为ECE配置pfSense社区负载均衡器

目录

简介

先决条件

- 要求
- 使用的组件

安装pfSense

- 解决方案概述
- 准备
- 安装
- 网络设置
- 完成初始设置
- 配置基本管理员设置
- 添加所需的包
- 配置证书
- 添加虚拟IP
- 配置防火墙

配置HAProxy

- HAProxy概念
- 初始DHCProxy设置
- 配置HAProxy后端
- 配置HAProxy前端

简介

本文档介绍将pfSense Community Edition设置为企业聊天和电子邮件(ECE)的负载均衡器的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- ECE 12.x
- pfSense社区版

使用的组件

本文档中的信息基于以下软件版本：

- 欧洲经委会12.6(1)

- pfSense社区版2.7.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

安装pfSense

解决方案概述

pfSense社区版是一款多功能产品，可在单个服务器中提供防火墙、负载均衡器、安全扫描程序和许多其他服务。pfSense基于免费BSD构建，具有最低的硬件要求。负载均衡器是HAProxy的实现，提供易于使用的GUI来配置产品。

您可以将此负载均衡器与ECE和联系中心管理门户(CCMP)配合使用。 本文档提供了为ECE配置pfSense的步骤。

准备

步骤1.下载pfSense软件

使用pfSense网站下载iso安装程序映像。

步骤2.配置VM

按照最低要求配置VM:

· 64位amd64(x86-64)兼容CPU

· 1GB或更多RAM

· 8 GB或更大的磁盘驱动器（SSD、HDD等）

·一个或多个兼容网络接口卡

·用于初始安装的可启动USB驱动器或大容量光驱（DVD或BD）

实验室安装只需要一个网络接口(NIC)。运行设备的方法有多种，但最简单的方法是使用单个网卡，也称为单臂模式。在单臂模式下，有一个接口与网络通信。虽然这种方法简单，且适用于实验，但它并不是最安全的方式。

配置设备的更安全的方法是至少拥有两个NIC。一个NIC是WAN接口，直接与公共互联网通信。第二个NIC是LAN接口，与内部公司网络通信。您还可以添加其他接口，以便与具有不同安全和防火墙规则的网络各个部分通信。例如，您可以让一个NIC连接到公共互联网，一个连接到DMZ网络（所有外部可访问Web服务器都位于其中），第三个网卡连接到企业网络。这样，您就可以让内部和外部用户安全地访问保留在DMZ中的同一组Web服务器。确保在实施之前了解任何设计的安全影响。与安全工程师协商，确保遵循最佳实践进行具体实施。

安装

步骤1.将ISO安装到VM

步骤2.打开VM电源并按照提示进行安装。

有关逐步说明，请参阅此文档。

网络设置

您必须为设备分配IP地址才能继续配置。

注意：本文档显示以单臂模式配置的设备。

步骤1.配置VLAN

如果您需要VLAN支持，请回答y以回答第一个问题。否则，请回答n。

步骤2.分配WAN接口

WAN接口是双臂模式下设备的非安全端，也是单臂模式下的唯一接口。出现提示时，输入接口名称。

步骤3.分配LAN接口

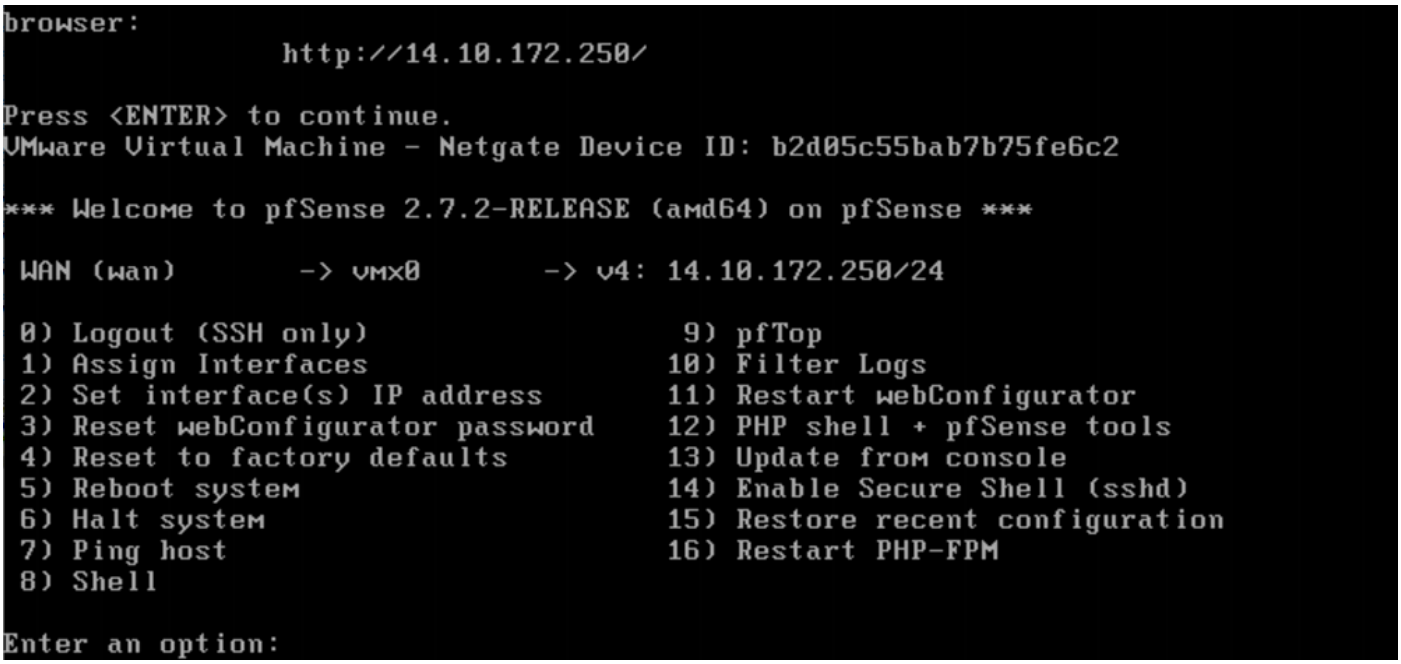
LAN接口是双臂模式下设备的安全端。如果需要，请在提示时输入接口名称。

步骤4.分配任何其他接口

配置特定安装所需的任何其他接口。这些是可选的，并不常见。

步骤5.将IP地址分配给管理接口

如果您的网络支持DHCP，则分配的IP地址将显示在控制台屏幕中。

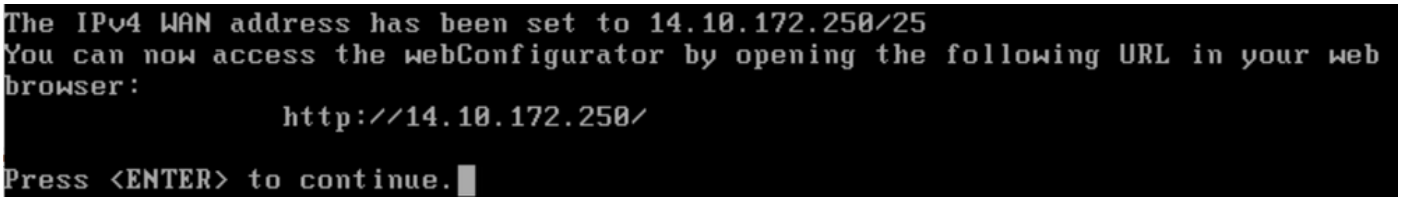


pfSense控制台

如果没有分配地址，或者如果您希望分配特定地址，请执行以下步骤。

1. 从控制台菜单中选择选项2。
2. 回答n以禁用DHCP。
3. 输入广域网接口的IPv4地址。
4. 输入位计数中的网络掩码。(24 = 255.255.255.0,16 = 255.255.0.0,8 = 255.0.0.0)
5. 输入广域网接口的网关地址。
6. 如果您希望此网关成为设备的默认网关，请对gateway提示符回答y，否则回答n。
7. 根据需要配置IPv6的NIC。
8. 禁用接口上的DHCP服务器。
9. 回答y以在webConfigurator协议上启用HTTP。这将在后续步骤中使用。

