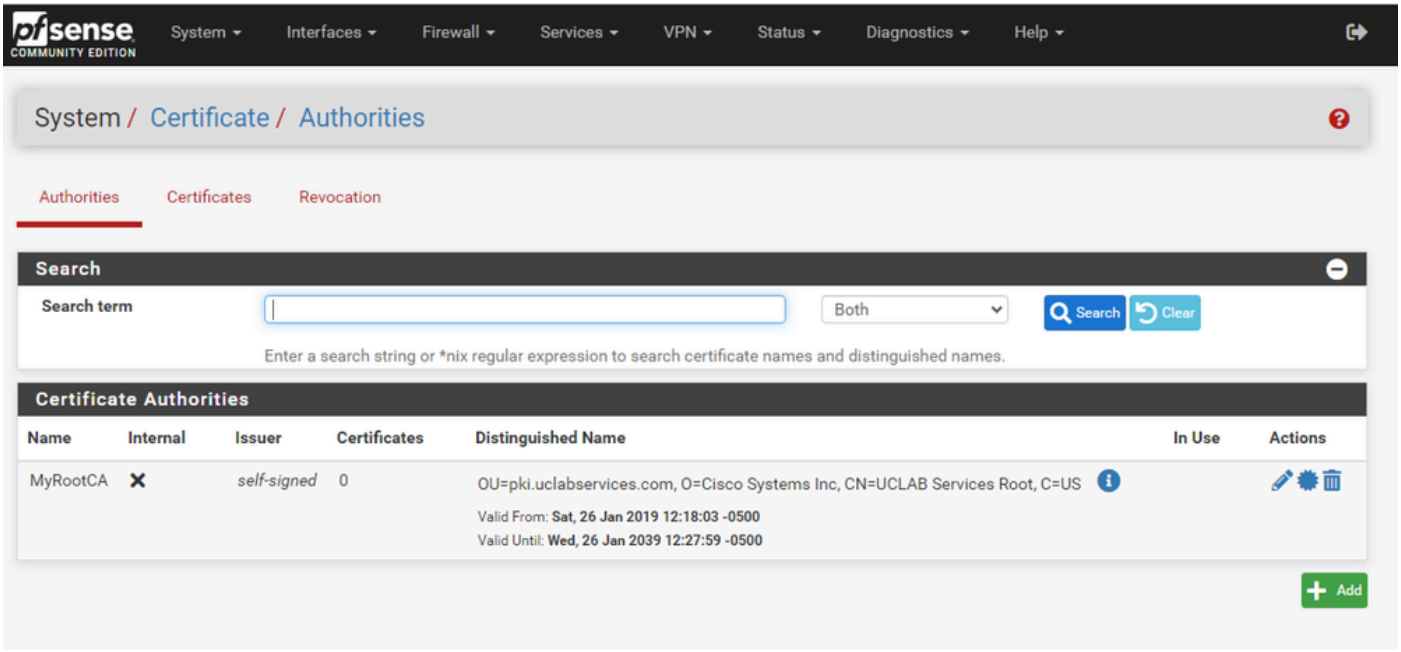
2.「方法」ドロップダウンから「既存の認証局のインポート」を選択します。

3.「信頼ストア」および「シリアルのランダム化」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。

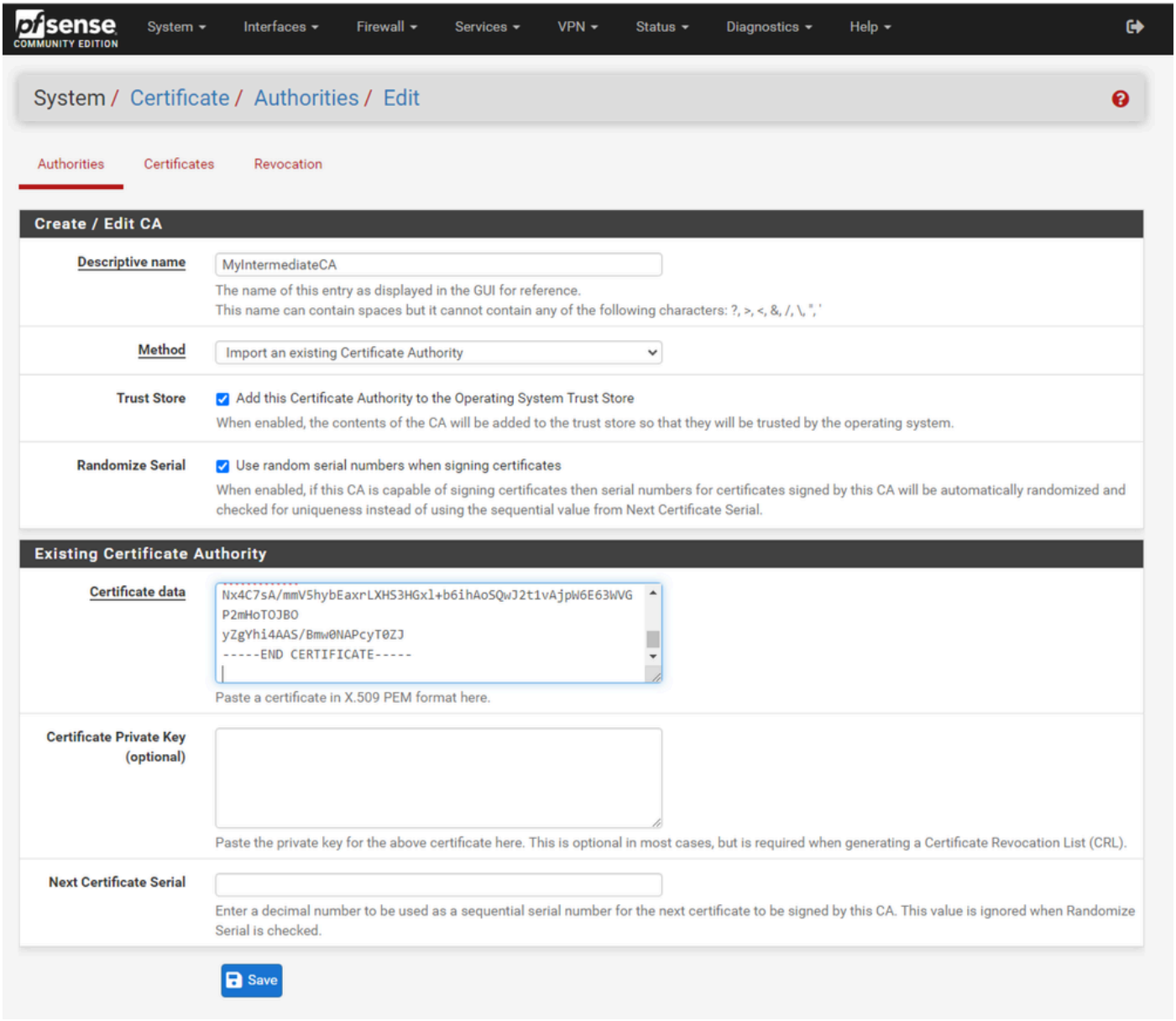
5. Saveを選択します。

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。



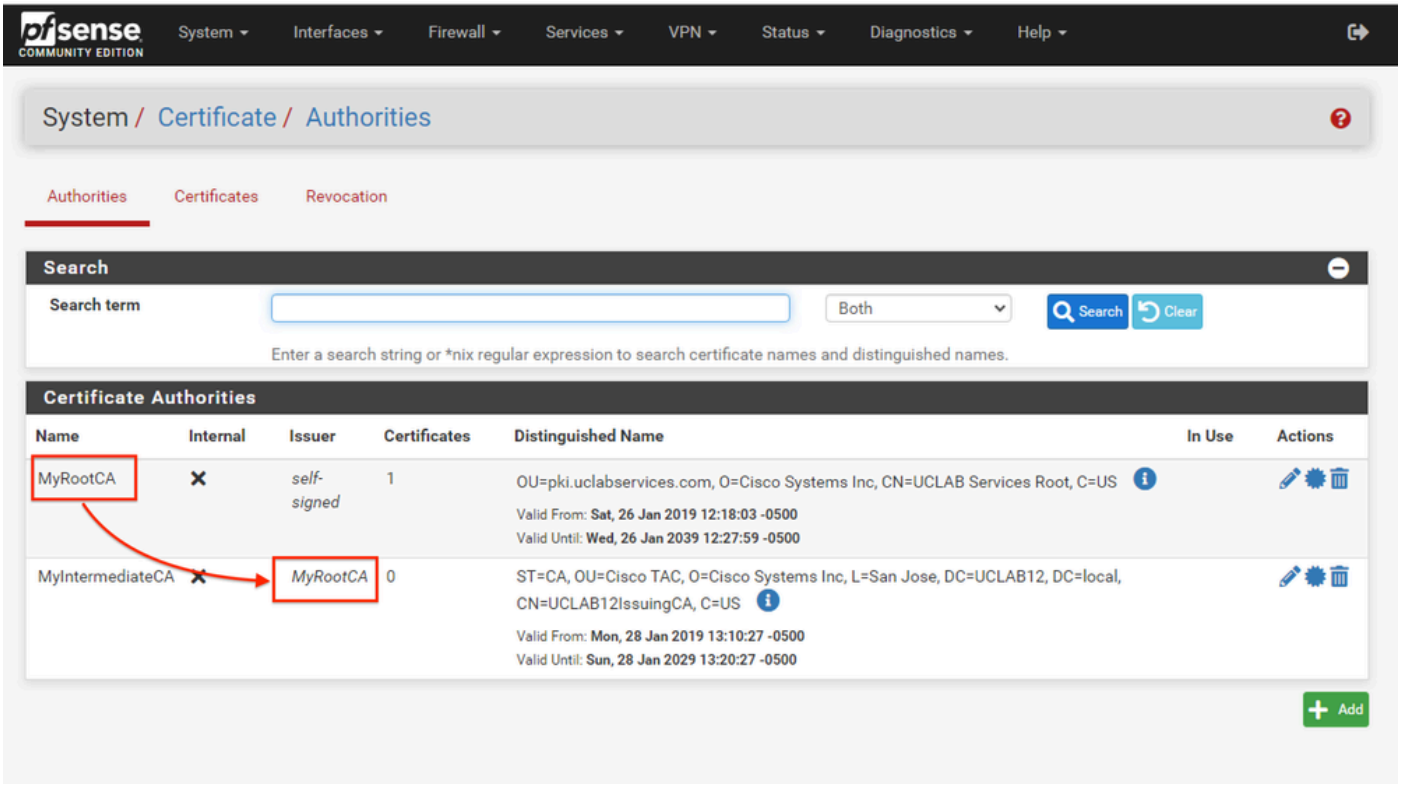
pfSense GUI:CAリスト

ステップ 3：CA中間証明書のインポート



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。



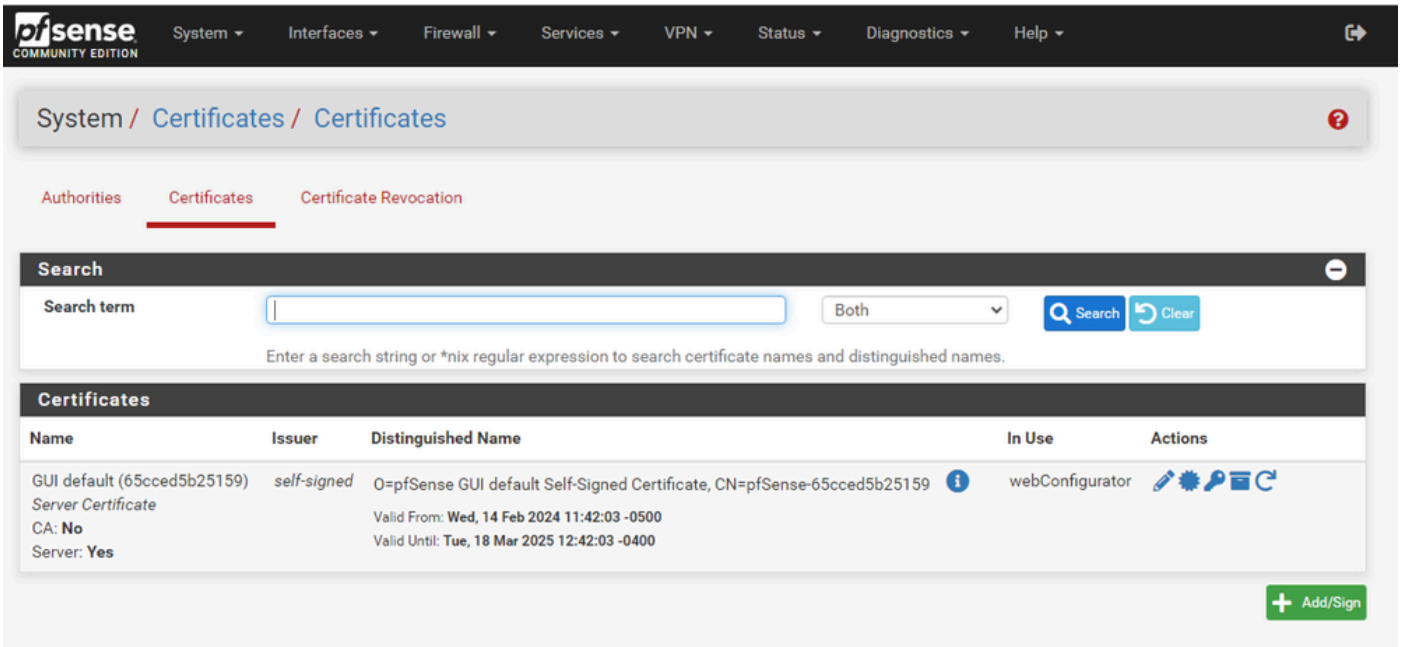
pfSense GUI:CAリンク

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

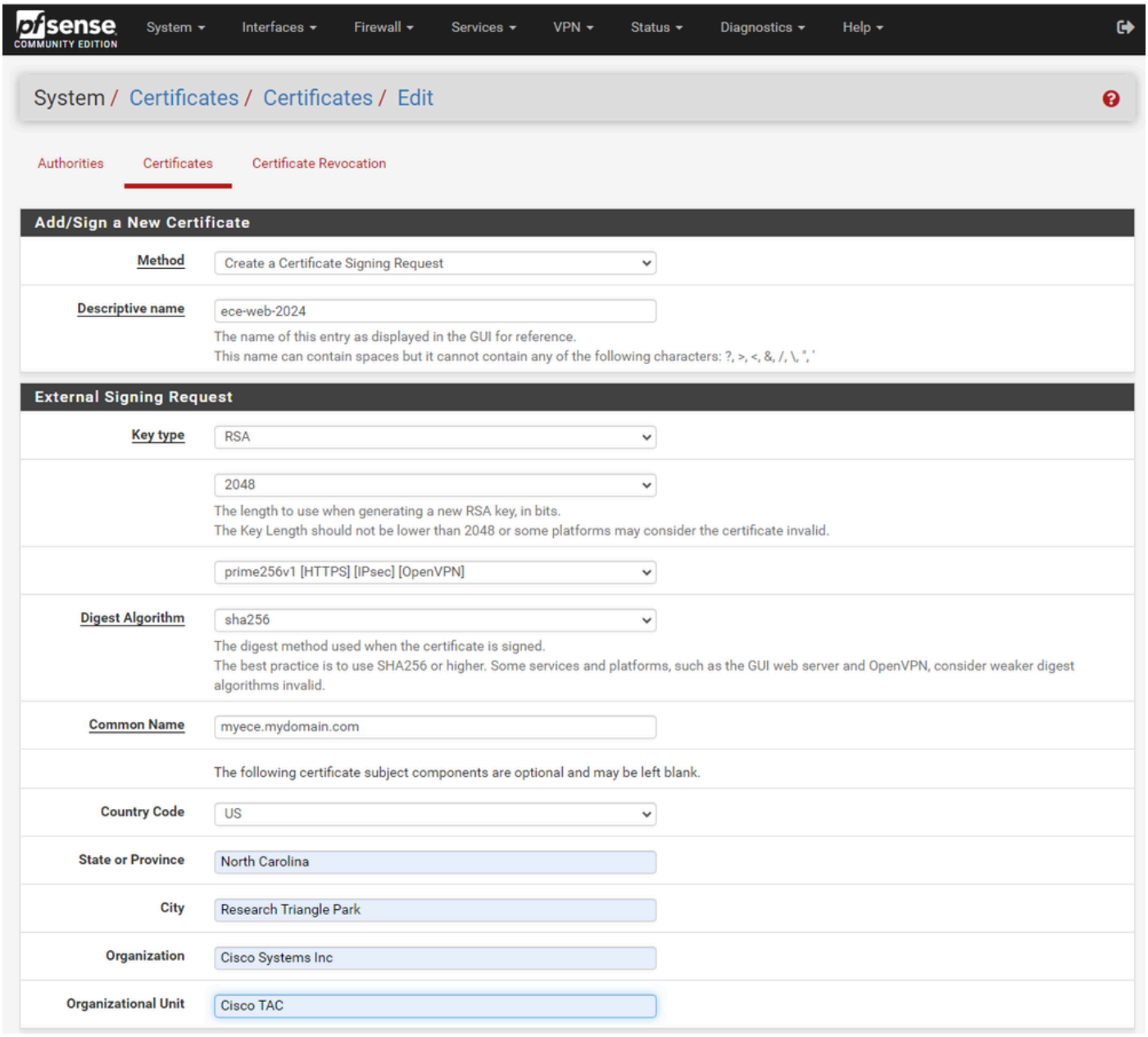
ここでは、CSRの作成、CSRのエクスポート、署名付き証明書のインポートの手順について説明します。PFX形式の既存の証明書がある場合は、この証明書をインポートできます。これらの手順については、pfSenseのドキュメントを参照してください。

