Configurar o Balanceador de Carga da Comunidade pfSense para ECE

Contents

Introdução

Este documento descreve as etapas para instalar e configurar o pfSense Community Edition como um Balanceador de Carga para Bate-papo e E-mail Corporativos (ECE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ECE 12.x
- Edição de comunidade do pfSense

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instalar o pfSense

Visão geral da solução

O pfSense Community Edition é um produto multifuncional que fornece um Firewall, Balanceador de Carga, Scanner de Segurança e muitos outros serviços em um único servidor. O pfSense é construído no Free BSD e tem requisitos mínimos de hardware. O Balanceador de carga é uma implementação do HAProxy e uma GUI fácil de usar é fornecida para configurar o produto.

Você pode usar esse balanceador de carga com o ECE e o Contact Center Management Portal (CCMP). Este documento fornece as etapas para configurar o pfSense para ECE.

Preparação

Etapa 1. Download do software pfSense

Use o site do pfSense para fazer o download da imagem do instalador iso.

Etapa 2. Configurar VM

Configure uma VM com os requisitos mínimos:

· CPU compatível com amd64 (x86-64) de 64 bits

· 1 GB ou mais de RAM

· Unidade de disco de 8 GB ou mais (SSD, HDD, etc.)

· Uma ou mais placas de rede compatíveis

· Unidade USB inicializável ou unidade óptica de alta capacidade (DVD ou BD) para instalação inicial

Para a instalação em laboratório, somente uma interface de rede (NIC) é necessária. Há várias maneiras de executar o dispositivo, mas a mais fácil é com uma única placa de rede, também chamada de modo de um braço. No modo de um braço, há uma única interface que se comunica com a rede. Embora essa seja uma maneira fácil e adequada para um laboratório, não é a maneira mais segura.

Uma maneira mais segura de configurar o dispositivo é ter pelo menos duas NICs. Uma placa de rede é a interface WAN e se comunica diretamente com a Internet pública. A segunda placa de rede é a interface LAN e se comunica com a rede corporativa interna. Você também pode adicionar outras interfaces para se comunicar com várias partes da rede que têm regras de segurança e firewall diferentes. Por exemplo, você pode ter uma placa de rede conectada à Internet pública, uma conectada à rede DMZ, onde estão todos os servidores Web acessíveis externamente, e uma terceira placa de rede conectada à rede corporativa. Isso permite que usuários internos e externos acessem com segurança o mesmo conjunto de servidores Web mantidos em uma DMZ. Assegure-se de que o compreenda as implicações de segurança de qualquer projeto antes da implementação. Consulte um engenheiro de segurança para garantir que as melhores práticas sejam seguidas para sua implementação específica.

Instalação

Etapa 1. Montar o ISO na VM

Etapa 2. Ligue a VM e siga os avisos para instalar.

Consulte este documento para obter instruções passo a passo.

Instalação de rede

Você deve atribuir endereços IP ao equipamento para continuar a configuração.

Observação: este documento mostra um dispositivo configurado no modo one-arm.

Etapa 1. Configurar VLANs

Se você precisar de suporte para VLAN, responda y à primeira pergunta. Caso contrário, responda n.

Etapa 2. Atribuir interface WAN

A interface WAN é o lado não seguro do dispositivo no modo de dois braços e a única interface no modo de um braço. Digite o nome da interface quando solicitado.

Etapa 3. Atribuir a interface LAN

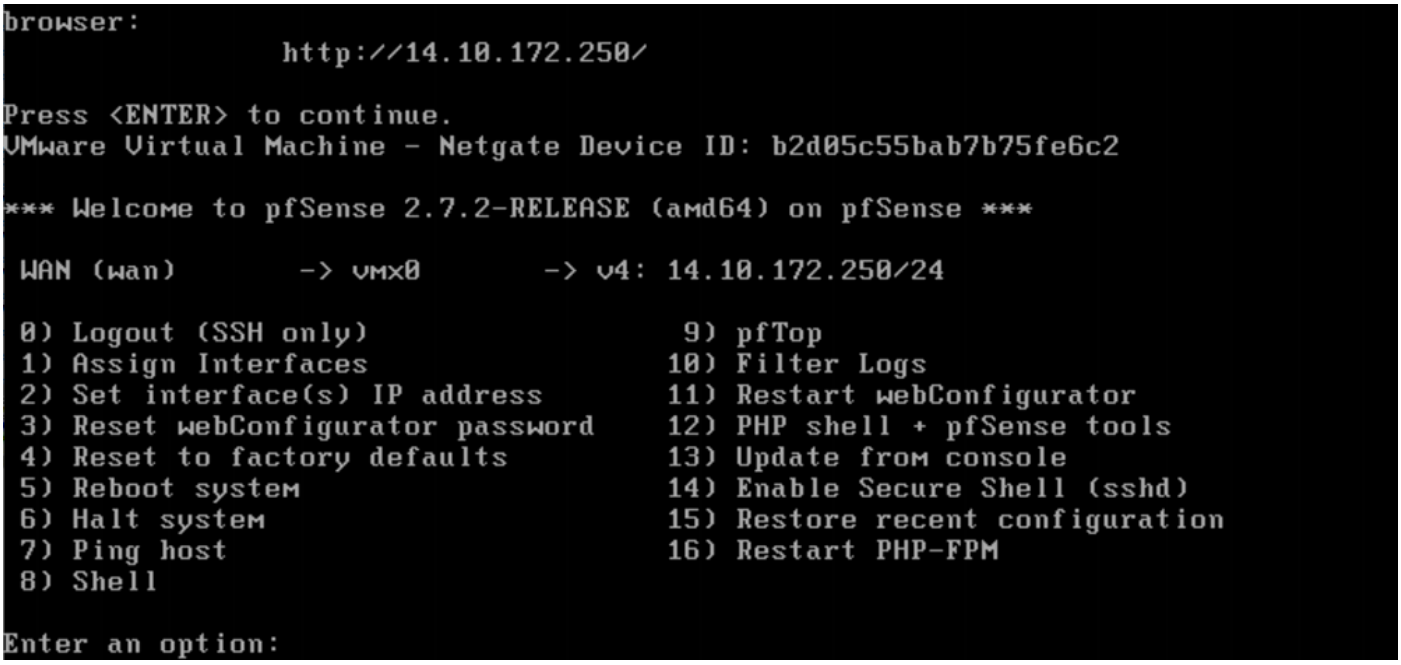
A interface LAN é o lado seguro do dispositivo no modo de dois braços. Se necessário, insira o nome da interface quando solicitado.

Etapa 4. Atribuir qualquer outra interface

Configure quaisquer outras interfaces necessárias para sua instalação específica. Elas são opcionais e não comuns.

Etapa 5. Atribuir endereço IP à interface de gerenciamento

Se a sua rede suportar DHCP, o endereço IP atribuído será mostrado na tela do console.

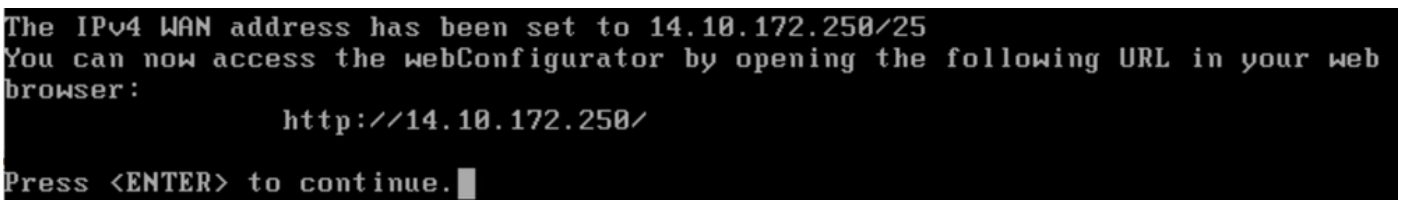


Console pfSense

Se não houver endereço atribuído ou se você quiser atribuir um endereço específico, execute estas etapas.

1. Escolha a opção 2 no menu do console.
2. Responda n para desativar o DHCP.
3. Insira o endereço IPv4 da interface WAN.
4. Insira a máscara de rede em contagens de bits. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Digite o endereço de gateway para a interface WAN.
6. Se quiser que esse gateway seja o gateway padrão do equipamento, responda y ao prompt do gateway, caso contrário, responda n.
7. Configure a placa de rede para IPv6, se desejado.
8. Desative o servidor DHCP na interface.
9. Responda y para ativar o HTTP no protocolo webConfigurator. Isso é usado nas próximas etapas.

Em seguida, você receberá uma confirmação de que as configurações foram atualizadas.

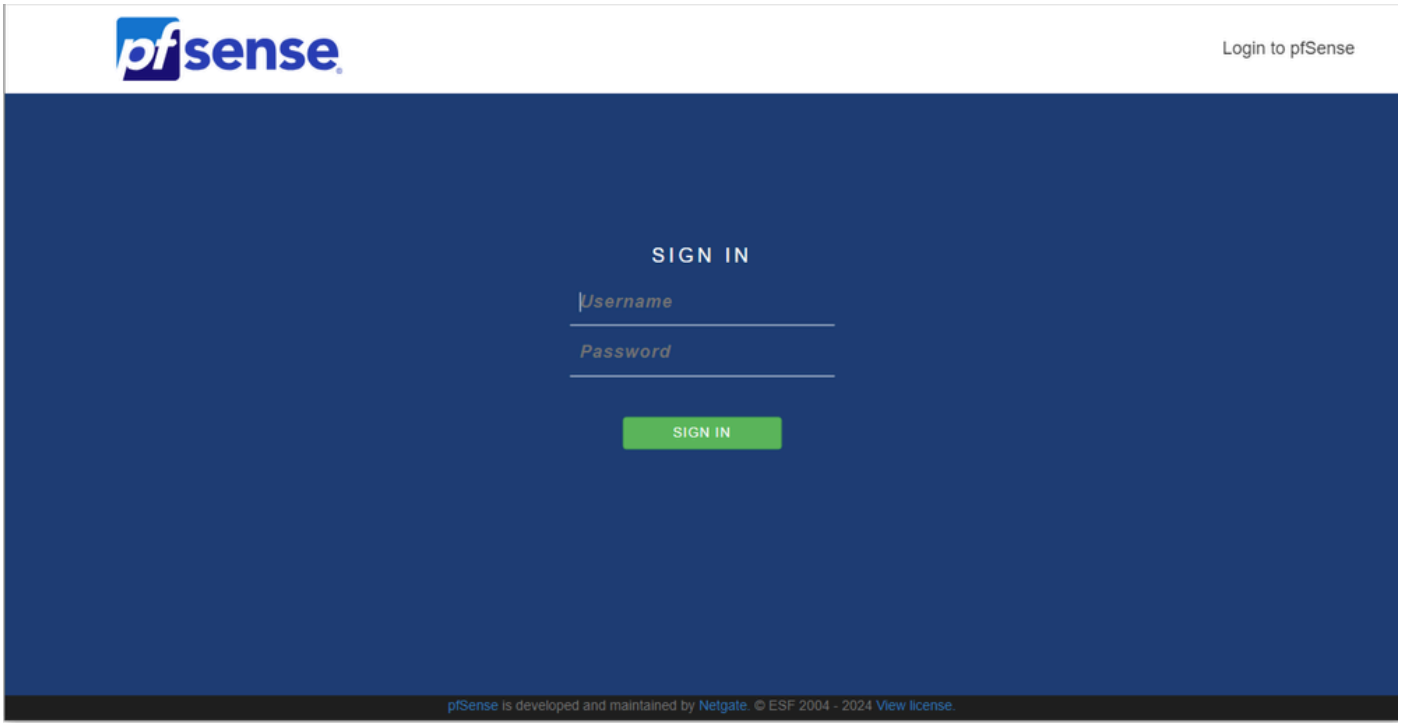


Confirmação do pfSense

Concluir configuração inicial

Etapa 1. Abra um navegador da Web e navegue até: http://<ip_address_of_appliance>

Observação: você deve usar HTTP e não HTTPS inicialmente.

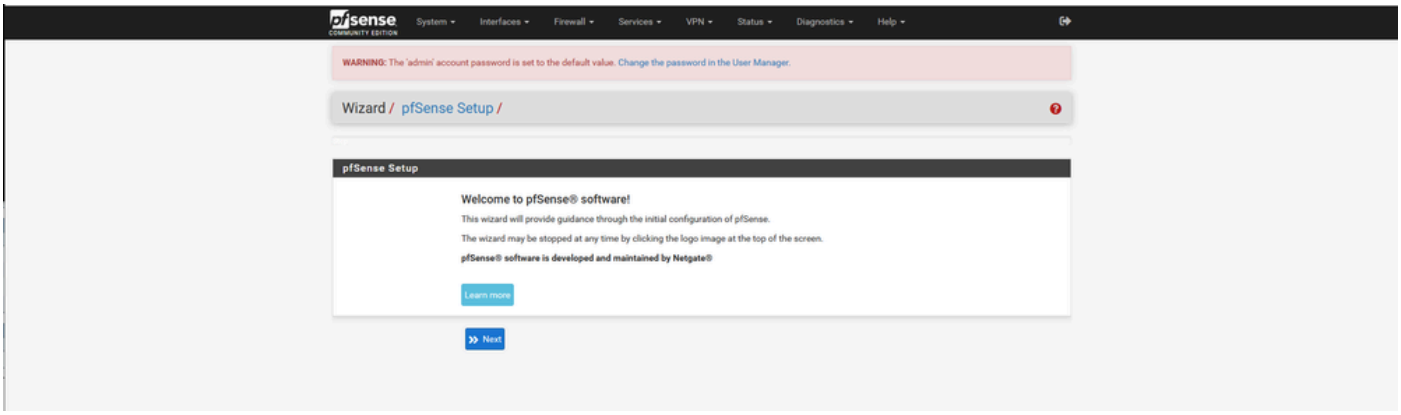


Logon do administrador do pfSense

Etapa 2. Faça login com o login padrão admin / pfSense

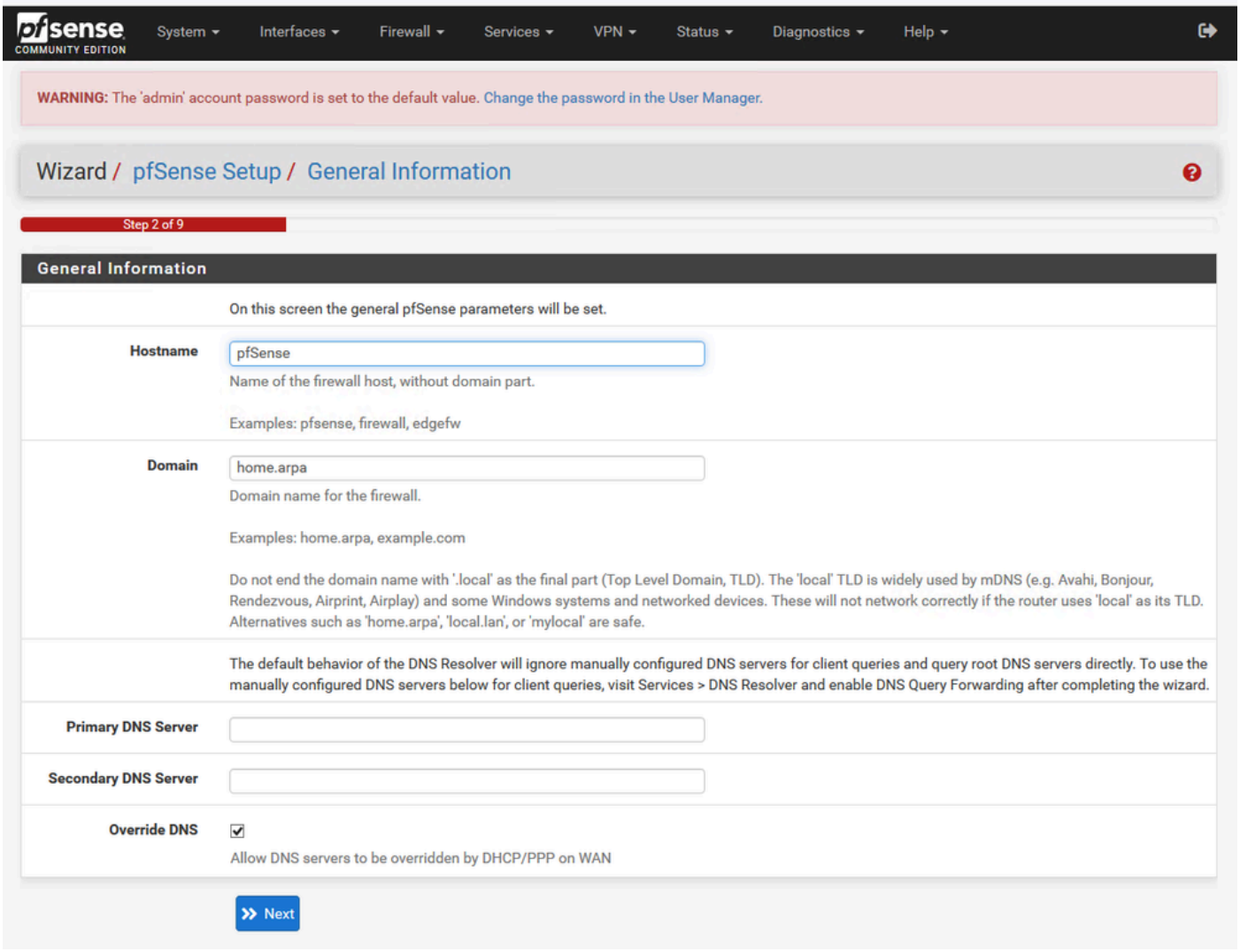
Etapa 3. Concluir a configuração inicial

Clique em Next (Avançar) nas duas primeiras telas.



Assistente para configuração do pfSense - 1

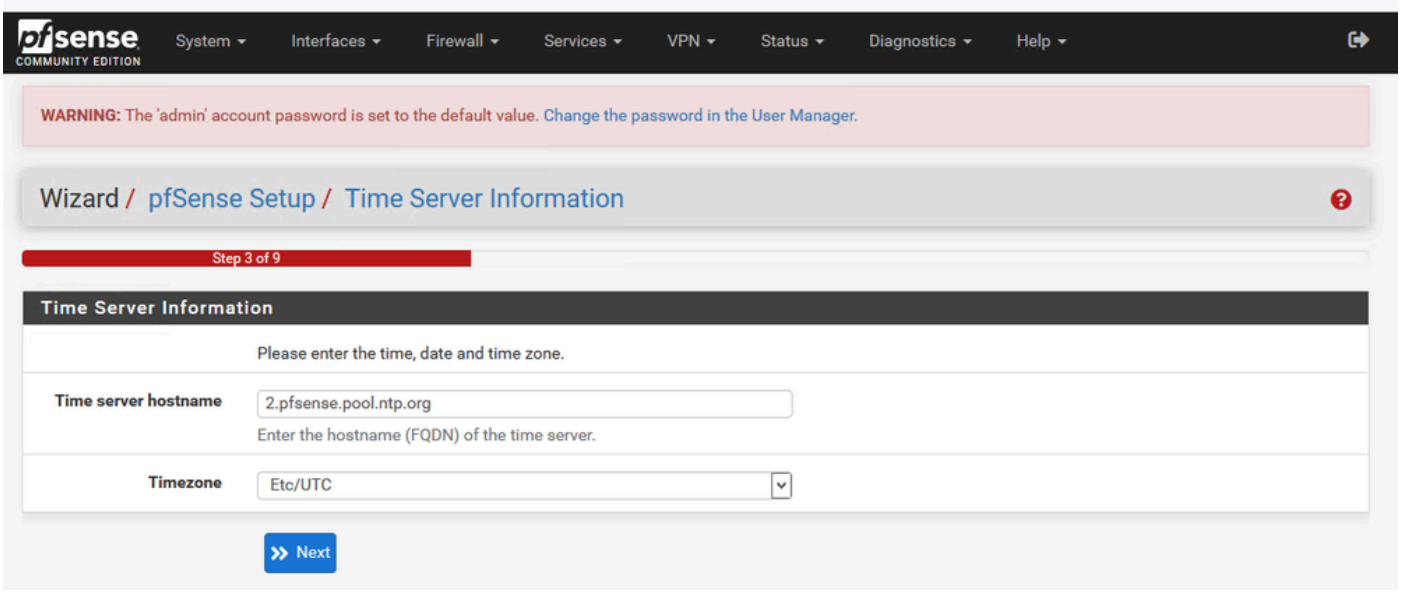
Forneça o nome do host, o nome do domínio e as informações do servidor DNS.



Assistente para configuração do pfSense - 2

Valide as informações de endereço IP. Se você escolheu DHCP inicialmente, poderá alterá-lo agora.

Forneça o nome de host do servidor de horário NTP e selecione o fuso horário correto na lista suspensa.