然后，您将收到设置已更新的确认。

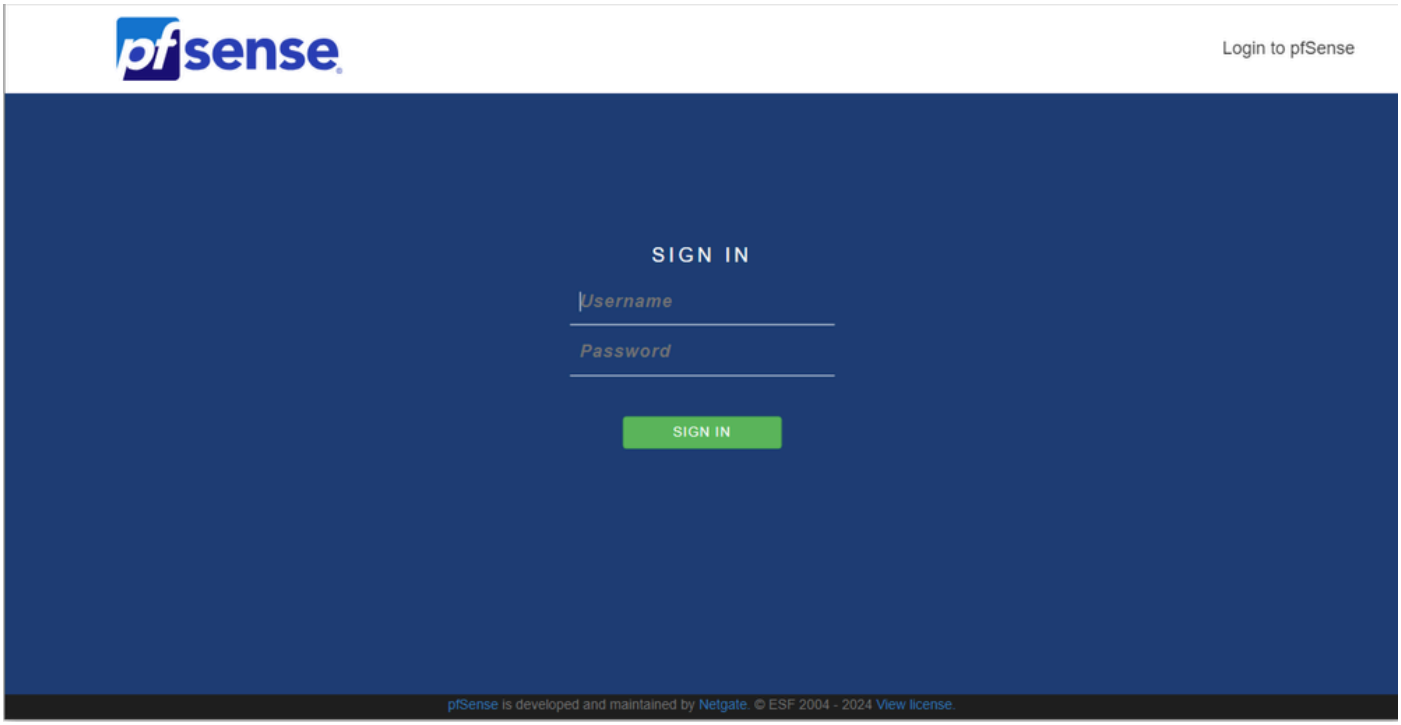


pfSense确认

完成初始设置

步骤1.打开Web浏览器并导航至：http://<ip_address_of_appliance>

注意：您必须首先使用HTTP而不是HTTPS。

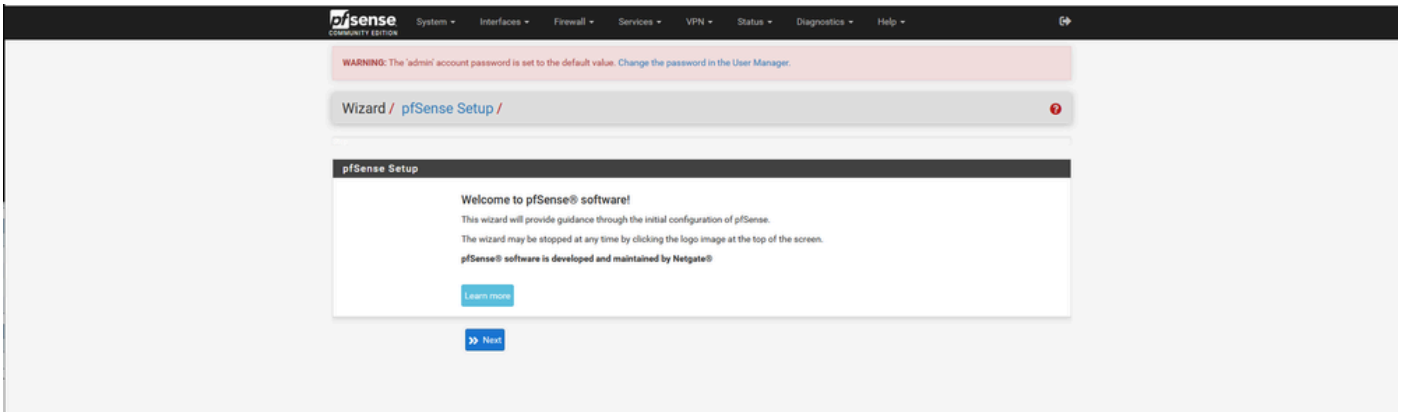


pfSense管理员登录

步骤2.使用默认登录名admin / pfSense登录

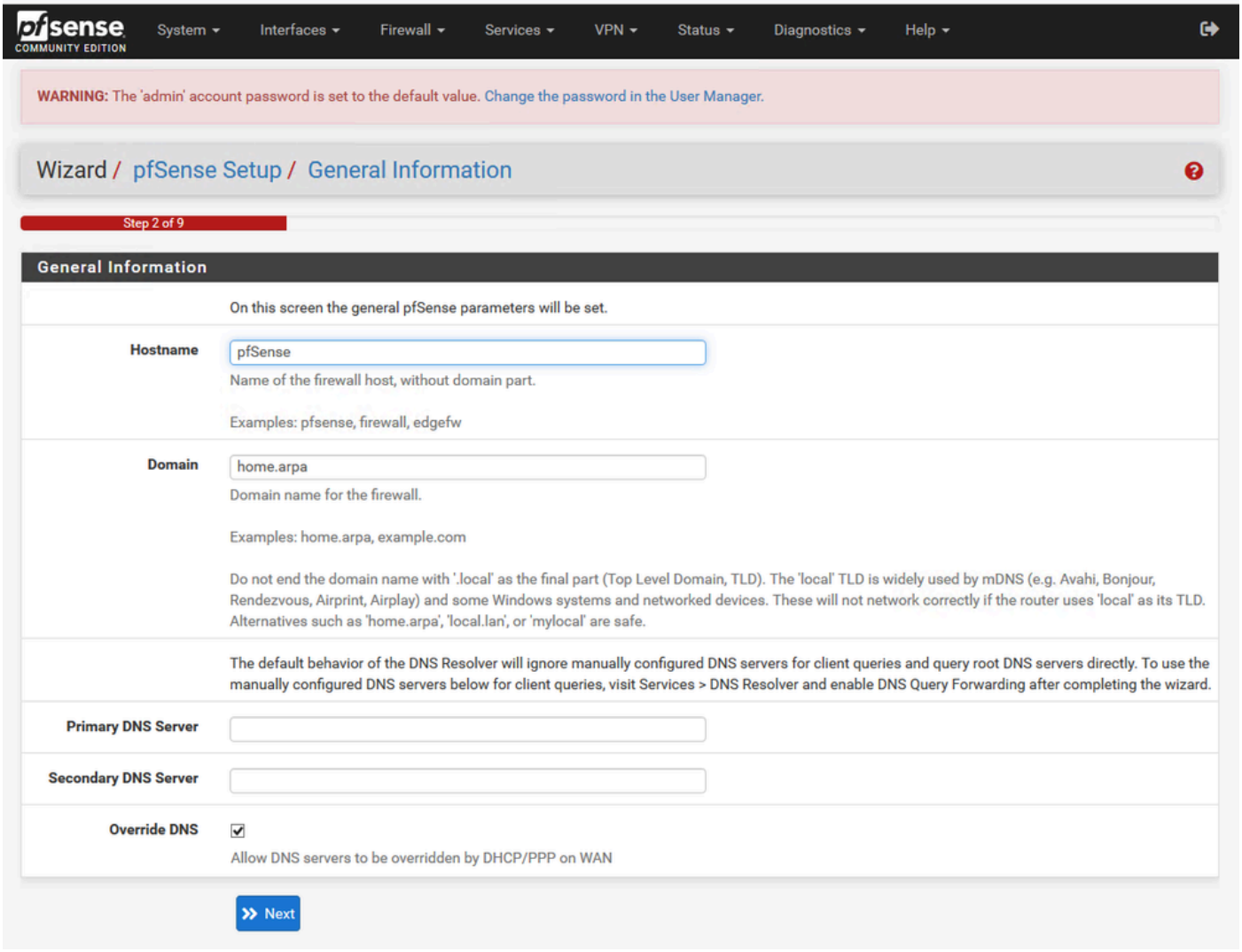
步骤3.完成初始设置

单击前两个屏幕中的“下一步”。



pfSense安装向导 — 1

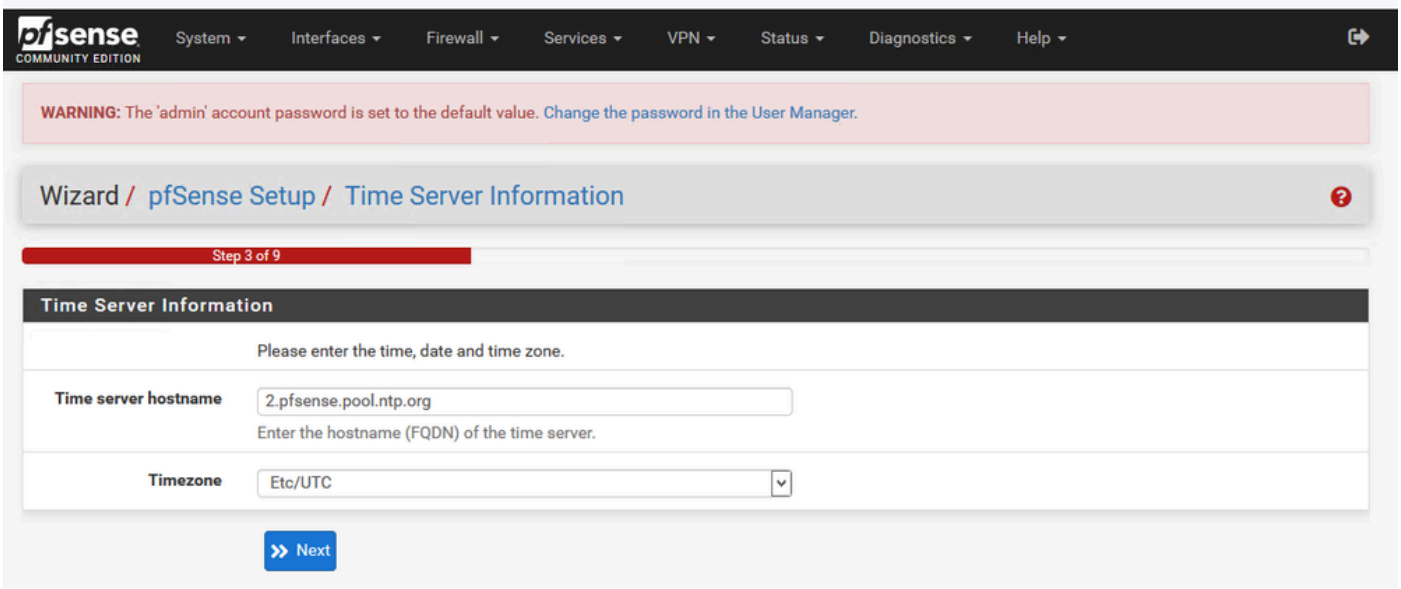
提供主机名、域名和DNS服务器信息。



pfSense安装向导 — 2

验证IP地址信息。如果您最初选择了DHCP，现在您可以更改它。

提供NTP时间服务器主机名并在下拉列表中选择正确的时区。



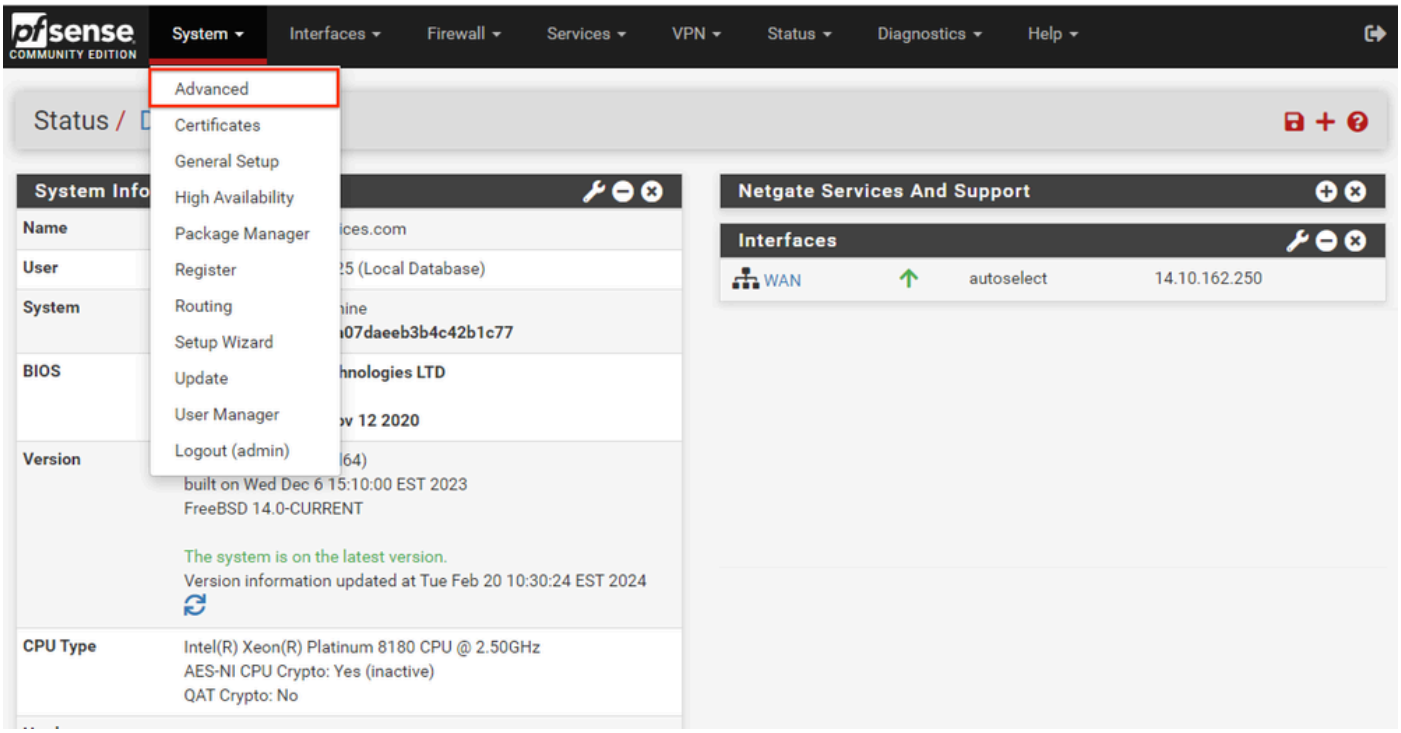
pfSense安装向导 — 3

继续完成安装向导，直到结束。界面GUI重新启动，完成后，您将重定向到新URL。

配置基本管理员设置

步骤1.登录管理界面

步骤2.从System下拉菜单中选择Advanced



pfSense GUI — 管理员下拉列表

步骤3.更新webConfigurator设置



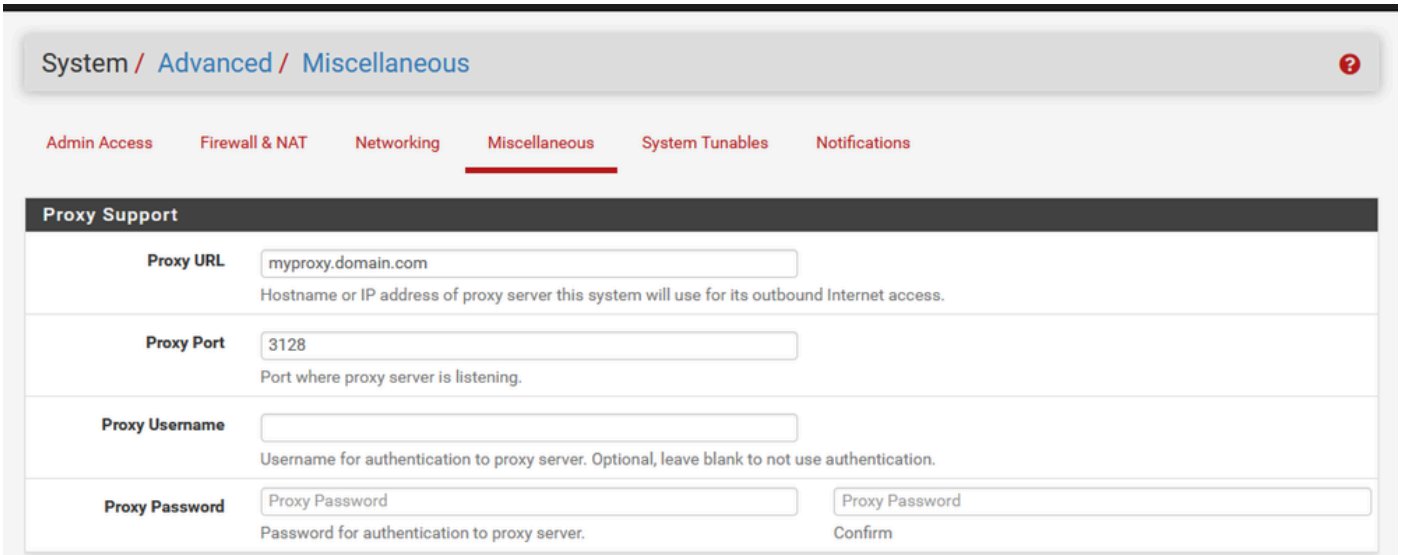
pfSense GUI — 管理员配置

1. 选择HTTPS(SSL/TLS)协议。
2. 此时将SSL/TLS证书保留为自签名证书。
3. 将TCP端口更改为除443之外的端口，以更好地保护接口并防止端口重叠问题。
4. 选择WebGUI重定向选项以禁用端口80上的管理界面。
5. 选择Browser HTTP_REFERER enforcement选项。
6. 通过选择Enable Secure Shell选项启用Secure Shell。