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。



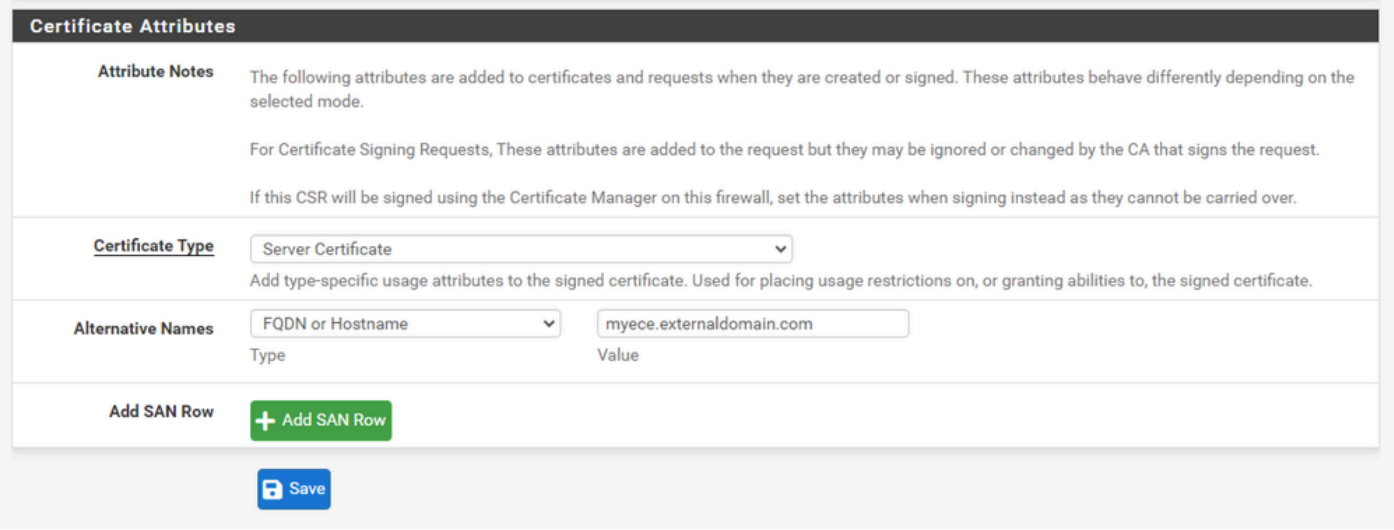
pfSense GUI：証明書リスト

2.証明書署名要求フォームに記入します。



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



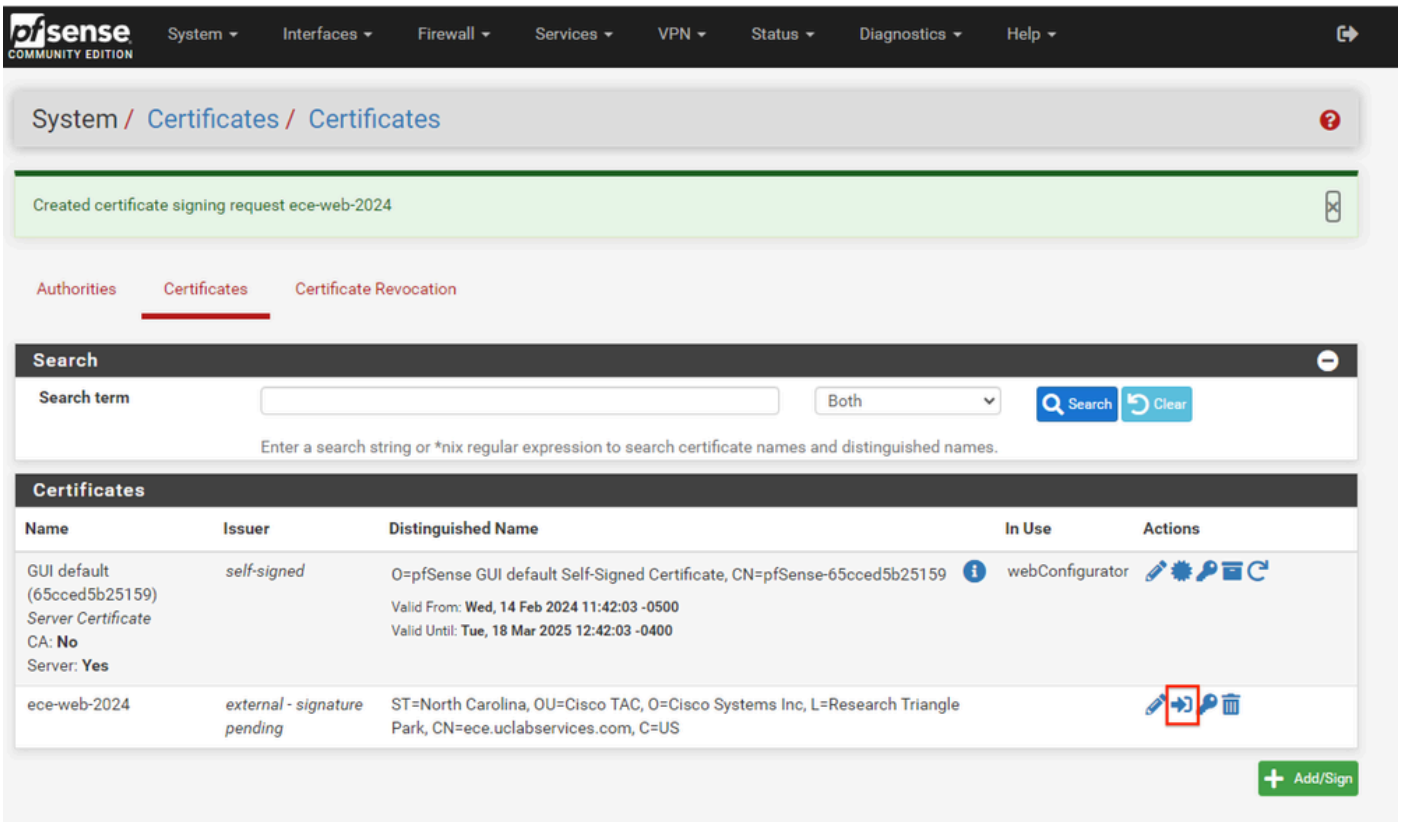
pfSense GUI:CSR上級

- 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。

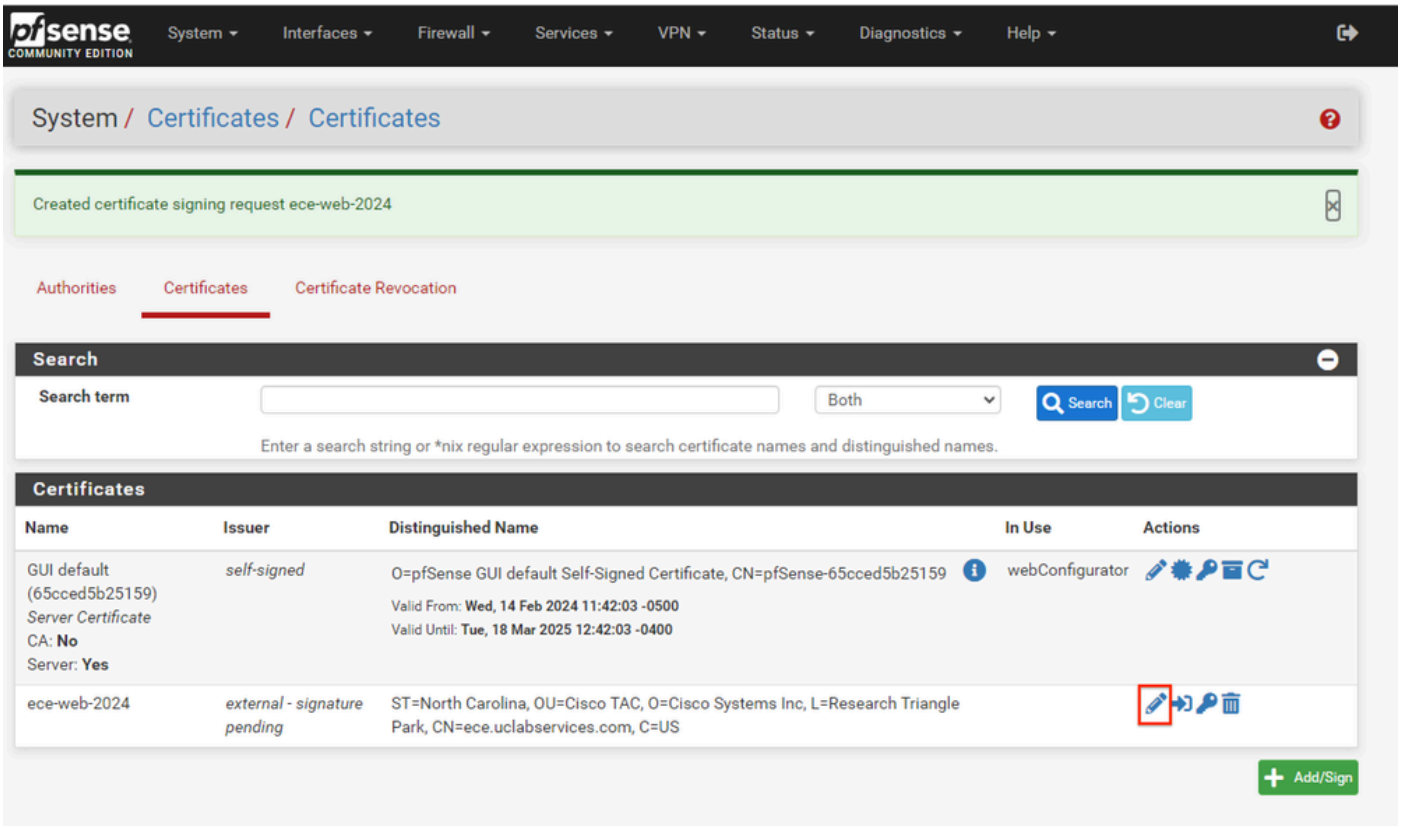
3. CSRをファイルにエクスポートします。



pfSense 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。