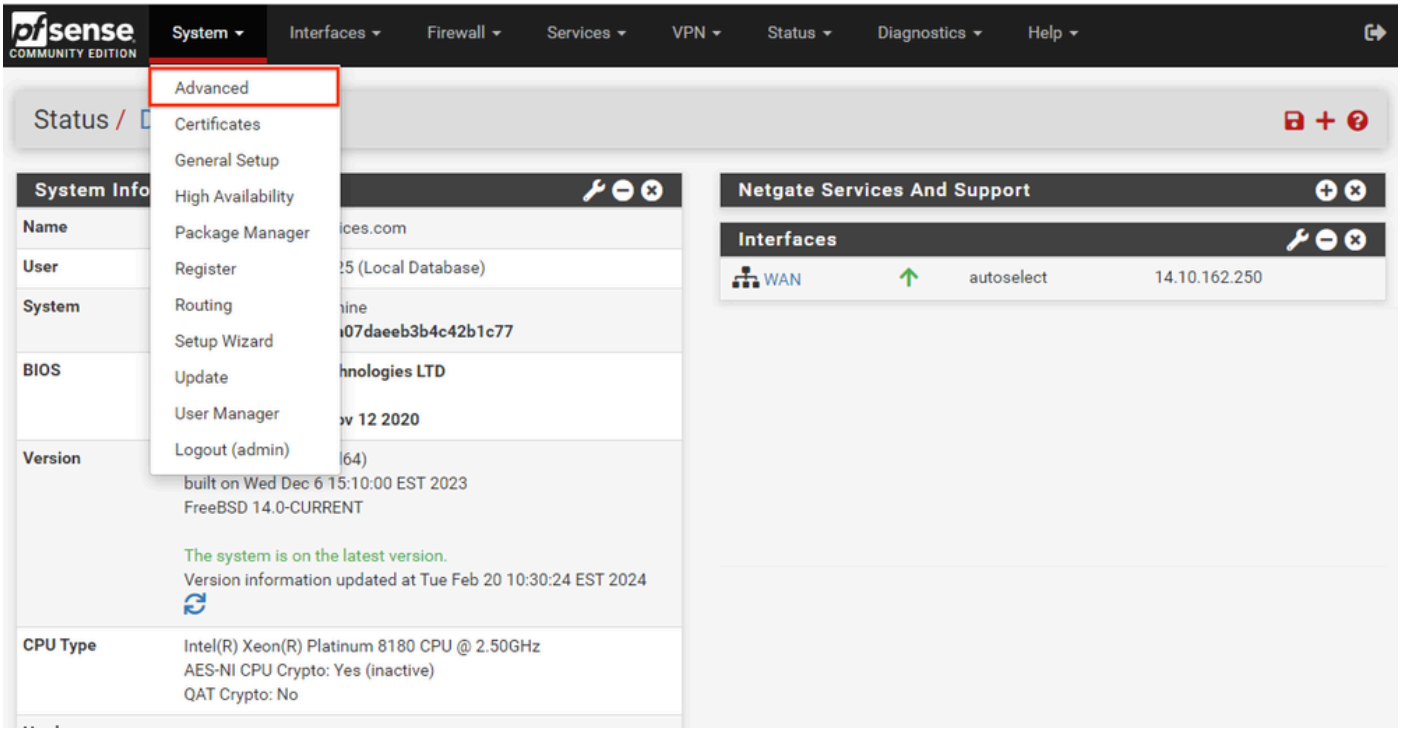
Assistente para configuração do pfSense - 3

Continue no assistente de configuração até o final. A interface GUI é reiniciada e você é redirecionado para a nova URL depois de concluído.

Definir Configurações Básicas de Administração

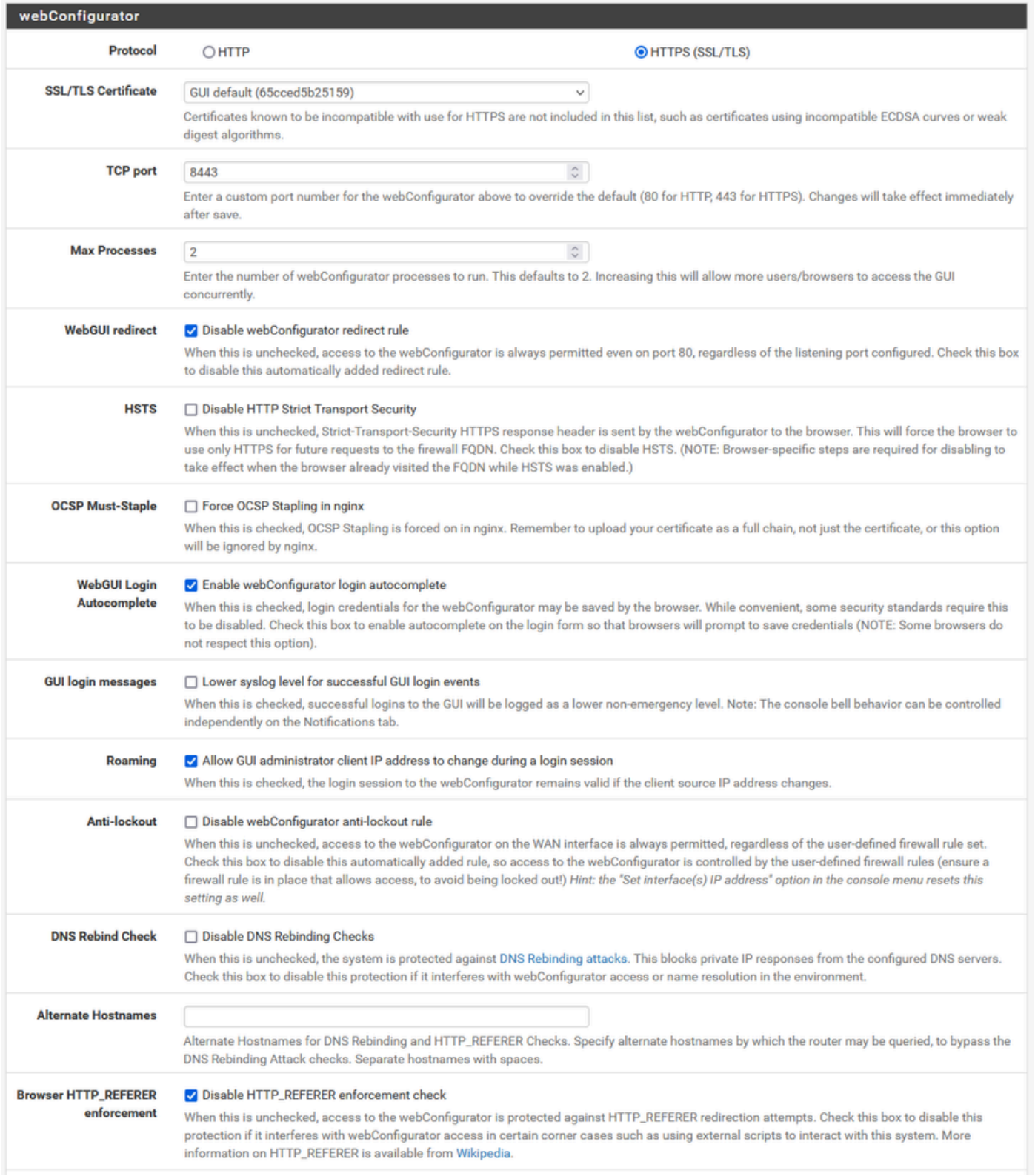
Etapa 1. Faça login na interface do administrador

Etapa 2. Selecione Avançado no menu suspenso Sistema



GUI pfSense - menu suspenso Admin

Etapa 3. Atualizar configurações do WebConfigurator



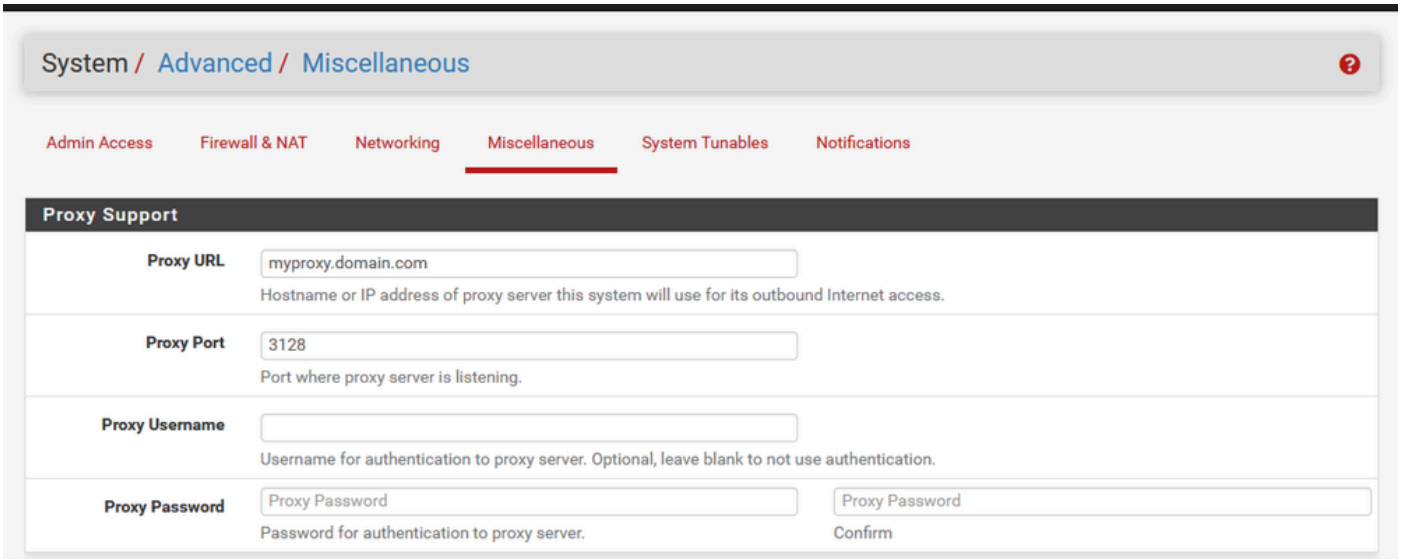
GUI pfSense - Configuração do administrador

1. Selecione o protocolo HTTPS (SSL/TLS).
2. Deixe o certificado SSL/TLS para o certificado autoassinado neste momento.
3. Altere a porta TCP para uma porta diferente de 443 para proteger melhor a interface e evitar problemas com sobreposição de porta.
4. Selecione a opção WebGUI redirect para desativar a interface admin na porta 80.
5. Selecione a opção de imposição Navegador HTTP_REFERER.
6. Habilite o Secure Shell selecionando a opção Habilitar Secure Shell.

Observação: certifique-se de selecionar o botão Salvar antes de continuar. Em seguida, você é redirecionado para o novo link https.

Etapa 4. Configurar o servidor proxy, se necessário

Se necessário, configure as informações de proxy na guia Diversos. Para concluir a instalação e a configuração, o equipamento deve ter acesso à Internet.



GUI pfSense - Configuração de proxy

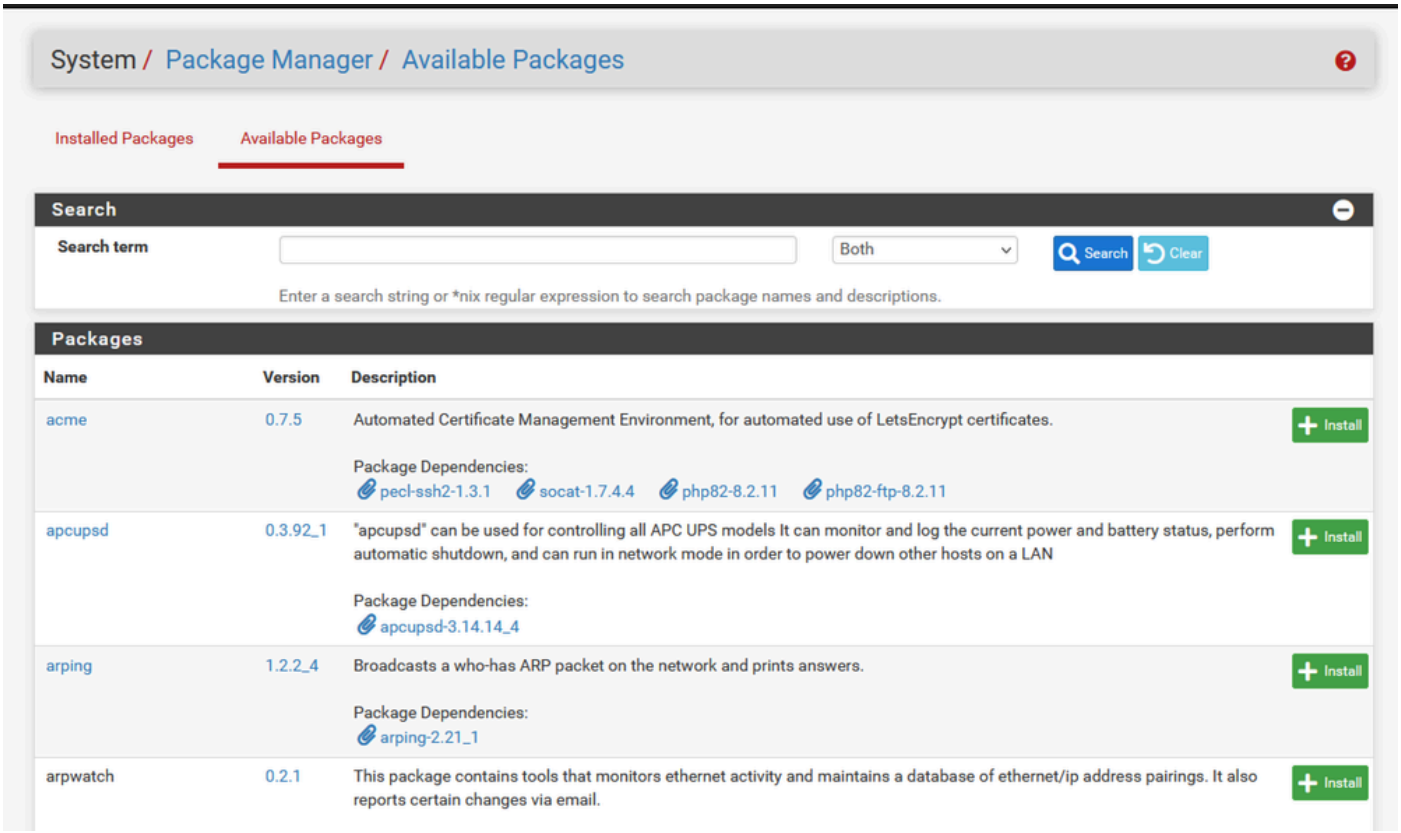
Observação: certifique-se de selecionar o botão Salvar depois de fazer as alterações.

Adicionar Pacotes Necessários

Etapa 1. Selecione System > Package Manager

Etapa 2. Selecionar pacotes disponíveis

Observação: pode levar alguns minutos para carregar todos os pacotes disponíveis. Se o tempo limite for excedido, verifique se os servidores DNS estão configurados corretamente. Frequentemente, uma reinicialização do dispositivo corrige a conectividade com a Internet.



GUI pfSense - Lista de pacotes

Etapa 3. Localizar e instalar os pacotes necessários

1. haproxy
2. Ferramentas Open-VM

Observação: não selecione o pacote haproxy-devel.

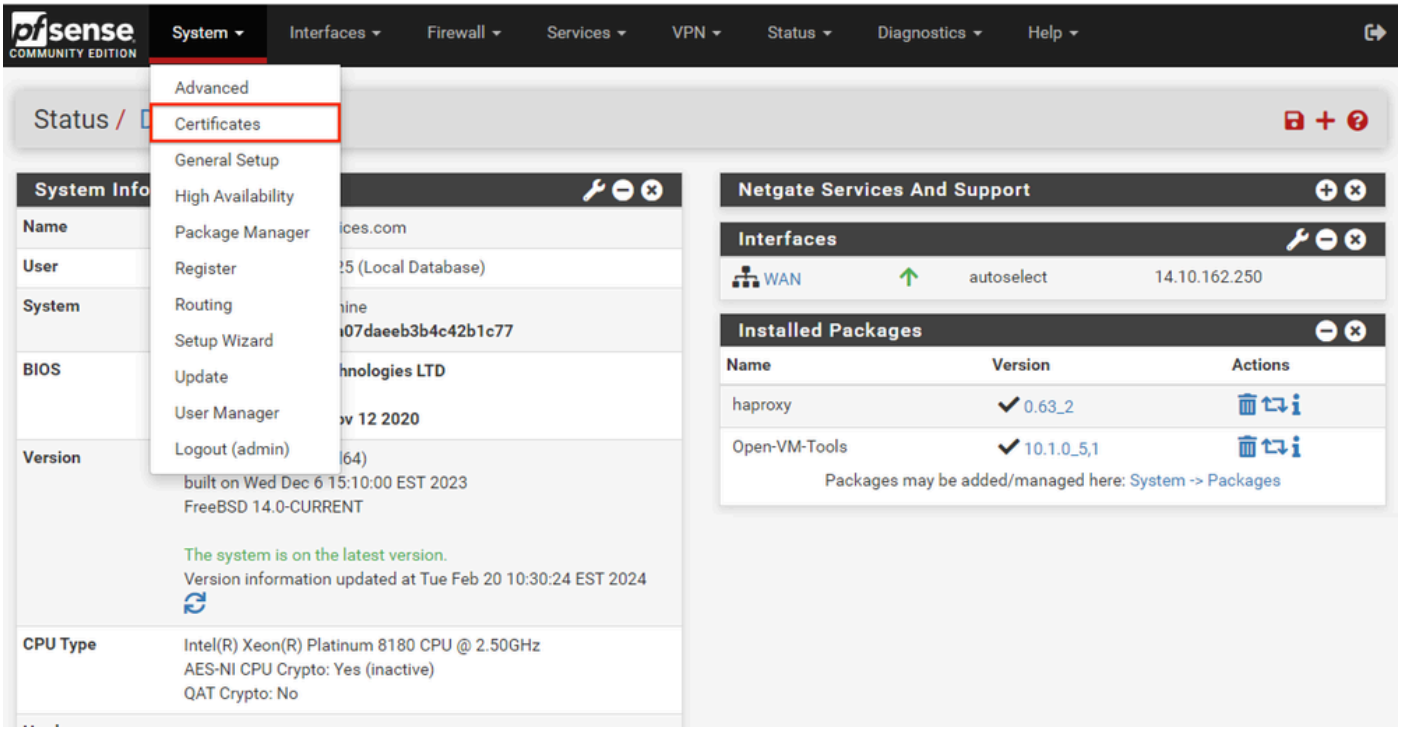
Configurar certificados

O pfSense pode criar um certificado autoassinado ou pode integrar-se com uma CA pública, uma CA interna ou pode atuar como uma CA e emitir certificados assinados por uma CA. Este guia mostra as etapas para integração com uma CA interna.

Antes de iniciar esta seção, verifique se você tem esses itens disponíveis.

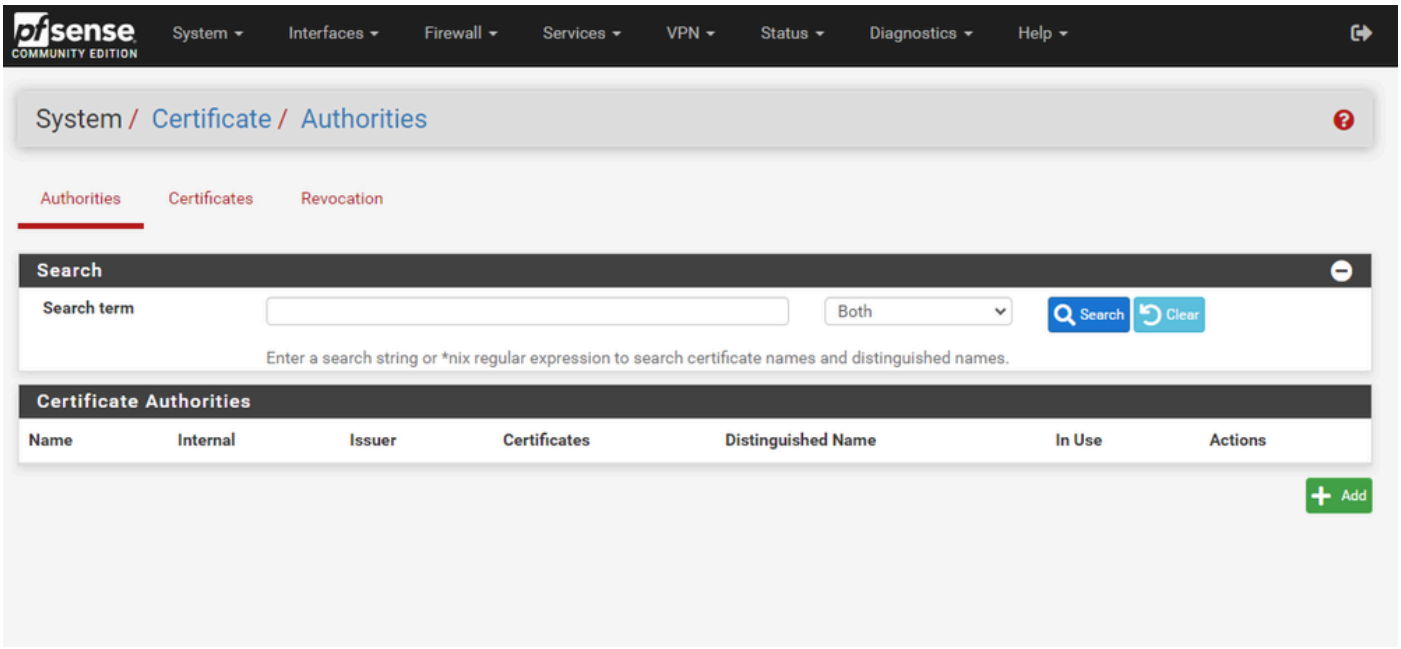
1. Certificado raiz para CA salvo como um formato codificado PEM ou Base-64.
2. Todos os certificados intermediários (às vezes chamados de emissores) para CA salvos como um formato codificado PEM ou Base-64.