注意：请确保选择Save按钮后再继续。然后您将重定向到新的https链接。

步骤4.根据需要配置代理服务器

如果需要，请在Miscellaneous选项卡上配置代理信息。要完成设置和配置，设备必须能够访问互联网。



pfSense GUI — 代理配置

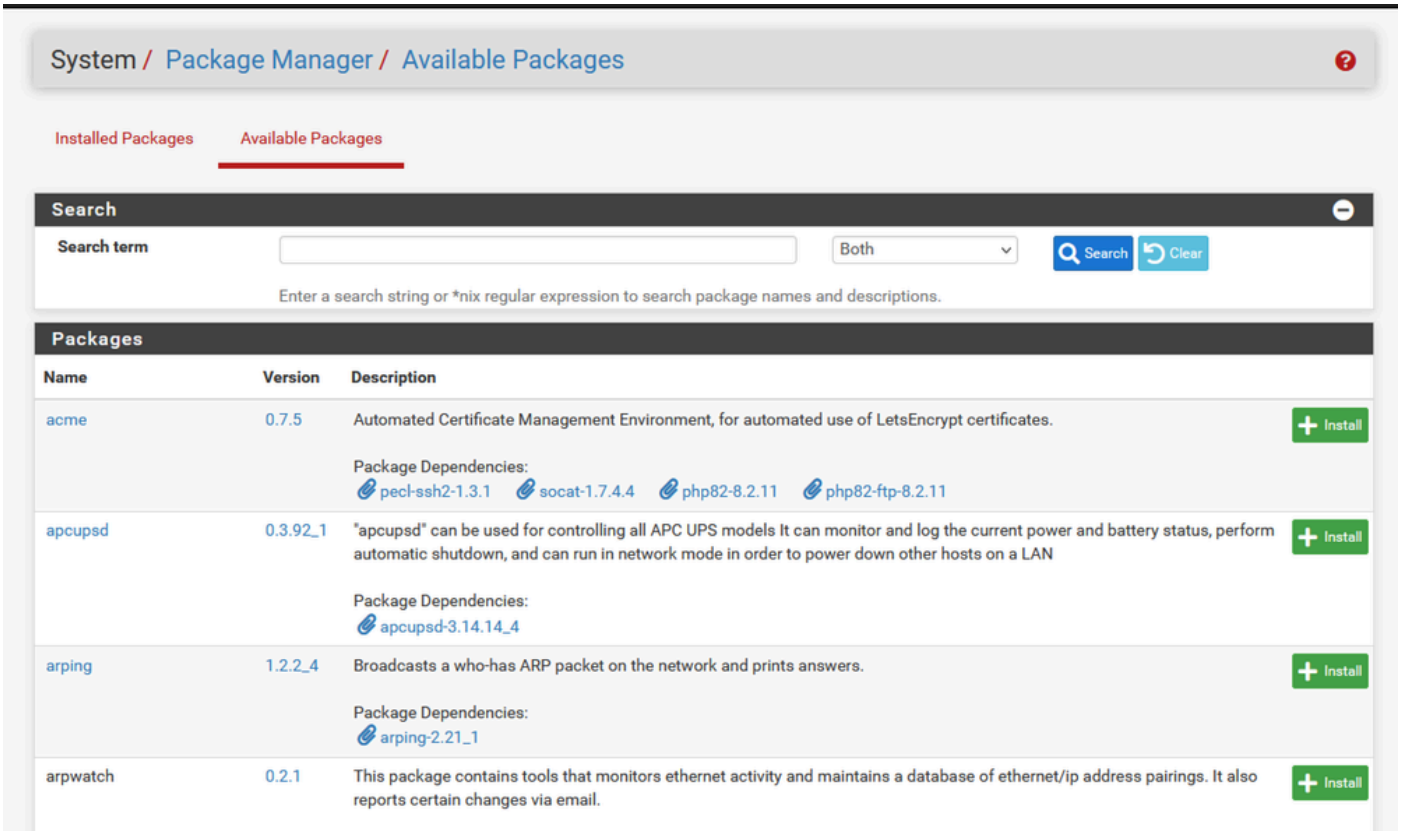
注意：请确保在进行更改后选择Save按钮。

添加所需的包

步骤1.选择System > Package Manager

步骤2.选择可用包

注意：加载所有可用的软件包可能需要几分钟时间。如果超时，请验证DNS服务器配置是否正确。通常，设备重新启动会修复Internet连接。



pfSense GUI — 软件包列表

步骤3.查找并安装所需的软件包

1. haproxy
2. Open-VM工具

注意：请勿选择haproxy-level包。

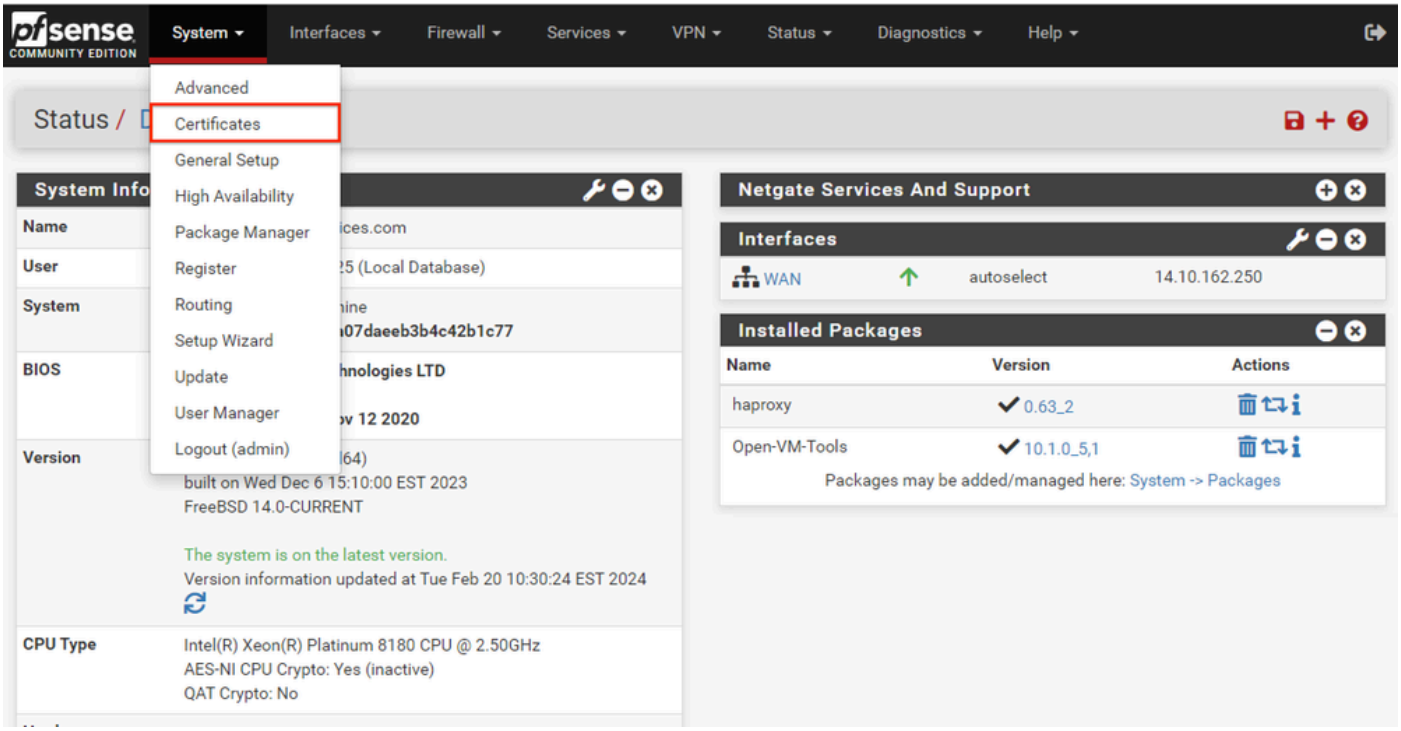
配置证书

pfSense可以创建自签名证书，也可以与公共CA、内部CA集成，或者可以充当CA并颁发CA签名证书。本指南介绍与内部CA集成的步骤。

开始本节之前，请确保您有这些可用项目。

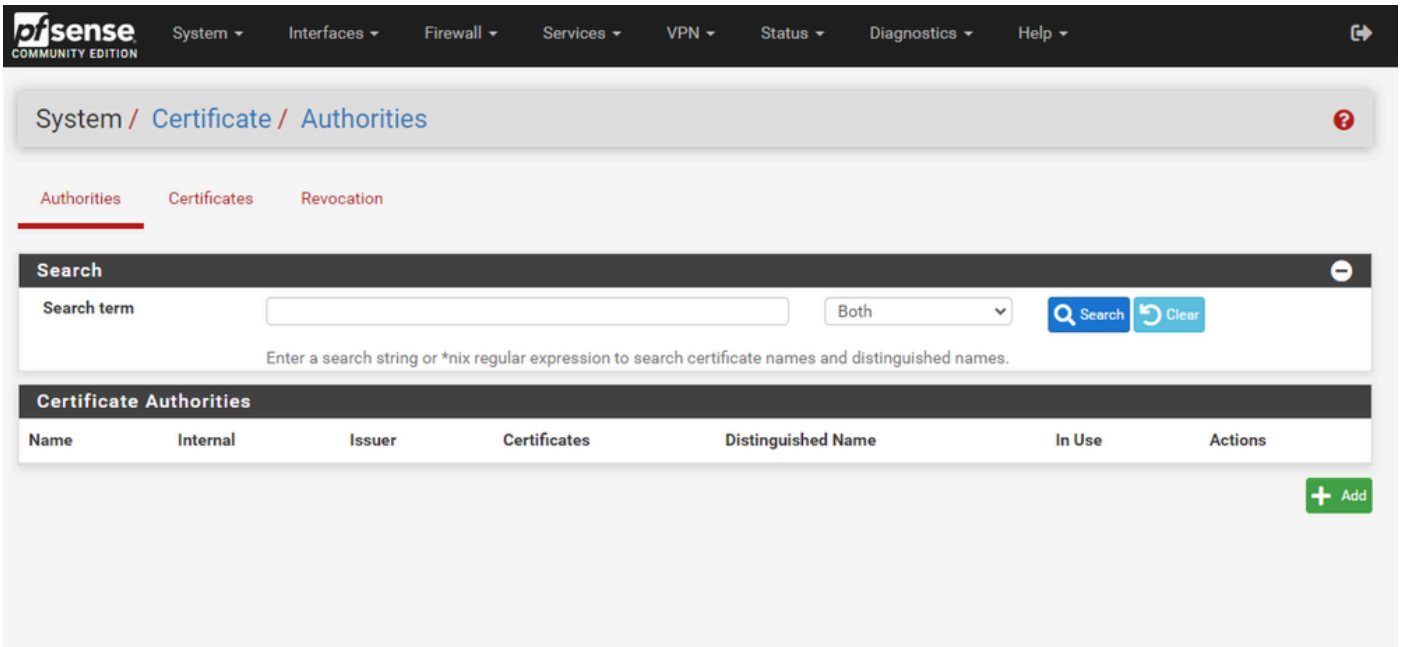
1. CA的根证书保存为PEM或Base-64编码格式。
2. CA的所有中间（有时称为颁发）证书保存为PEM或Base-64编码格式。

步骤1.从System下拉菜单中选择Certificates



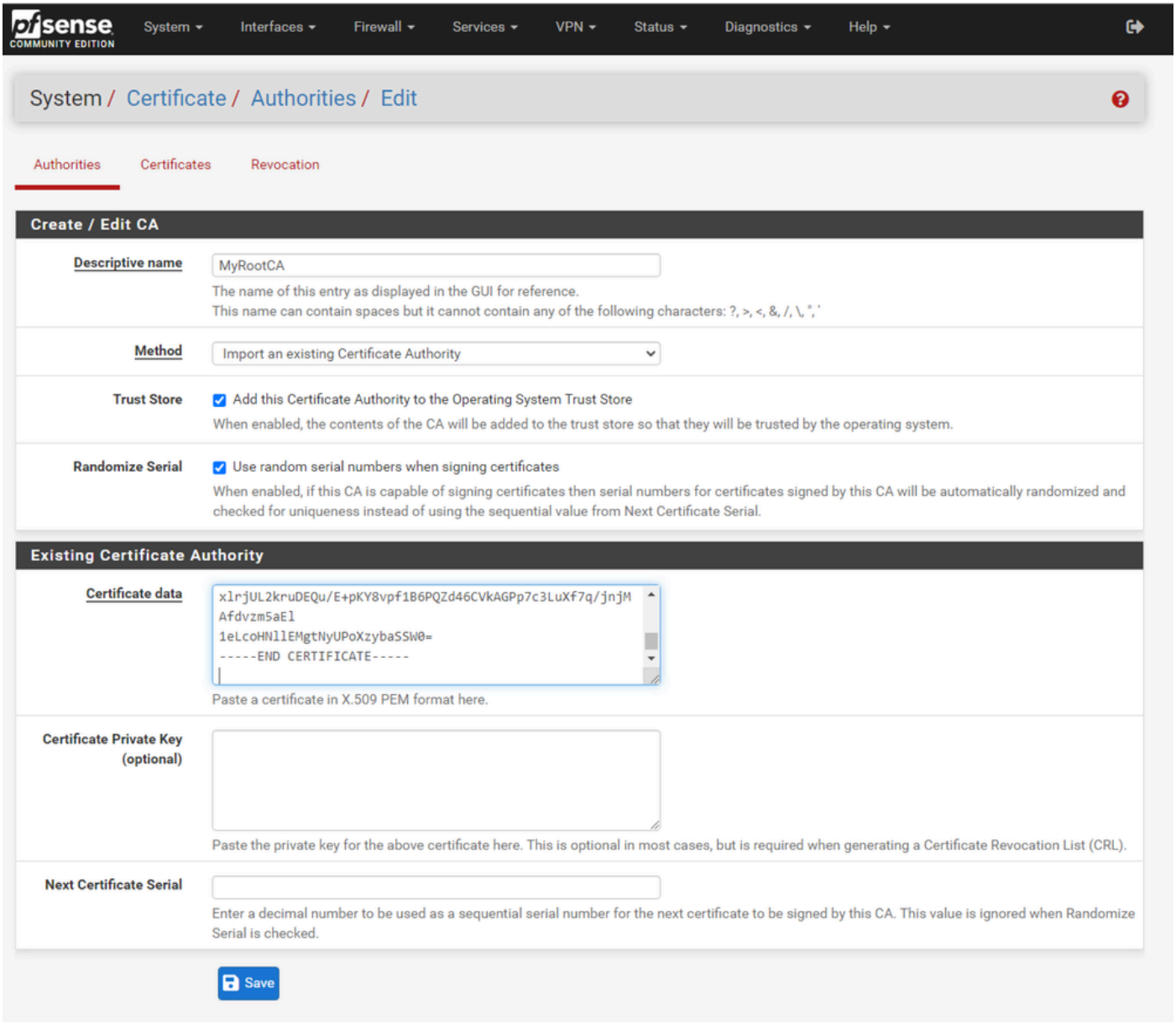
pfSense GUI — 证书下拉列表

步骤2.导入CA根证书



pfSense GUI - CA证书列表

选择Add按钮。



pfSense GUI - CA导入

如图所示:

1.提供唯一的描述性名称

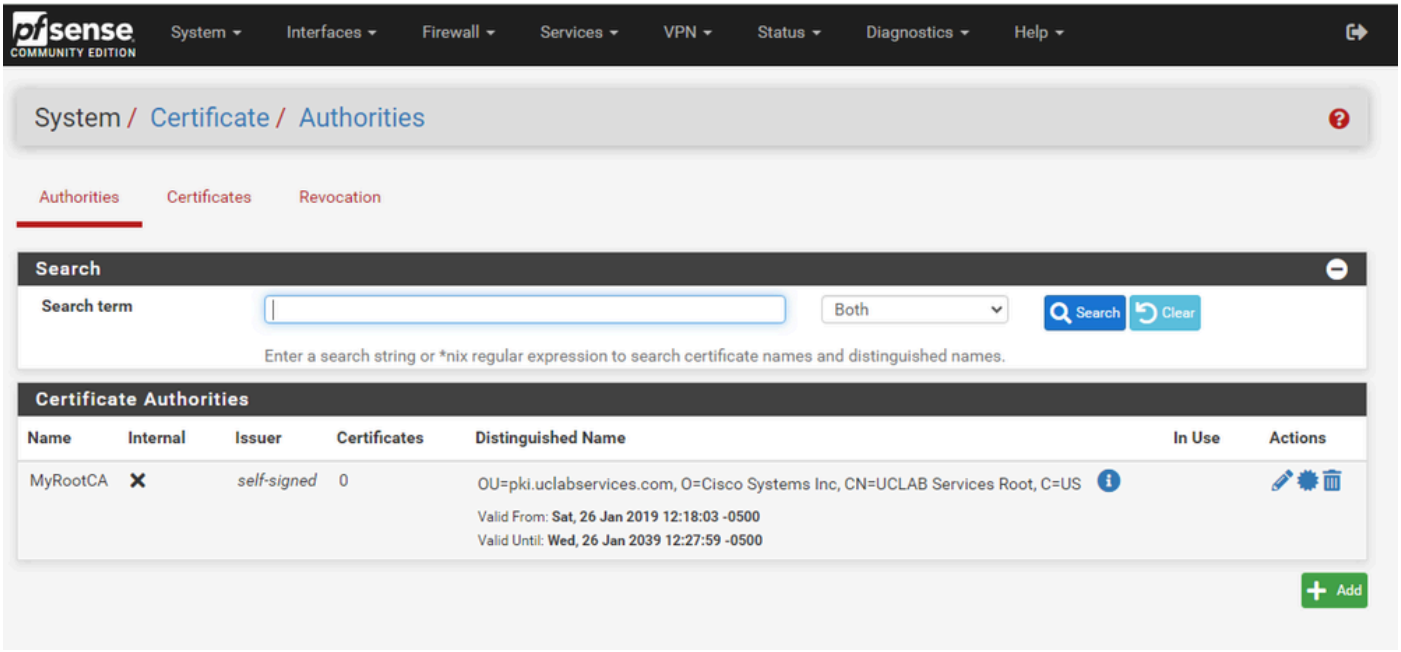
2.从“方法”下拉列表中选择“导入现有证书颁发机构”。

3.确保选中Trust Store和Randomize Serial复选框。

4.将整个证书粘贴到“证书数据”文本框中。确保包含-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----行。