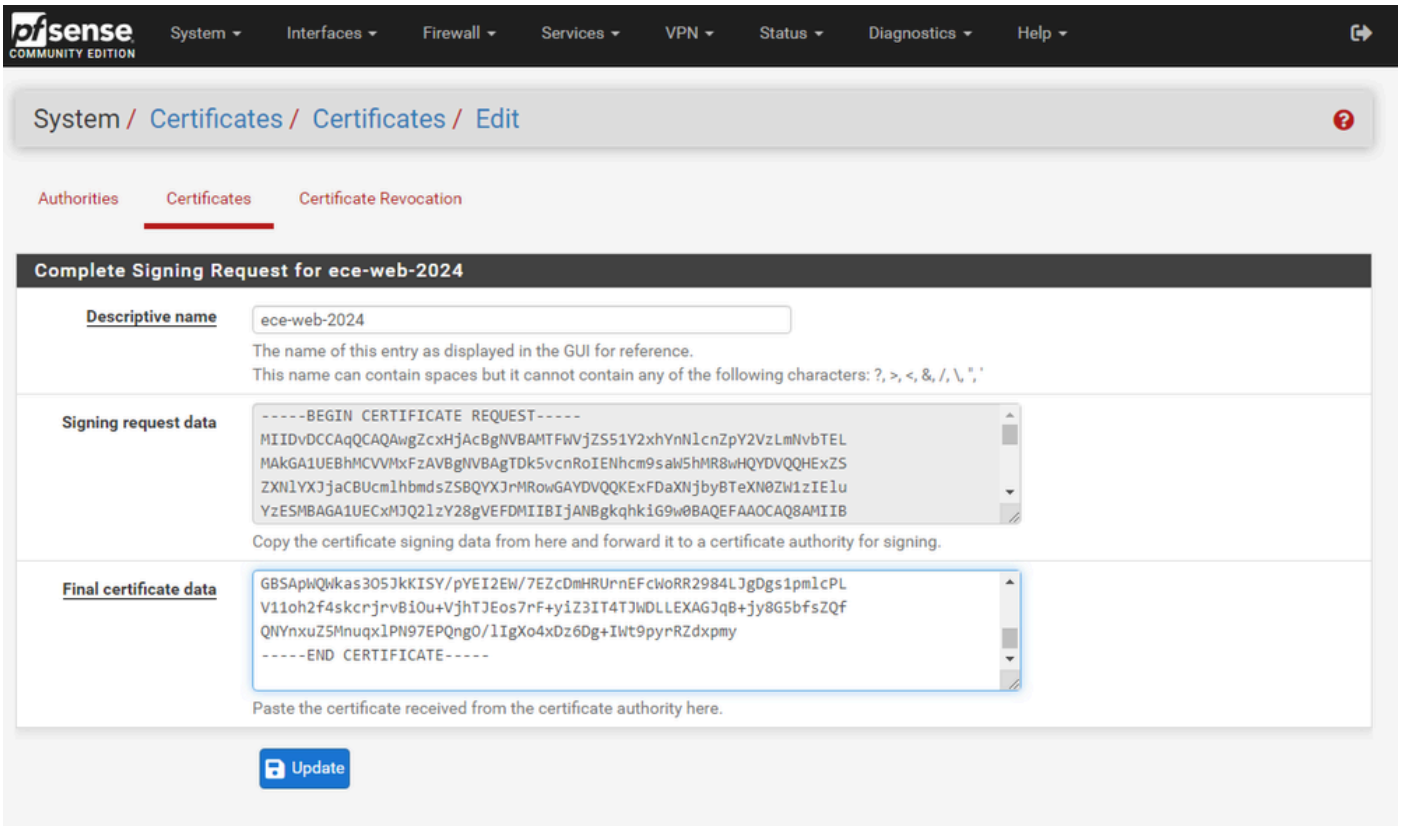
4.署名付き証明書をインポートします。



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。

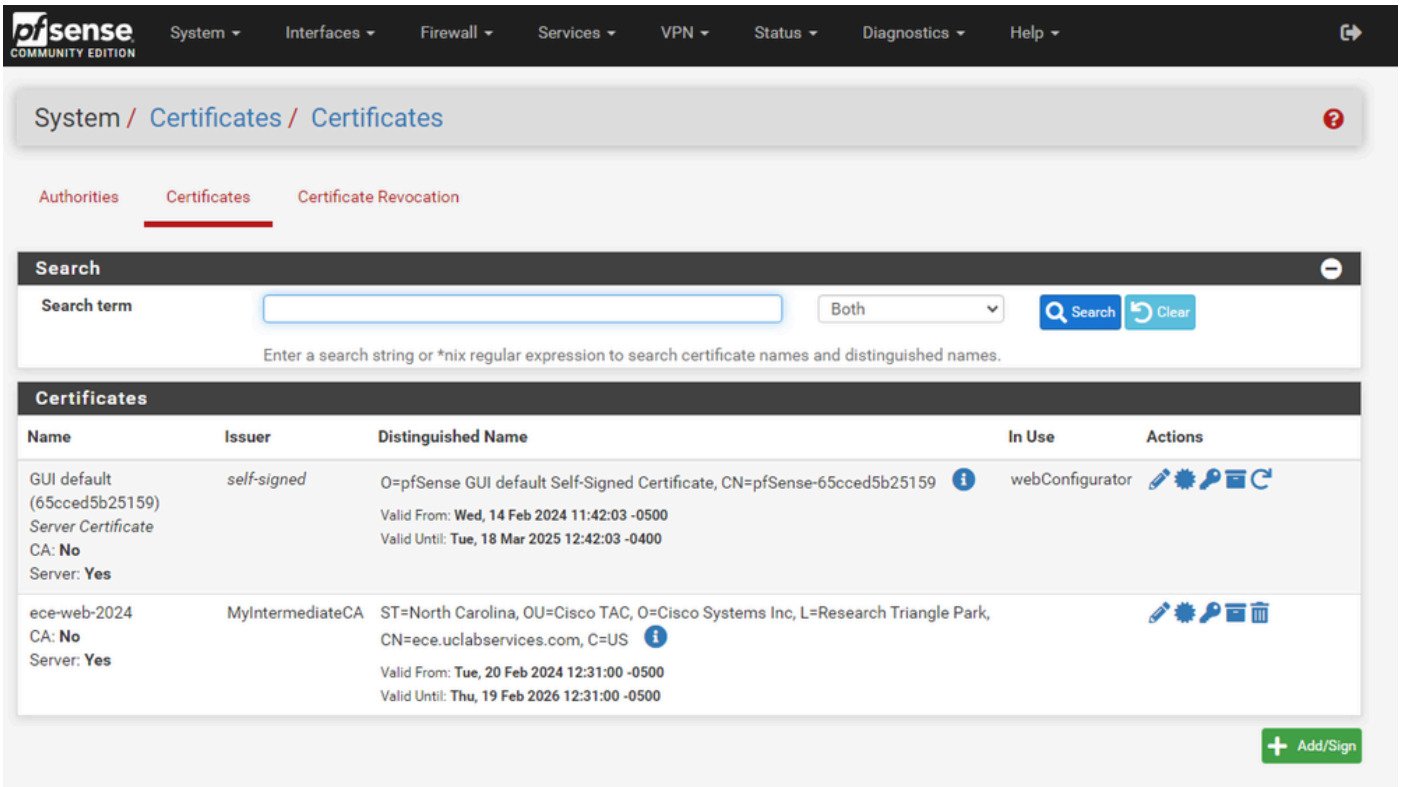
5.フォームに証明書データを貼り付けます。



pfSense 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。



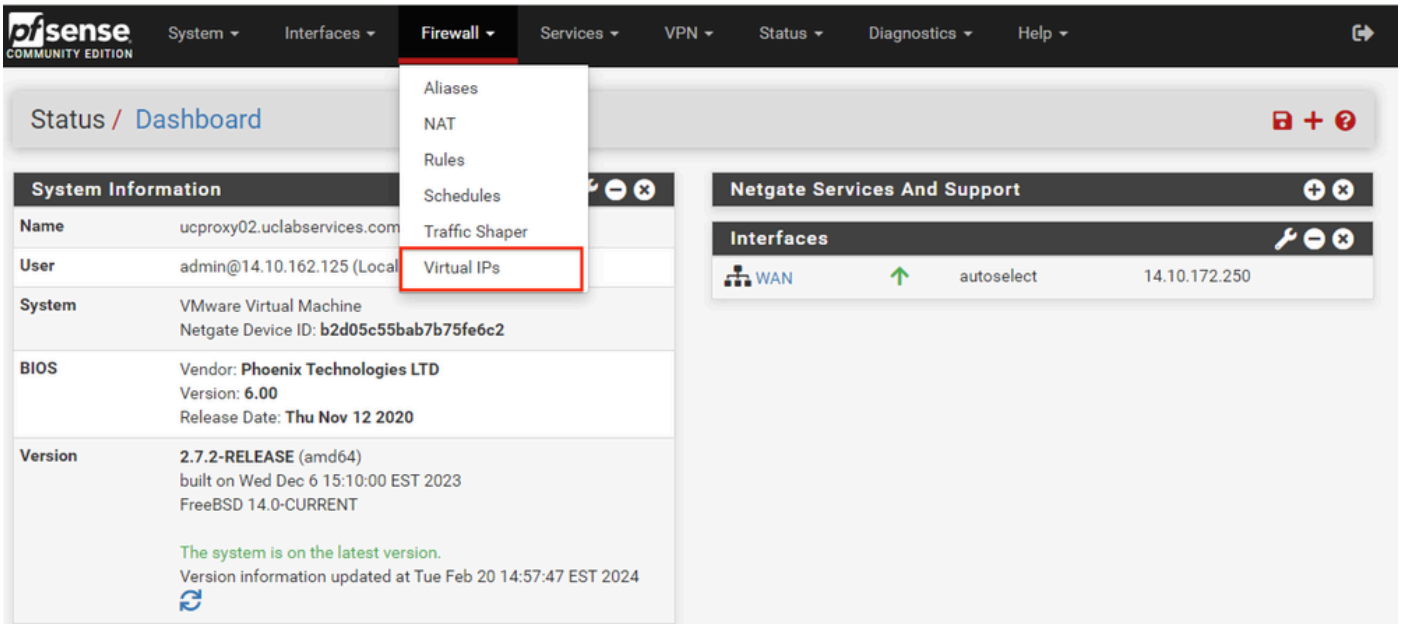
pfSense GUI：証明書リスト

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

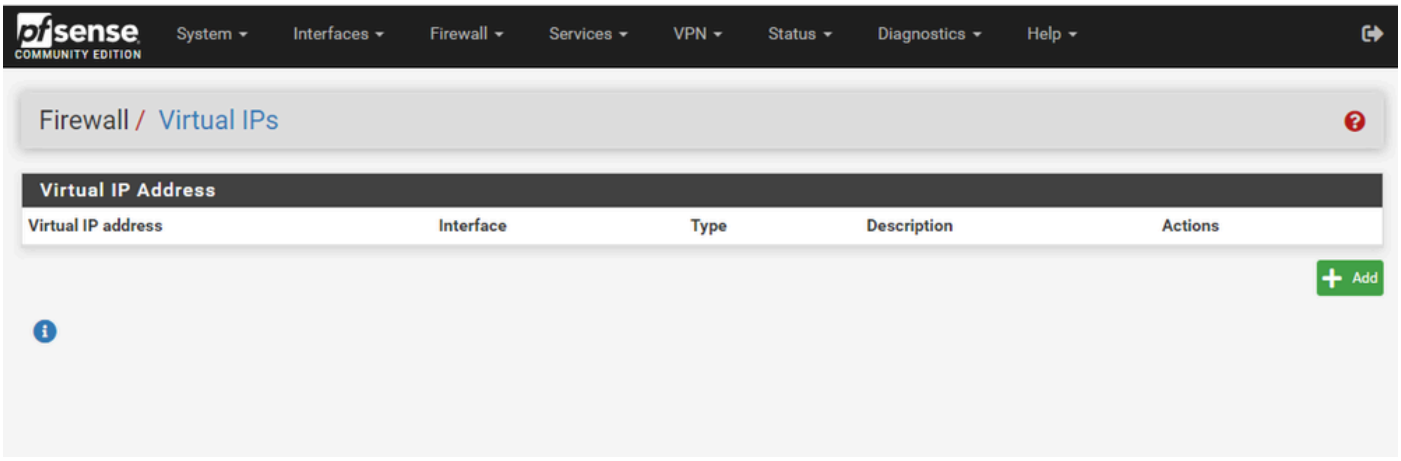
pfSenseでWebサイトをホストするには、少なくとも1つのIPが必要です。pfSenseでは、これは仮想IP(VIP)で実行されます。