Etapa 1. Selecione Certificados no menu suspenso Sistema



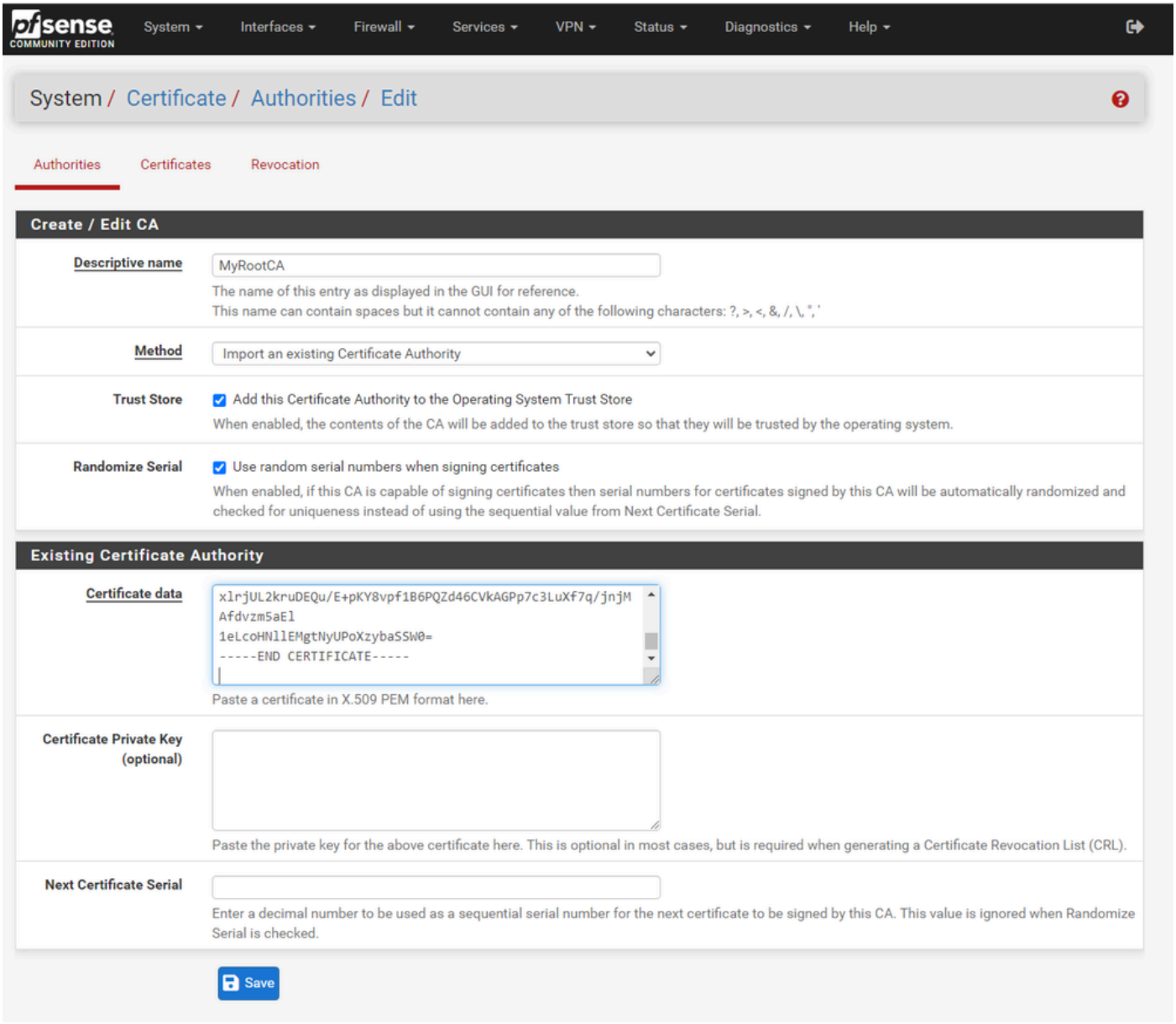
GUI pfSense - menu suspenso Certificados

Etapa 2. Importar o certificado raiz da autoridade de certificação



GUI pfSense - Lista de certificados CA

Selecione o botão Add.



GUI pfSense - Importação de CA

Conforme mostrado na imagem:

1. Forneça um nome exclusivo e descritivo

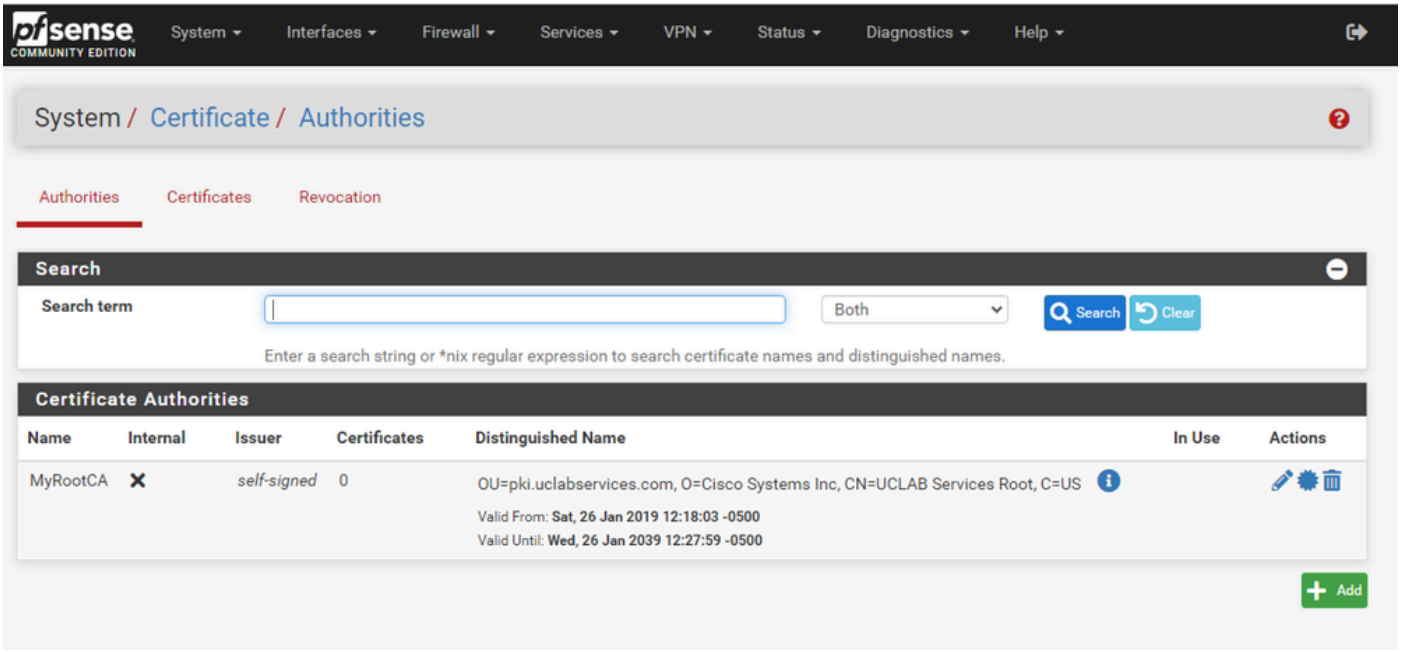
2. Selecione Importar uma Autoridade de Certificação existente na lista suspensa Método.

3. Verifique se as caixas de seleção Trust Store e Randomize Serial estão marcadas.

4. Cole o certificado inteiro na caixa de texto Dados do certificado. Certifique-se de incluir as linhas -----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----.

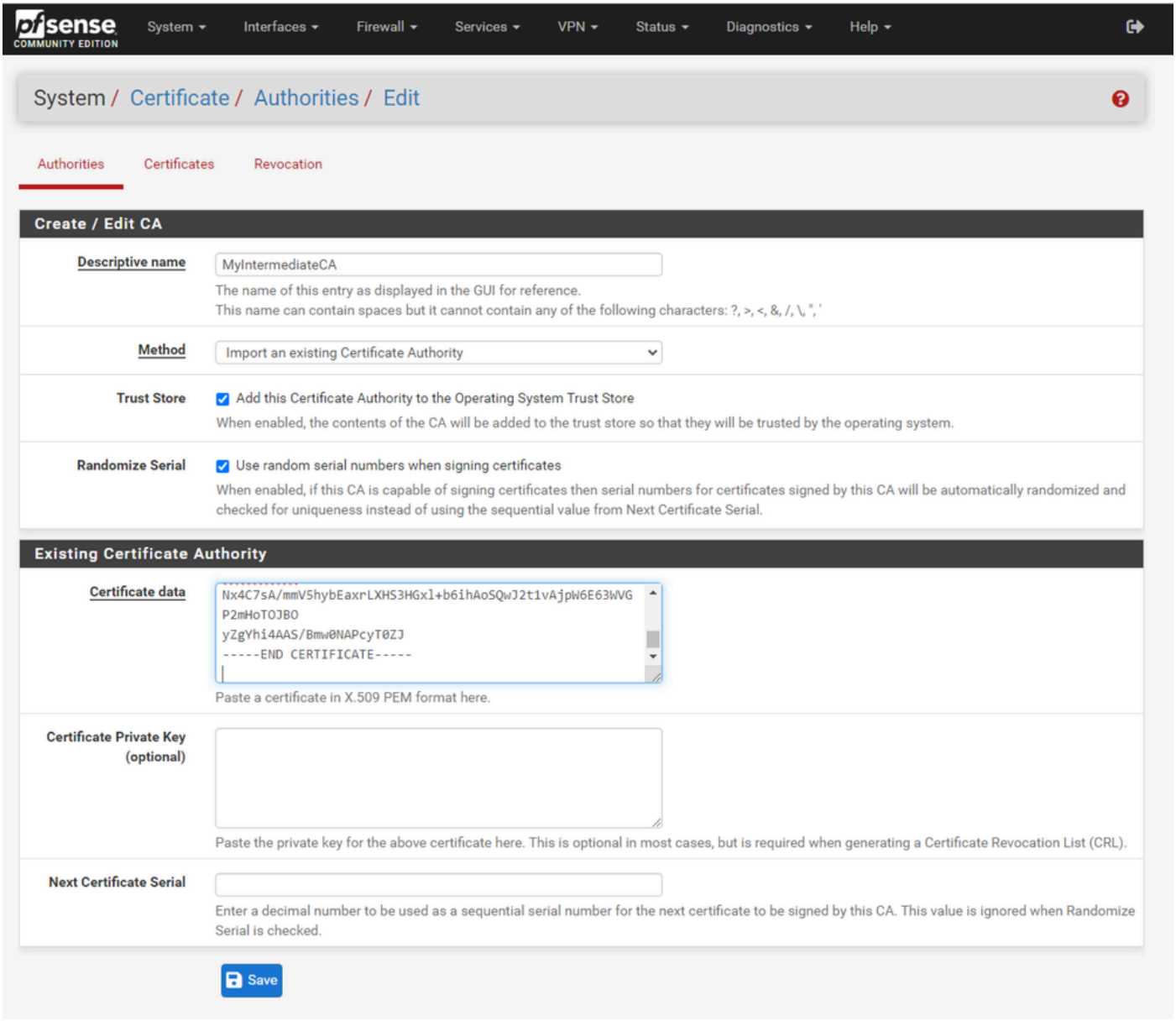
5. Selecione Salvar.

6. Verifique se o Certificado é importado conforme mostrado na imagem.



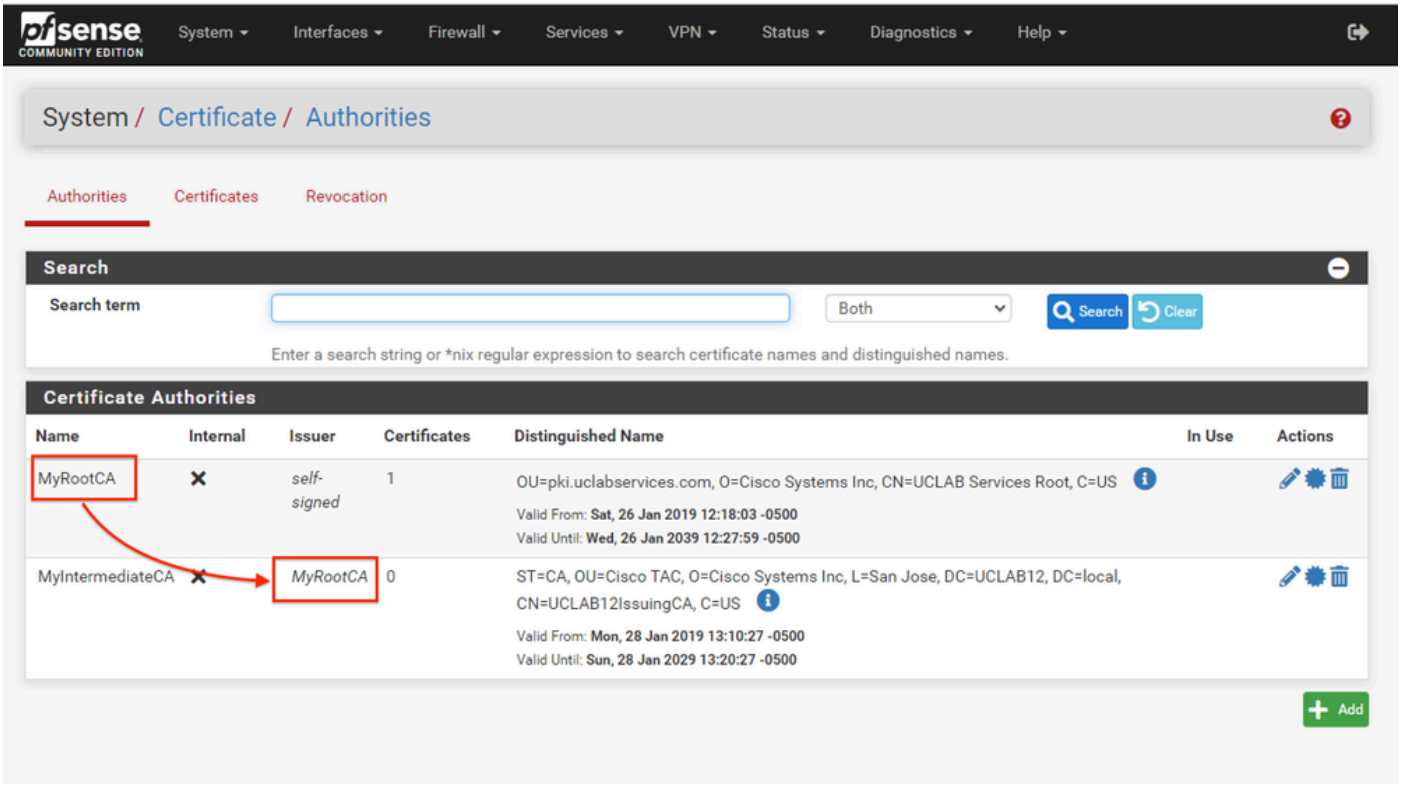
GUI pfSense - Lista de CA

Etapa 3. Importar o Certificado Intermediário da CA



GUI pfSense - CA Intermediate Import

Repita as etapas para importar o certificado CA raiz e importar o certificado CA intermediário.



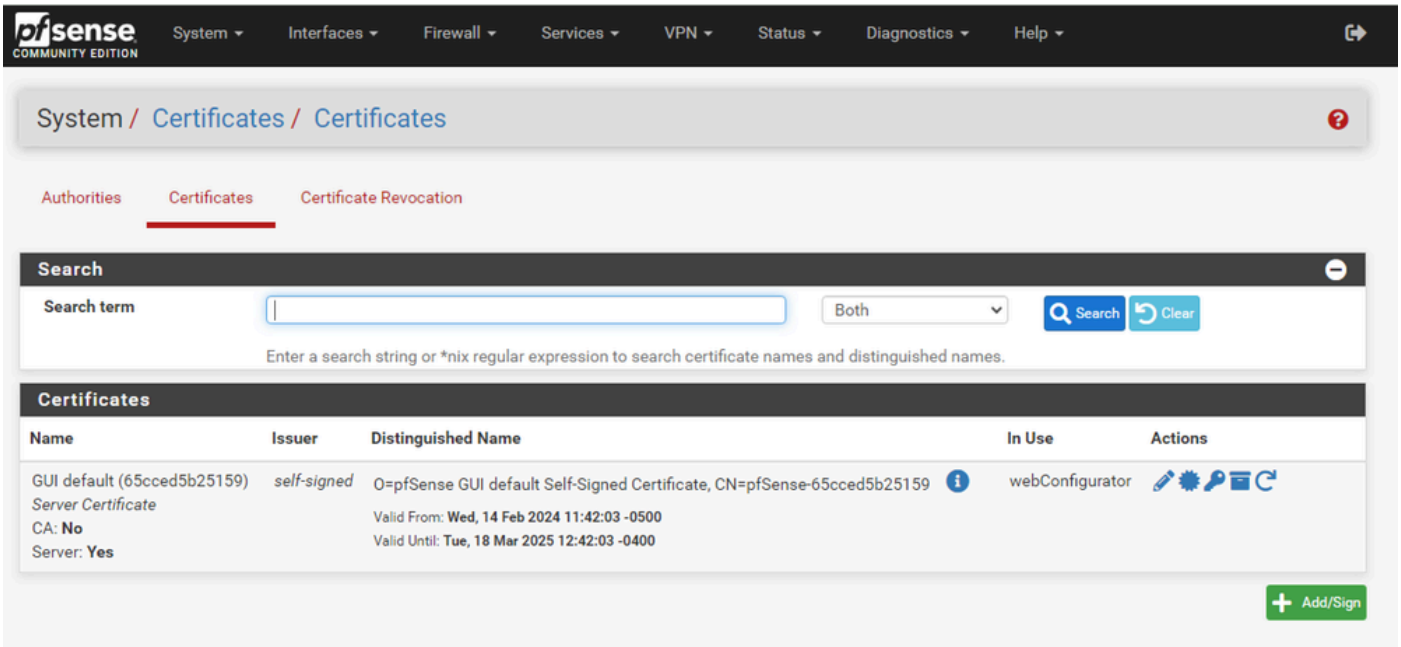
GUI pfSense - Links da CA

Revise as Autoridades de Certificação para garantir que o Intermediário esteja corretamente encadeado ao certificado raiz conforme mostrado na imagem.

Etapa 4. Criar e exportar um CSR para o site com balanceamento de carga

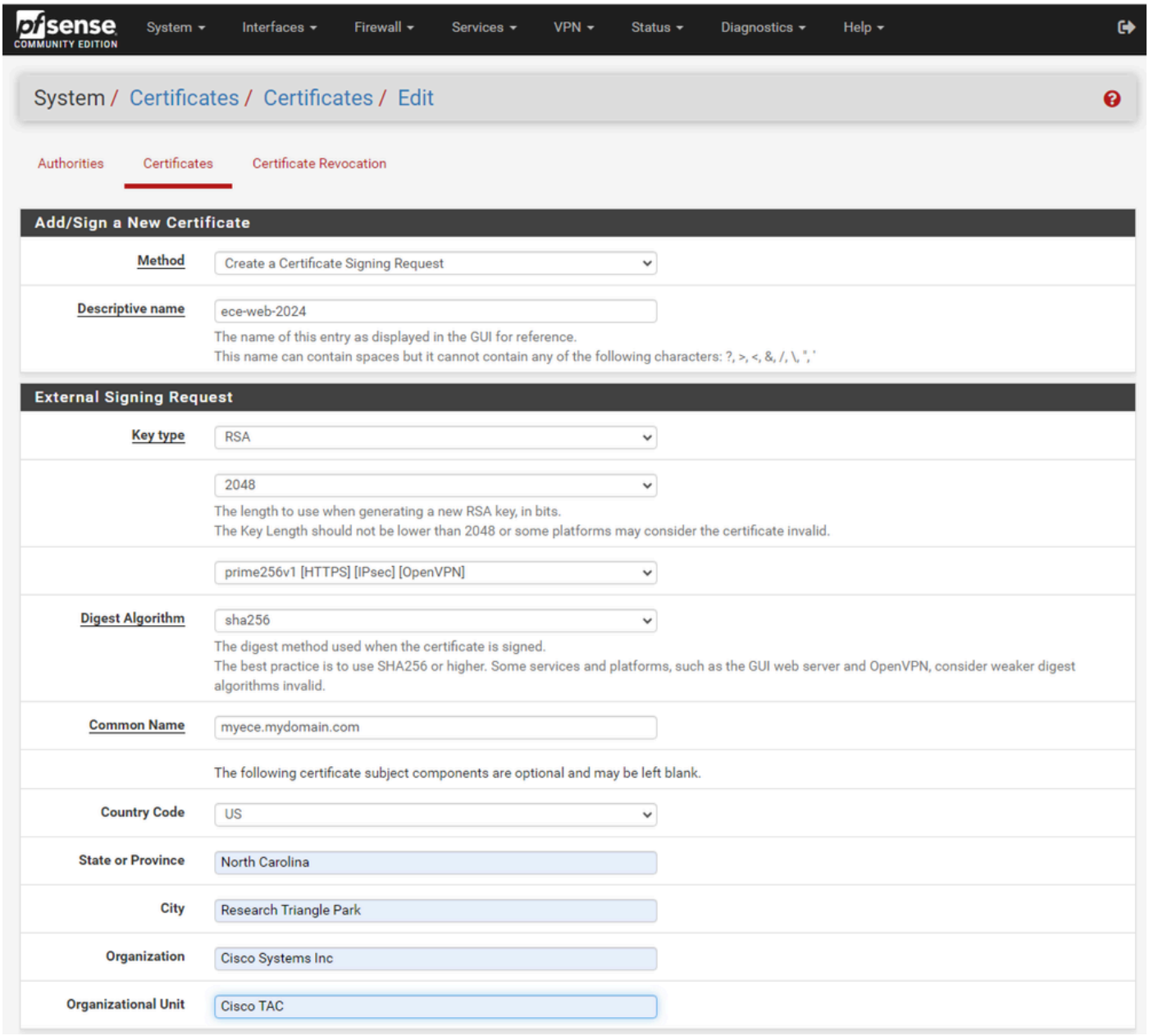
Descreve as etapas para criar um CSR, exportar o CSR e importar o certificado assinado. Se você já tiver um certificado existente em um formato PFX, poderá importar esse certificado. Consulte a documentação do pfSense para obter esses passos.