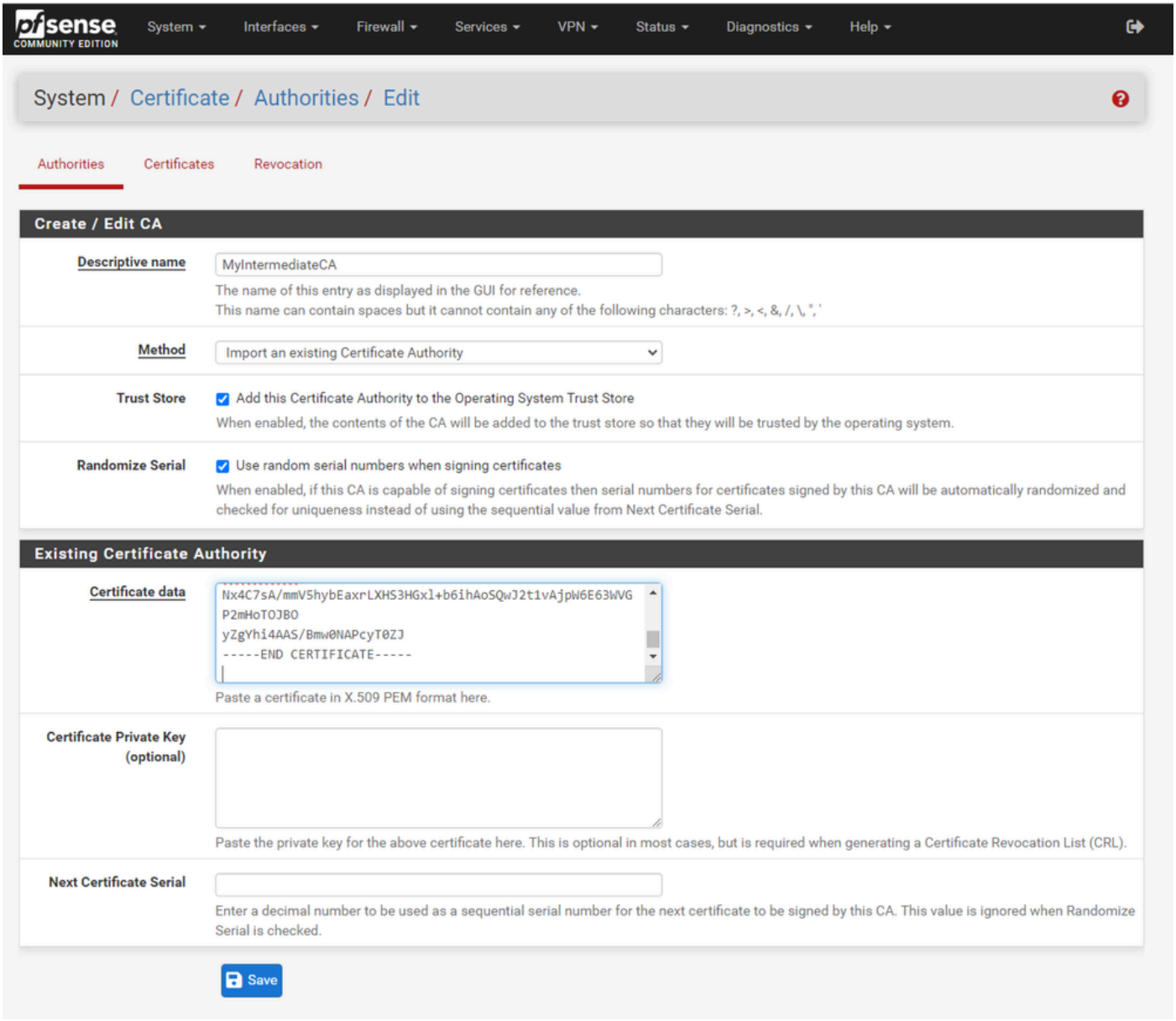
5.选择保存。

6.确认已导入证书，如图所示。



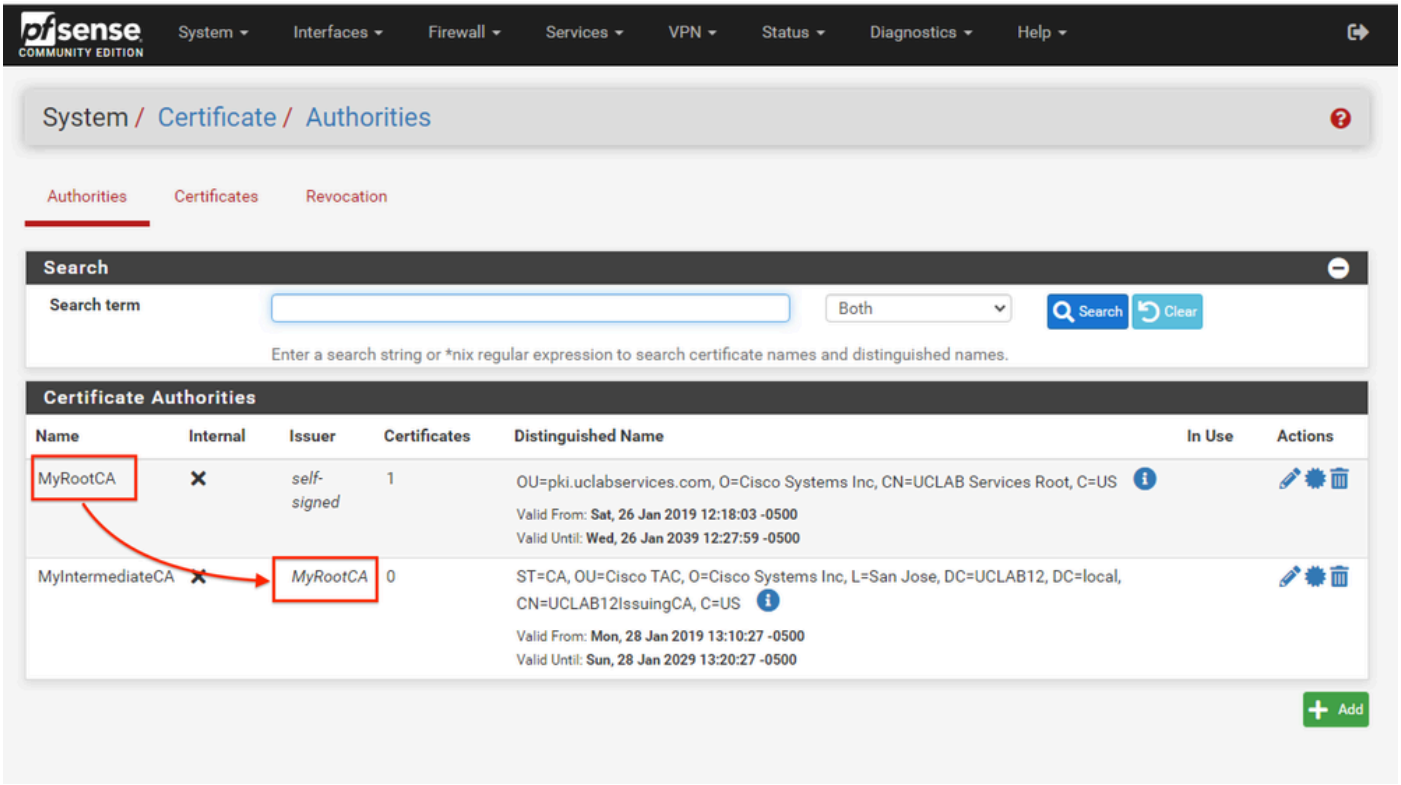
pfSense GUI - CA列表

步骤3.导入CA中间证书



pfSense GUI - CA中间导入

重复上述步骤以导入根CA证书以导入中间CA证书。



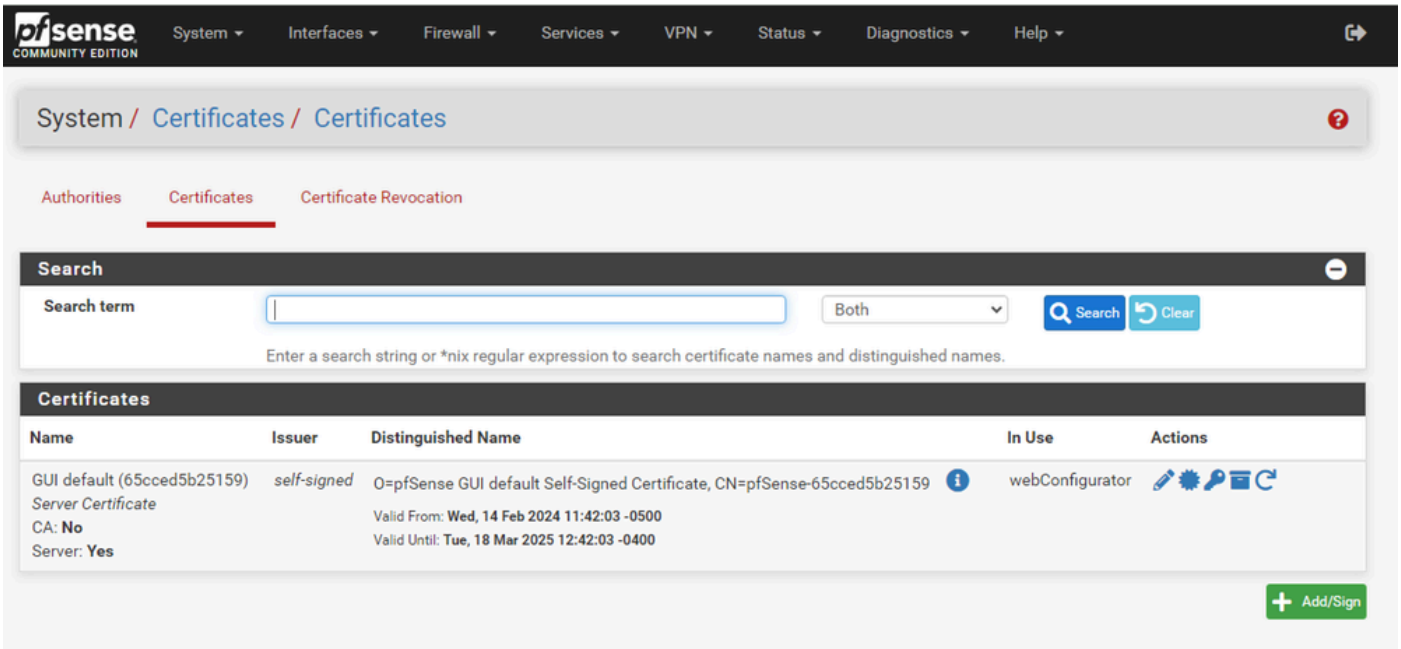
pfSense GUI - CA链接

查看证书颁发机构，确保中间证书正确链接到根证书，如图所示。

步骤4.为负载平衡网站创建和导出CSR

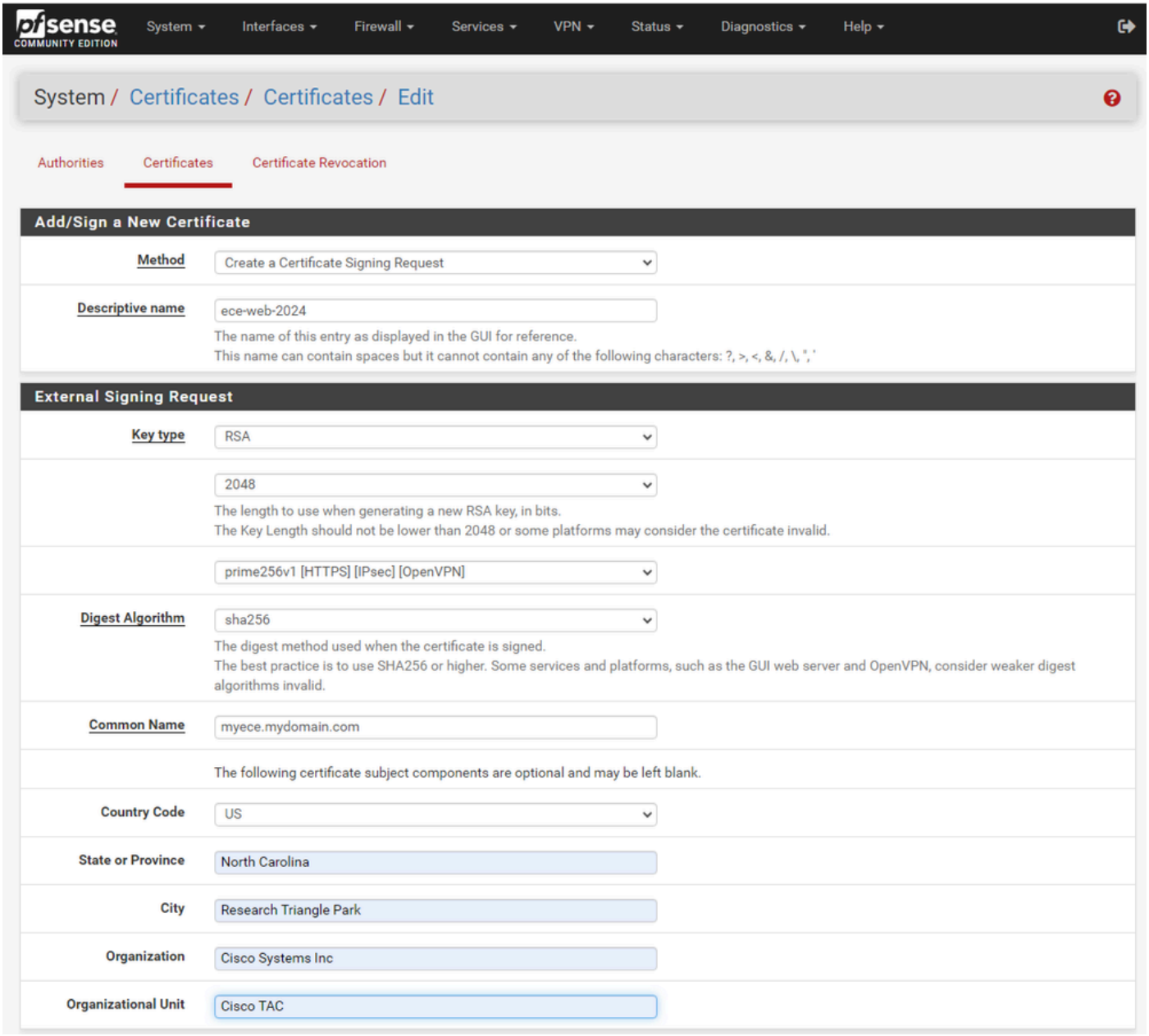
这描述了创建CSR、导出CSR，然后导入签名证书的步骤。如果已经具有PFX格式的现有证书，则可以导入此证书。有关这些步骤，请参阅pfSense文档。

1.选择“证书”菜单，然后选择添加/签名按钮。



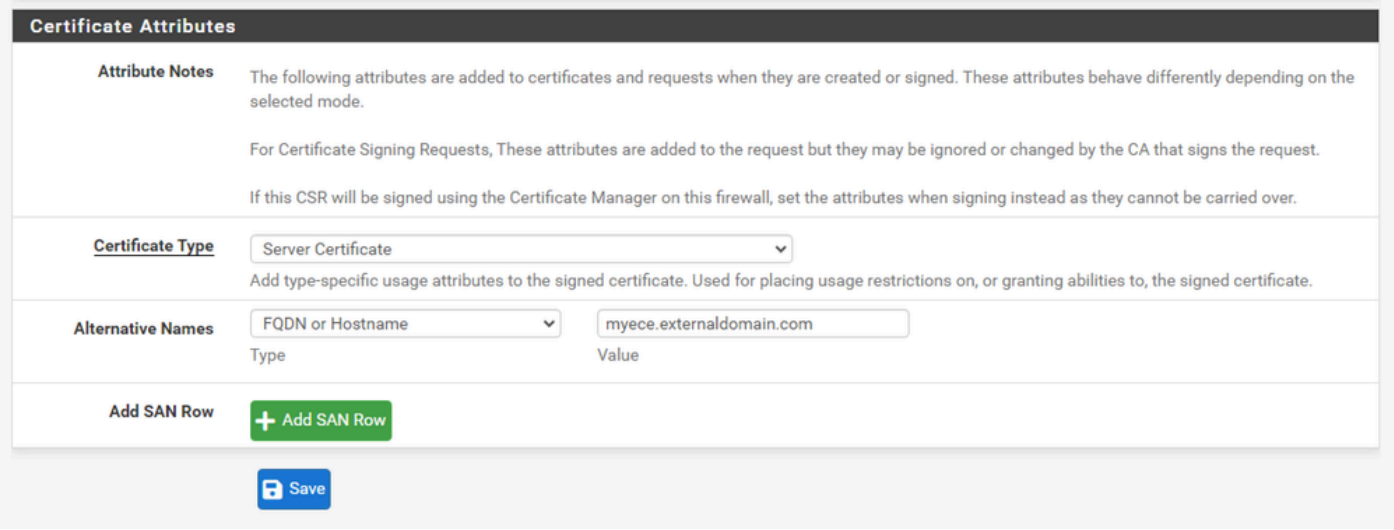
pfSense GUI — 证书列表

2.填写证书签名请求表。



pfSense GUI - CSR创建

- 方法：从下拉列表中选择Create a Certificate Signing Request
- 描述性名称：提供证书的名称
- 密钥类型和摘要算法：进行审核，确保它们符合您的要求
- 公用名：提供完全限定域名网站
- 根据您的环境要求提供其余证书信息