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



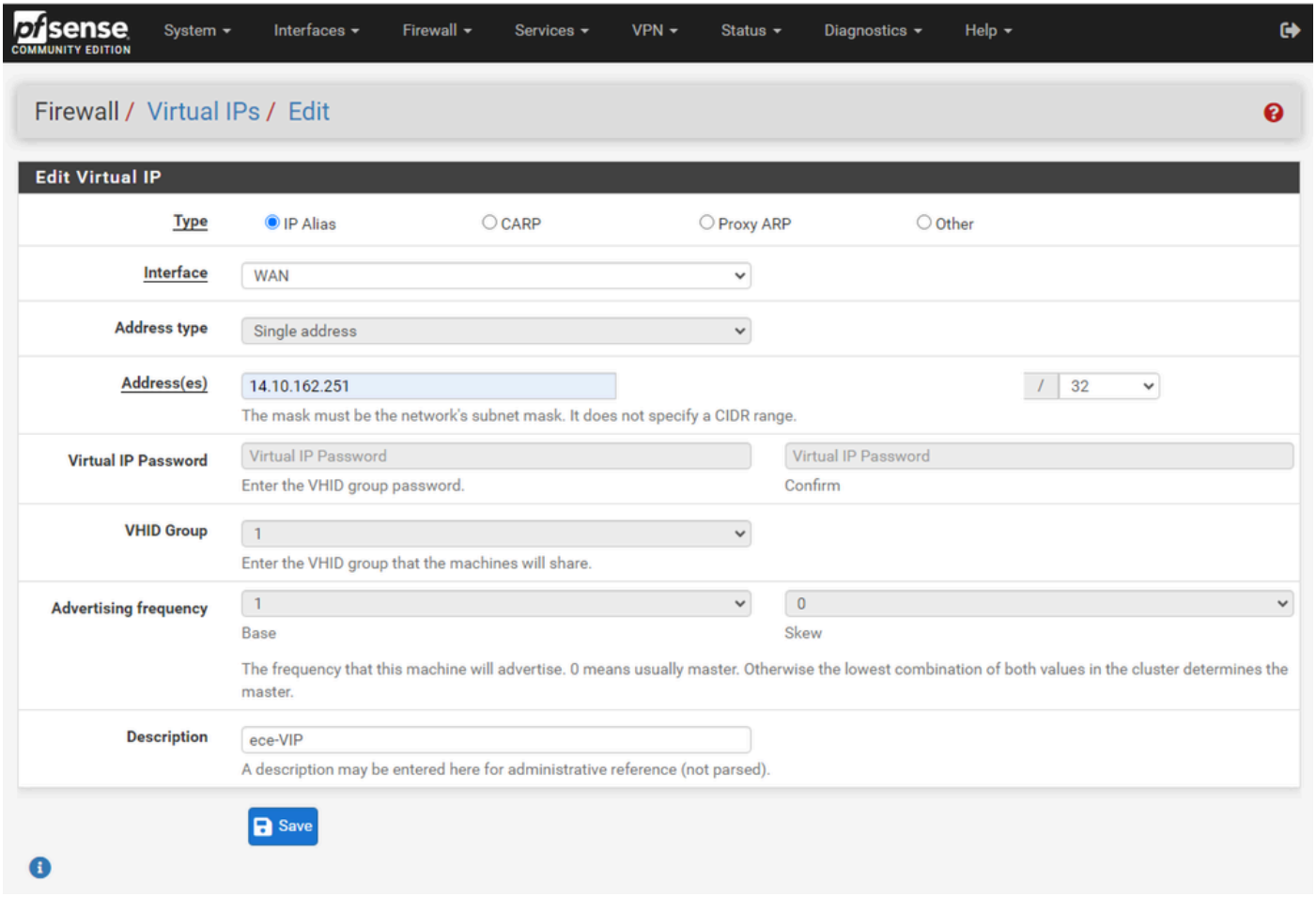
pfSense GUI:VIPドロップダウン

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 GUI:VIPの設定

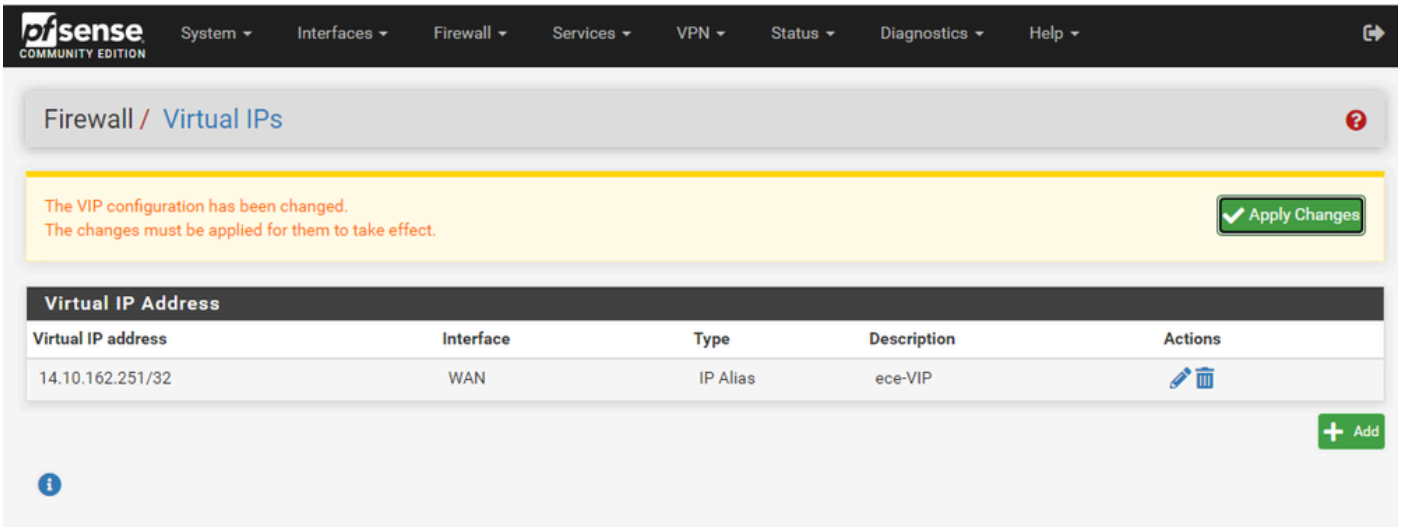
この情報を使用して、VIPを追加します。

- タイプ：IP工イリアスの選択
- 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



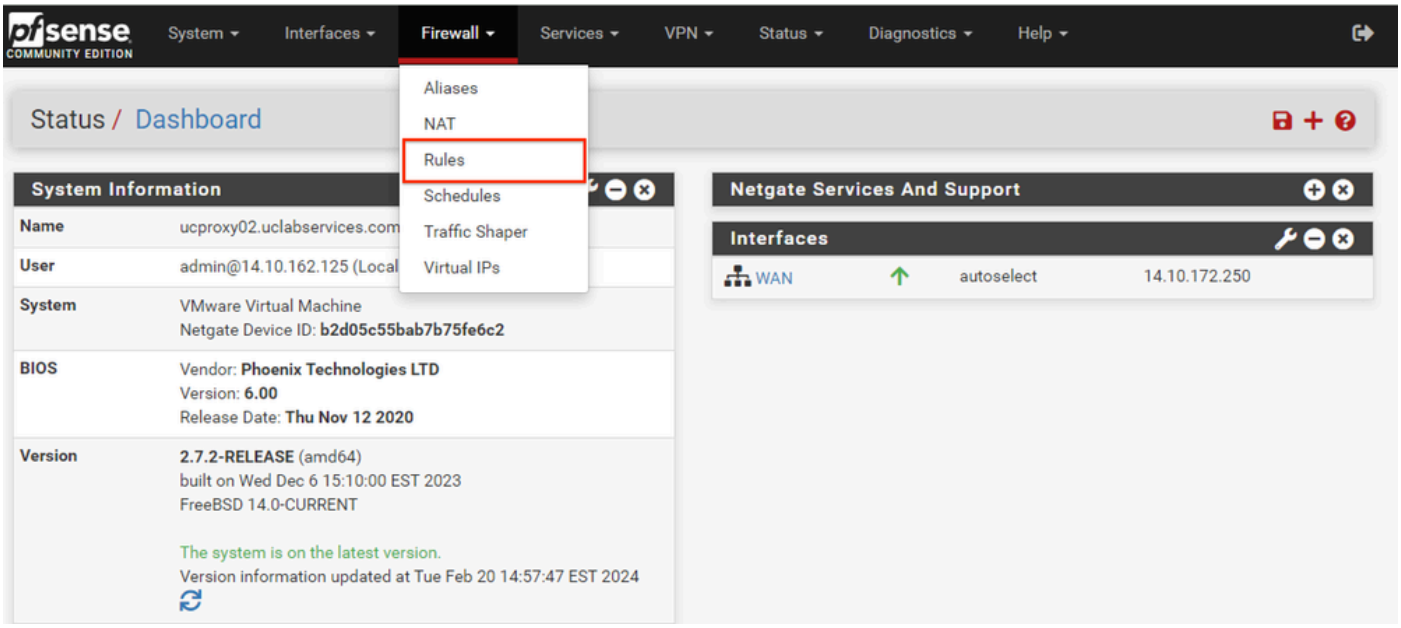
pfSense GUI:VIPリスト

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

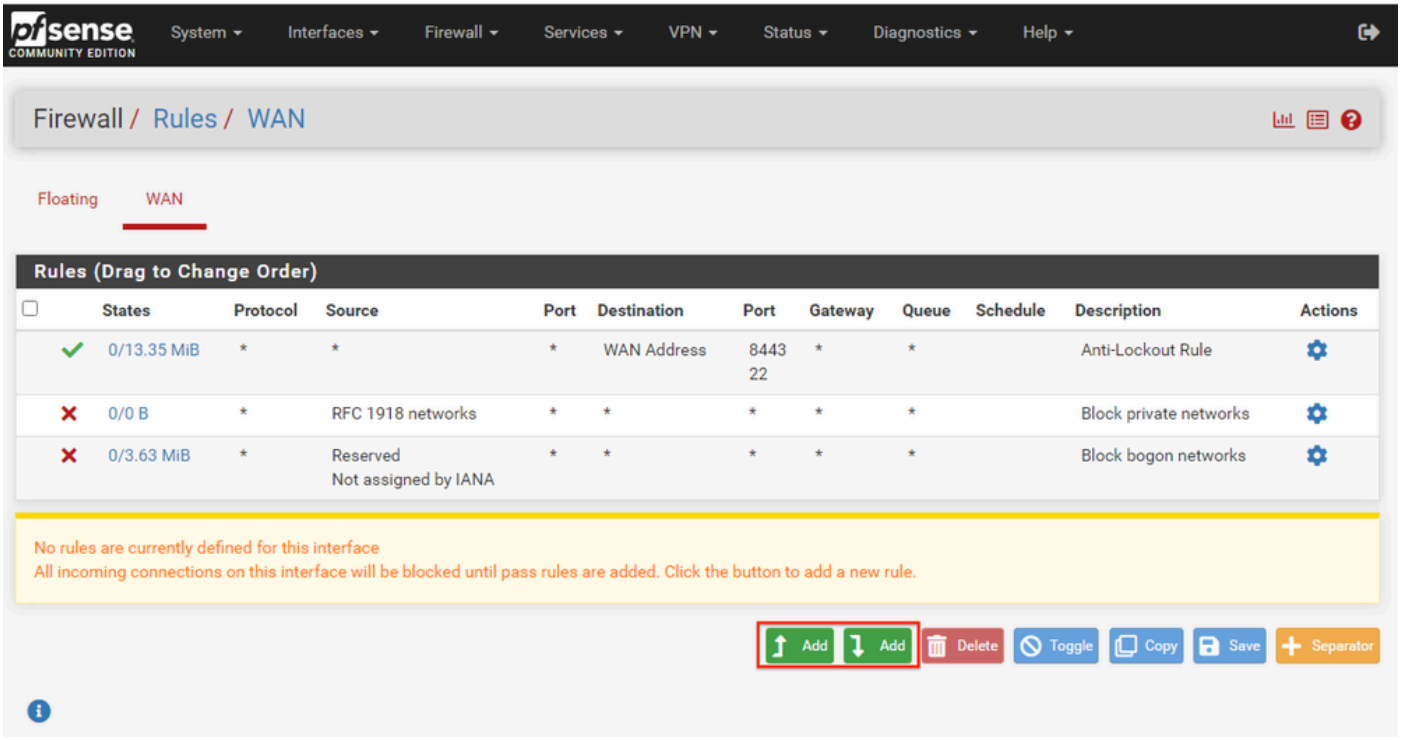
pfSenseにはファイアウォールが組み込まれています。デフォルトのルールセットは非常に制限されています。アプライアンスを実稼働環境に移行する前に、包括的なファイアウォールポリシーを構築する必要があります。

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

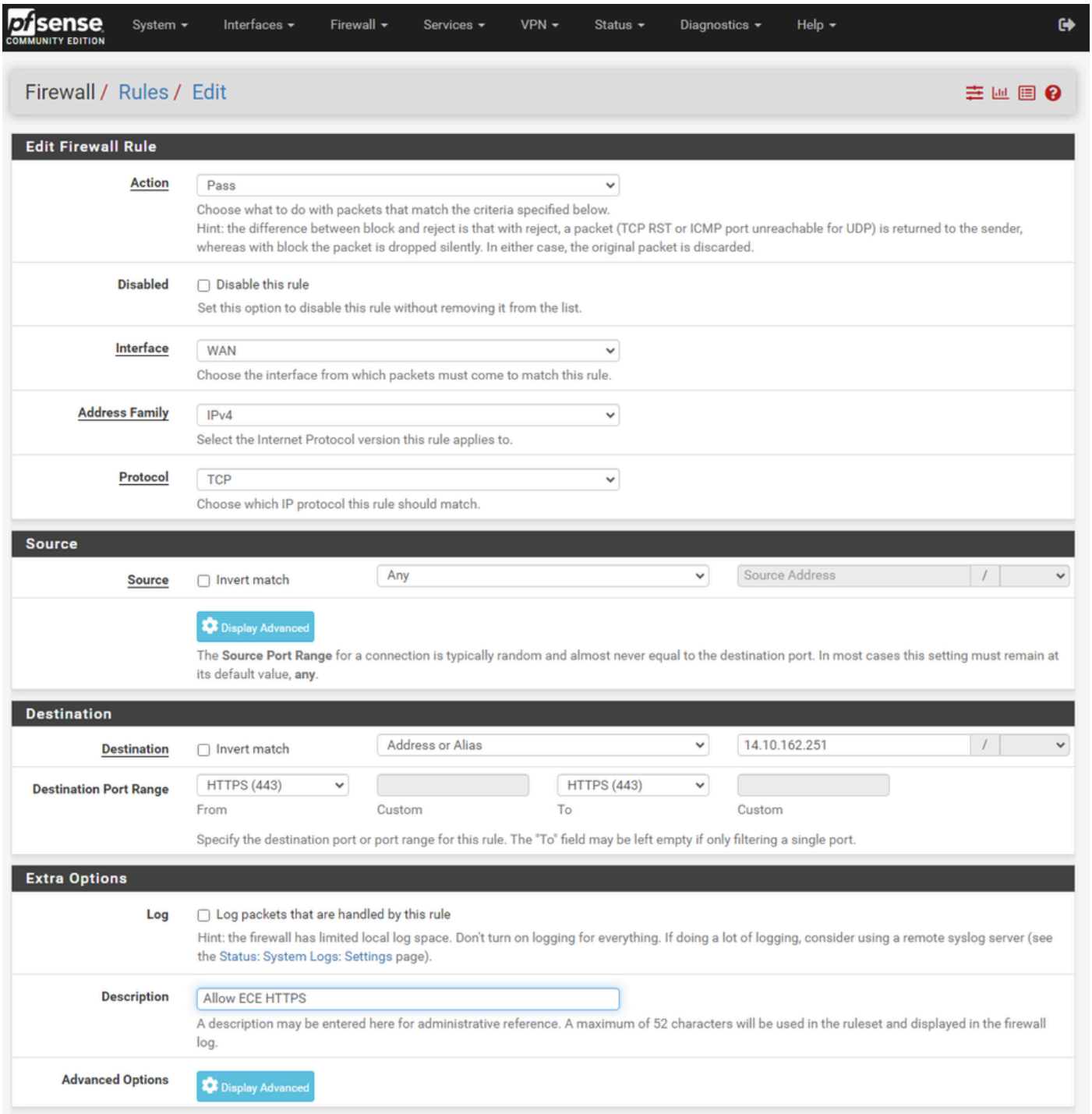
ステップ 2：いずれかの追加ボタンを選択します



pfSense 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 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。