1. Selecione o menu Certificados e, em seguida, selecione o botão Adicionar/Assinar.



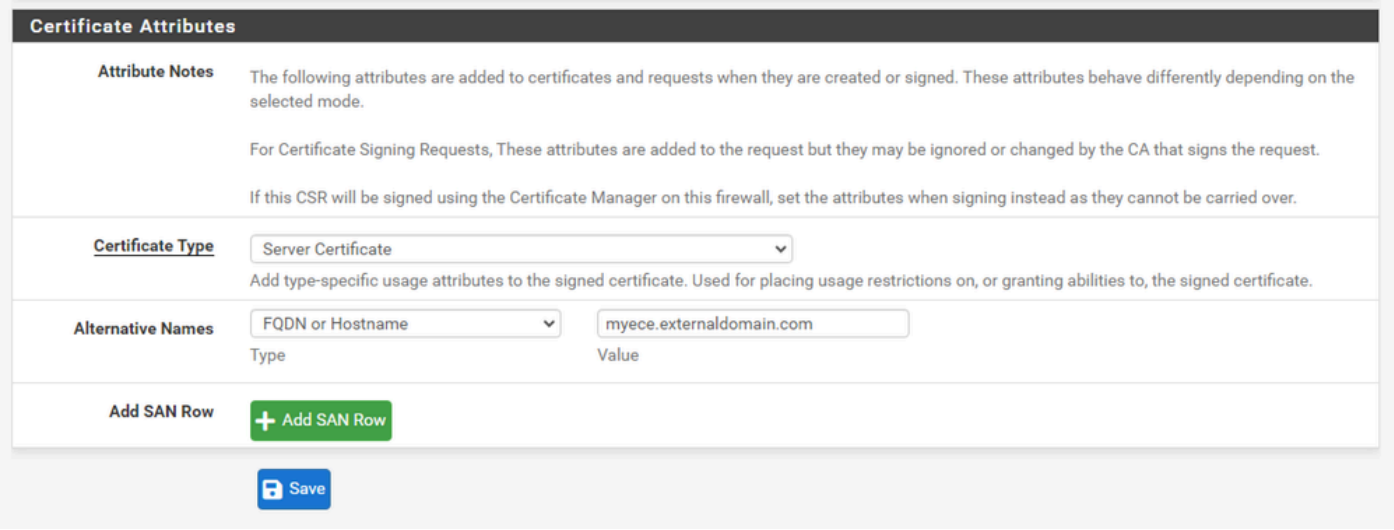
GUI pfSense - Lista de certificados

2. Preencha o formulário de Solicitação de Assinatura de Certificado.



GUI pfSense - Criação de CSR

- Método: selecione Criar uma solicitação de assinatura de certificado no menu suspenso
- Nome descritivo: forneça um nome para o certificado
- Tipo de chave e algoritmo de resumo: revise para garantir que eles correspondam aos seus requisitos
- Nome comum: forneça o site da Web de nome de domínio totalmente qualificado
- Forneça as informações de certificado restantes conforme necessário para o seu ambiente



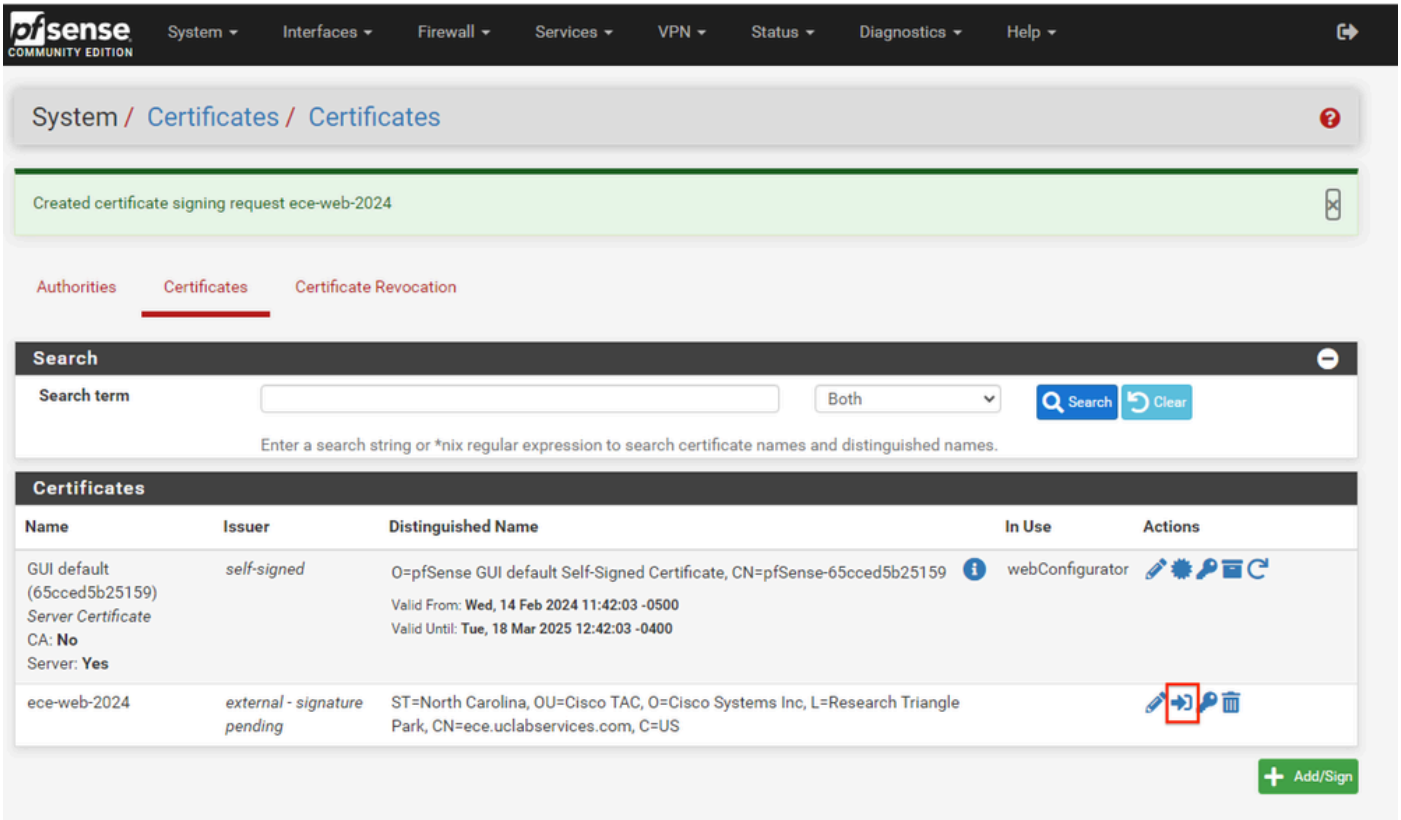
GUI pfSense - CSR Avançado

- Tipo de certificado: selecione Certificado do servidor na lista suspensa.
- Nomes alternativos: forneça todos os nomes alternativos do assunto (SAN) necessários para sua implementação.

Observação: o nome comum é automaticamente adicionado ao campo SAN. Você só precisa adicionar outros nomes necessários.

Selecione Salvar quando todos os campos estiverem corretos.

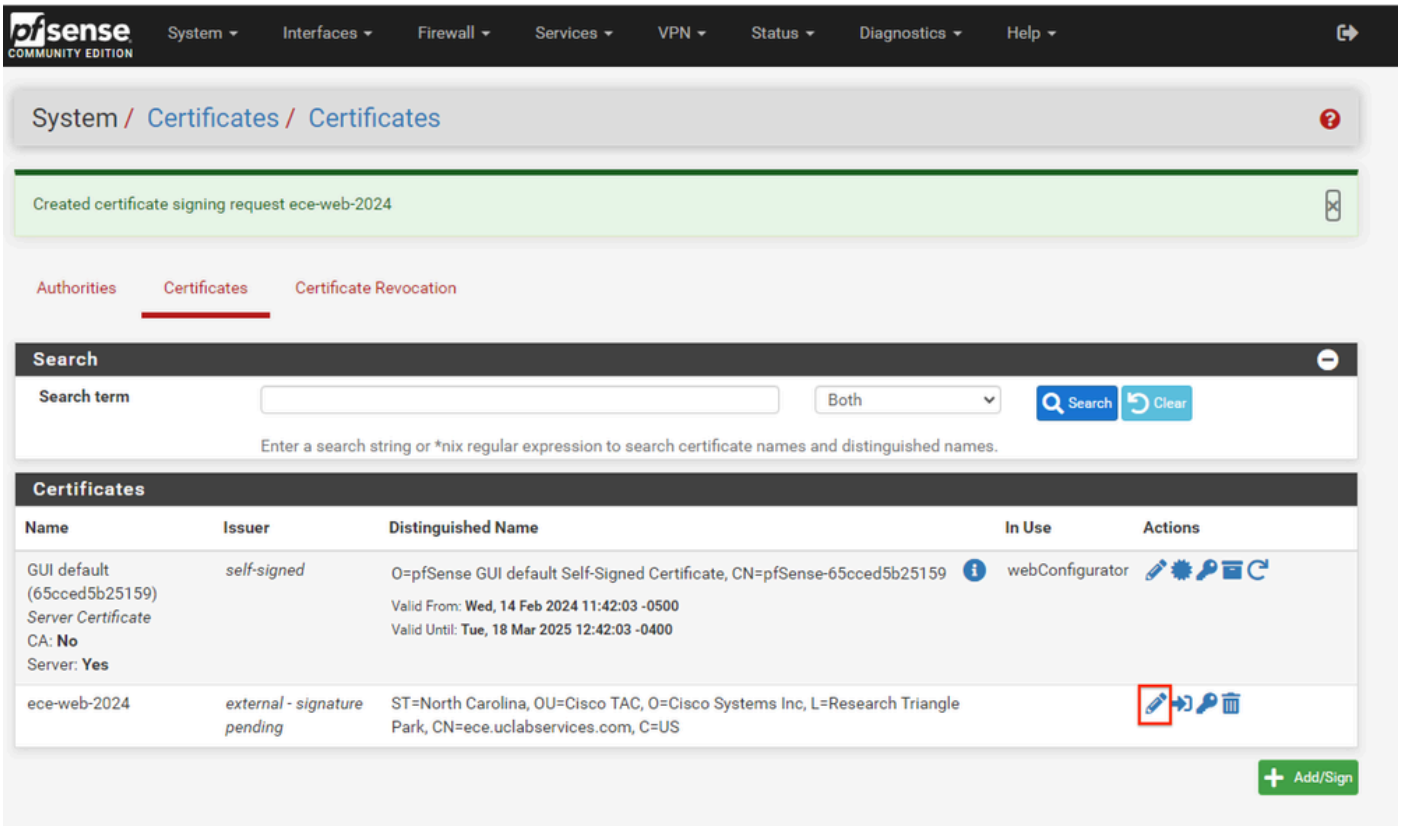
3. Exporte o CSR para um arquivo.



GUI pfSense - Exportação CSR

Selecione o botão Exportar para salvar o CSR e, em seguida, assine-o com sua CA. Quando tiver o certificado assinado, salve-o como um arquivo PEM ou Base-64 para concluir o processo.

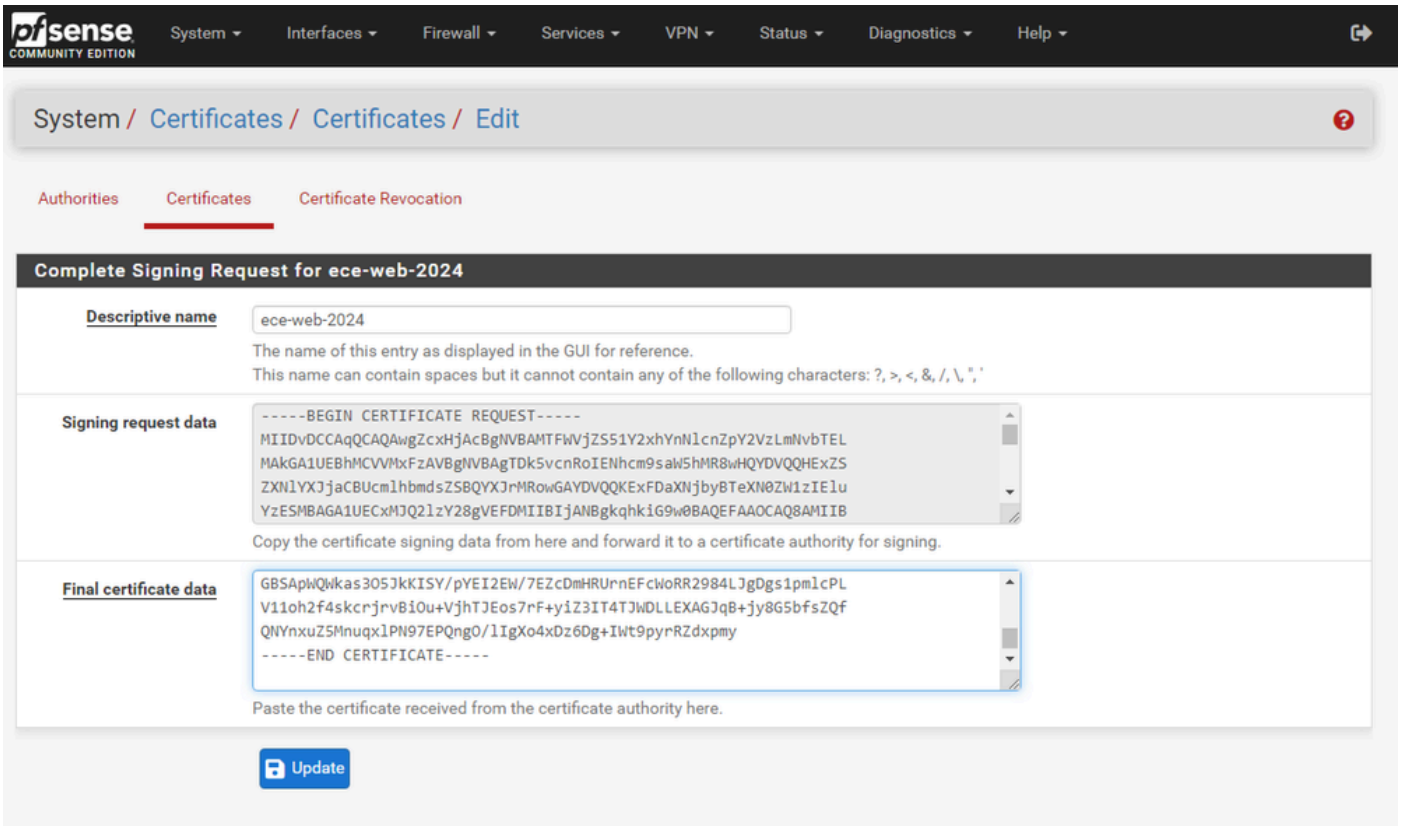
4. Importe o certificado assinado.



GUI do pfSense - Importação de certificado

Selecione o ícone do Lápis para importar o certificado assinado.

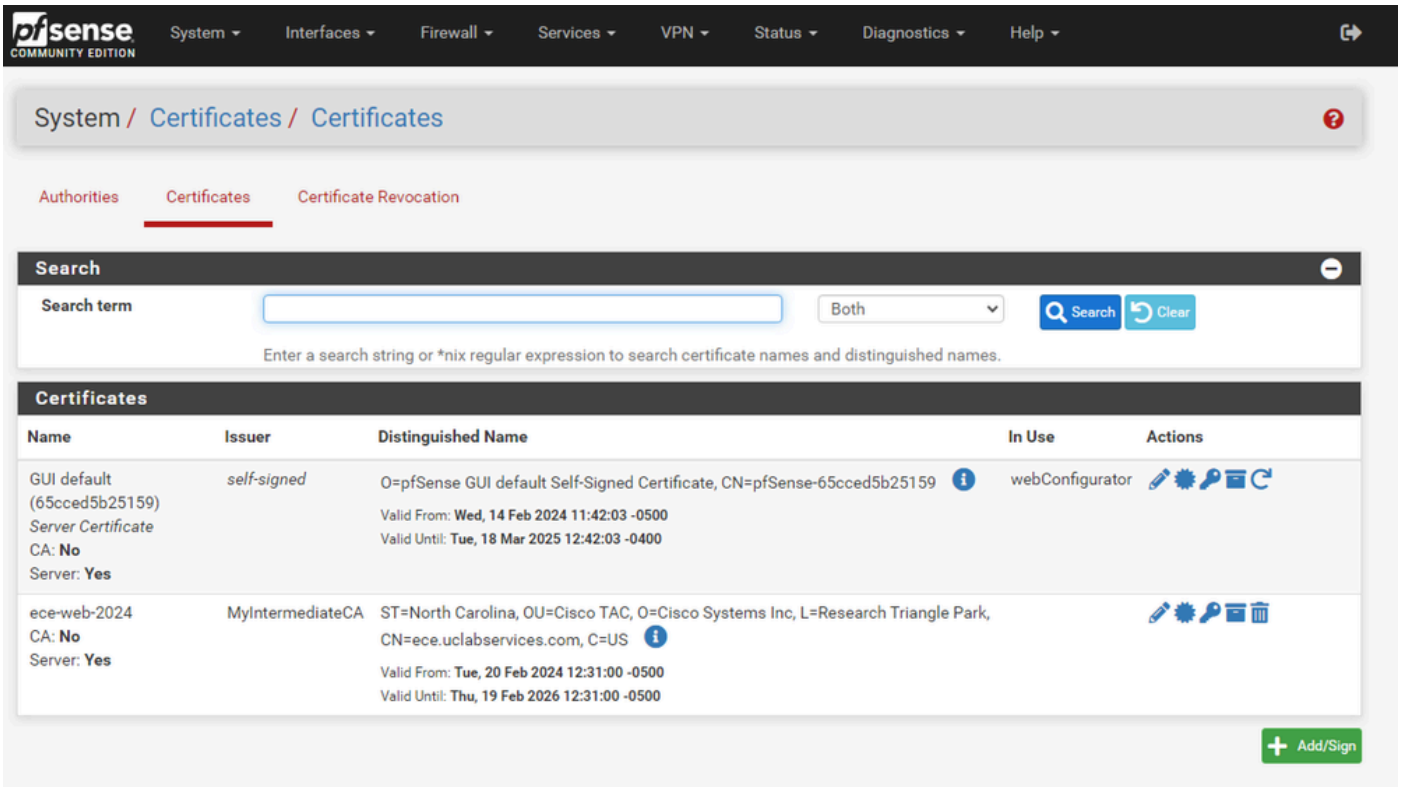
5. Cole os dados do certificado no form.



GUI do pfSense - Importação de certificado

Selecione Update para salvar o certificado.

6. Revise os dados do certificado para garantir que estejam corretos.



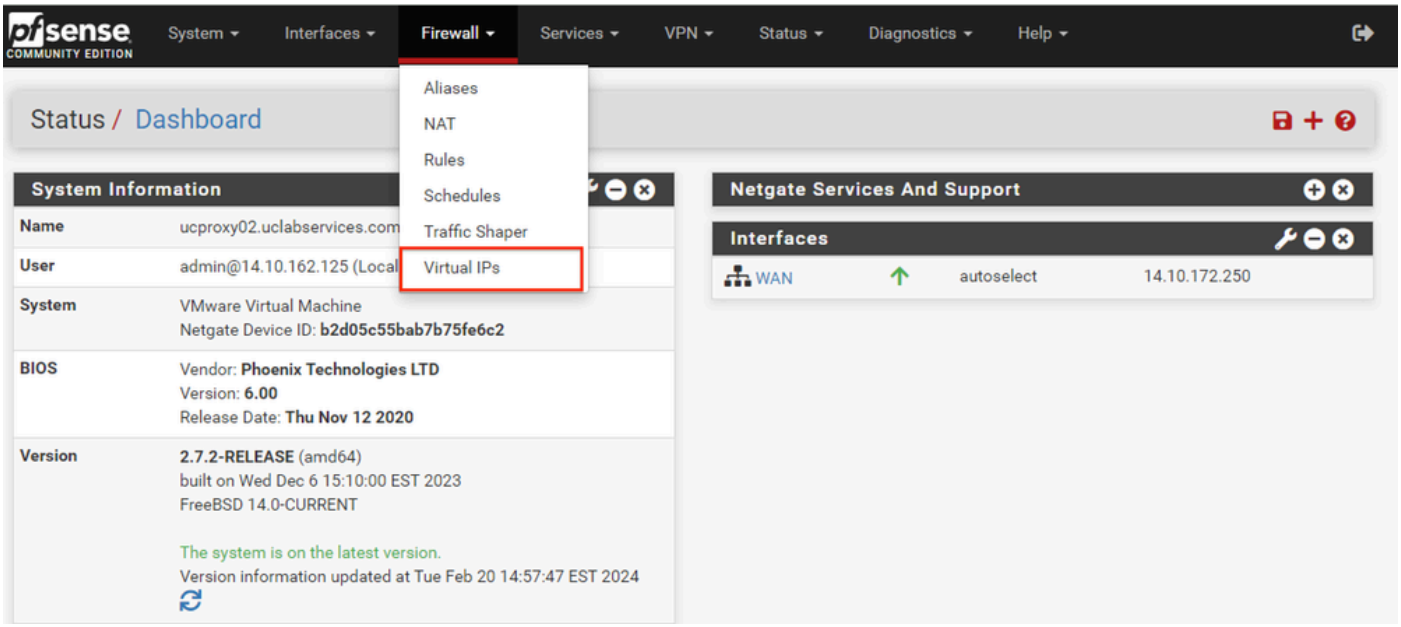
GUI pfSense - Lista de certificados

7. Repita esse processo se desejar hospedar vários sites neste pfSense.

Adicionar IPs Virtuais

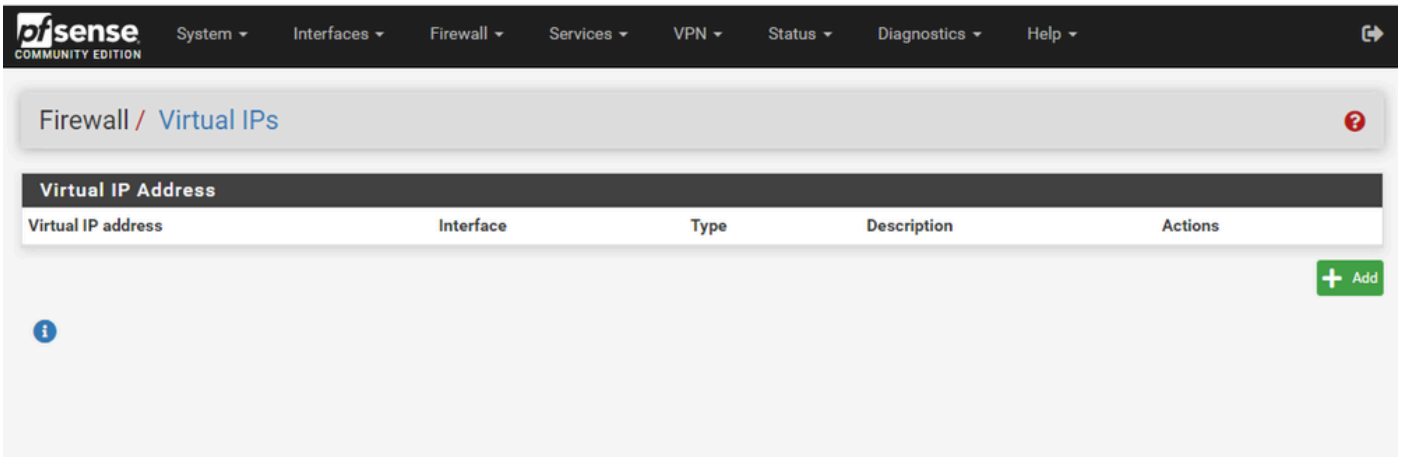
Pelo menos um IP é necessário para hospedar sites no pfSense. No pfSense, isso é feito com VIPs (IPs Virtuais).