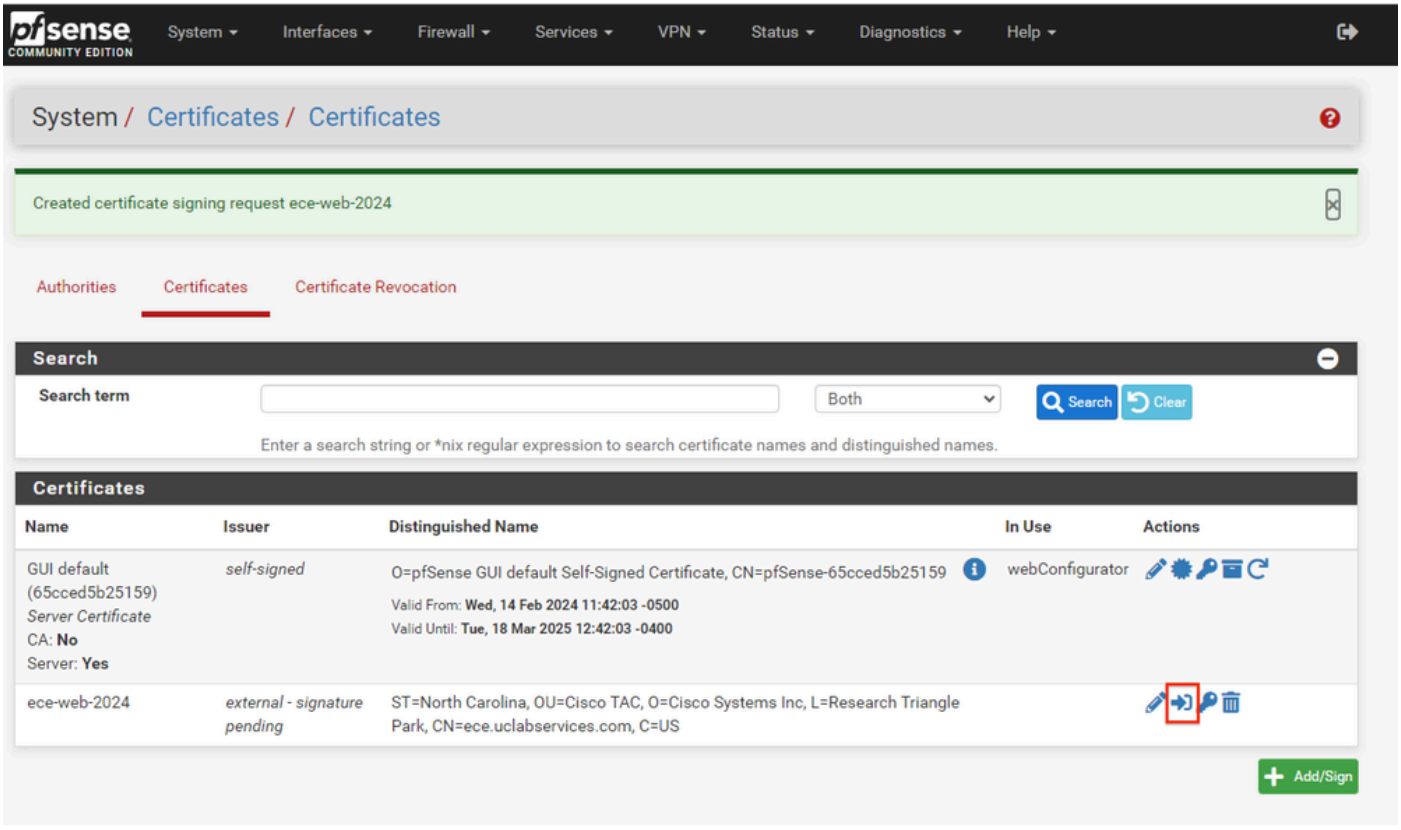
pfSense GUI - CSR高级

- 证书类型：在下拉列表中选择Server Certificate。
- 备用名称：提供实施所需的任何主题备用名称(SAN)。

注意：公用名将自动添加到SAN字段中。您只需要添加其他名称。

所有字段都正确后，选择Save。

3.将CSR导出到文件。

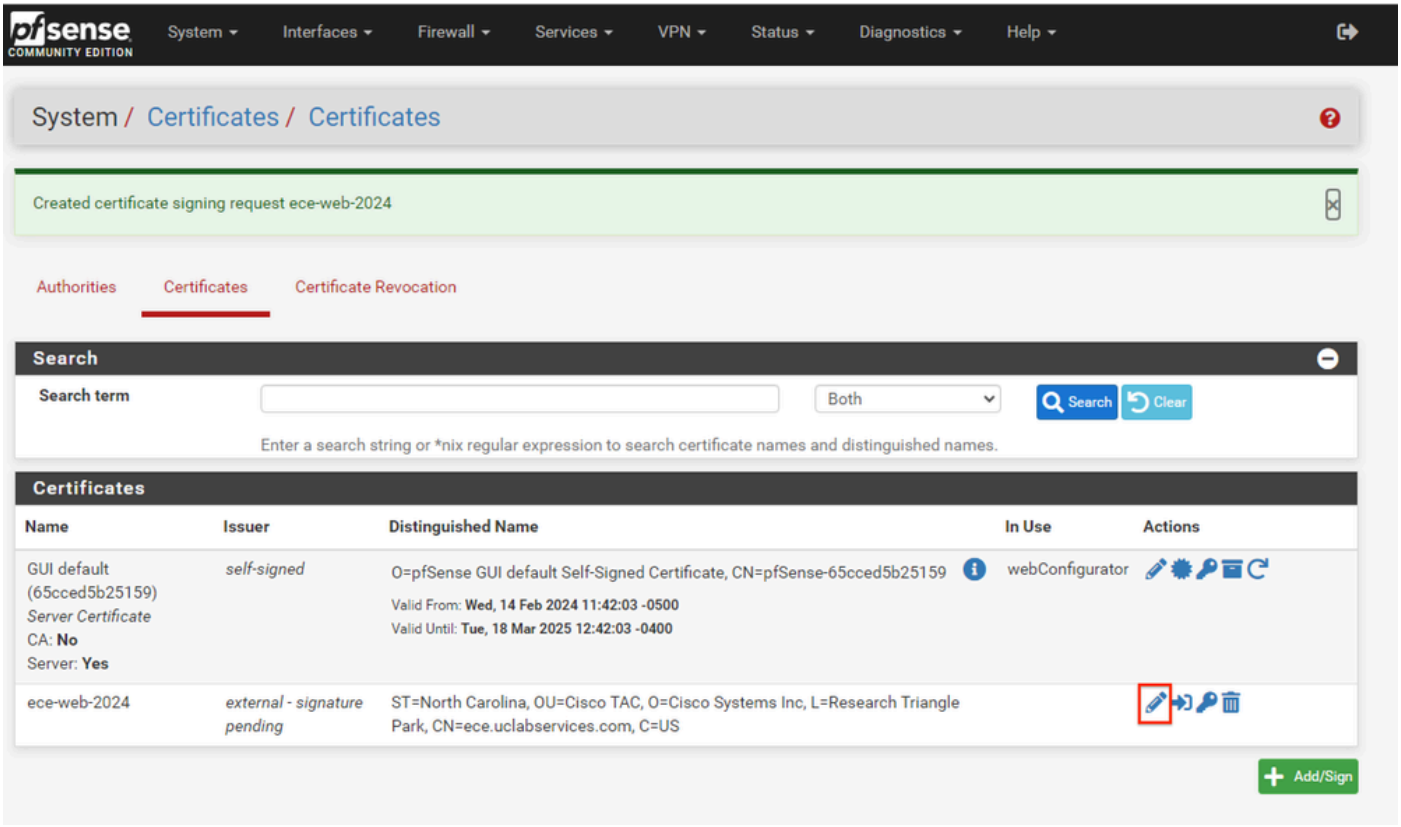


pfSense GUI - CSR导出

选择Export按钮保存CSR，然后与您的CA进行签名。获得签名证书后，请将其另存为PEM或Base-

64文件以完成此过程。

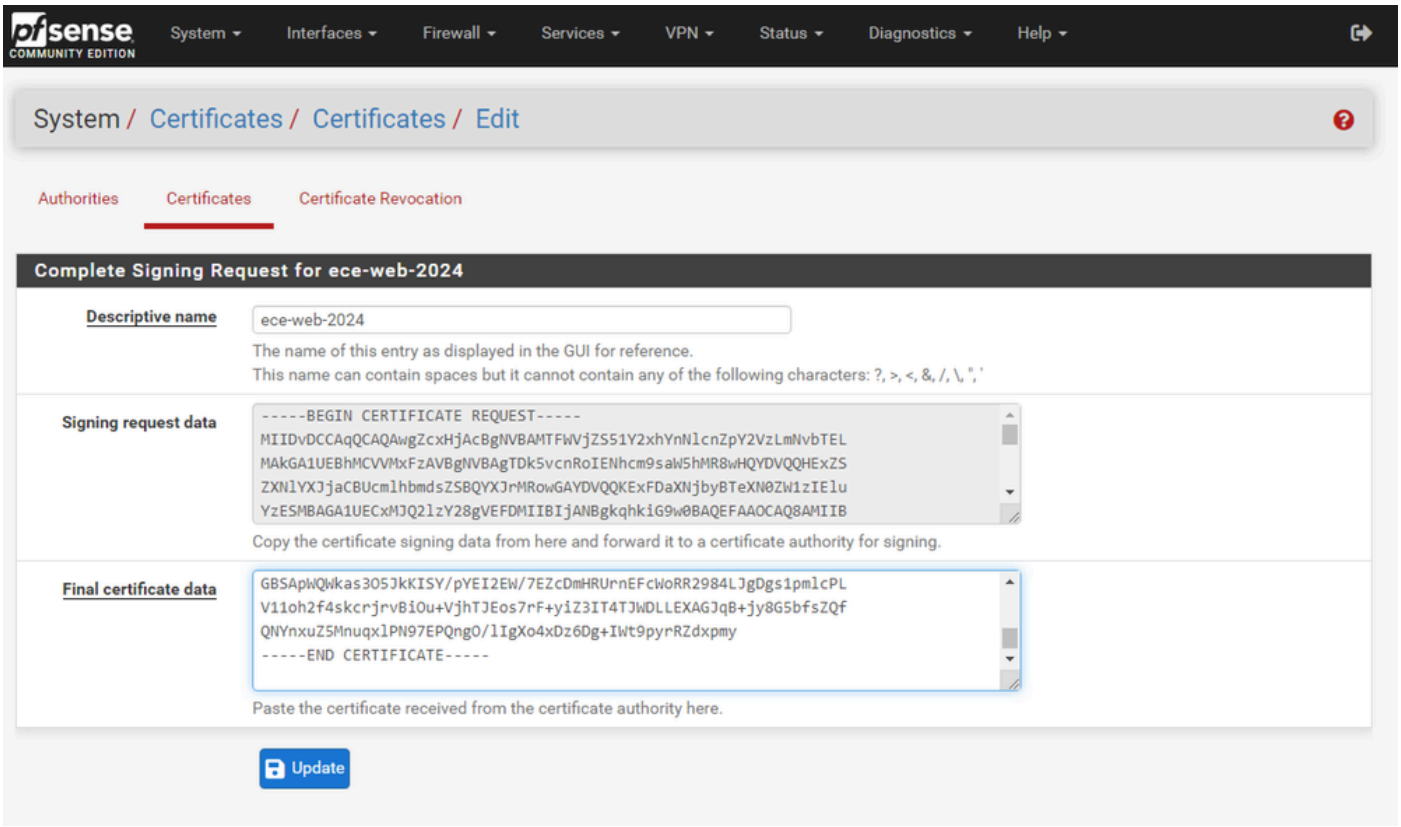
4.导入签名证书。



pfSense GUI — 证书导入

选择铅笔图标以导入签名证书。

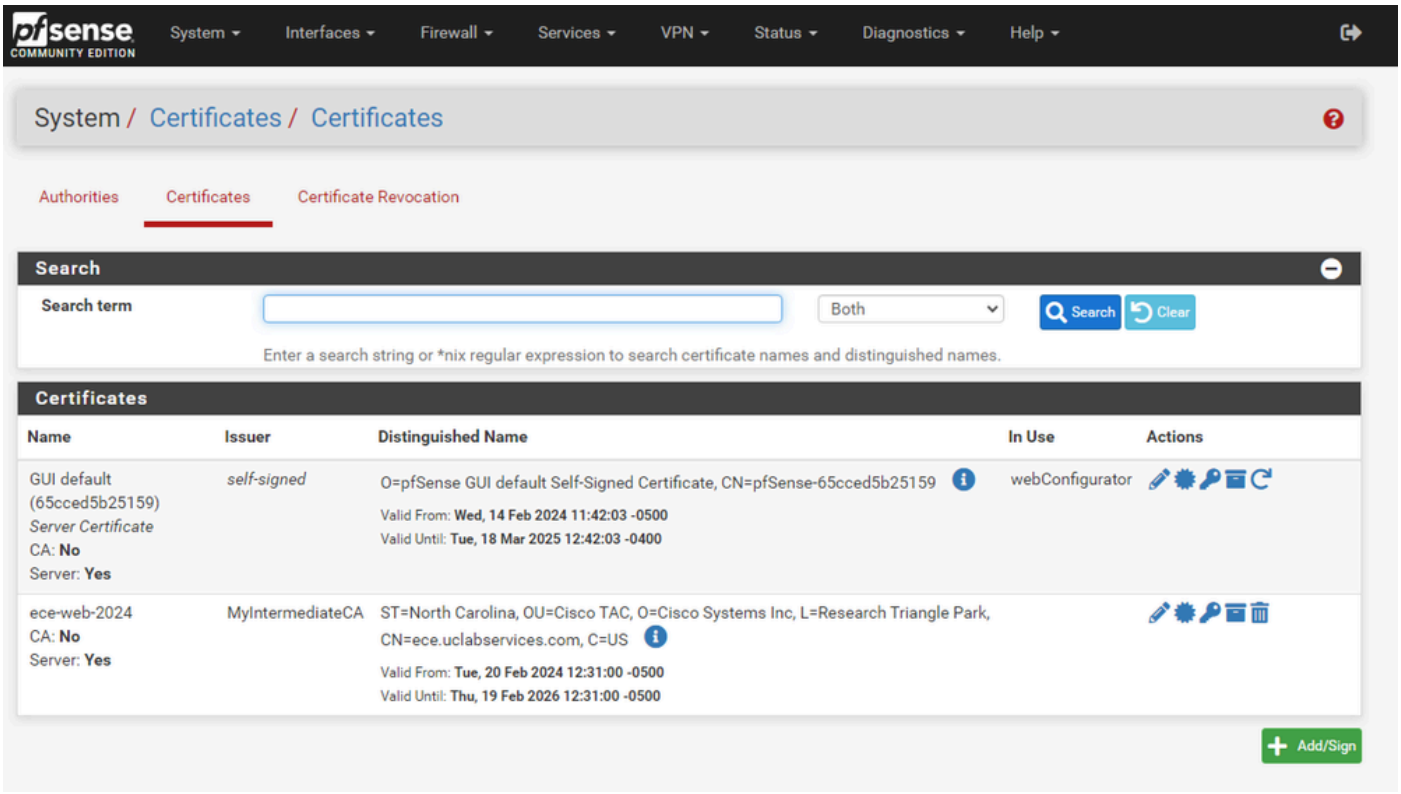
5.在表单中粘贴证书数据。



pfSense GUI — 证书导入

选择Update以保存证书。

6.检查证书数据以确保其正确。



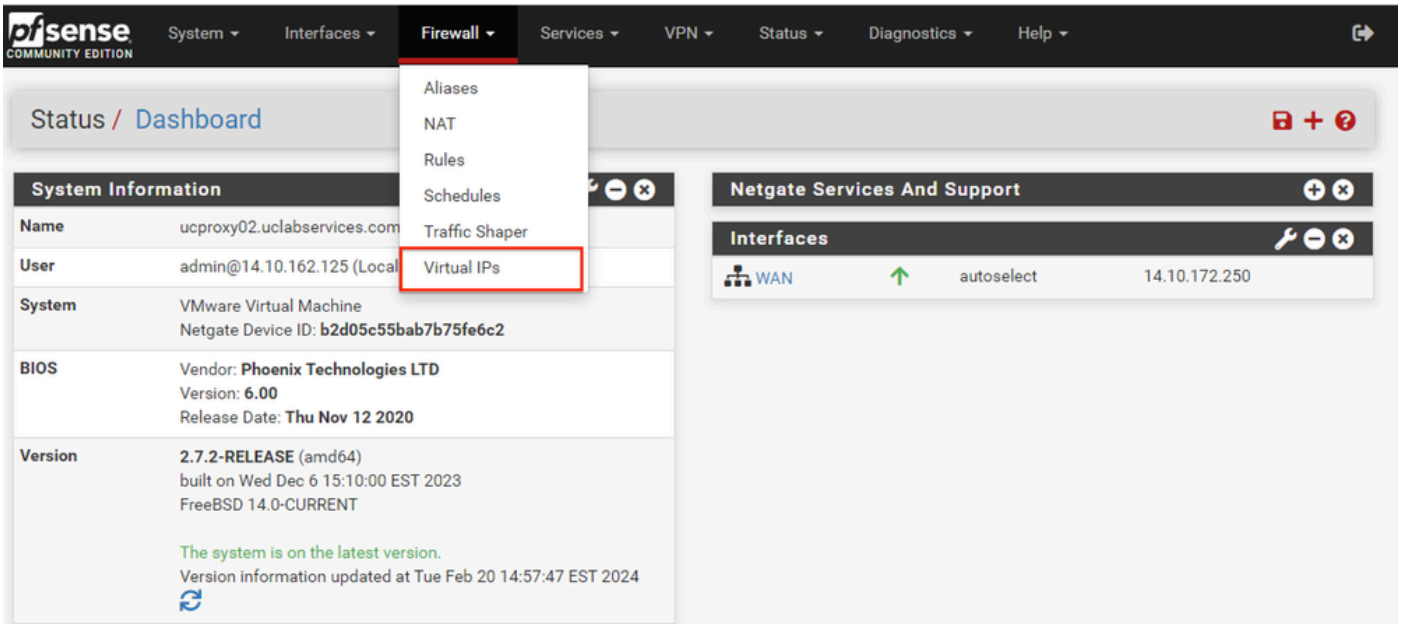
pfSense GUI — 证书列表

7.如果要在此pfSense上托管多个站点，请重复此过程。

添加虚拟IP

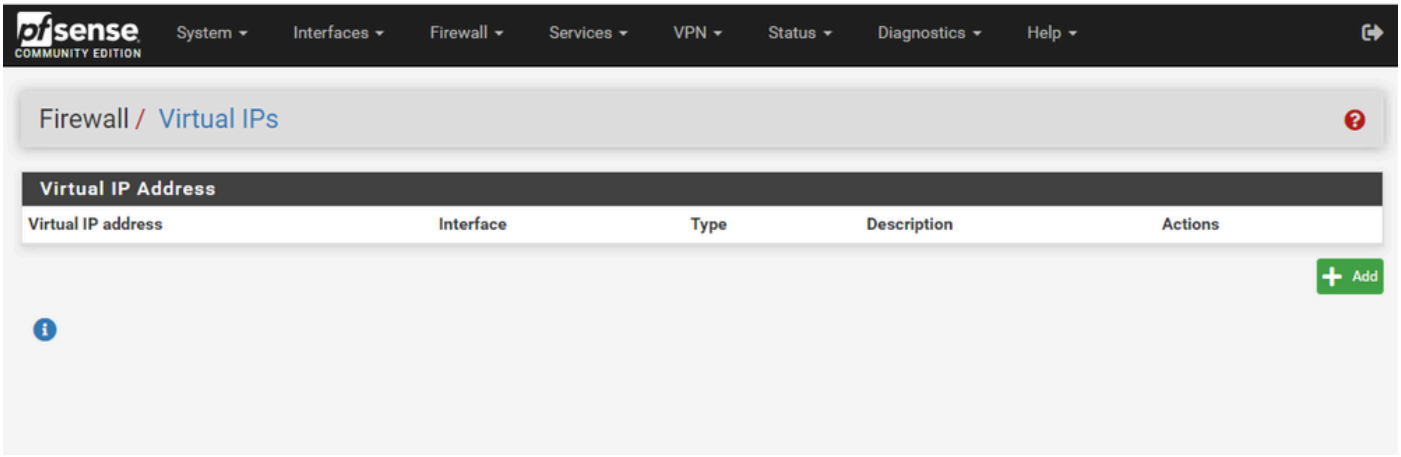
在pfSense上托管网站至少需要一个IP。在pfSense中，此操作通过虚拟IP(VIP)完成。