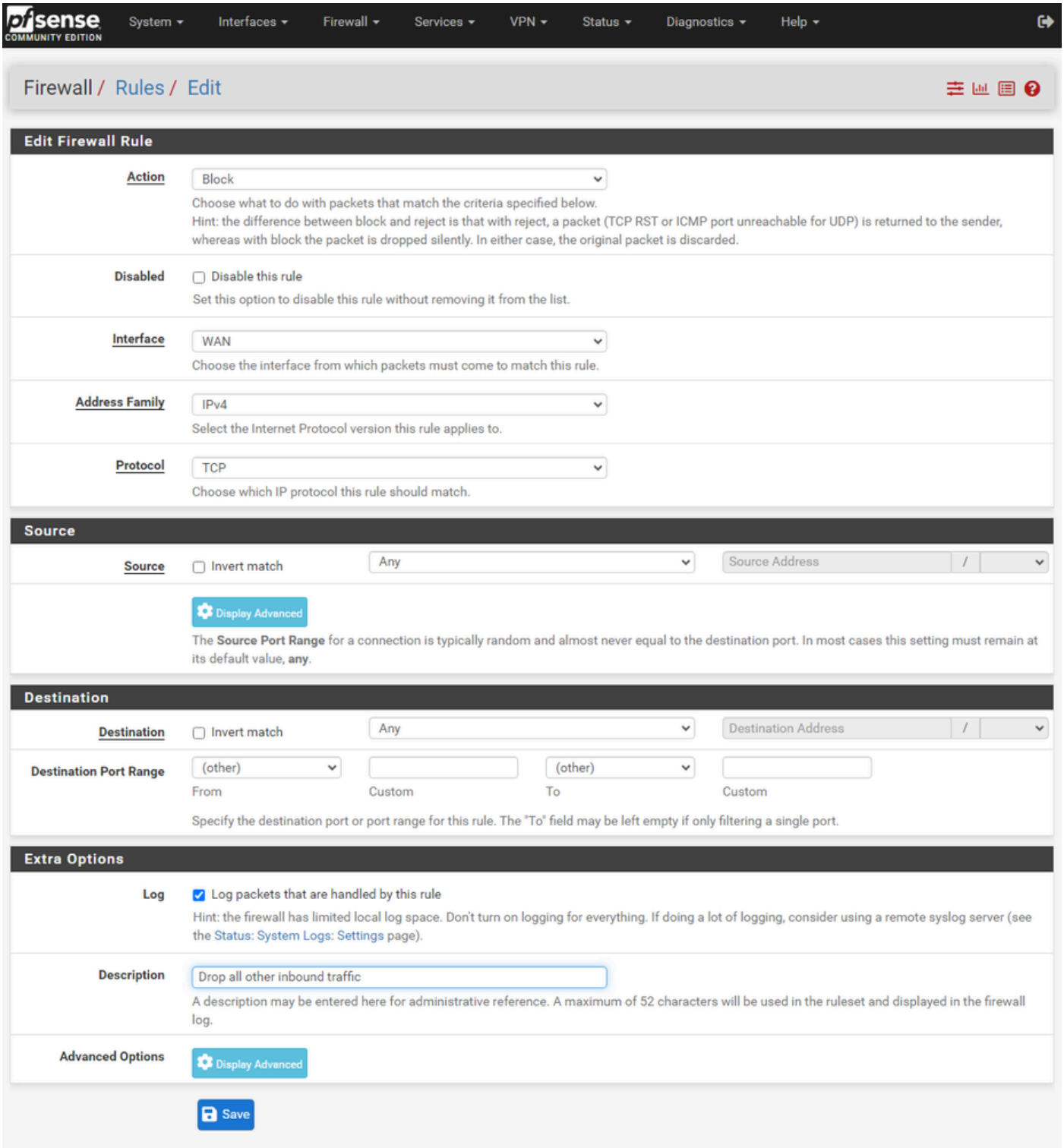
- アクション： [パス]を選択します
- Interface：ルールが適用されるインターフェイスを選択します。
- アドレスファミリとプロトコル：必要に応じて選択
- ソース： 「任意」として選択したままにします。
- Destination: DestinationドロップダウンからAddressまたはAliasを選択し、ルールが適用されるIPアドレスを入力します
- Destination Port Range:FromとToの両方のドロップダウンでHTTPS(443)を選択します。
- ログ：このルールに一致するパケットをアカウンティング用としてログに記録するには、チェックボックスをオ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

- 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。

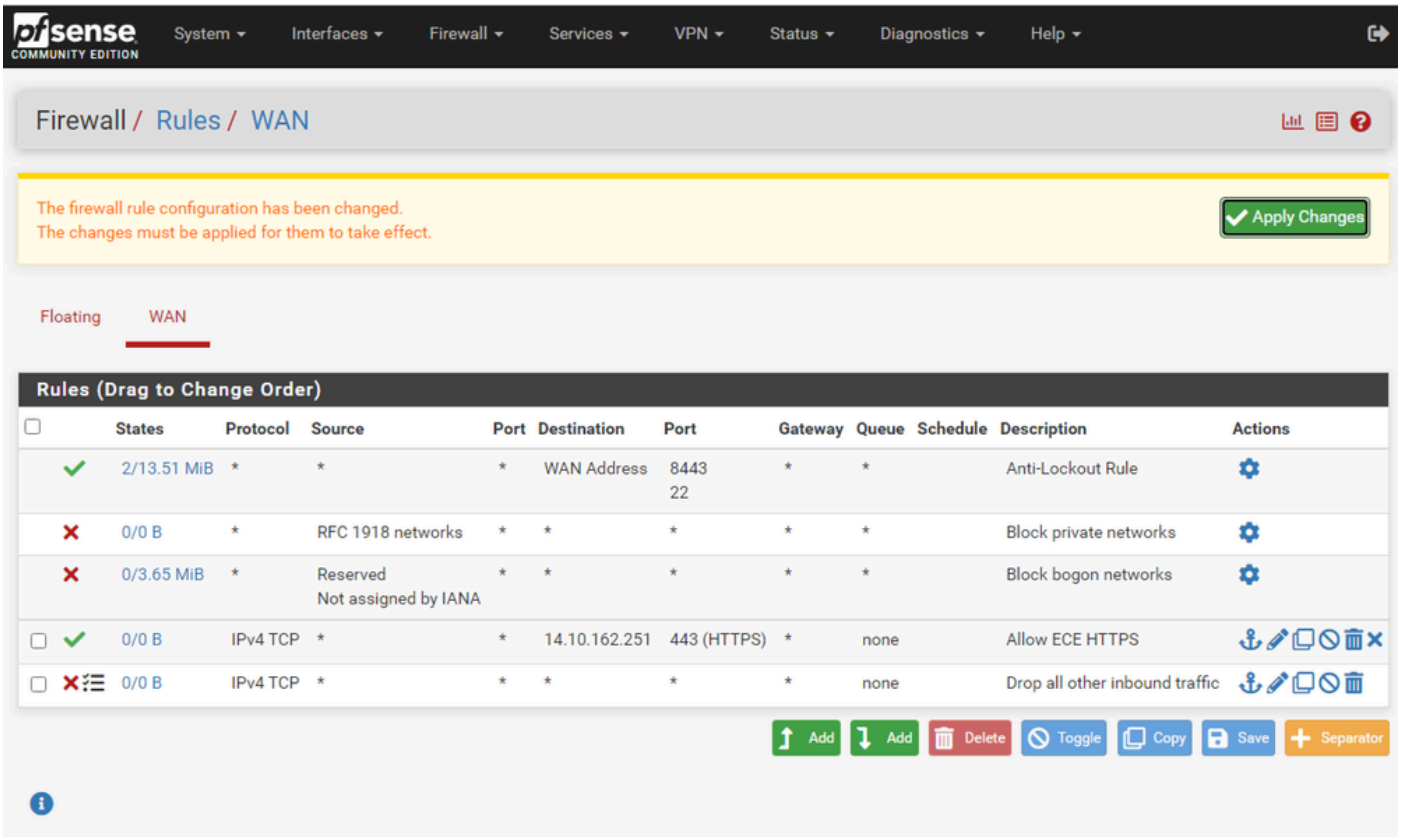


pfSense GUI：ファイアウォールドロップルールの設定

- 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 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



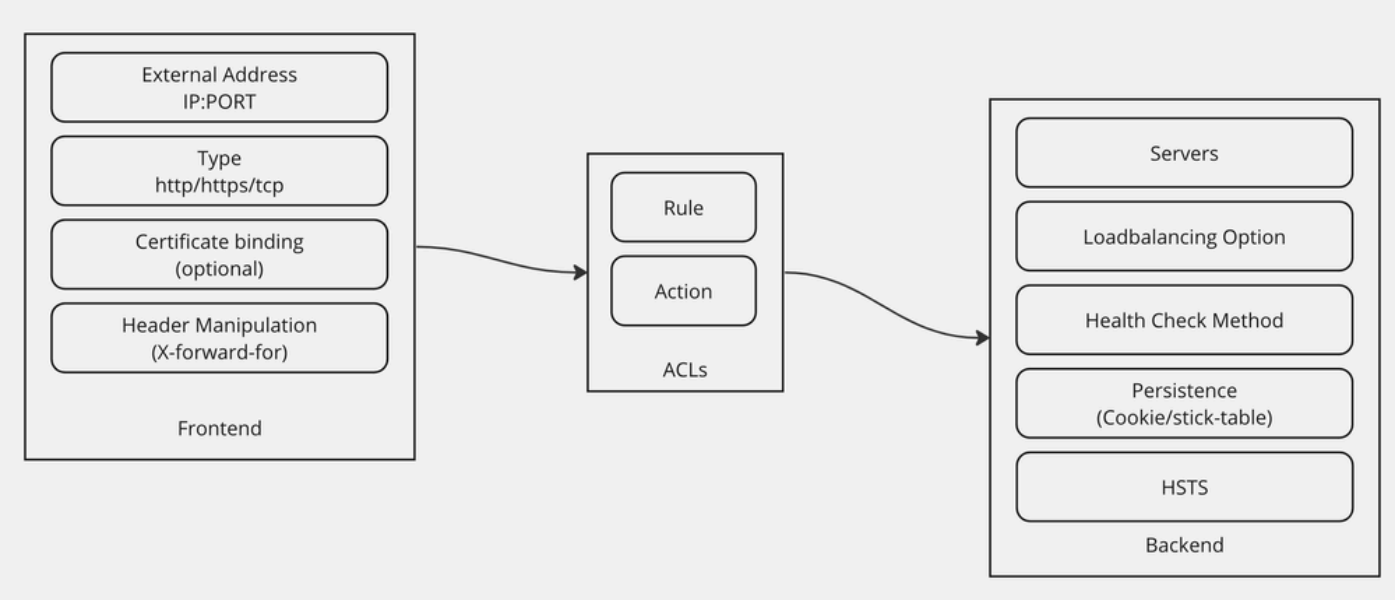
pfSense GUI：ファイアウォール規則リスト

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。

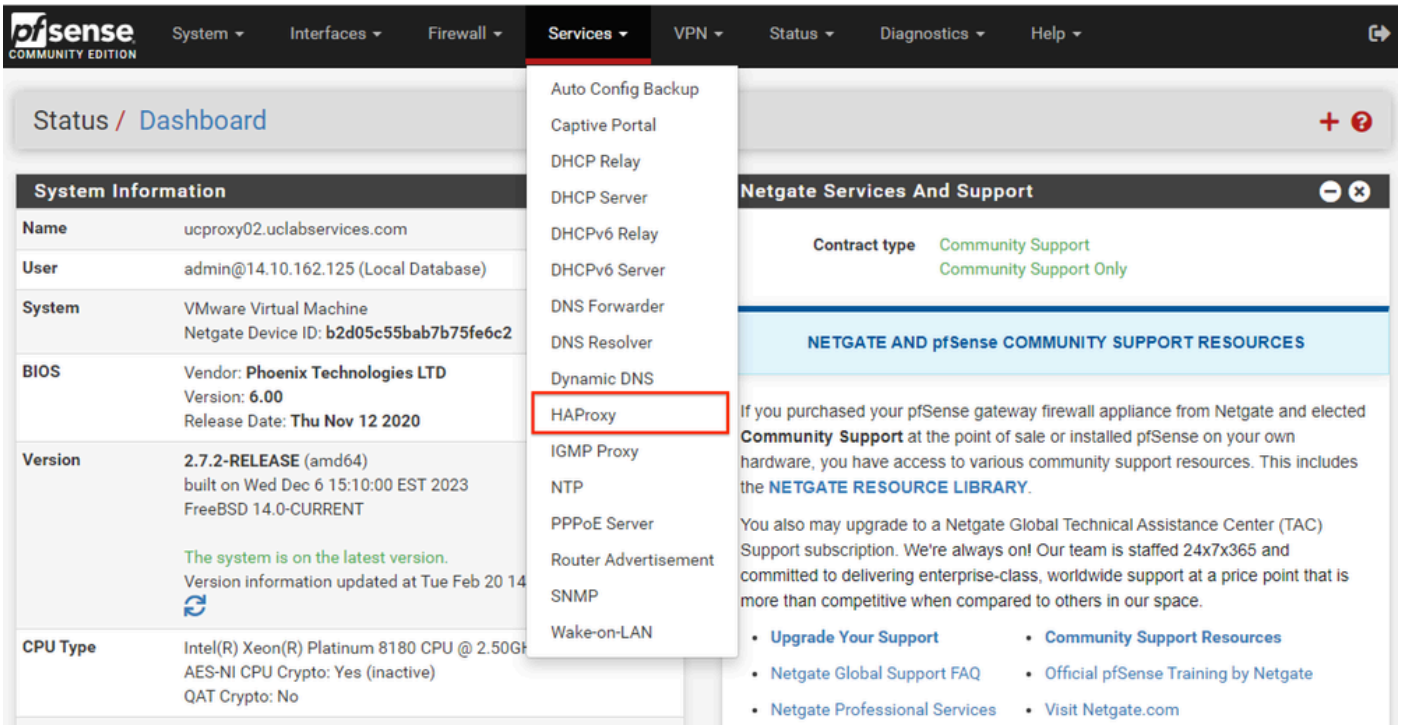
バックエンドは、実際のサーバとポート、初期割り当て、ヘルスチェック、持続性のためのロードバランシング方式を定義します。