Etapa 1. Selecione IPs virtuais no menu suspenso Firewall



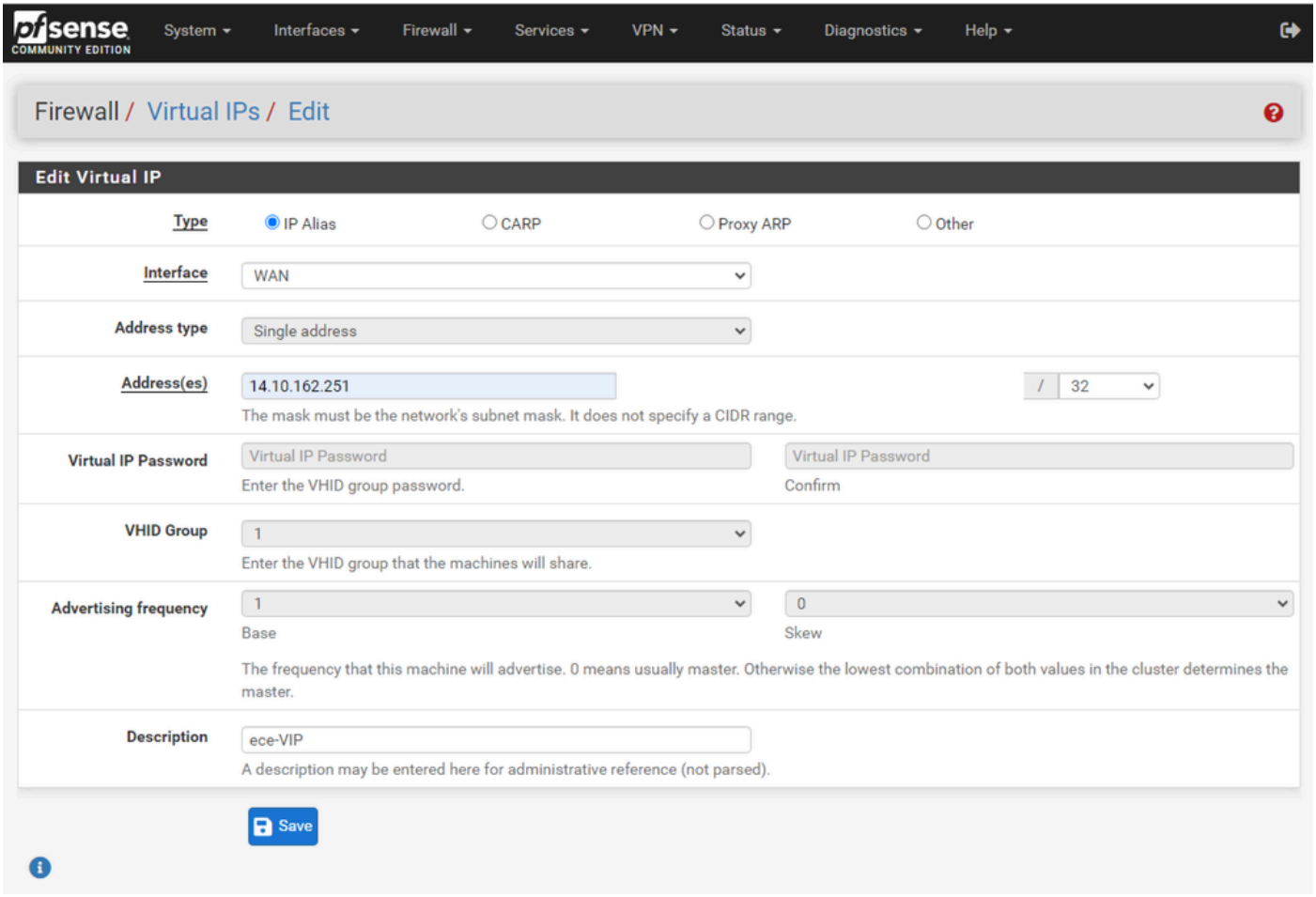
GUI pfSense - Menu suspenso VIP

Etapa 2. Selecione o botão Adicionar



GUI pfSense - Página inicial do VIP

Etapa 3. Fornecer informações de endereço



GUI pfSense - Configuração VIP

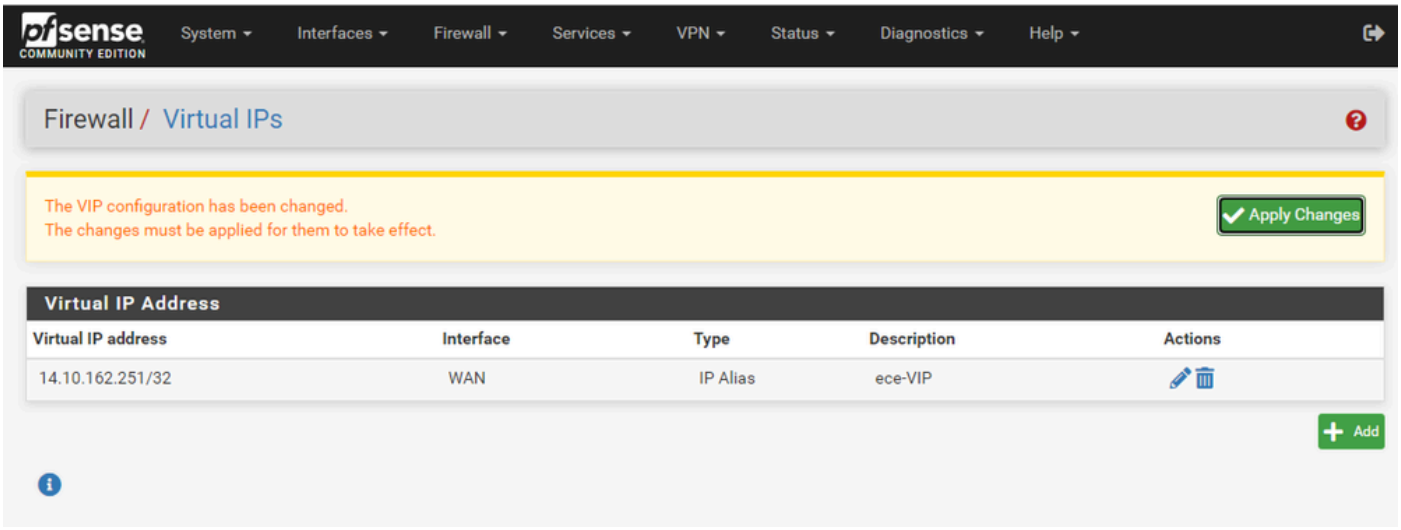
Use as informações para adicionar um VIP.

- Tipo: Selecionar Apelido de IP
- Interface: selecione a interface para este endereço IP ser transmitido
- Endereço(s): insira o endereço IP
- Máscara de endereço: para endereços IP usados para balanceamento de carga, a máscara deve ser /32
- Descrição: forneça um texto curto para facilitar a compreensão da configuração posteriormente

Selecione Save para confirmar a alteração.

Repita esse procedimento para cada endereço IP necessário para a sua configuração.

Etapa 4. Aplicar configuração



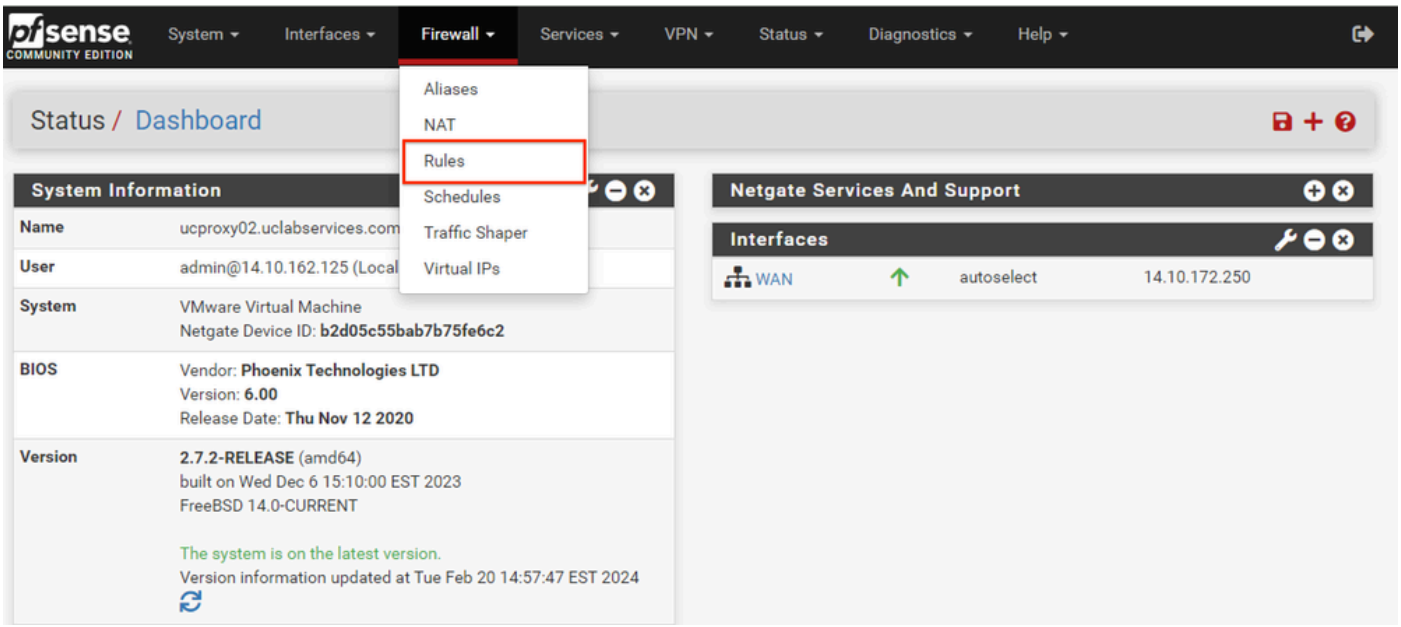
GUI pfSense - Lista VIP

Selecione o botão Apply Changes depois que todos os VIPs tiverem sido adicionados.

Configurar firewall

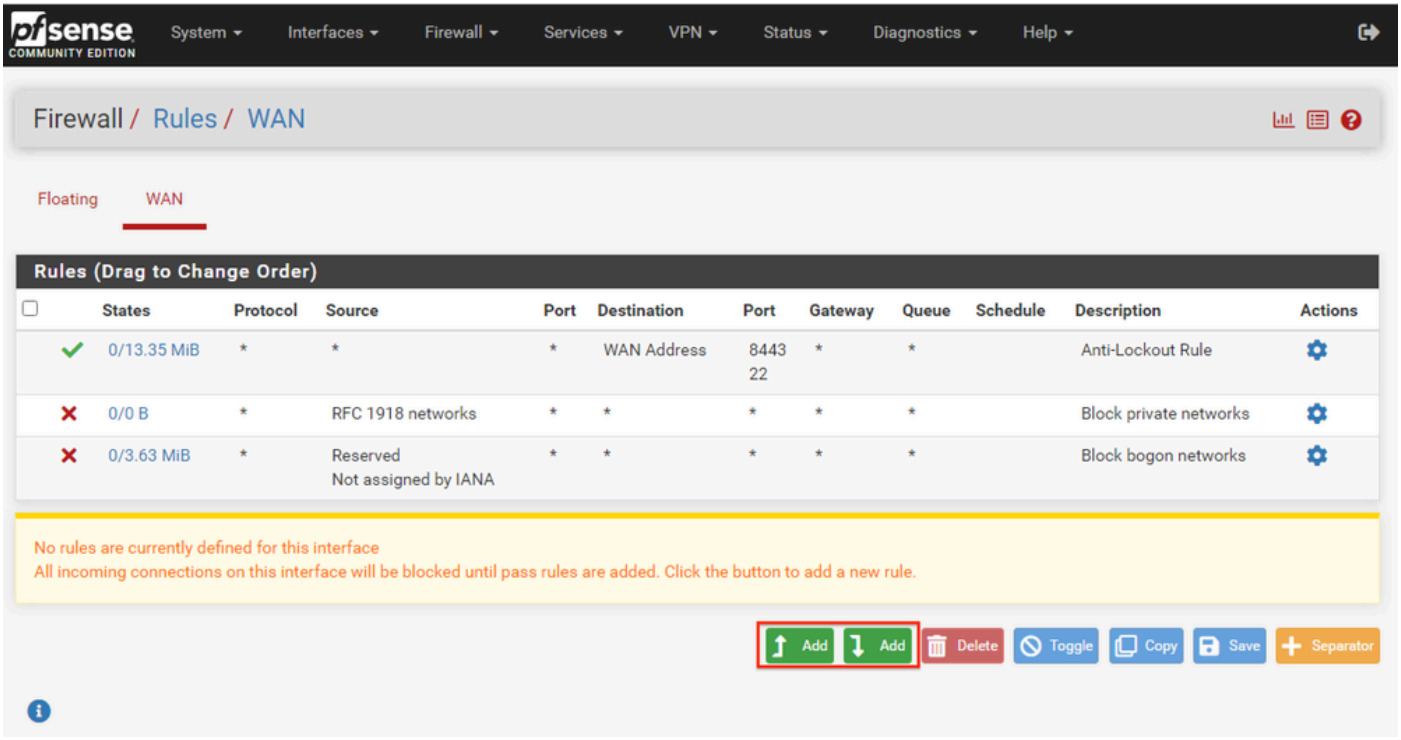
o pfSense tem um firewall integrado. O conjunto de regras padrão é muito limitado. Antes de colocar o dispositivo em produção, certifique-se de criar uma política de firewall abrangente.

Etapa 1. Selecione Regras na lista suspensa Firewall



GUI pfSense - Lista suspensa de regras de firewall

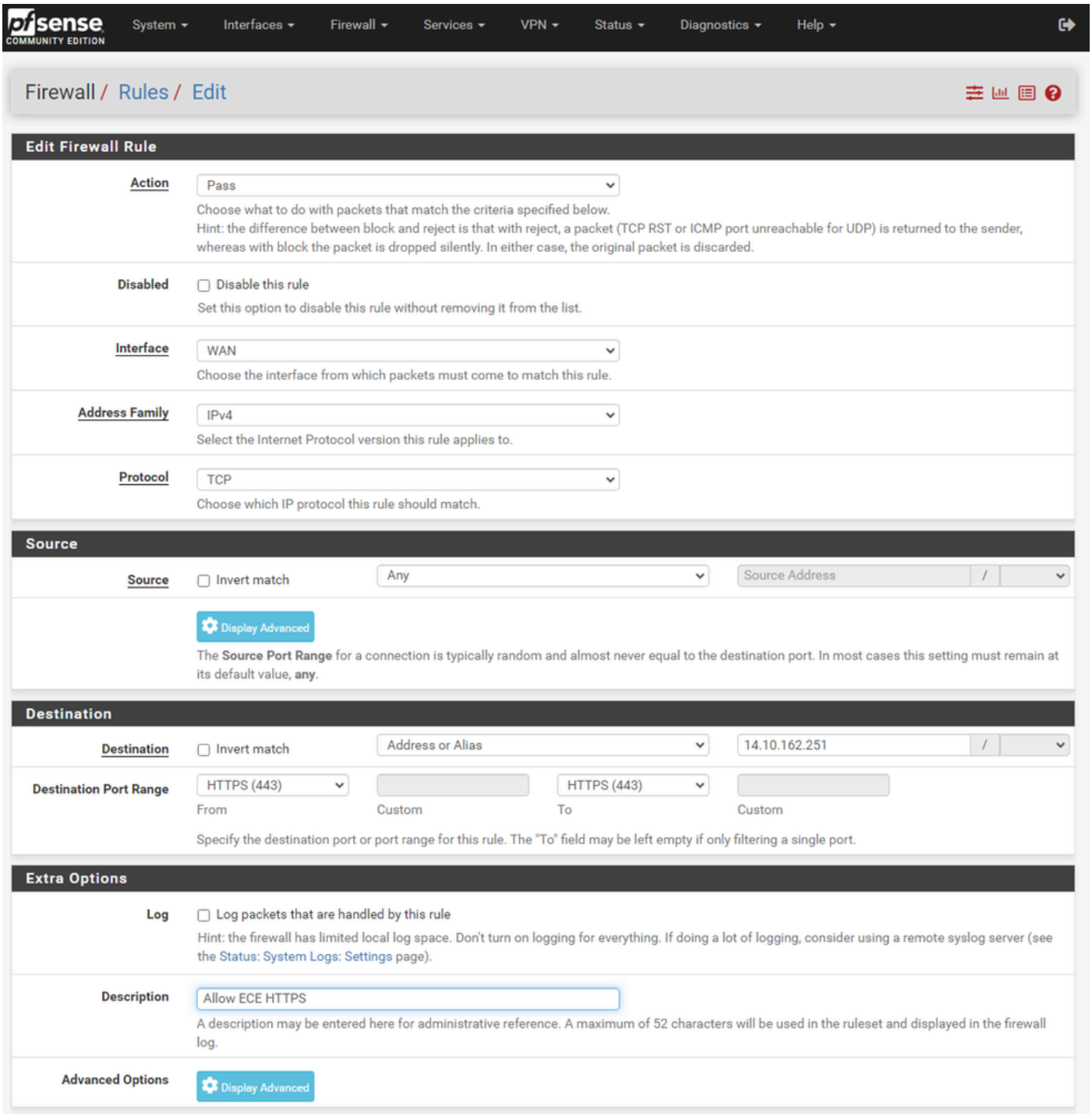
Etapa 2. Selecione um dos botões Adicionar



GUI pfSense - Lista de regras de firewall

Observe que um botão adiciona a nova regra acima da linha selecionada, enquanto o outro adiciona a regra abaixo da regra selecionada. Qualquer botão pode ser usado para a primeira regra.

Etapa 3. Crie uma regra de firewall para permitir o tráfego para o endereço IP na porta 443



GUI pfSense - Configuração da regra de passagem de firewall

Use as informações para criar a regra.