步骤1.从Firewall下拉列表中选择Virtual IPs



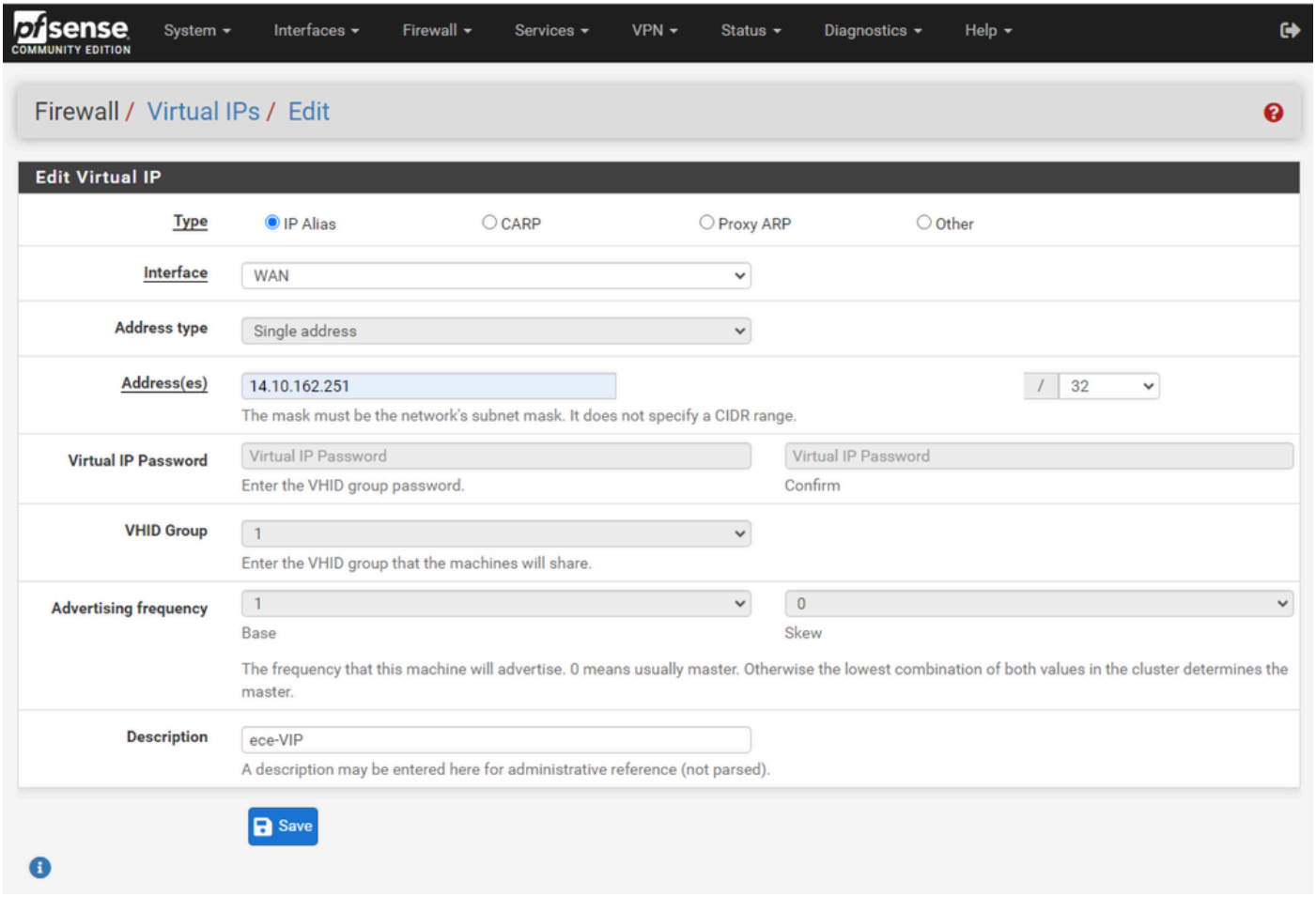
pfSense GUI - VIP下拉列表

步骤2.选择Add按钮



pfSense GUI - VIP登录页

步骤3.提供地址信息



pfSense GUI - VIP配置

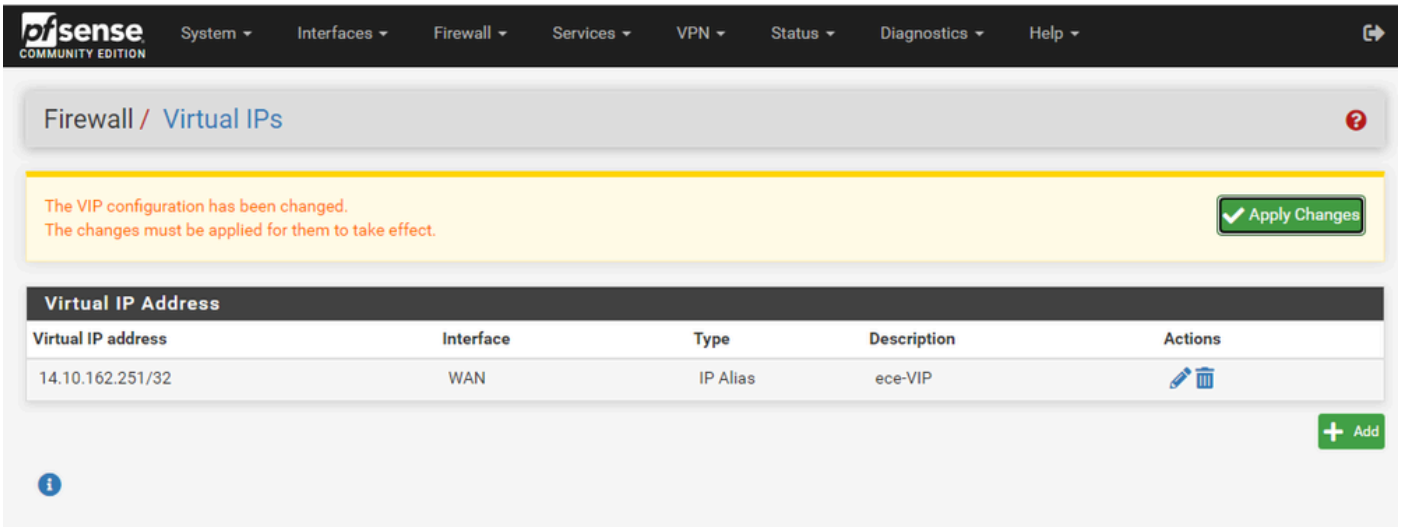
使用这些信息添加VIP。

- type：选择IP别名
- 接口:选择要广播的此IP地址的接口
- 地址：输入IP地址
- 地址掩码:对于用于负载均衡的IP地址，掩码必须为/32
- 描述:提供简短文本，以便以后更容易理解配置

选择保存以提交更改。

对配置所需的每个IP地址重复此步骤。

步骤4.应用配置



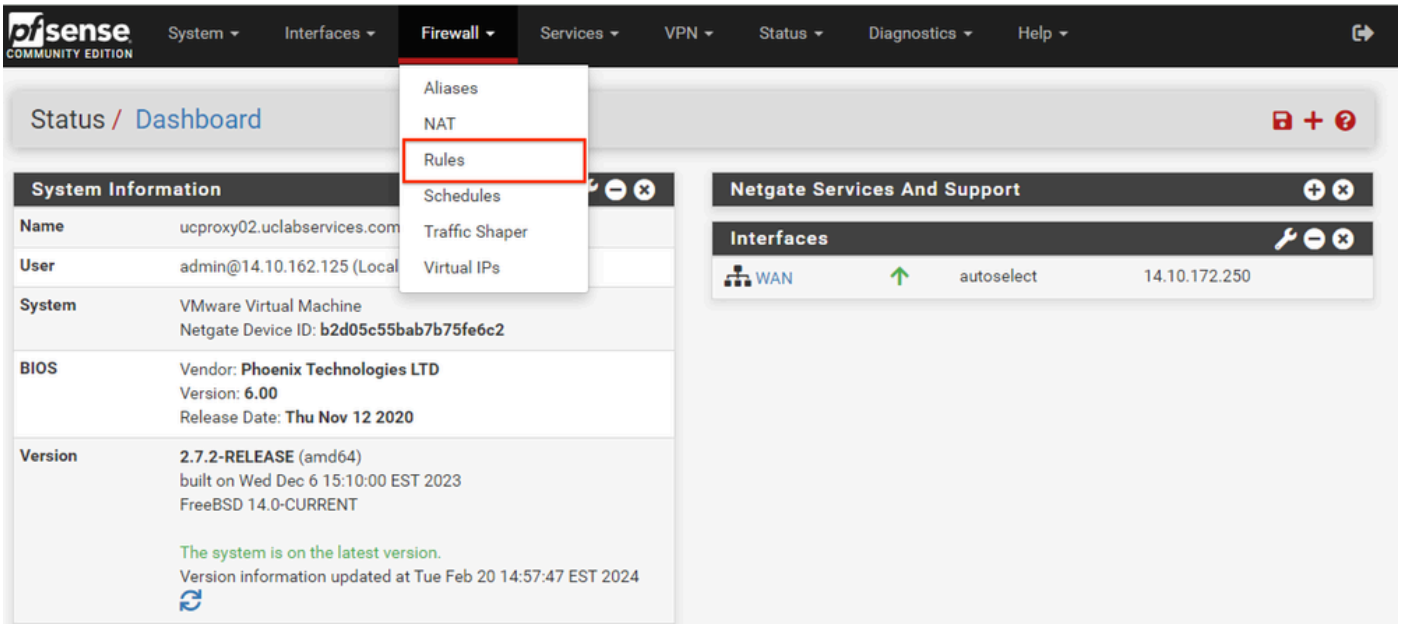
pfSense GUI - VIP列表

添加所有VIP后，选择Apply Changes按钮。

配置防火墙

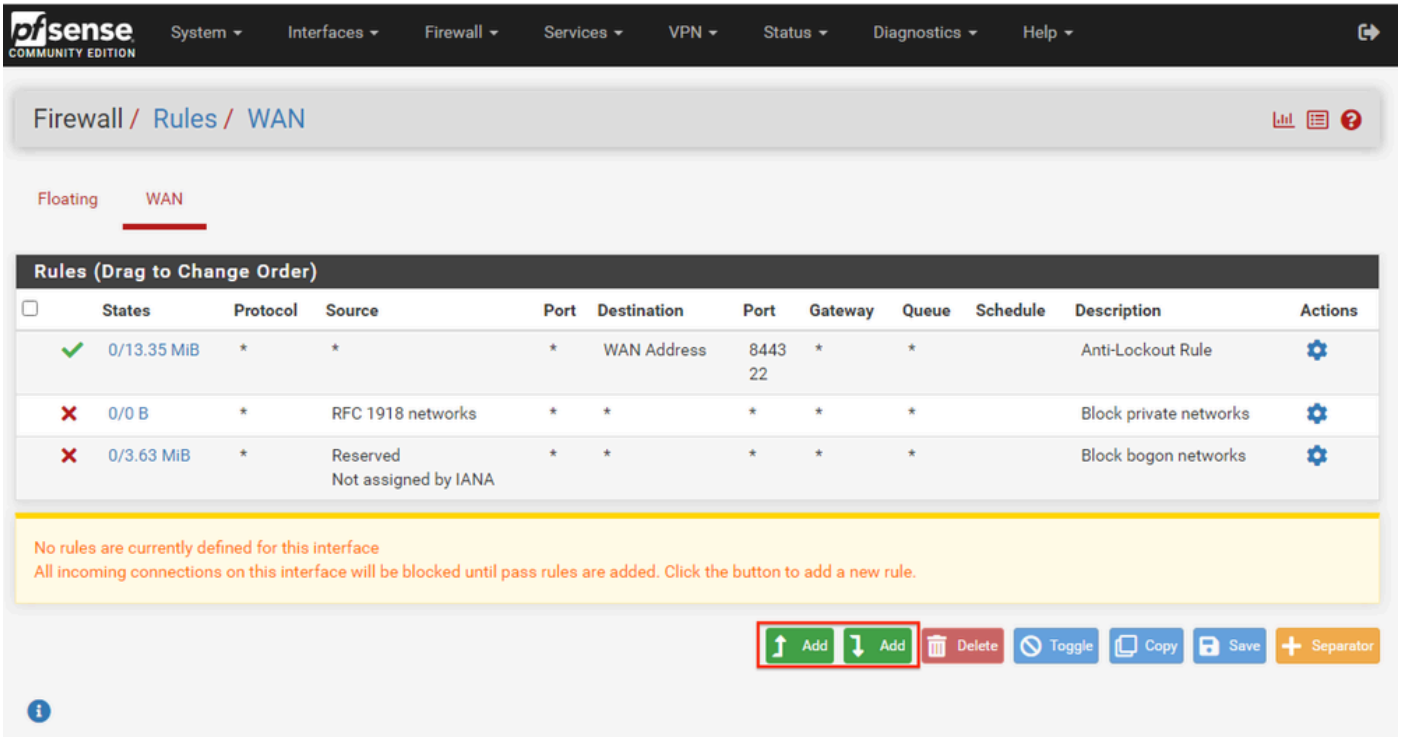
pfSense具有内置防火墙。默认规则集非常有限。在设备投入生产之前，请确保构建全面的防火墙策略。

步骤1.从Firewall下拉列表中选择Rules



pfSense GUI — 防火墙规则下拉列表

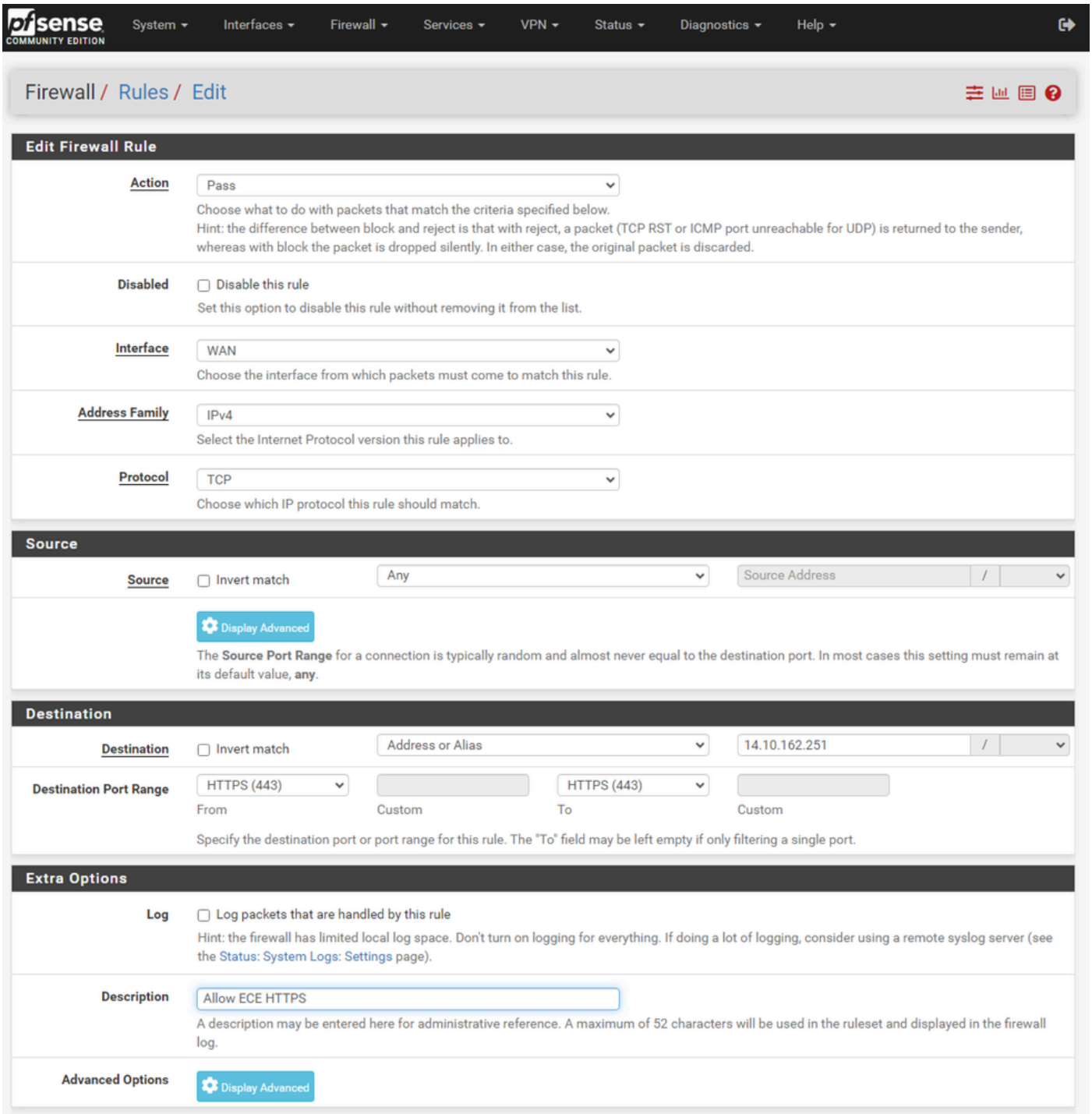
步骤2.选择一个Add按钮



pfSense GUI — 防火墙规则列表

请注意，一个按钮将新规则添加到所选行上方，而另一个按钮将规则添加到所选规则下方。任一按钮都可用于第一条规则。

步骤3.创建防火墙规则以允许流量传输到IP地址的端口443



pfSense GUI — 防火墙通过规则配置

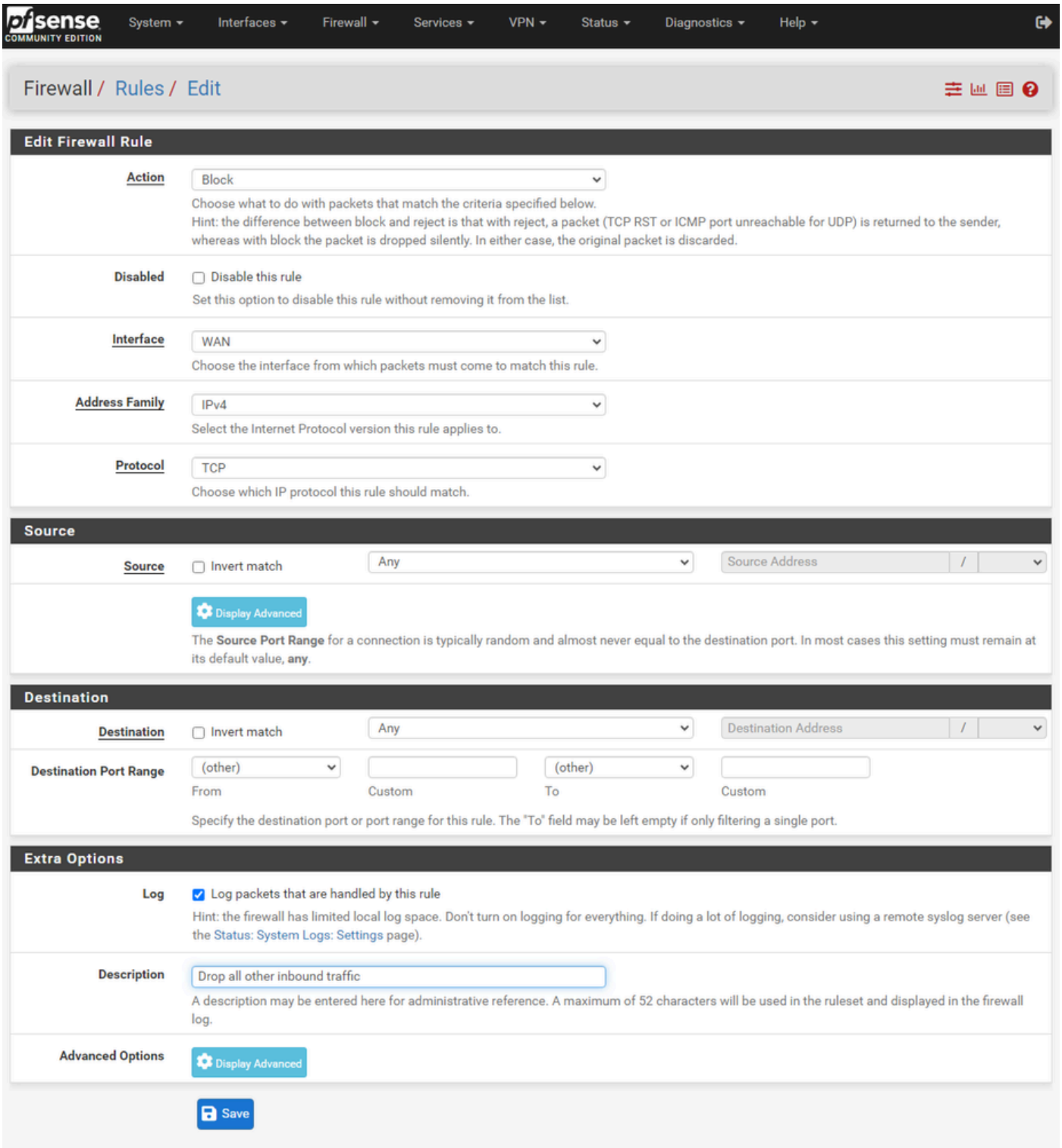
使用信息创建规则。

- 操作：选择通过
- 接口:选择规则应用到的接口
- 地址系列和协议：根据情况选择
- 来源：将选定项保留为“任意”
- 目的地：从Destination下拉列表中选择Address或Alias，然后输入应用规则的IP地址
- 目标端口范围：选择，在From和To下拉列表中选择HTTPS(443)
- 日志:选中此复选框可记录与此规则匹配的所有记帐数据包
- 描述:提供文本以稍后引用规则