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。

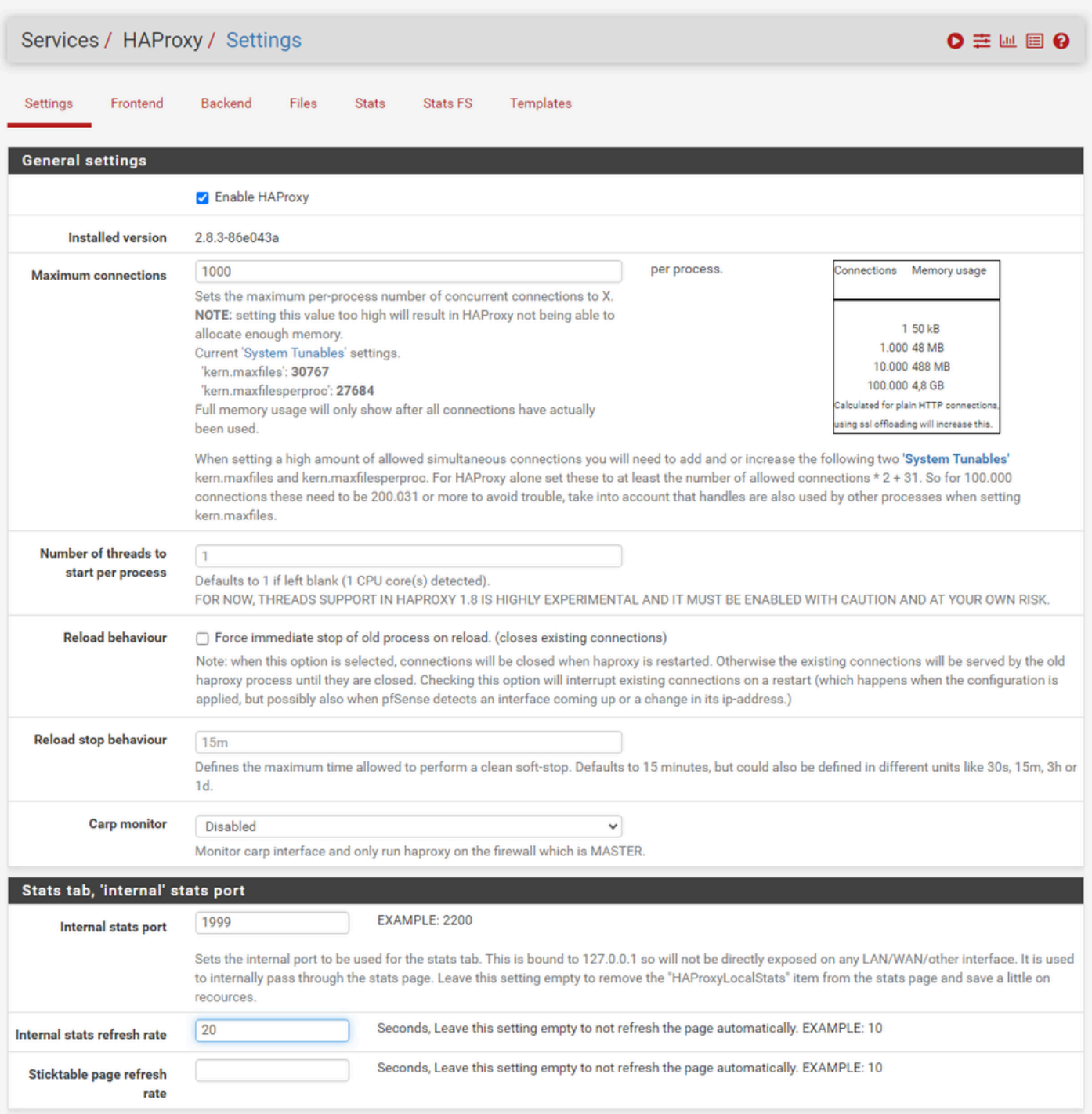
HAProxyの初期設定

ステップ 1：ServicesドロップダウンからHAProxyを選択します



pfSense GUI - HAProxyドロップダウン

ステップ 2：基本設定の構成



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。

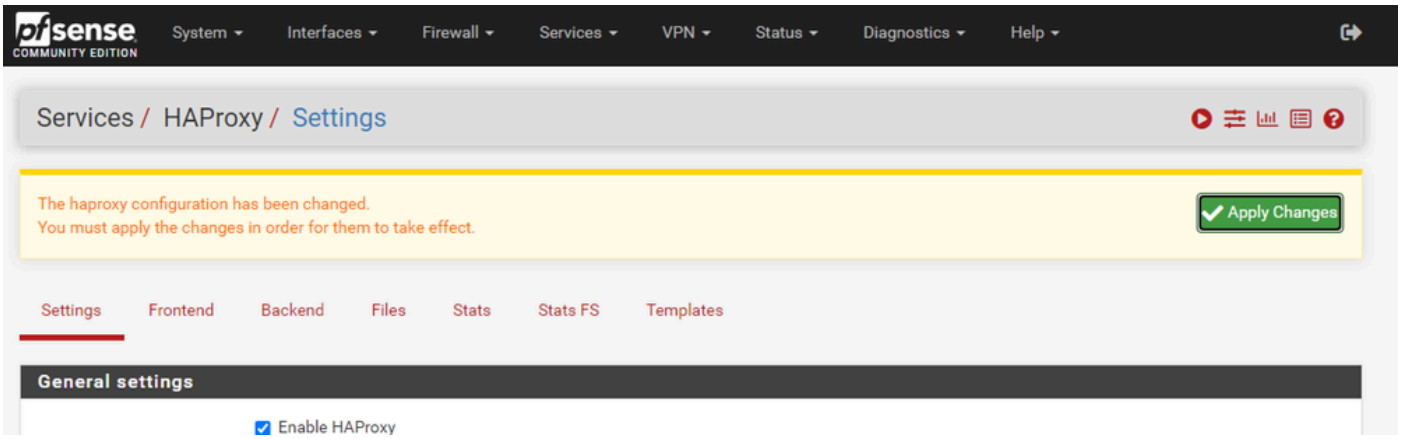
[最大接続数]に値を入力します。必要なメモリの詳細については、このセクションの表を参照してください。