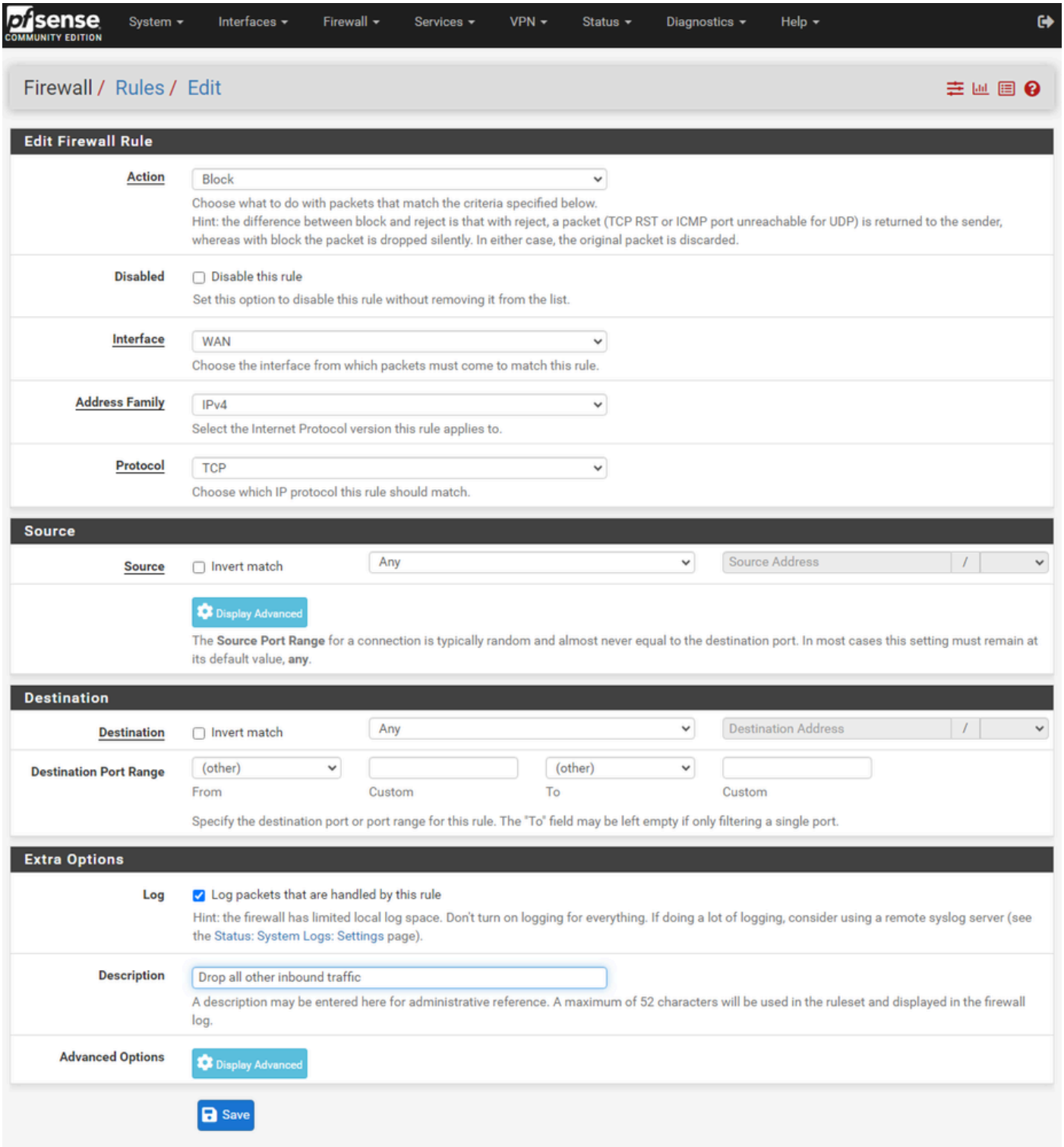
- Ação: Selecionar Aprovação
- Interface: Escolha a Interface à qual a regra se aplica
- Família de endereços e protocolo: selecione conforme apropriado
- Origem: Deixar selecionado como Qualquer
- Destino: Selecione Endereço ou Apelido na lista suspensa Destino e, em seguida, informe o endereço IP ao qual a regra se aplica
- Intervalo de portas de destino: Selecione HTTPS (443) nas listas suspensas De e Até
- Log: Marque a caixa de seleção para registrar todos os pacotes que corresponderem a esta regra para contabilização

- Descrição: forneça o texto para fazer referência à regra posteriormente

Selecione Save.

Etapa 4. Crie uma regra de firewall para descartar todo o tráfego restante no pfSense

Selecione o botão Adicionar para inserir a regra abaixo da regra recém-criada.



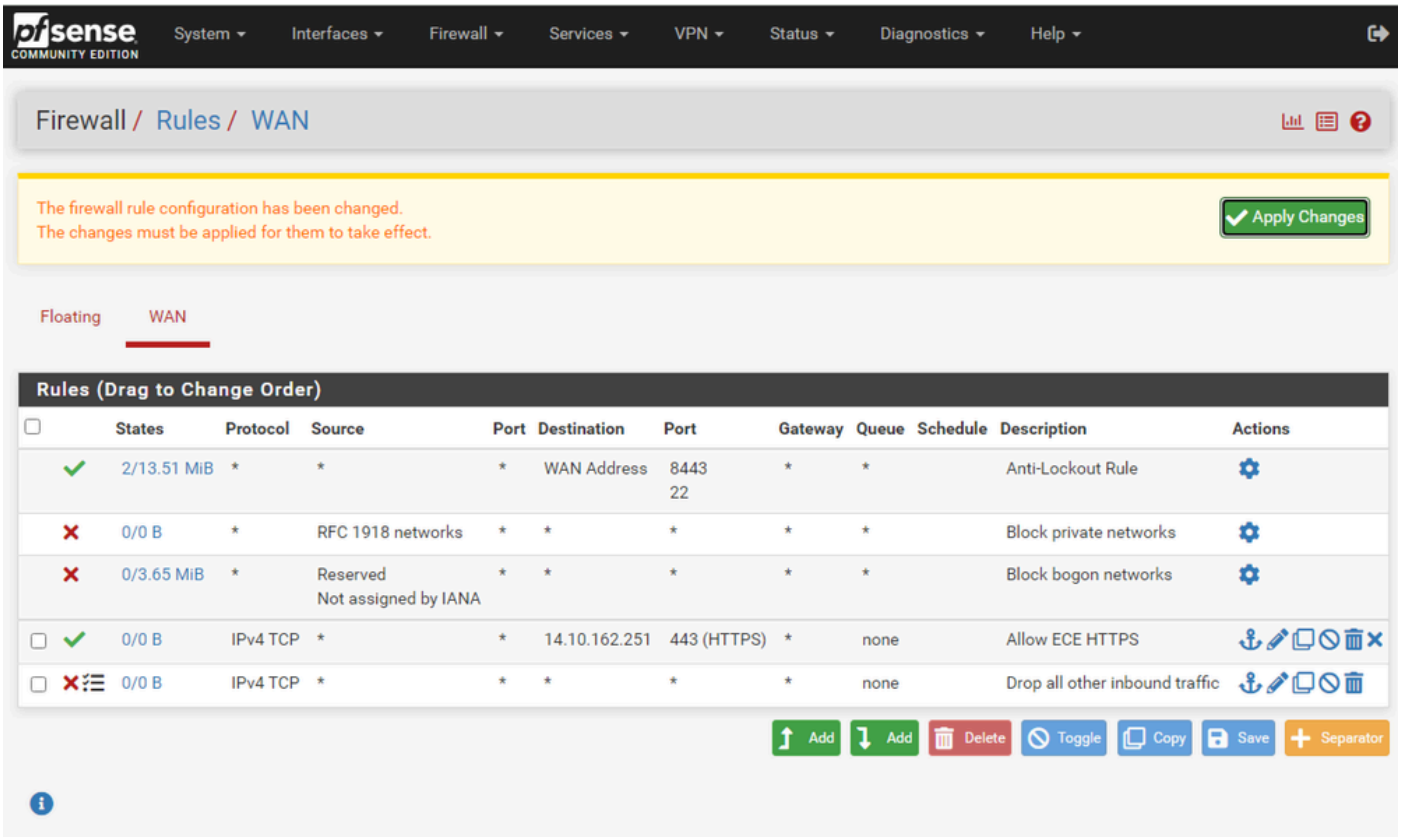
GUI pfSense - Configuração de regra de queda de firewall

- Ação: Selecionar Bloco

- Interface: Escolha a Interface à qual a regra se aplica
- Família de endereços e protocolo: selecione conforme apropriado
- Origem: Deixar selecionado como Qualquer
- Destino: deixe selecionado como Qualquer
- Log: Marque a caixa de seleção para registrar todos os pacotes que corresponderem a esta regra para contabilização
- Descrição: forneça o texto para fazer referência à regra posteriormente

Selecione Save.

Etapa 5. Revise as regras e verifique se a regra de bloqueio está na parte inferior



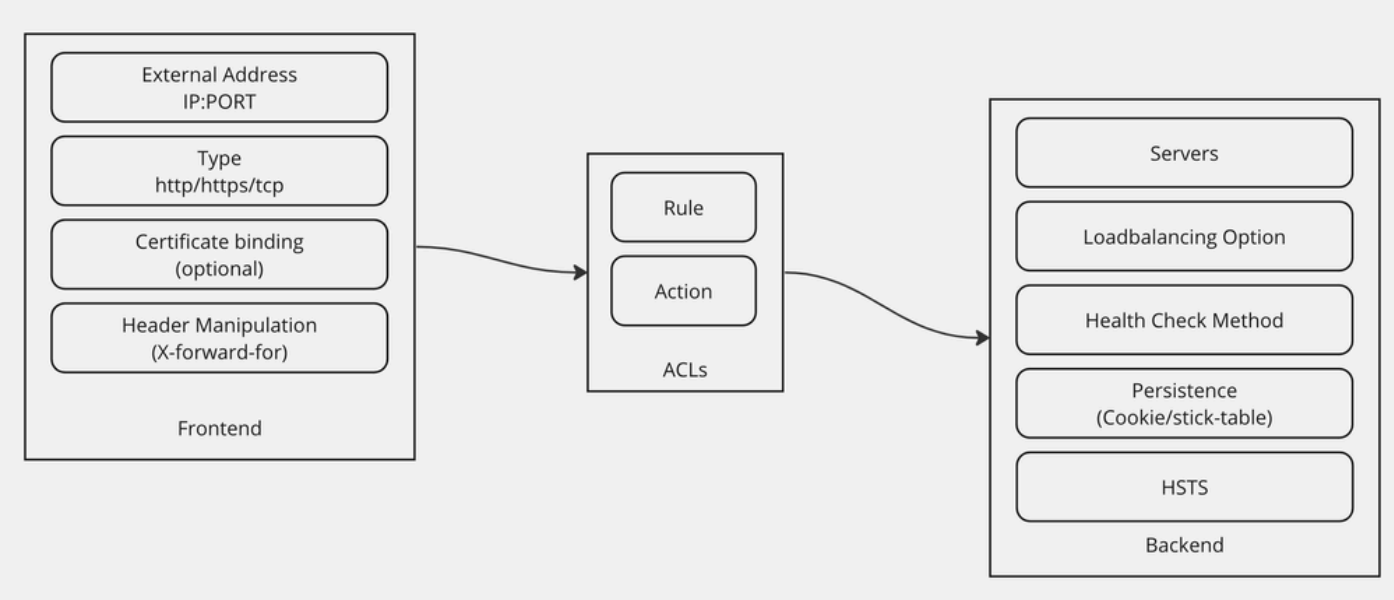
GUI pfSense - Lista de regras de firewall

Se necessário, arraste as regras para classificá-las.

Selecione Aplicar alterações quando as regras de firewall estiverem na ordem necessária para o seu ambiente.

Configurar HAProxy

Conceitos do HAProxy



Conceitos do HAProxy

O HAProxy é implementado com um modelo de front-end/back-end.

O Front-end define o lado do proxy com o qual os clientes se comunicam.

O Front-end consiste em uma combinação de IP e Porta, vinculação de certificado e pode implementar alguma manipulação de cabeçalho.

A infraestrutura define o lado do proxy que se comunica com os servidores Web físicos.

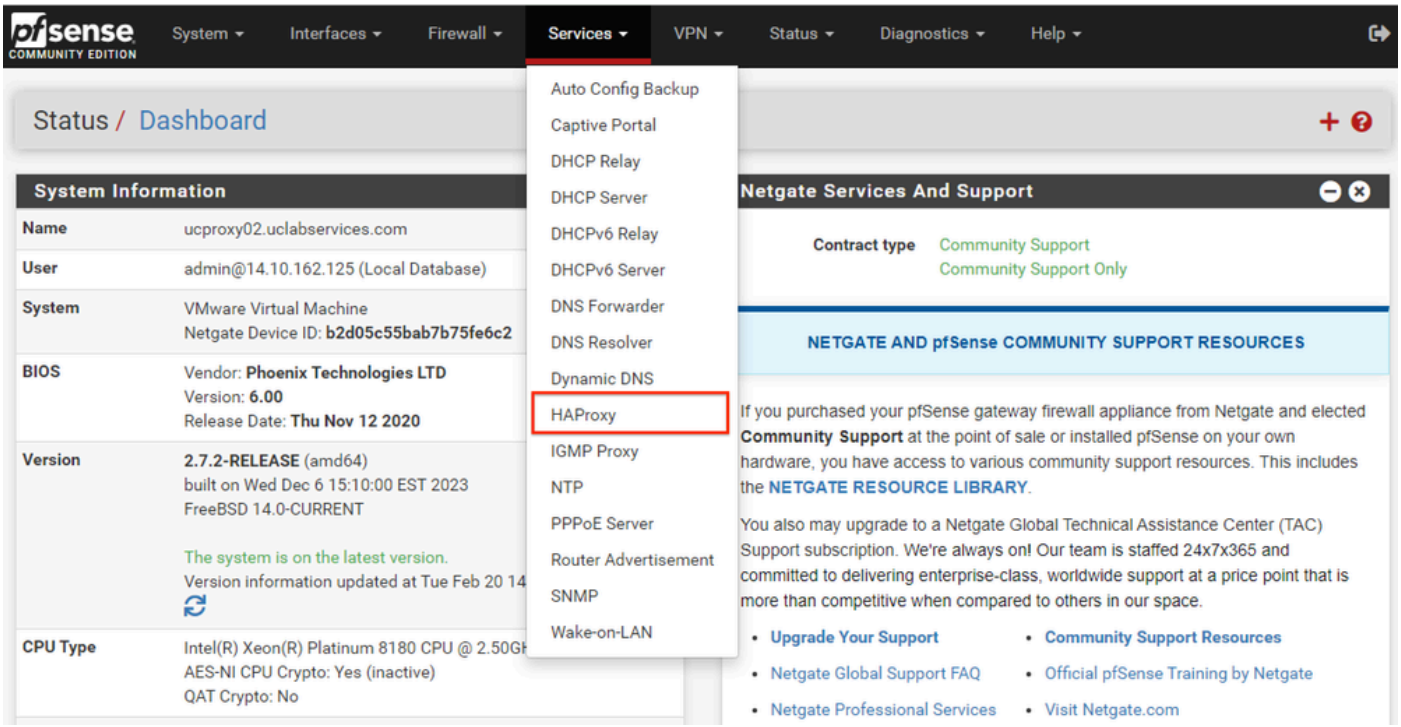
O back-end define os servidores e portas reais, o método de balanceamento de carga para atribuição inicial, verificações de integridade e persistência.

Um front-end sabe com qual back-end se comunicar usando um back-end dedicado ou ACLs.

As ACLs podem criar regras diferentes para que um determinado front-end possa se comunicar com backends diferentes, dependendo de várias coisas.

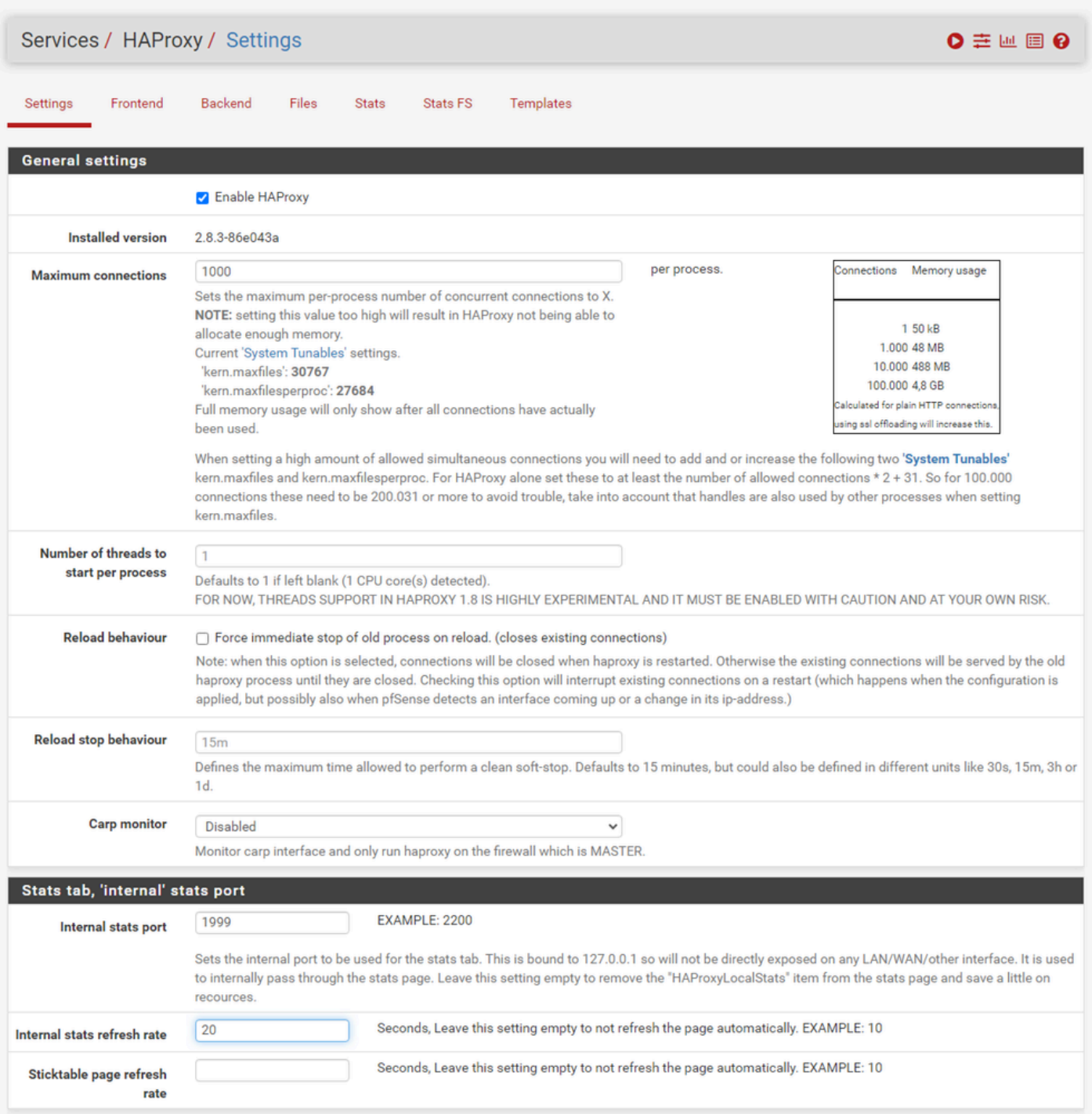
Configurações iniciais do HAProxy

Etapa 1. Selecione HAProxy no menu suspenso Serviços



GUI pfSense - menu suspenso HAProxy

Etapa 2. Definir configurações básicas



GUI pfSense - Configurações principais do HAProxy

Marque a caixa de seleção Habilitar HAProxy.

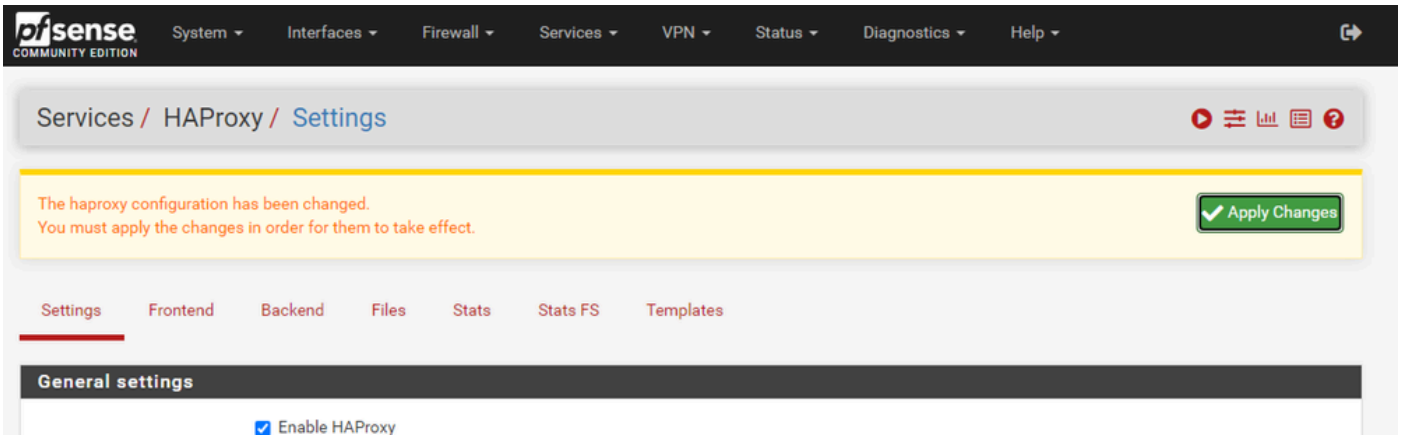
Digite um valor para Máximo de conexões. Consulte o gráfico nesta seção para obter detalhes sobre a memória necessária.

Insira um valor para a porta de estatísticas internas. Essa porta é usada para mostrar estatísticas de HAProxy no equipamento, mas não é exposta fora do equipamento.

Informe um valor para a taxa de atualização de estatísticas Internas.

Revise a configuração restante e atualize-a conforme necessário para o seu ambiente.

Selecione Salvar.

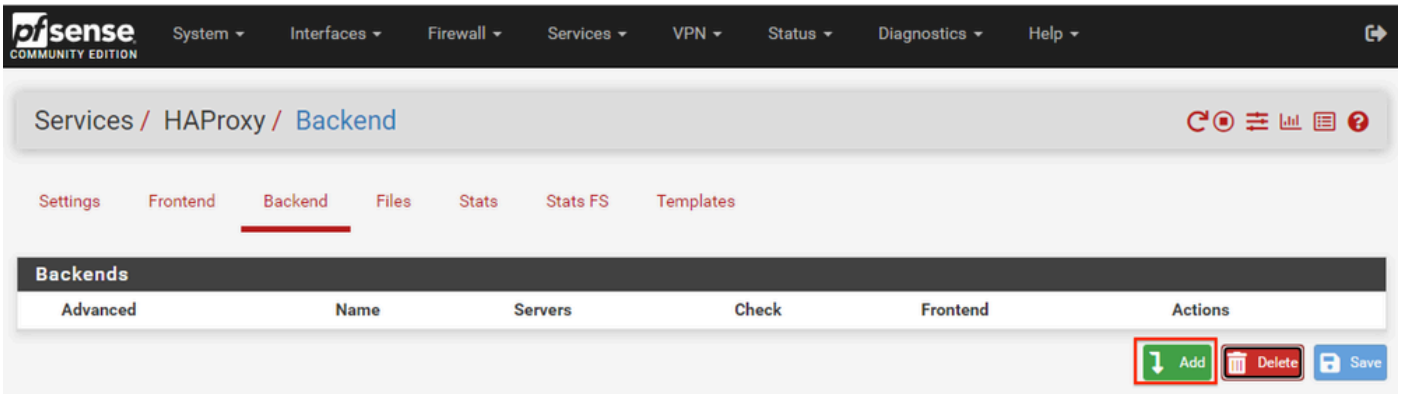


GUI pfSense - HAProxy Aplicar alterações

Observação: as alterações de configuração não são ativadas até que você selecione o botão Aplicar alterações. Você pode fazer várias alterações de configuração e aplicá-las todas de uma vez. A configuração não precisa ser aplicada para ser usada em outra seção.