选择Save。

步骤4.创建防火墙规则以丢弃到pfSense的所有其他流量

选择Add按钮将规则插入到新创建的规则下方。



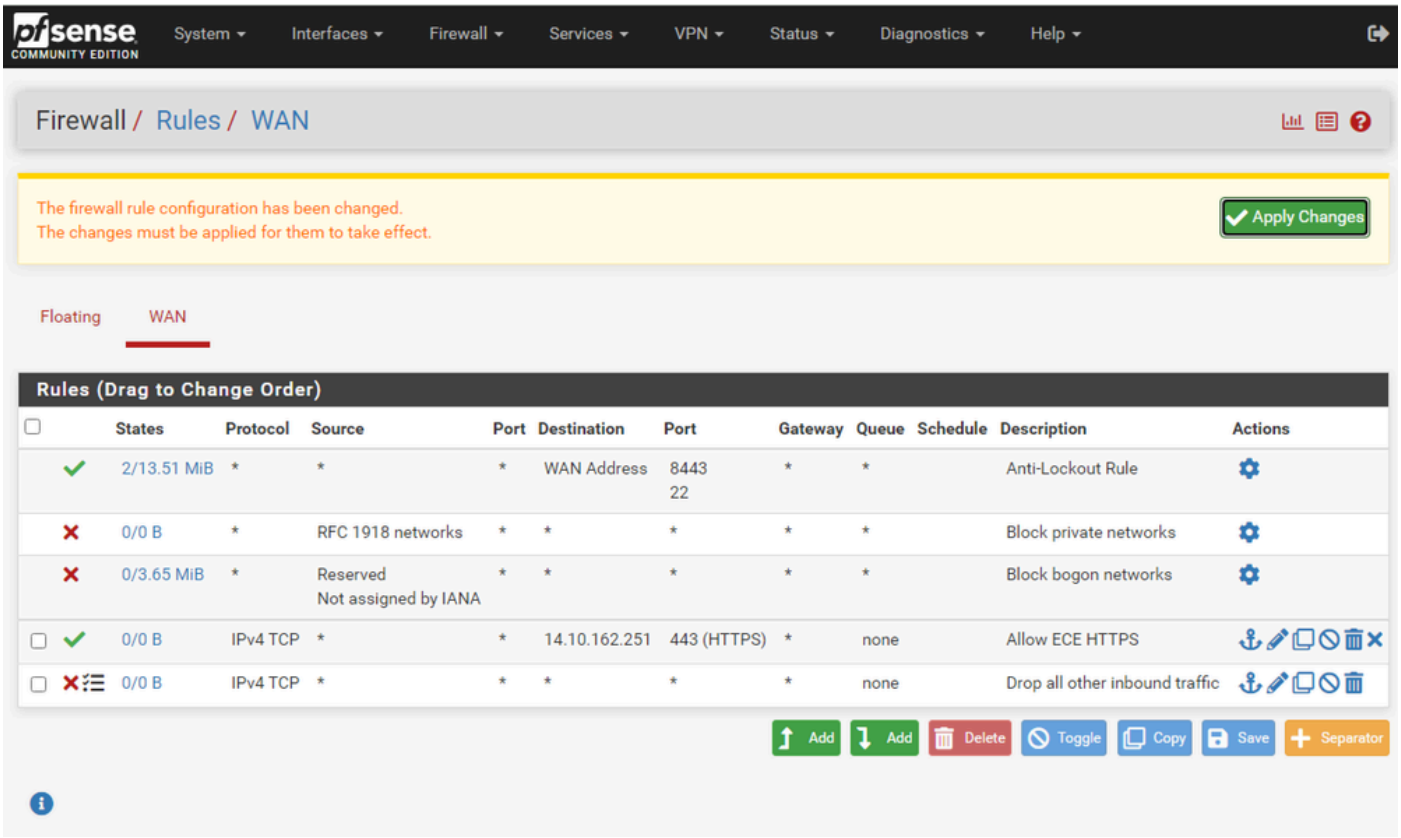
pfSense GUI — 防火墙丢弃规则配置

- 操作：选择屏蔽
- 接口:选择规则应用到的接口
- 地址系列和协议：根据情况选择

- 来源：将选定项保留为“任意”
- 目的地：将选定项保留为“任意”
- 日志:选中此复选框可记录与此规则匹配的所有记帐数据包
- 描述:提供文本以稍后引用规则

选择Save。

步骤5.检查规则并确保阻止规则位于底部



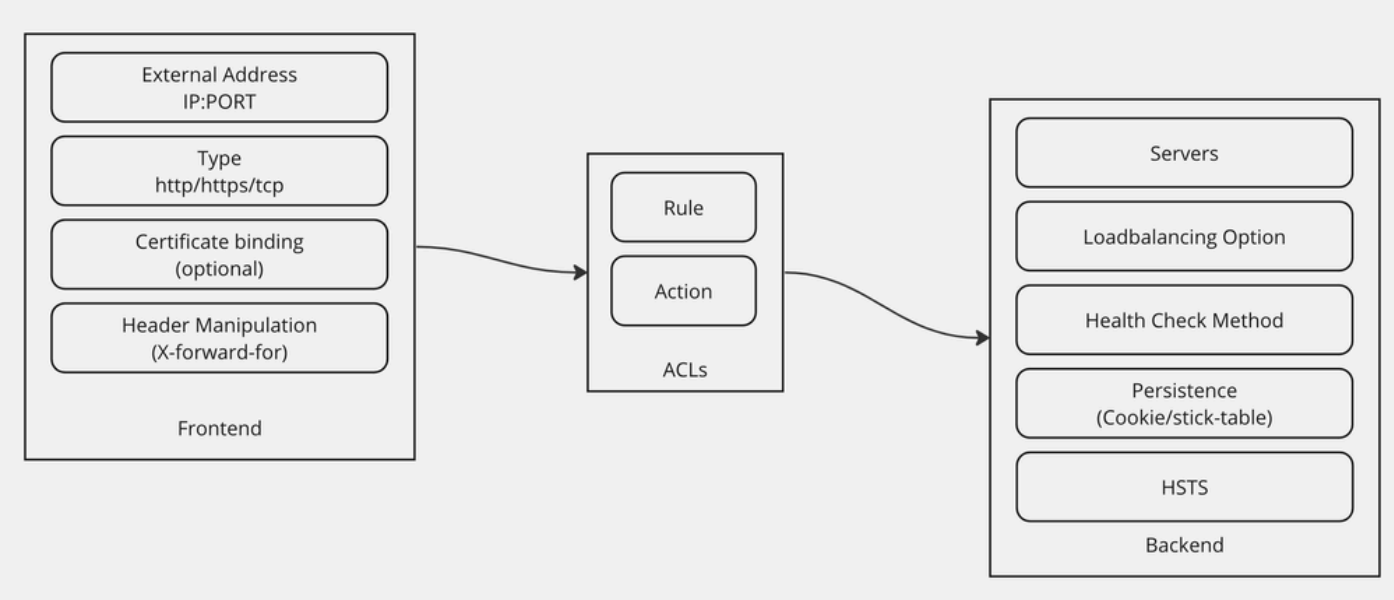
pfSense GUI — 防火墙规则列表

如果需要，请拖动规则对它们进行排序。

选择Apply Changes，当防火墙规则按您的环境所需的顺序进行时。

配置HAProxy

HAProxy概念



HAProxy概念

HAProxy通过前端/后端模型实施。

前端定义客户通信的代理端。

前端包括IP和端口组合、证书绑定，并可实现某些报头操作。

后端定义与物理Web服务器通信的代理端。

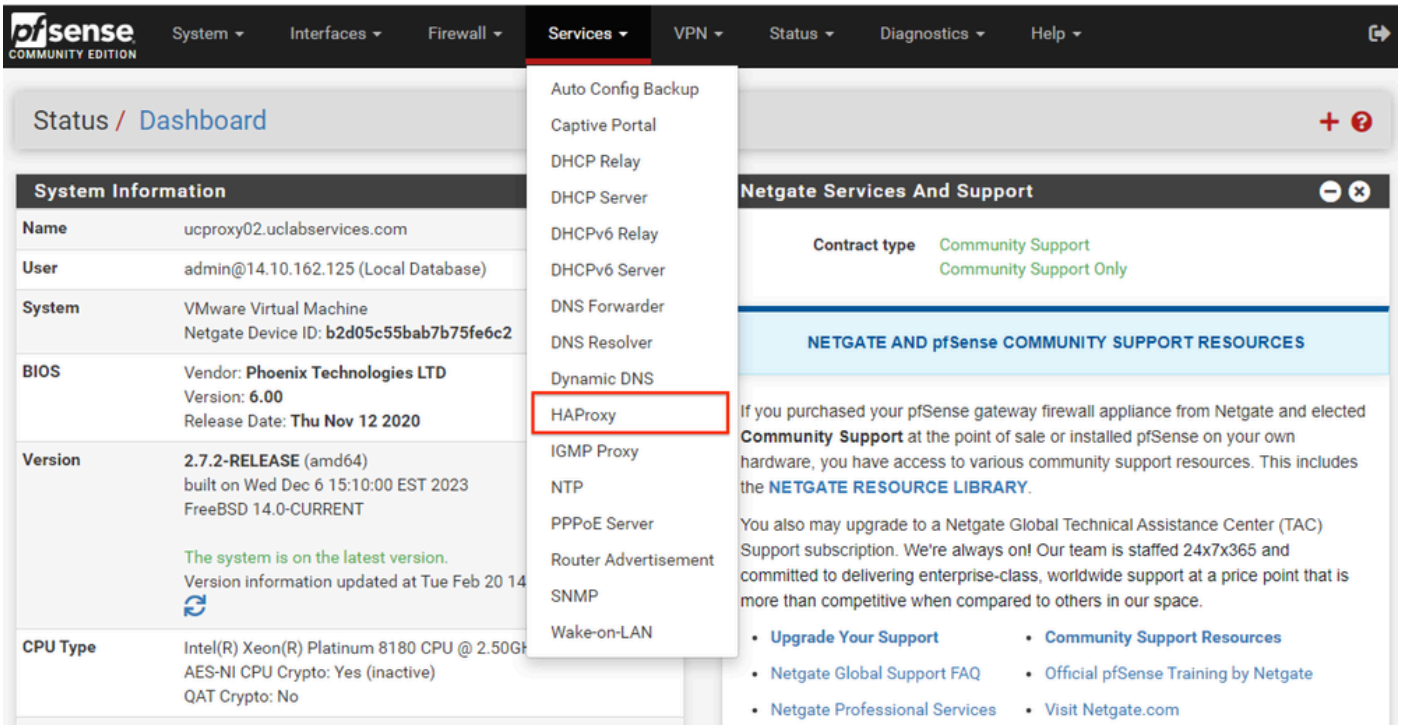
后端定义实际服务器和端口、初始分配的负载均衡方法、运行状况检查和持久性。

前端通过专用后端或使用ACL了解要与哪些后端通信。

ACL可以创建不同的规则，以便给定前端可以根据各种情况与不同的后端通信。

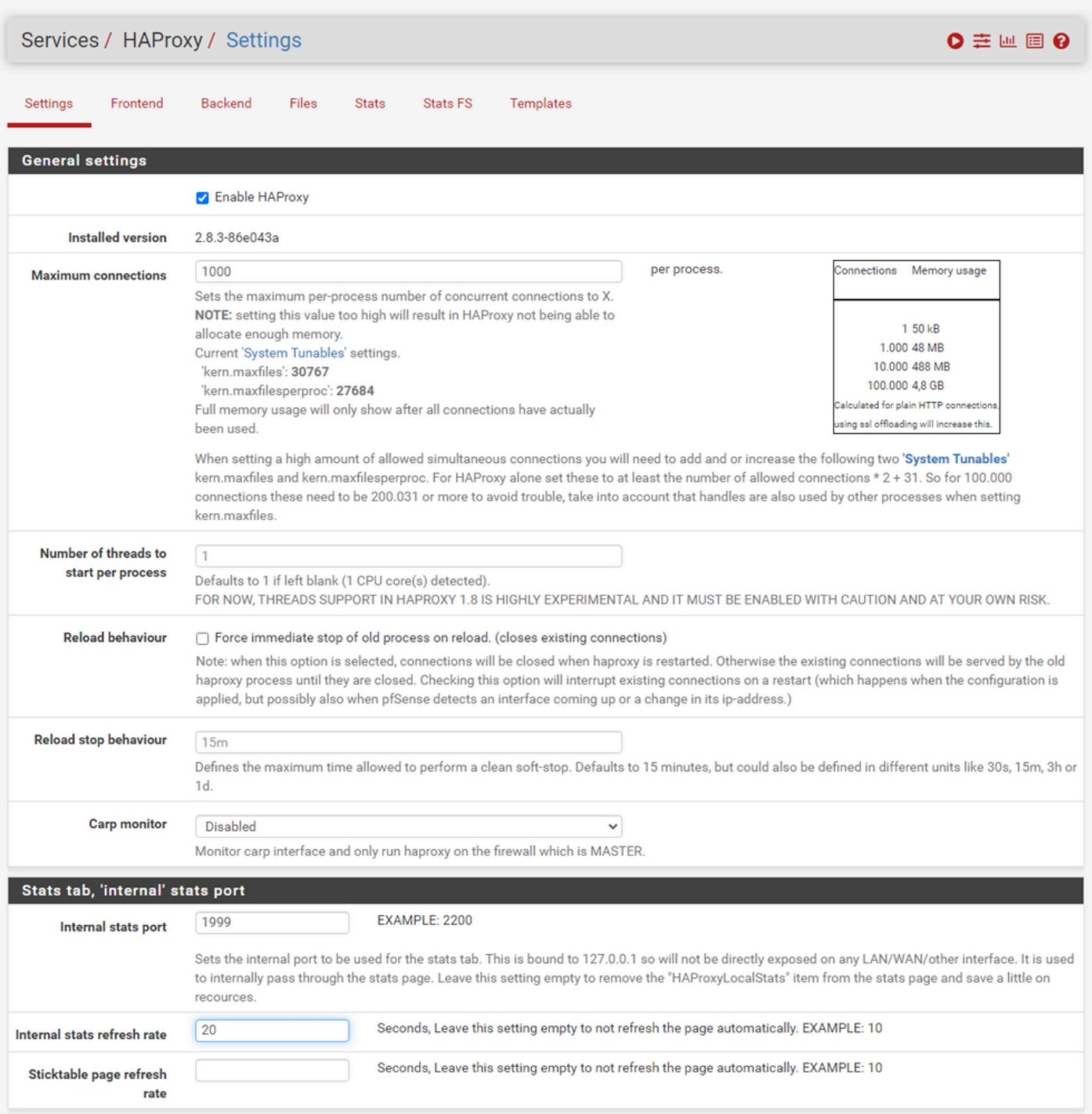
初始DHCProxy设置

步骤1.从Services下拉列表中选择HAProxy



pfSense GUI - HAProxy下拉列表

步骤2.配置基本设置



pfSense GUI - HAProxy主设置

选中Enable HAProxy复选框。

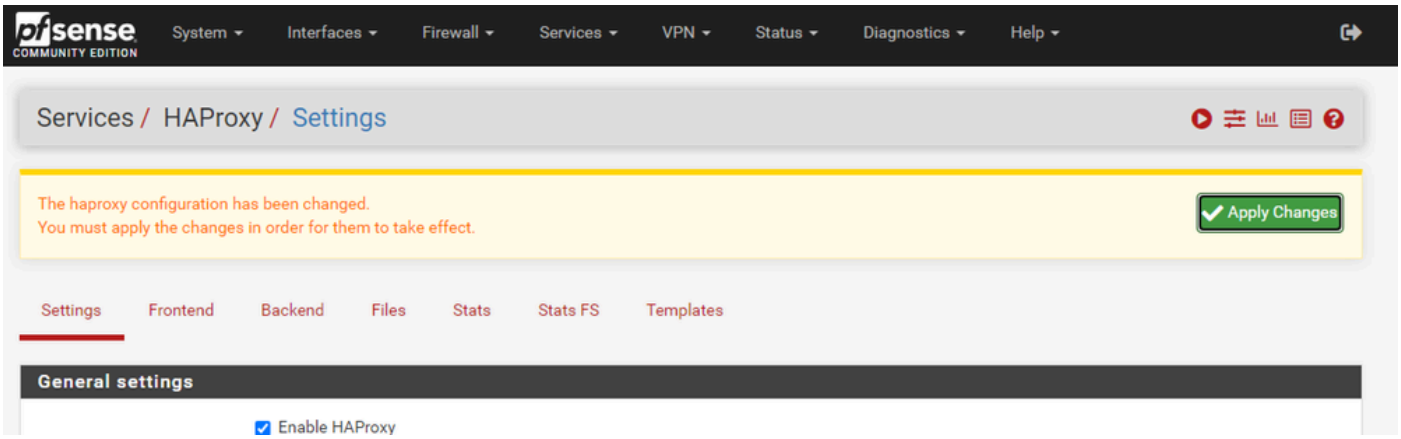
输入最大连接数(Maximum Connections)的值。请参阅本节中的图表以获取有关所需内存的详细信息。