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。

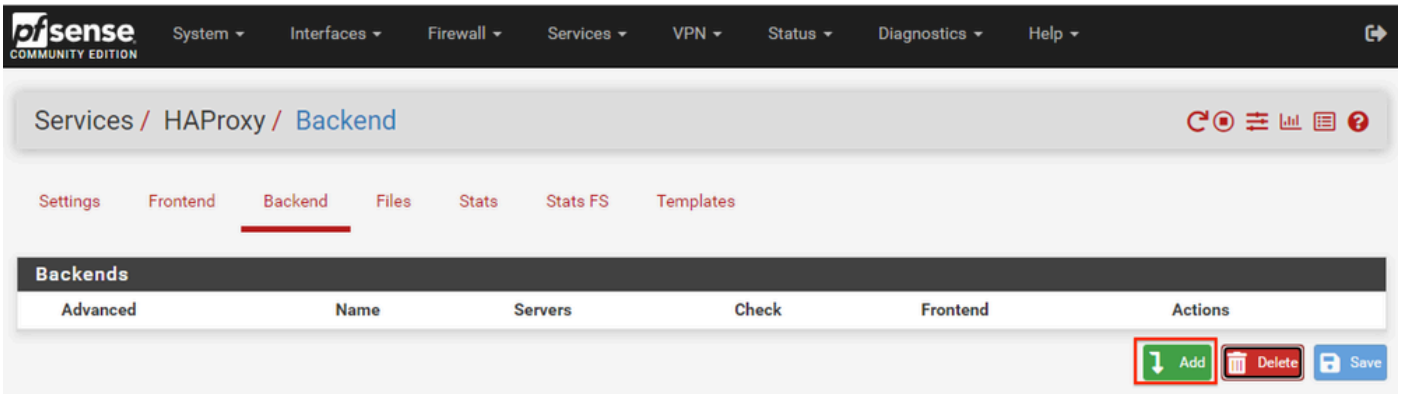


pfSense GUI:HAProxyによる変更の適用

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。

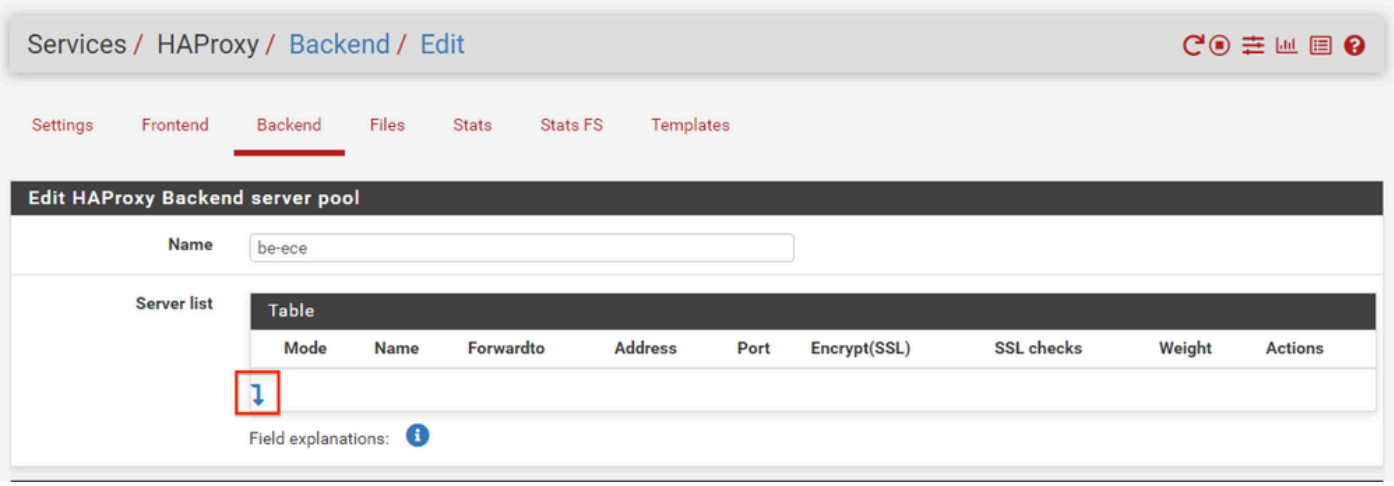
HAProxyバックエンドの設定

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。



pfSense GUI:HAProxyによるバックエンドの追加

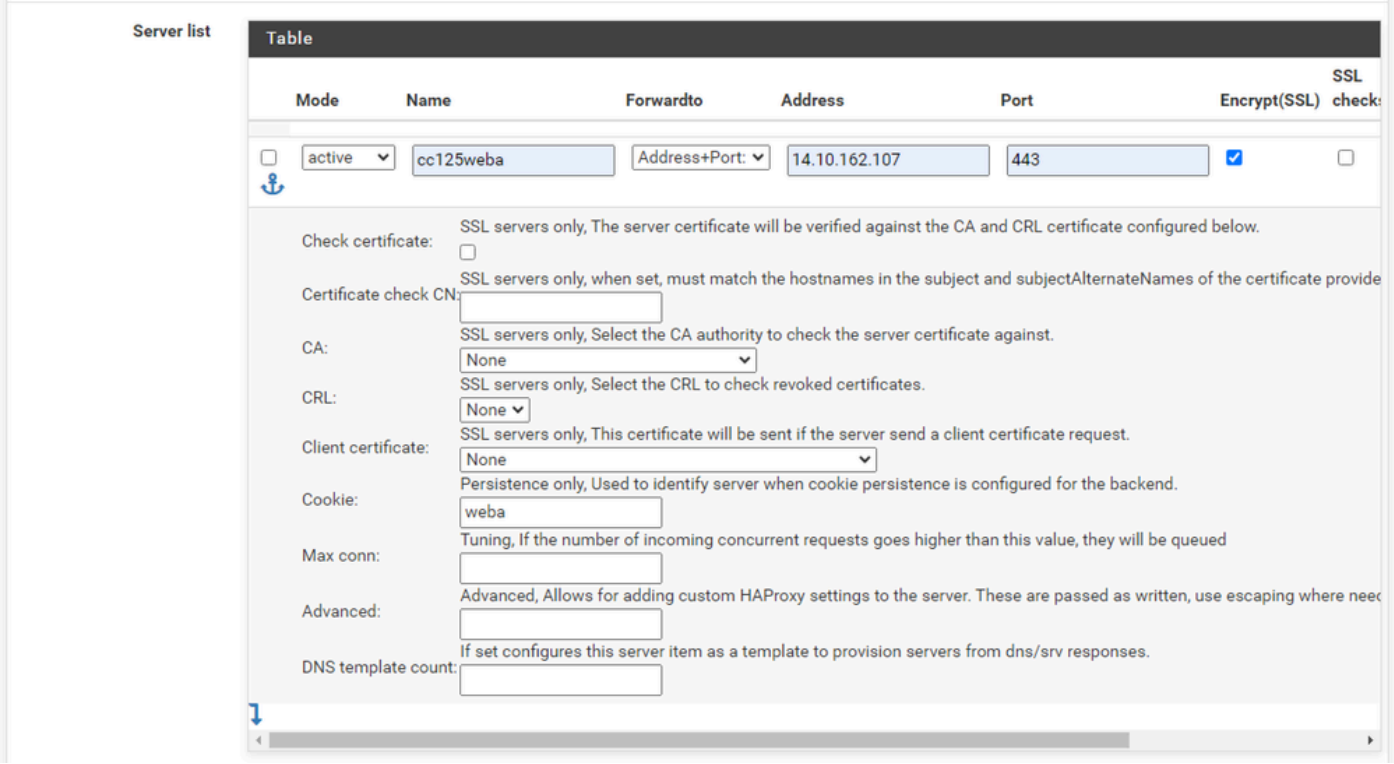
Addボタンを選択します。



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。

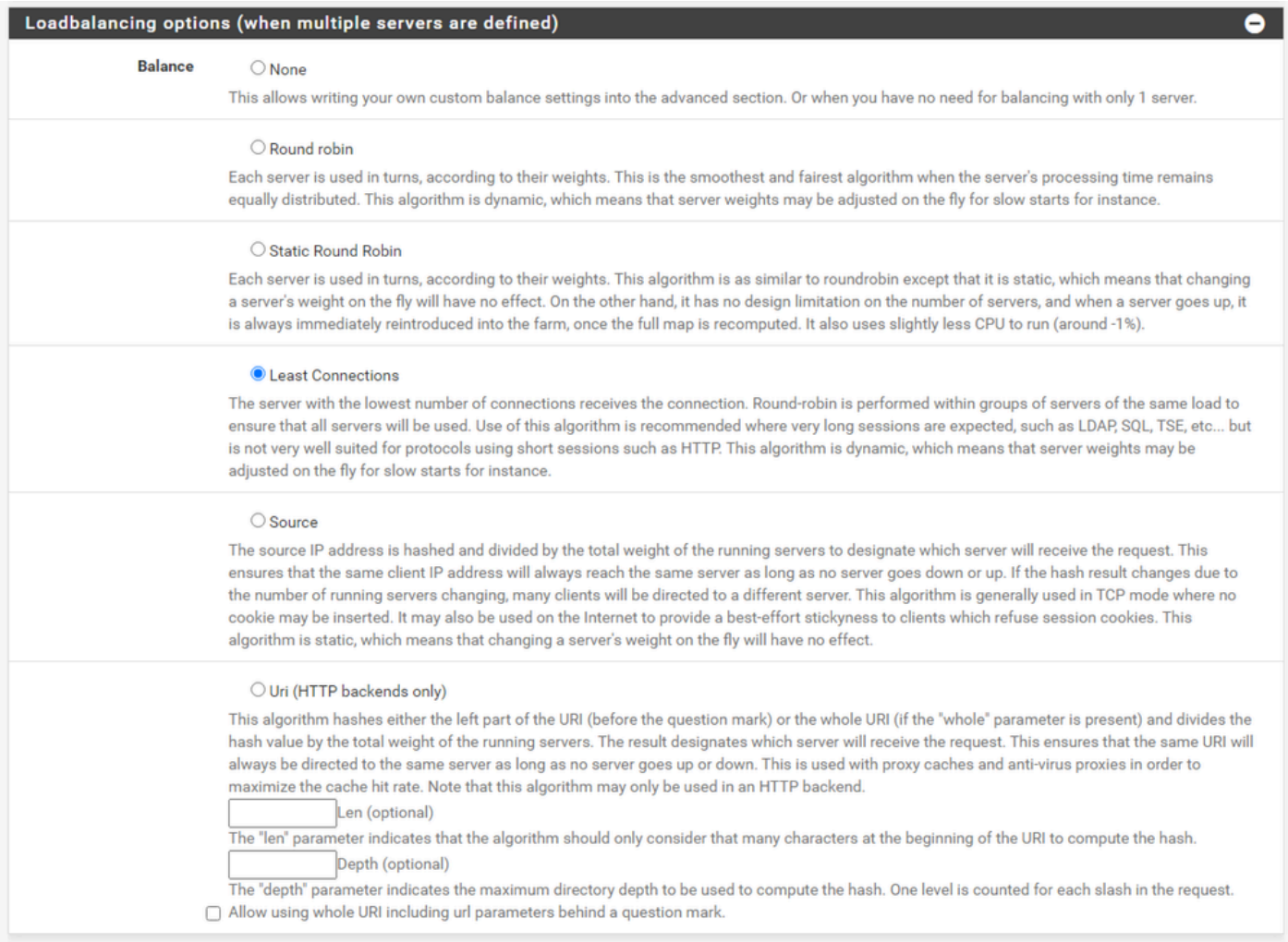
接続先のポートを指定します。ECEのポート443である必要があります。

「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、バッ

クエンド内で一意である必要があります。

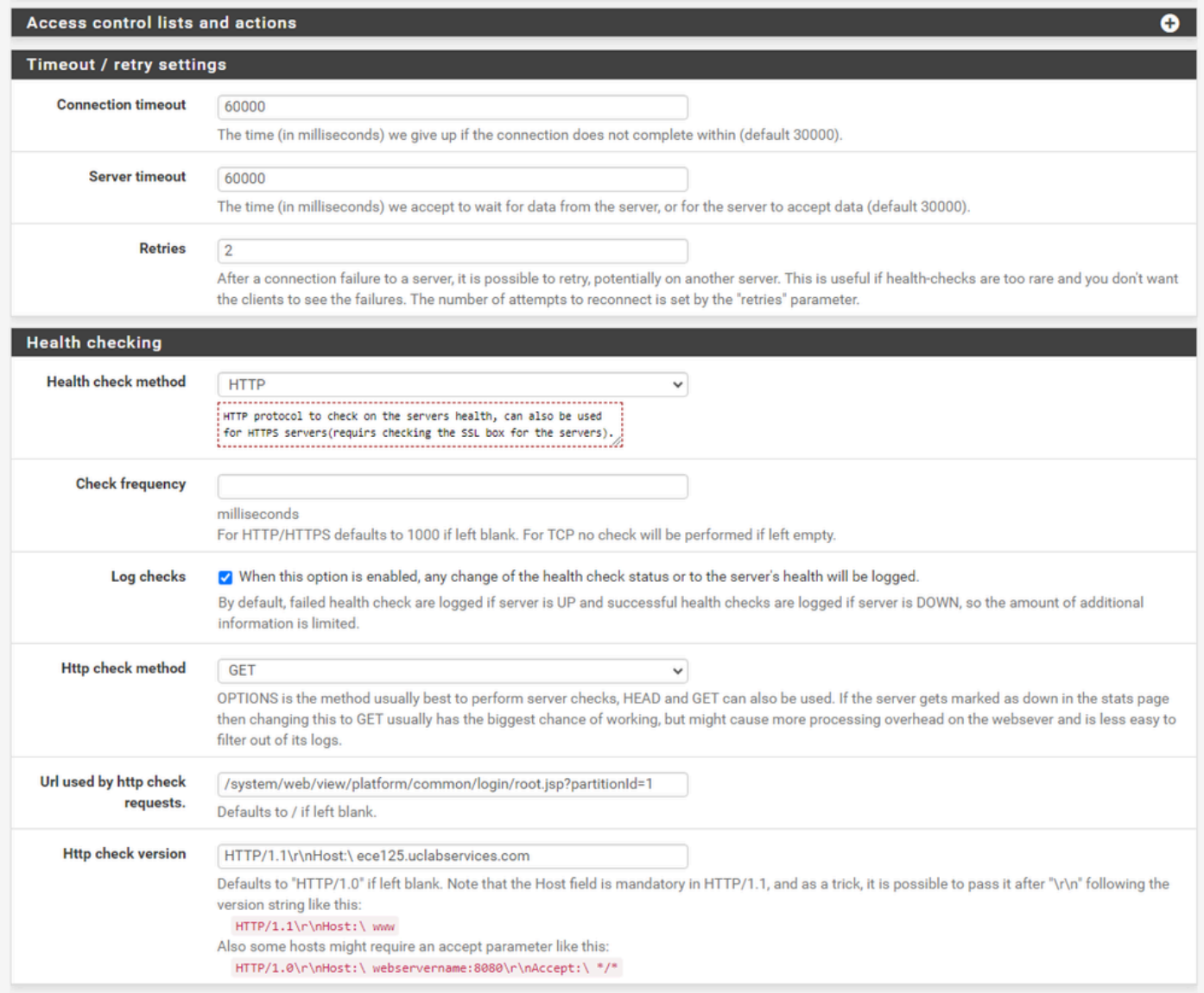
最初のサーバを設定した後、下向き矢印を選択して、環境内の他のWebサーバを設定します。



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。



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。

1. ヘルスチェック方法：HTTP
2. 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。
3. 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。
4. Httpチェック方法：リストからGETを選択します。
5. 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。
6. HTTPチェックバージョン： Enter、HTTP/1.1\r\n\Host:\ {fqdn_of_server}

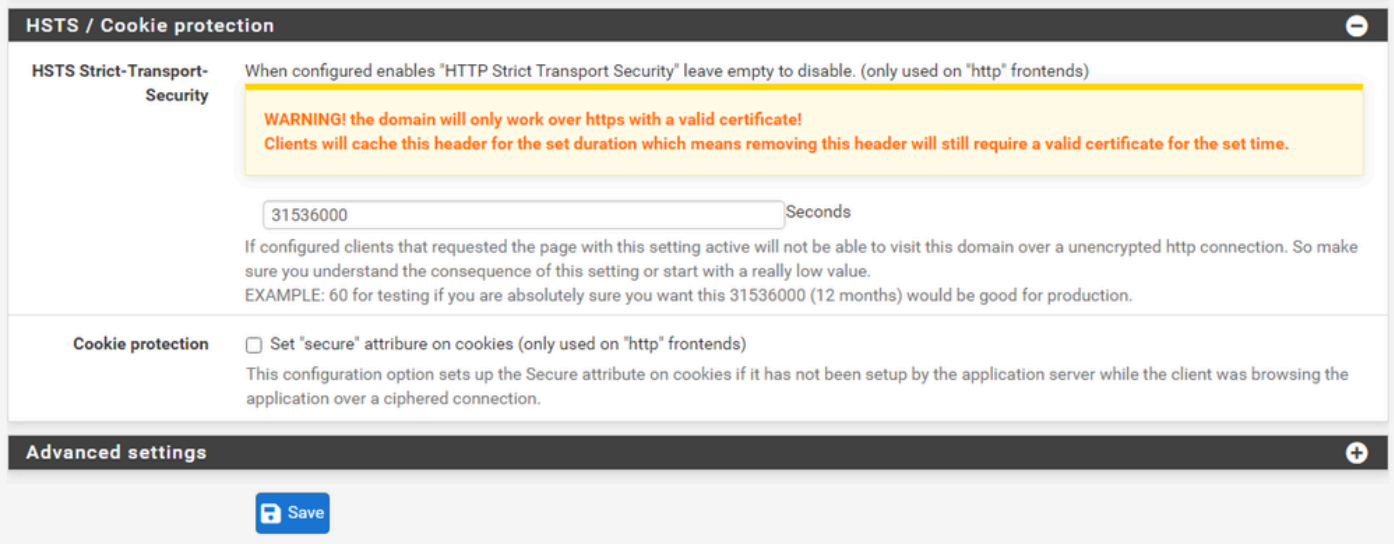
最後のバックスラッシュの後、サーバのFQDNの前にスペースを入れてください。

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

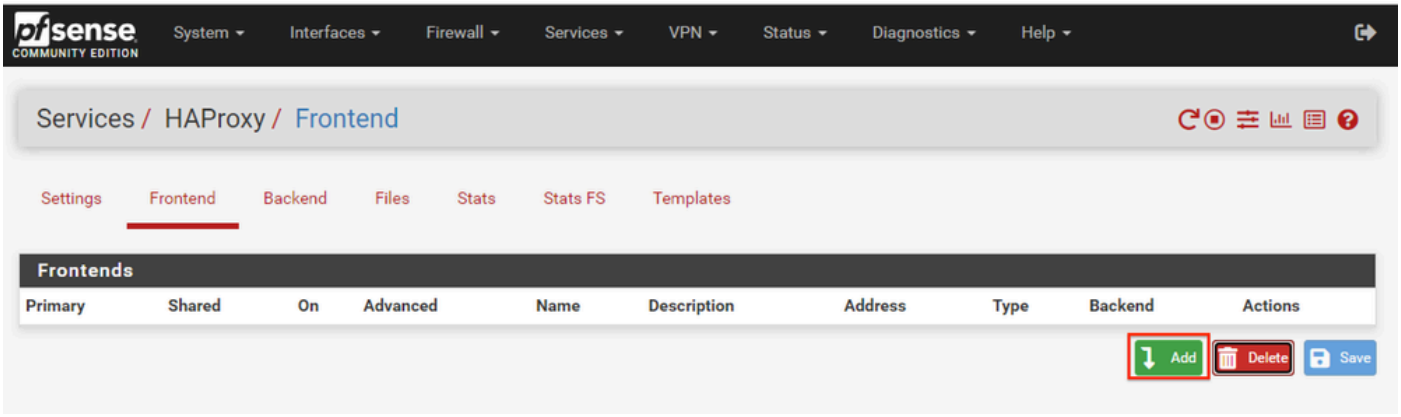
バックエンド構成フォームの残りのセクションは、デフォルト設定のままにしておくことができます。