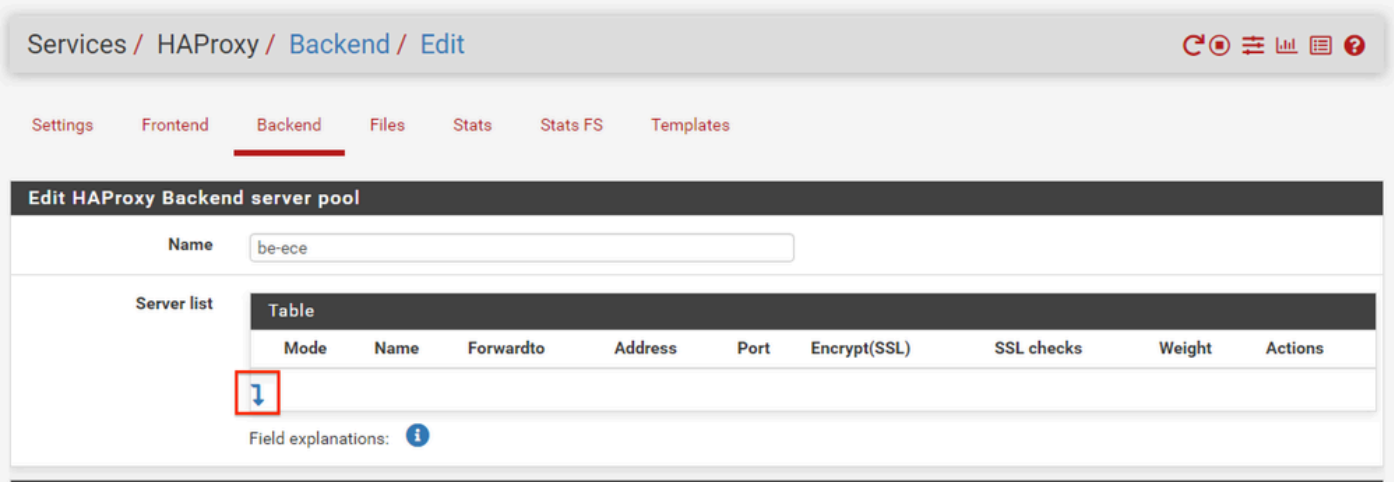
Configurar o back-end do HAProxy

Comece com a infraestrutura. A razão para isso é que o front-end deve referenciar um back-end. Verifique se você selecionou o menu Back-end.



GUI pfSense - HAProxy Adicionar Back-end

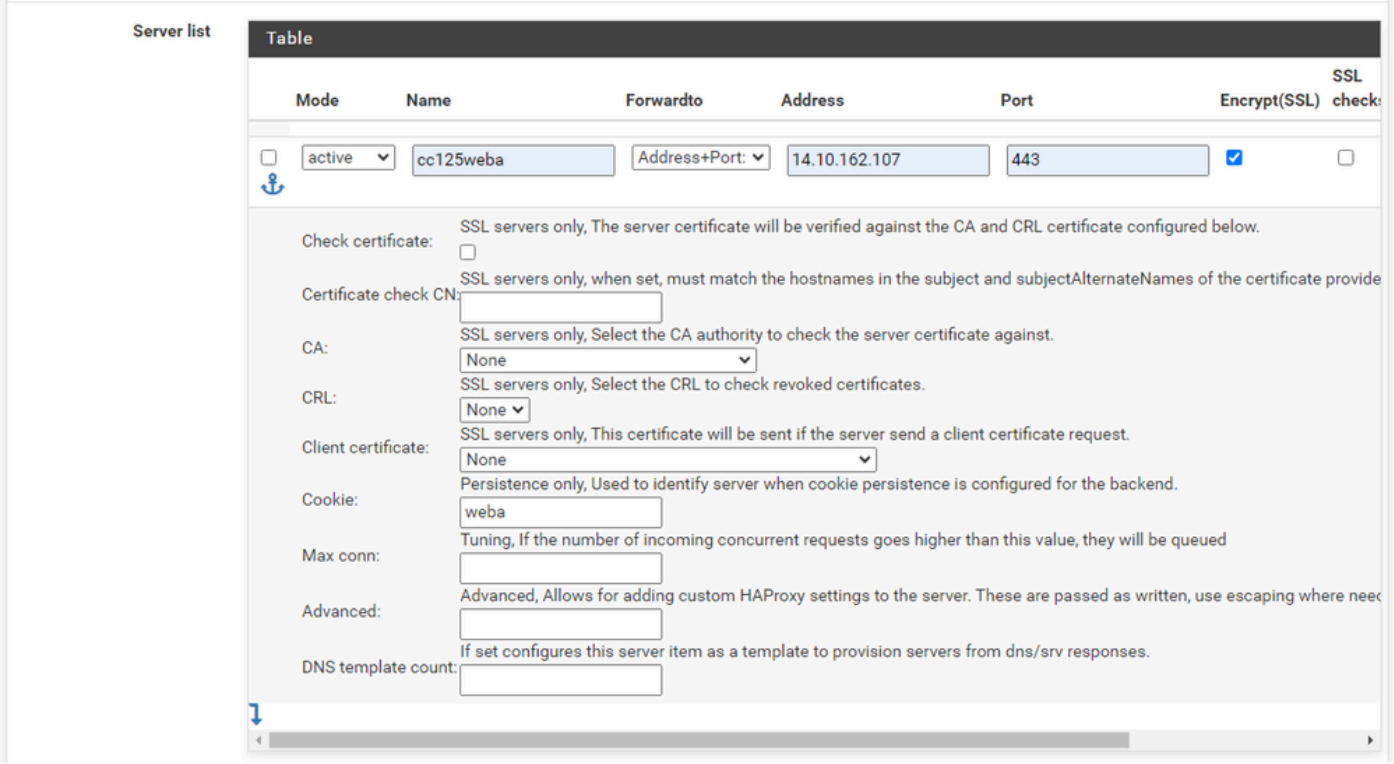
Selecione o botão Add.



GUI pfSense - Início do back-end do HAProxy

Forneça um nome para o back-end.

Selecione a seta para baixo para adicionar o primeiro servidor à lista de servidores



Infraestrutura - Lista de servidores

Forneça um nome para referenciar o servidor. Isso não precisa corresponder ao nome real do servidor. Este é o nome que é mostrado na página de estatísticas.

Forneça o endereço do servidor. Isso pode ser configurado como um Endereço IP para FQDN.

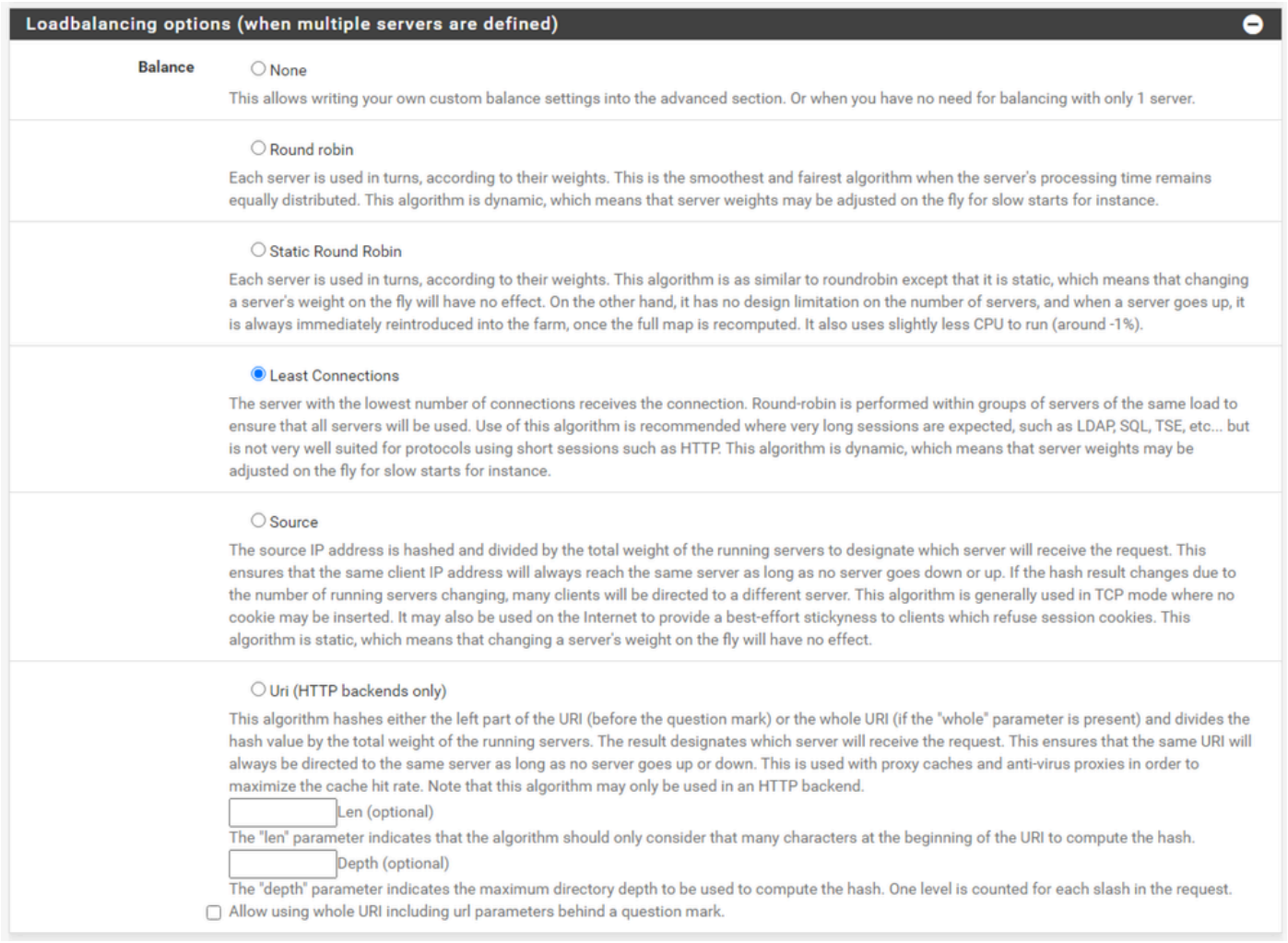
Forneça a porta à qual se conectar. Esta deve ser a porta 443 para ECE.

Marque a caixa de seleção Criptografar(SSL).

Forneça um valor no campo Cookie. Este é o conteúdo do cookie de fidelidade da sessão e deve

ser exclusivo dentro do back-end.

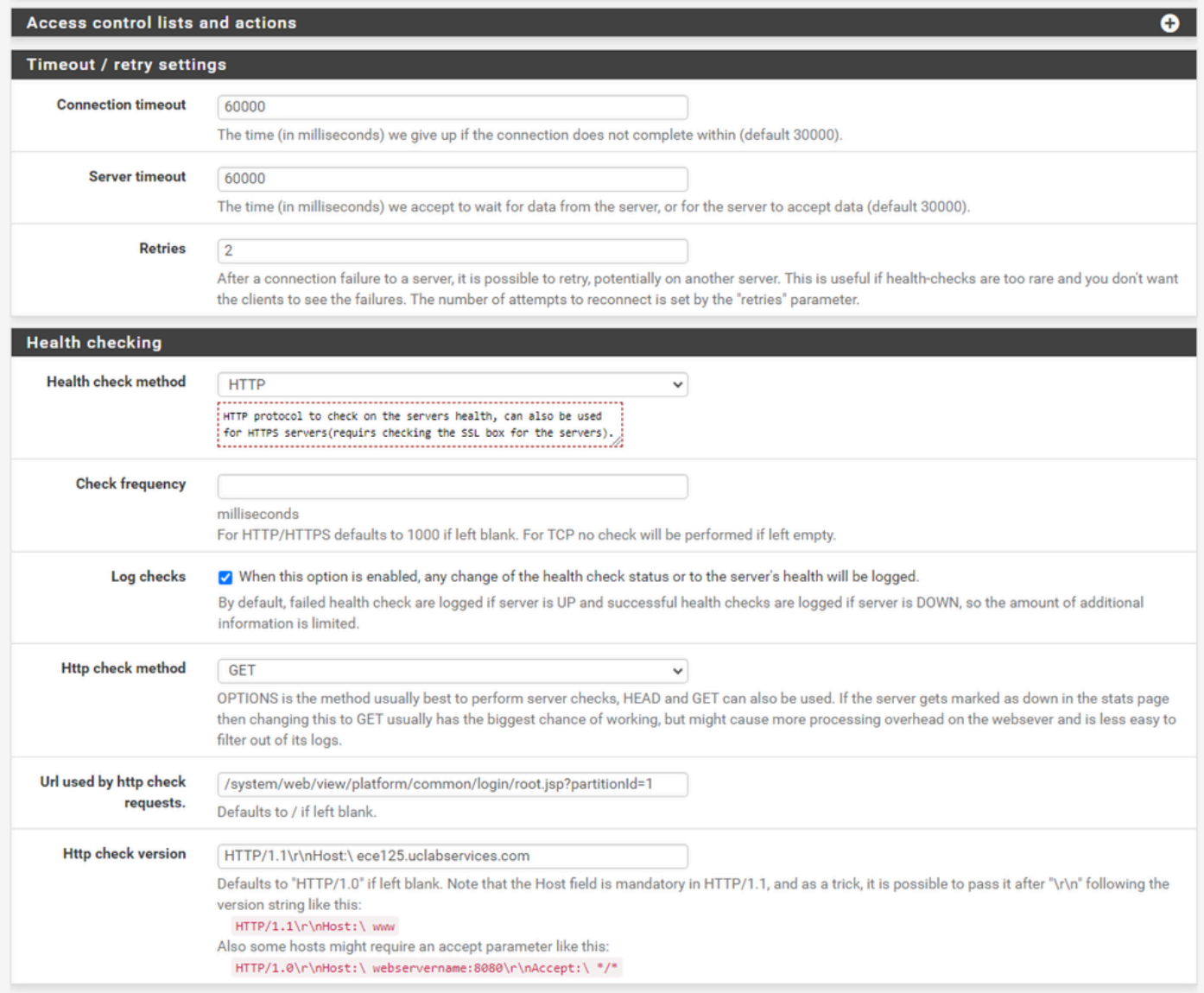
Depois que o primeiro servidor tiver sido configurado, selecione a seta para baixo para configurar quaisquer outros servidores Web no ambiente.



Infraestrutura HAProxy - Balanceamento de carga

Configure as opções de Balanceamento de carga.

Para servidores ECE, deve ser definido como Conexões Mínimas.



Infraestrutura HAProxy - Verificação de integridade

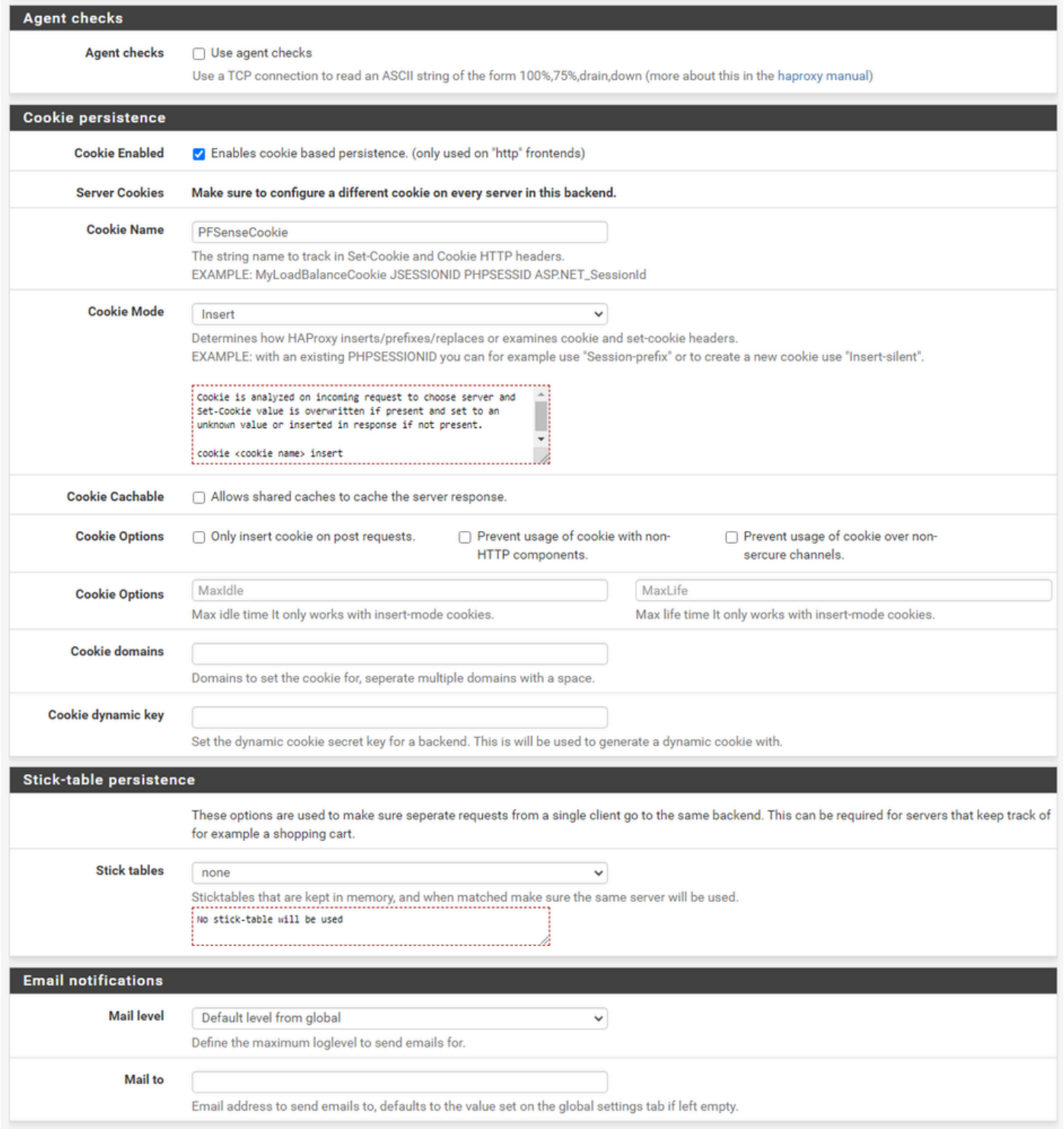
As listas de controle de acesso não são usadas nesta configuração.

As configurações de tempo limite/repetição podem ser deixadas com a configuração padrão.

Configurar a seção Verificação de integridade.

1. Método de verificação de integridade: HTTP
2. Verificar frequência: deixe em branco para usar o padrão a cada 1 segundo.
3. Verificações de log: Selecione esta opção para gravar quaisquer alterações de integridade nos logs.
4. Método de verificação HTTP: selecione GET na lista.
5. Url usada pelas solicitações de verificação http.: Para um servidor ECE, digite /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Versão de verificação HTTP: Enter, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

Certifique-se de incluir um espaço após a barra invertida final, mas antes do FQDN do servidor.

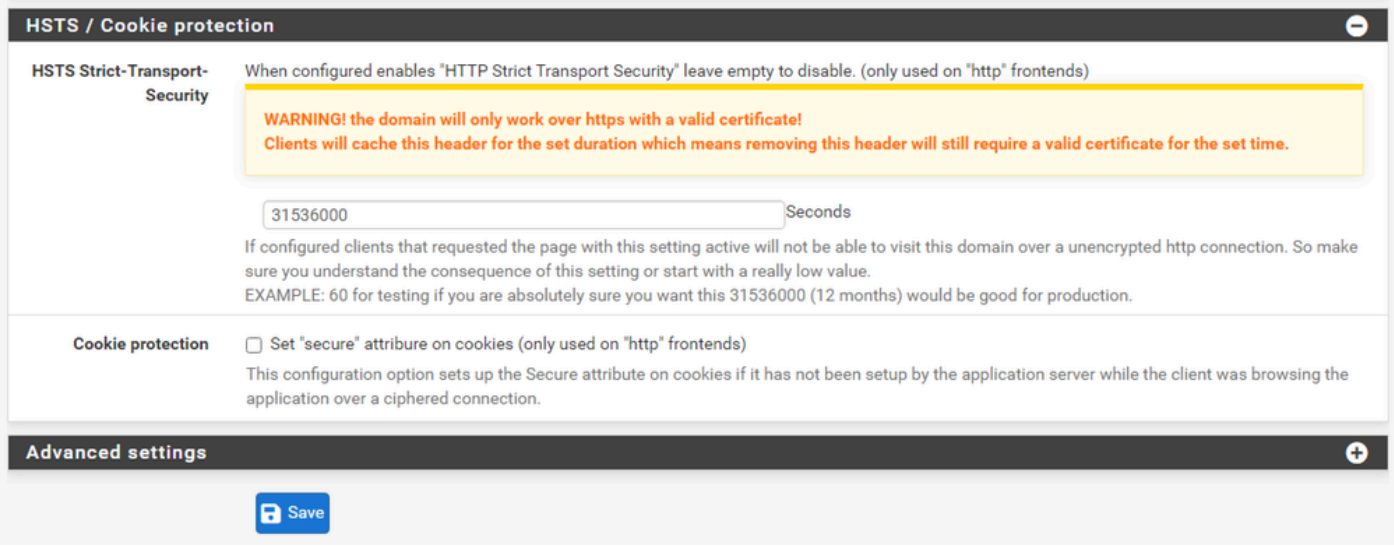


Infraestrutura HAProxy - Persistência de Cookies

Deixe as verificações do Agente desmarcadas.

Configurar a persistência do cookie:

1. Cookie ativado: selecione para ativar a persistência baseada em cookie.
2. Nome do cookie: forneça um nome para o cookie.
3. Modo Cookie: Selecione Inserir na caixa suspensa.
4. Deixe as opções restantes desmarcadas.



Infraestrutura HAProxy - HSTS

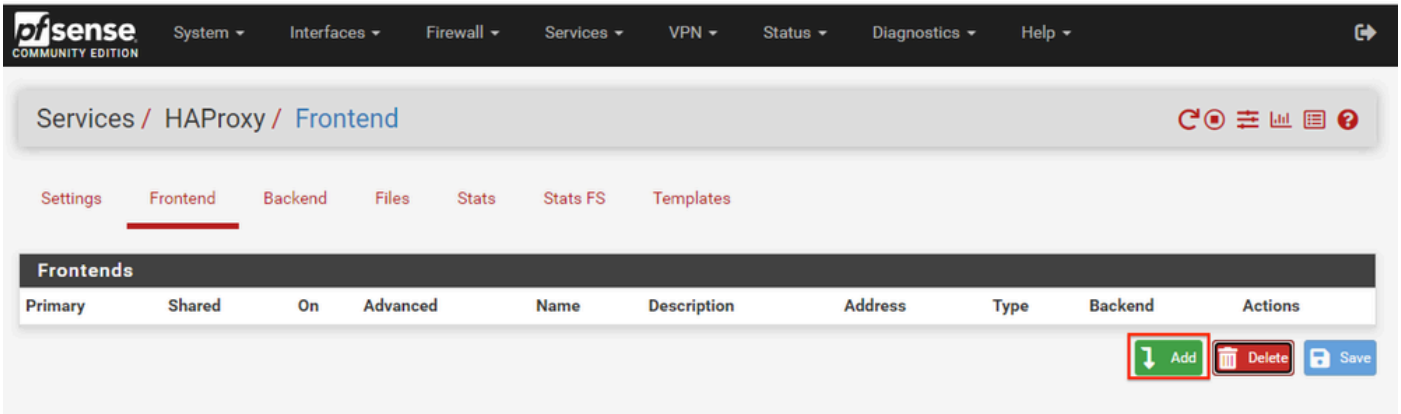
As seções restantes do formulário de configuração da infraestrutura podem ser deixadas com as suas configurações padrão.

Se desejar configurar o HSTS, configure um valor de tempo limite nesta seção. O ECE também insere um cookie HSTS para que essa configuração seja redundante.

Selecione Salvar.

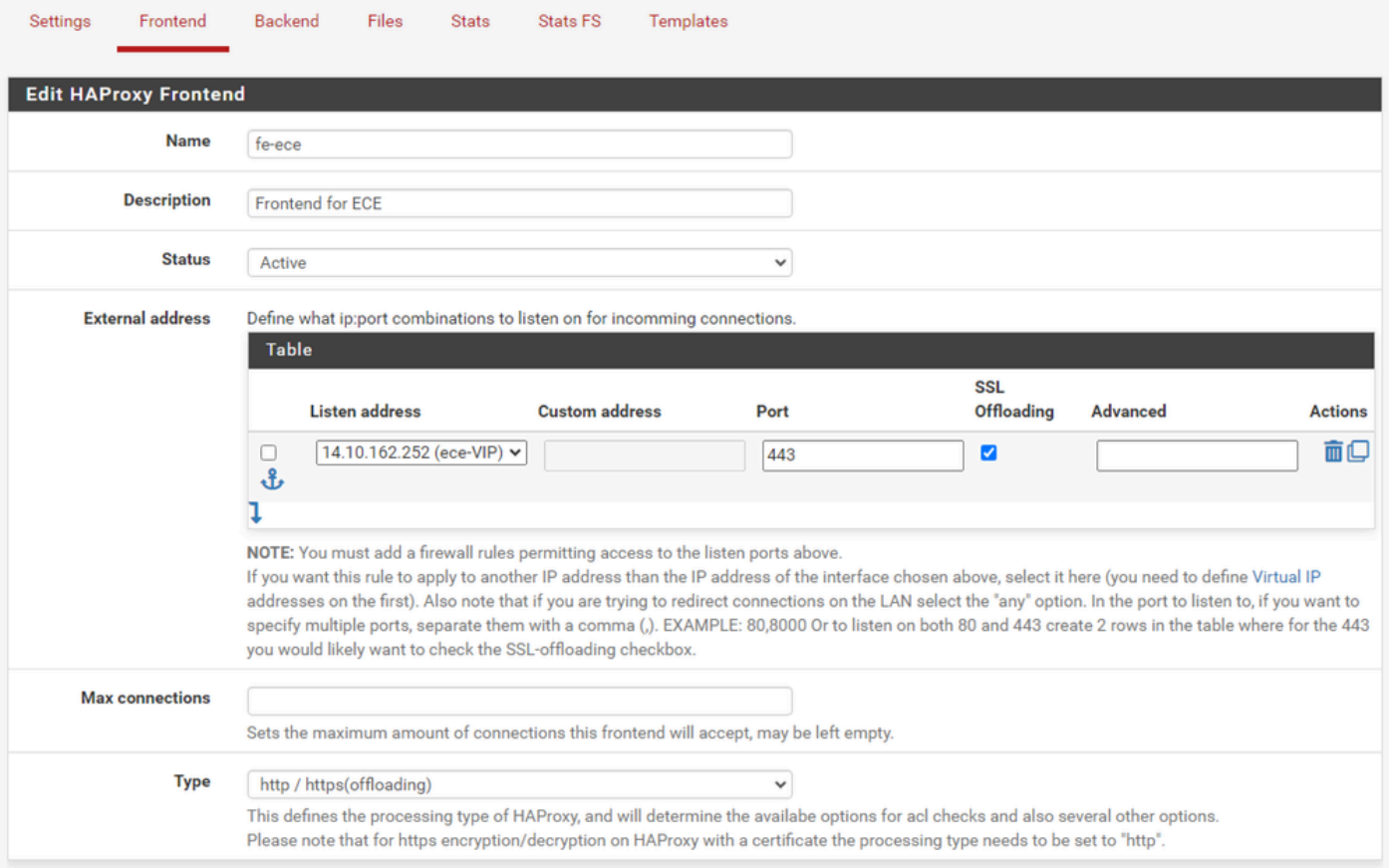
Configurar front-end do HAProxy

Mude para o menu de Interface.



GUI pfSense - HAProxy Adicionar front-end

Selecione o botão Adicionar,



HAProxy - Cabeçalho de front-end

Forneça um nome para o Front-end.

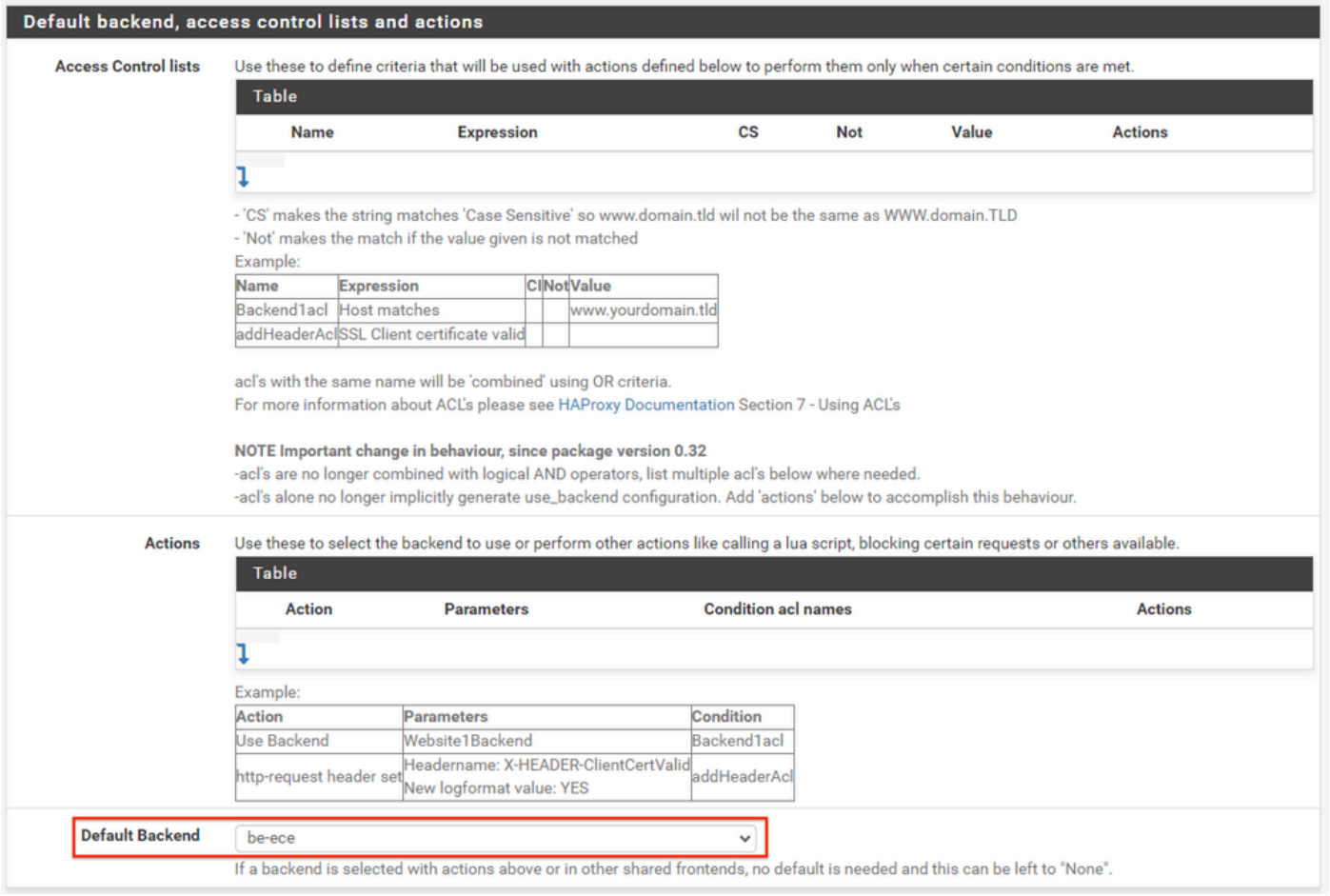
Forneça uma descrição para ajudar a identificar o front-end posteriormente.

Na tabela Endereço externo:

1. Endereço de escuta: Selecione o VIP que você criou para este site.
2. Porta: Digite 443.
3. Descarregamento de SSL: Selecione esta opção para que um cookie de sessão possa ser inserido.

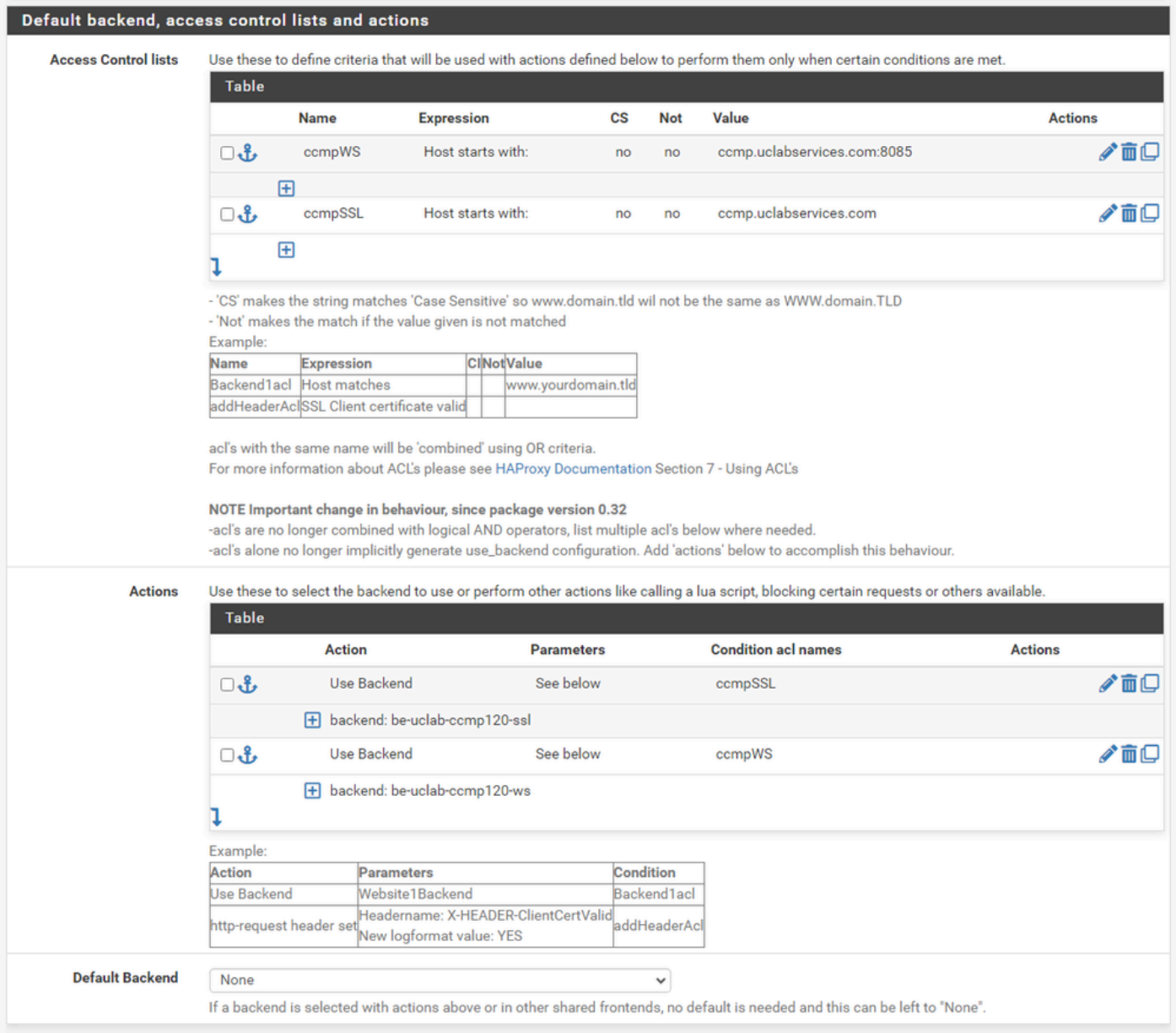
Deixe o Máximo de conexões em branco.

Verifique se o Tipo está selecionado como http / https(offloading).



Infraestrutura HAProxy - Seleção padrão da infraestrutura

A configuração mais fácil é escolher um back-end padrão no menu suspenso. Isso pode ser selecionado quando o VIP hospeda um único site.

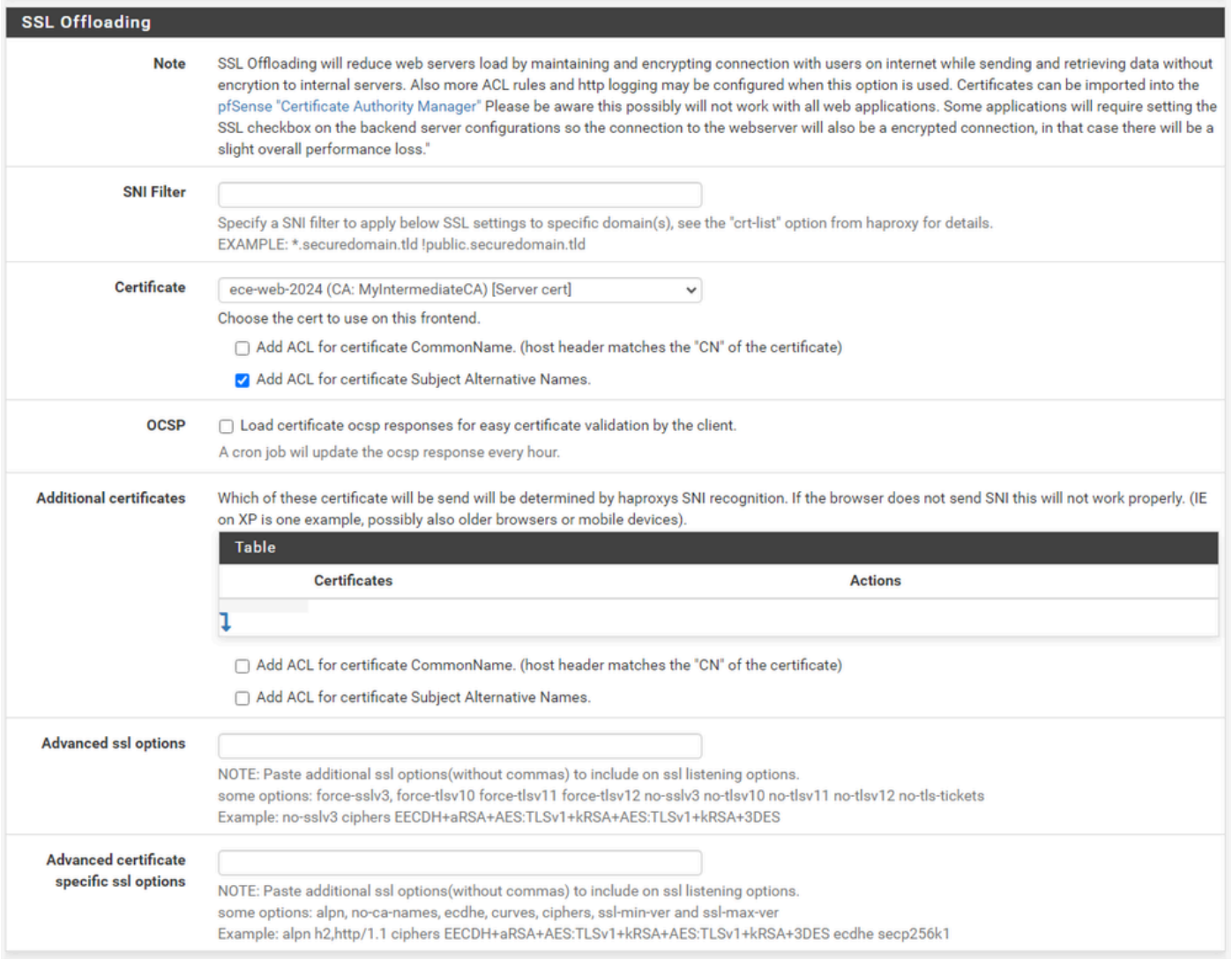


Infraestrutura HAProxy - ACL Avançada

Como mostrado na imagem, as ACLs podem ser usadas para redirecionar um único front-end para vários back-ends com base nas condições.

Você pode ver que a ACL verifica se o host na solicitação começa com um nome e um número de porta ou simplesmente o nome. Com base nisso, uma infraestrutura específica é usada.

Isso não é comum com ECE.



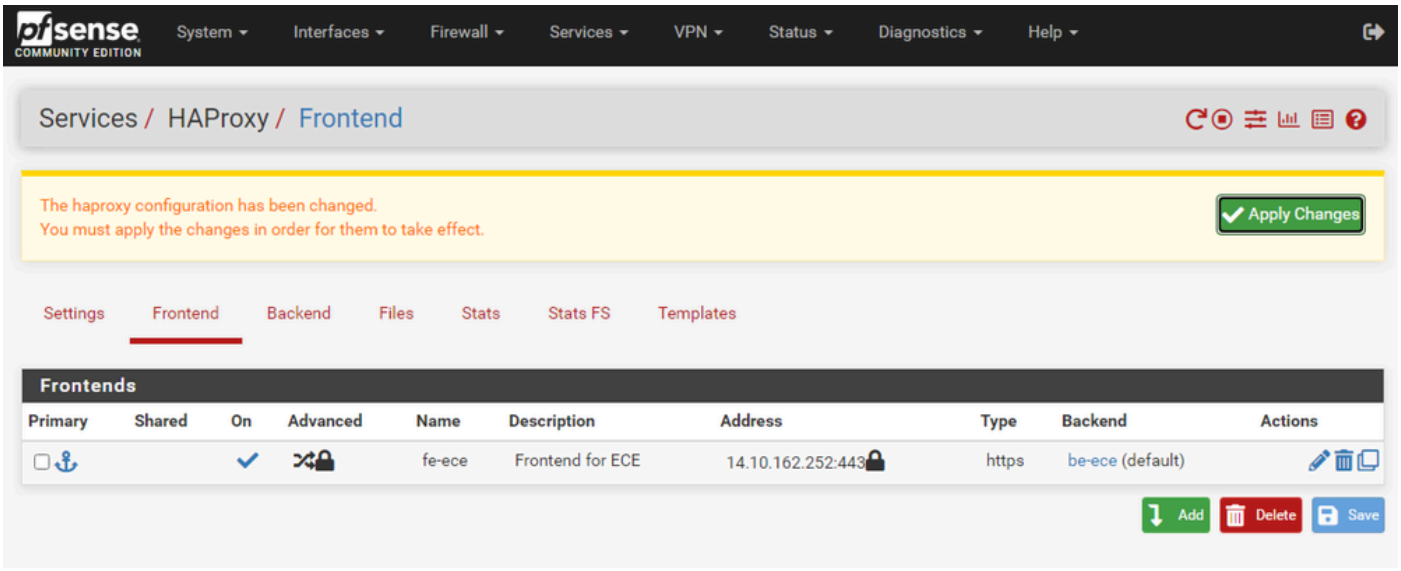
Interface HAProxy - Associação de certificado

Na seção Descarregamento de SSL, selecione o certificado criado para uso com este site. Este certificado deve ser um certificado de servidor.

Selecione a opção Add ACL para o certificado Subject Alternative Names.

Você pode deixar as opções restantes com seus valores padrão.

Selecione Salvar no final deste formulário.



HAProxy - Aplicar configuração

Selecione Apply Changes para confirmar as alterações de front-end e back-end na configuração atual.

Parabéns, você concluiu a instalação e a configuração do pfSense.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.