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。

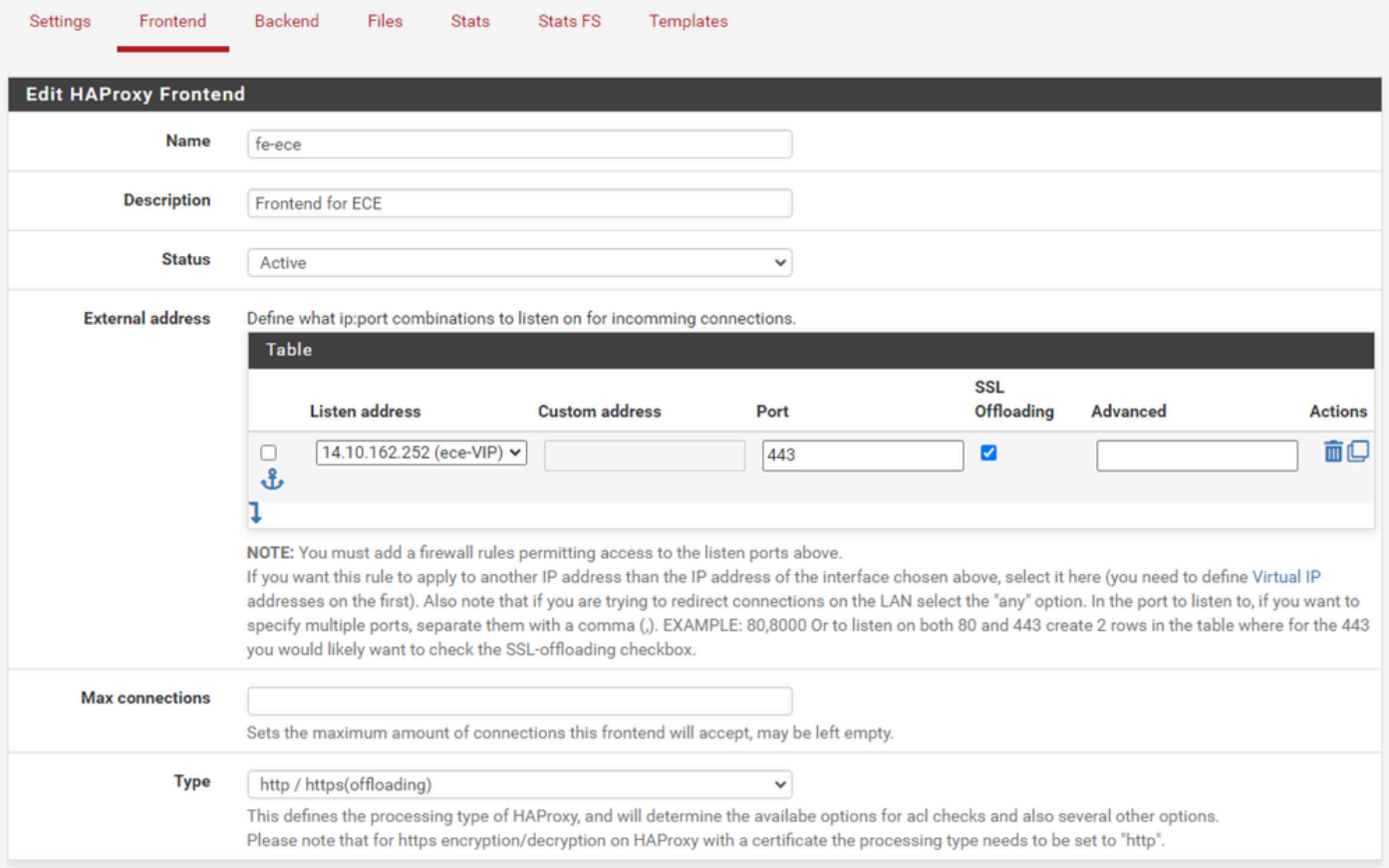
HAProxyフロントエンドの設定

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



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。

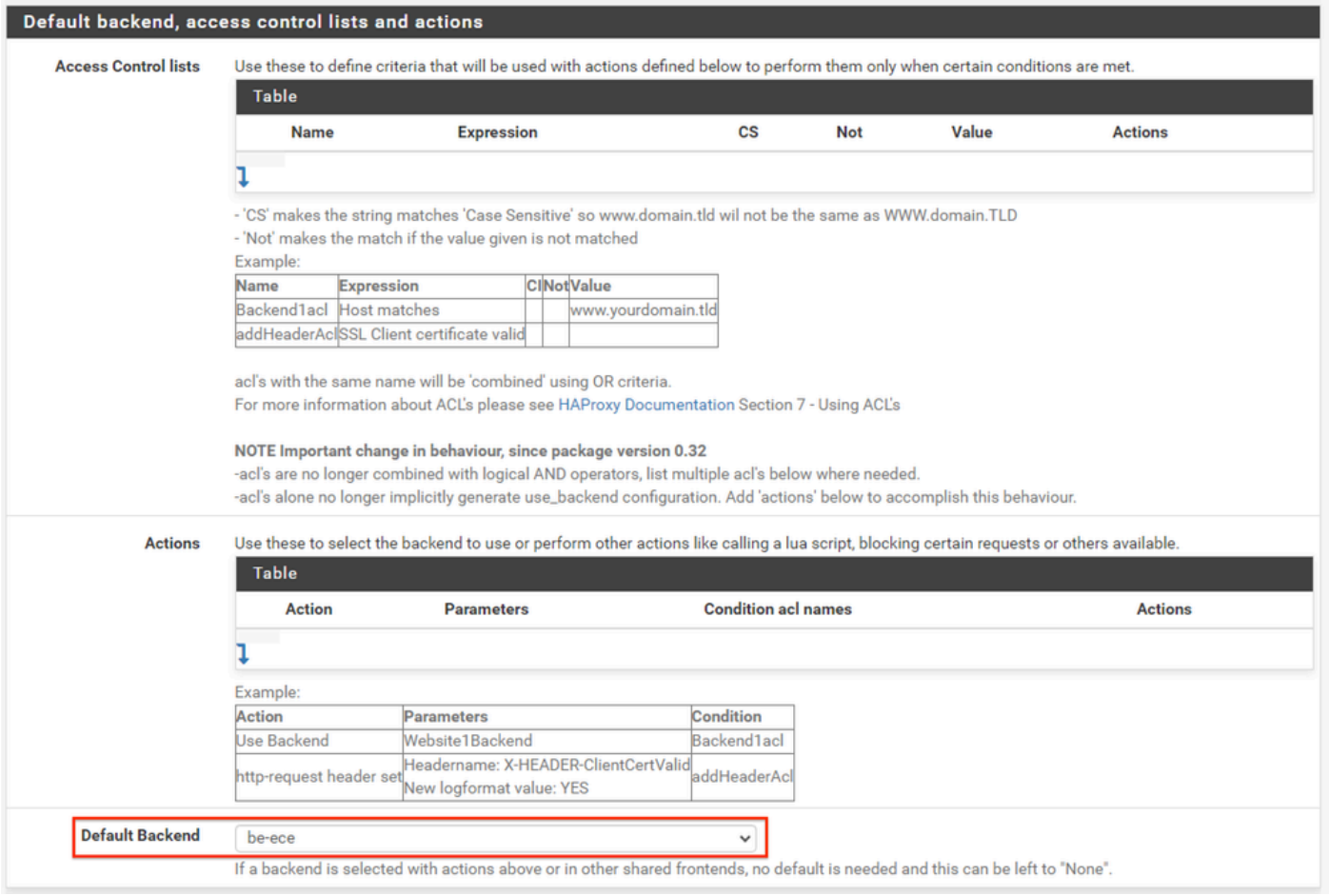
フロントエンドを後で識別するのに役立つ説明を提供します。

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。

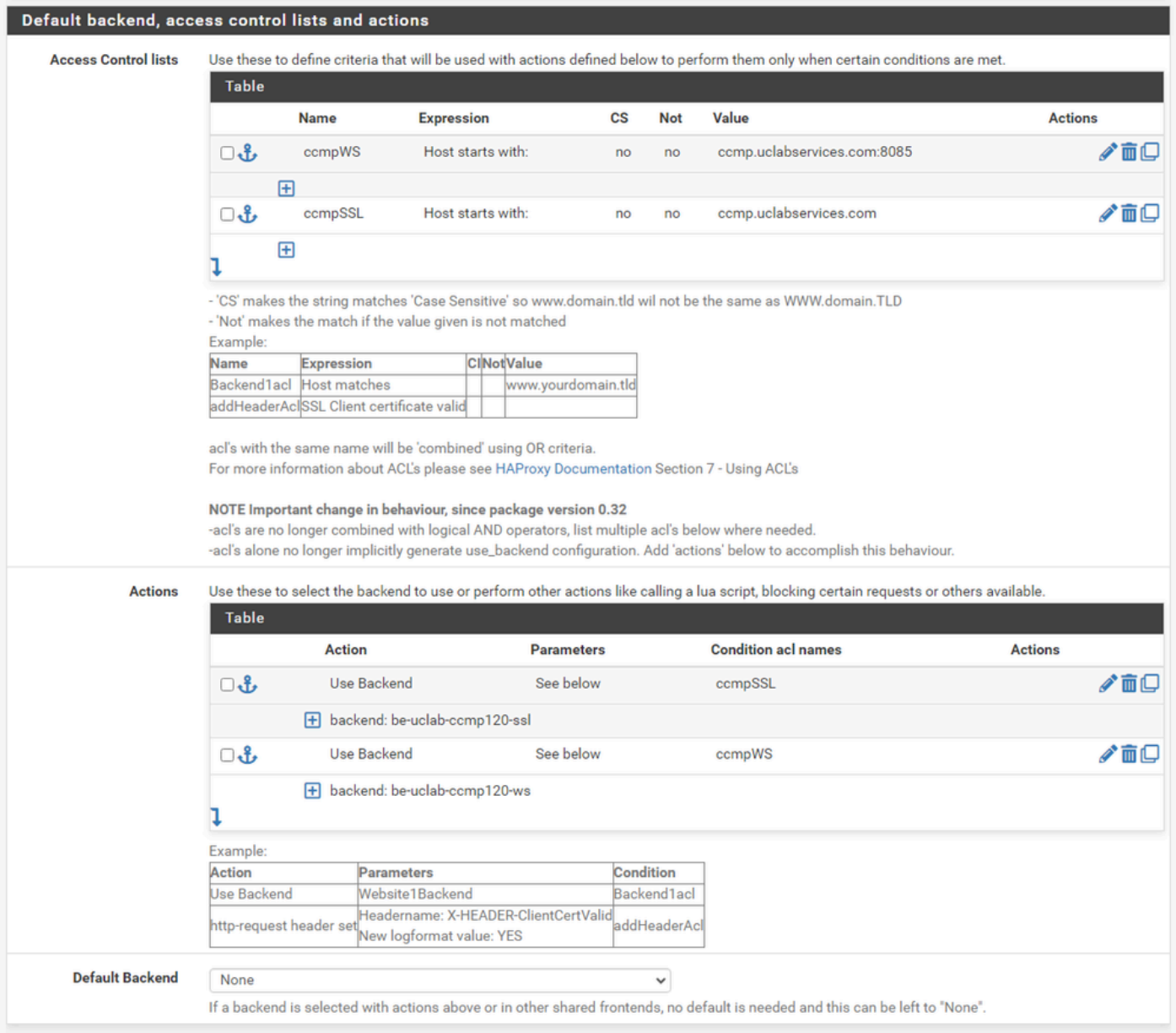
Max connectionsは空のままにします。

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



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。

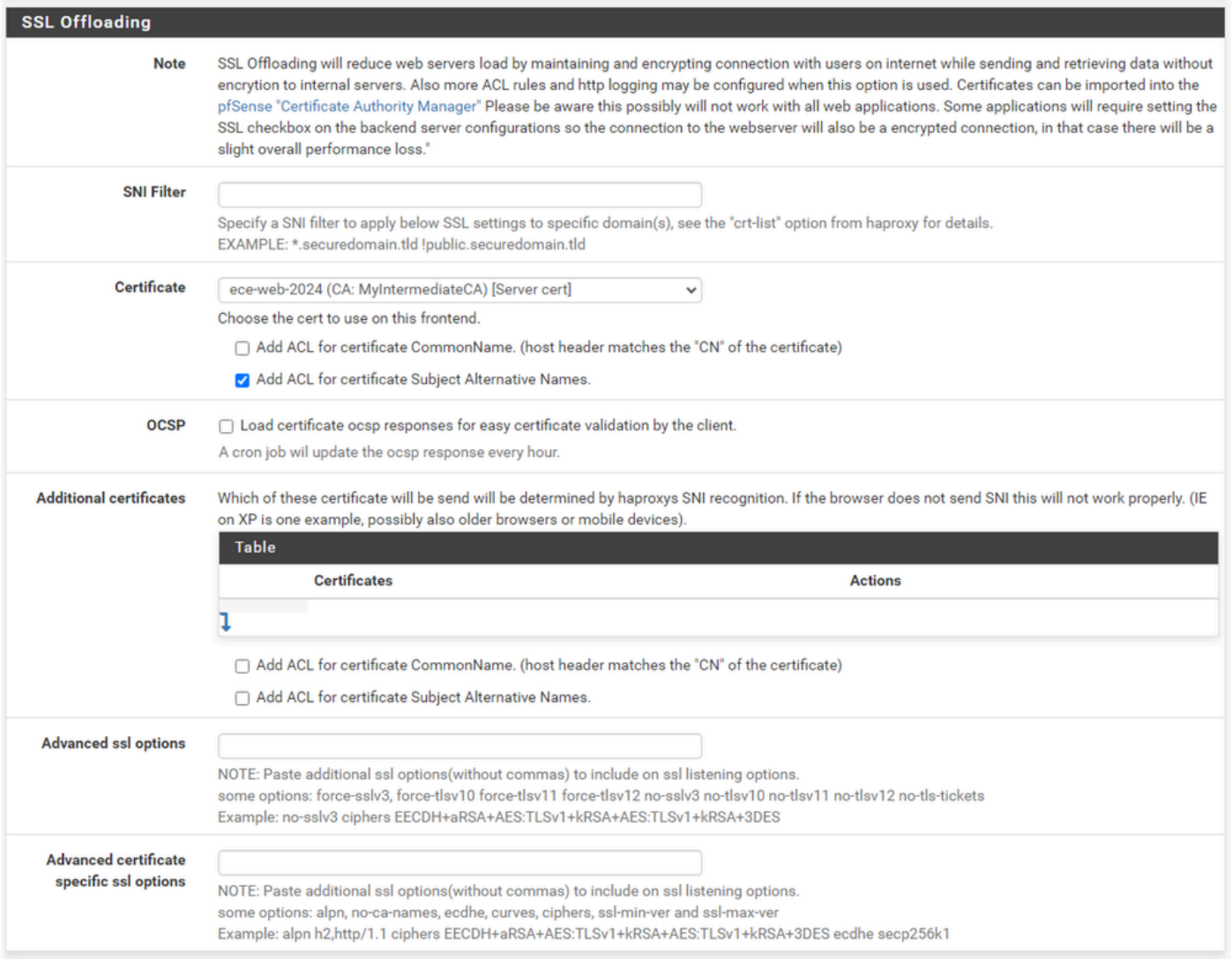


HAProxyバックエンド – ACLアドバンスド

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、または単に名前で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。



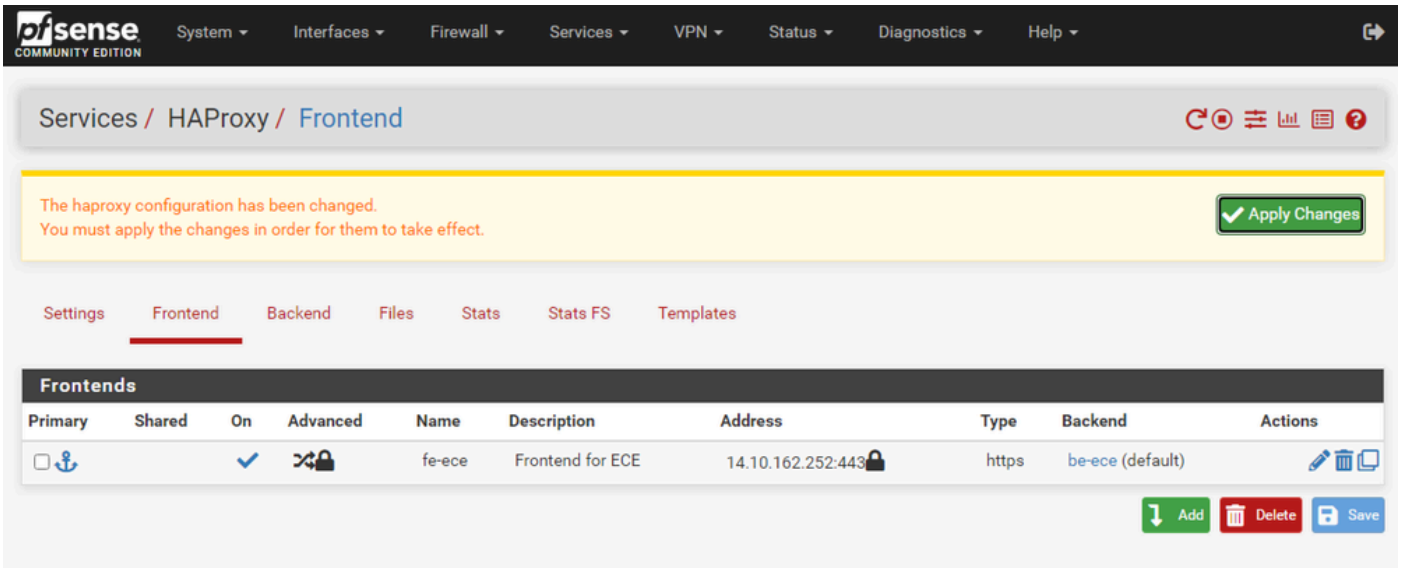
HAProxyフロントエンド – 証明書バインド

[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。



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。