为Internal stats端口输入一个值。此端口用于显示设备上的HAProxy统计信息，但不会在设备外部显示。

输入内部统计刷新率的值。

检查其余配置，并根据您的环境需要进行更新。

选择保存。

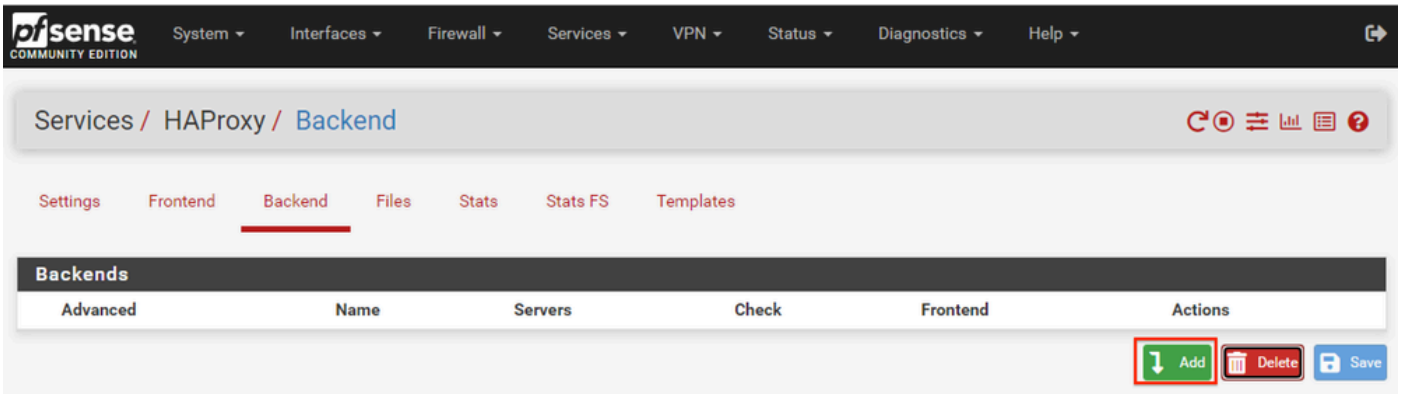


pfSense GUI - HAProxy应用更改

注意：只有选择Apply Changes按钮，配置更改才会激活状态。您可以同时进行多项配置更改并应用它们。配置无需应用即可用于其他部分。

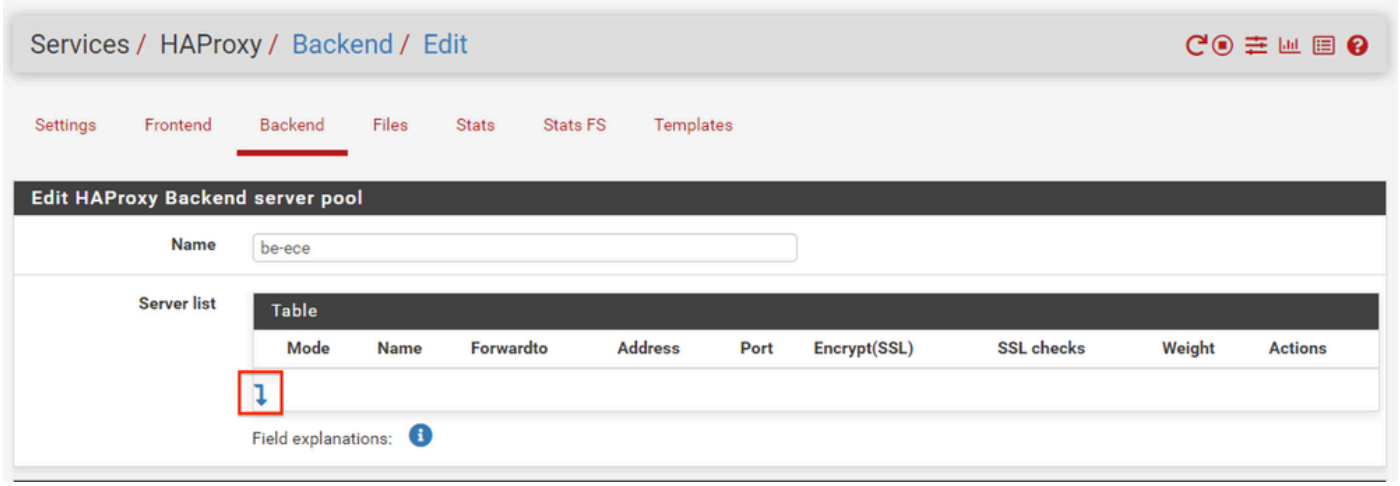
配置HAProxy后端

从后端开始。原因是前端必须引用后端。确保您已选择“后端”菜单。



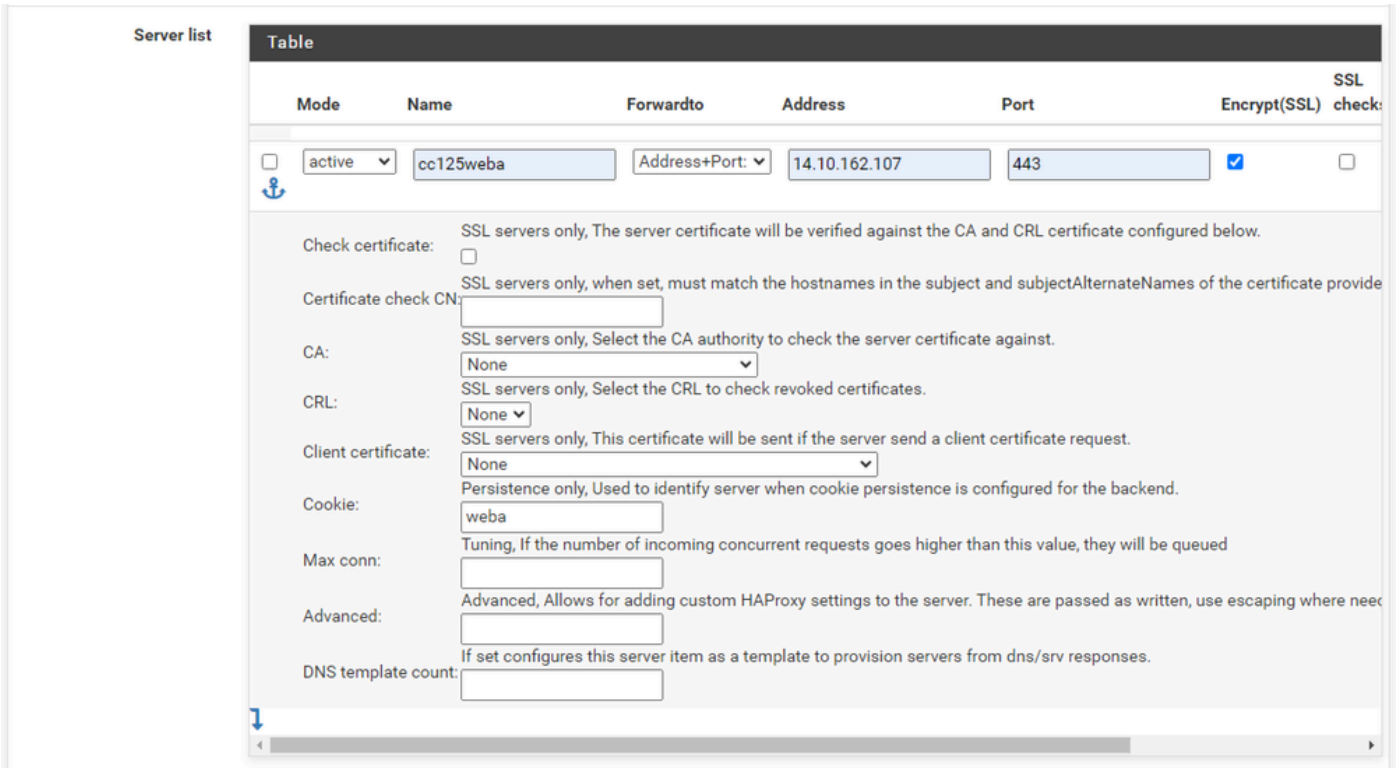
pfSense GUI - HAProxy添加后端

选择Add按钮。



为后端提供名称。

选择向下箭头，将第一个服务器添加到“服务器”列表中



后端 — 服务器列表

提供用于引用服务器的名称。这不需要与实际服务器名称匹配。这是显示在统计信息页面上的名称。

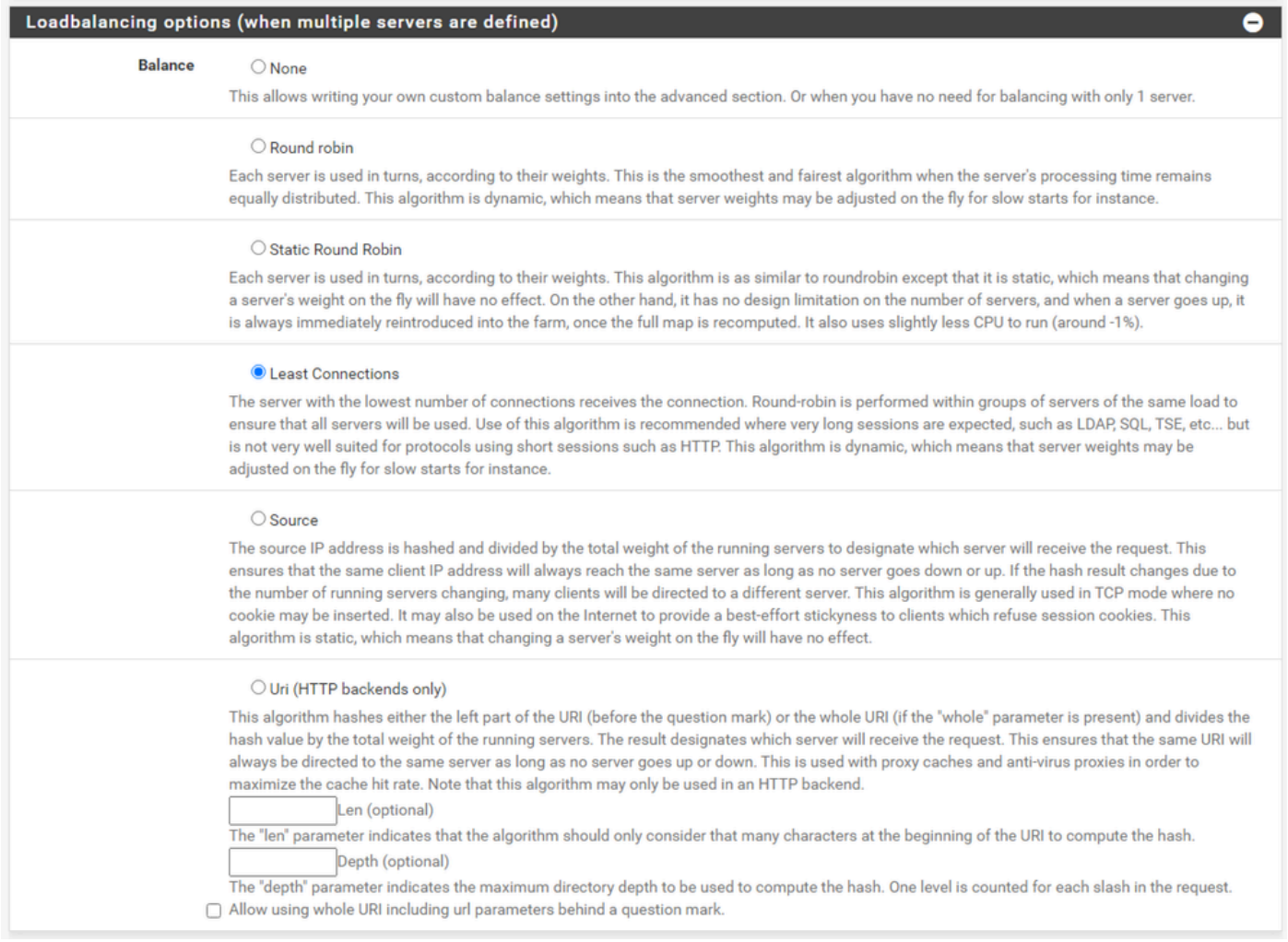
提供服务器的地址。这可以配置为FQDN的IP地址。

提供要连接的端口。这必须为ECE的端口443。

选中Encrypt(SSL)复选框。

在Cookie字段中提供一个值。这是会话粘性Cookie的内容，并且在后端内必须是唯一的。

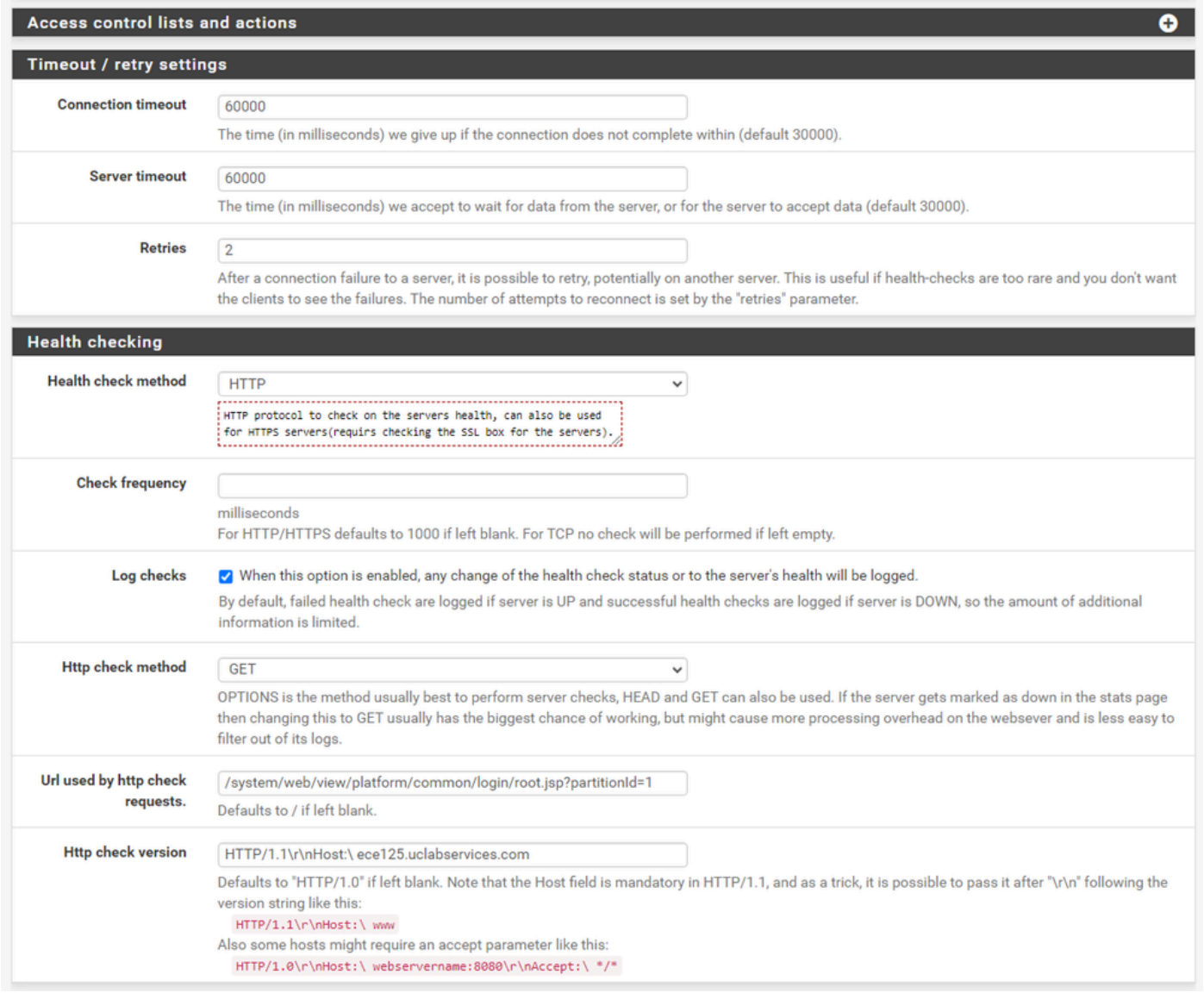
配置完第一个服务器后，选择向下箭头以配置环境中的任何其他Web服务器。



HAProxy后端 — 负载均衡

配置负载均衡选项。

对于ECE服务器，必须将其设置为“最小连接”。



HAProxy后端 — 运行状况检查

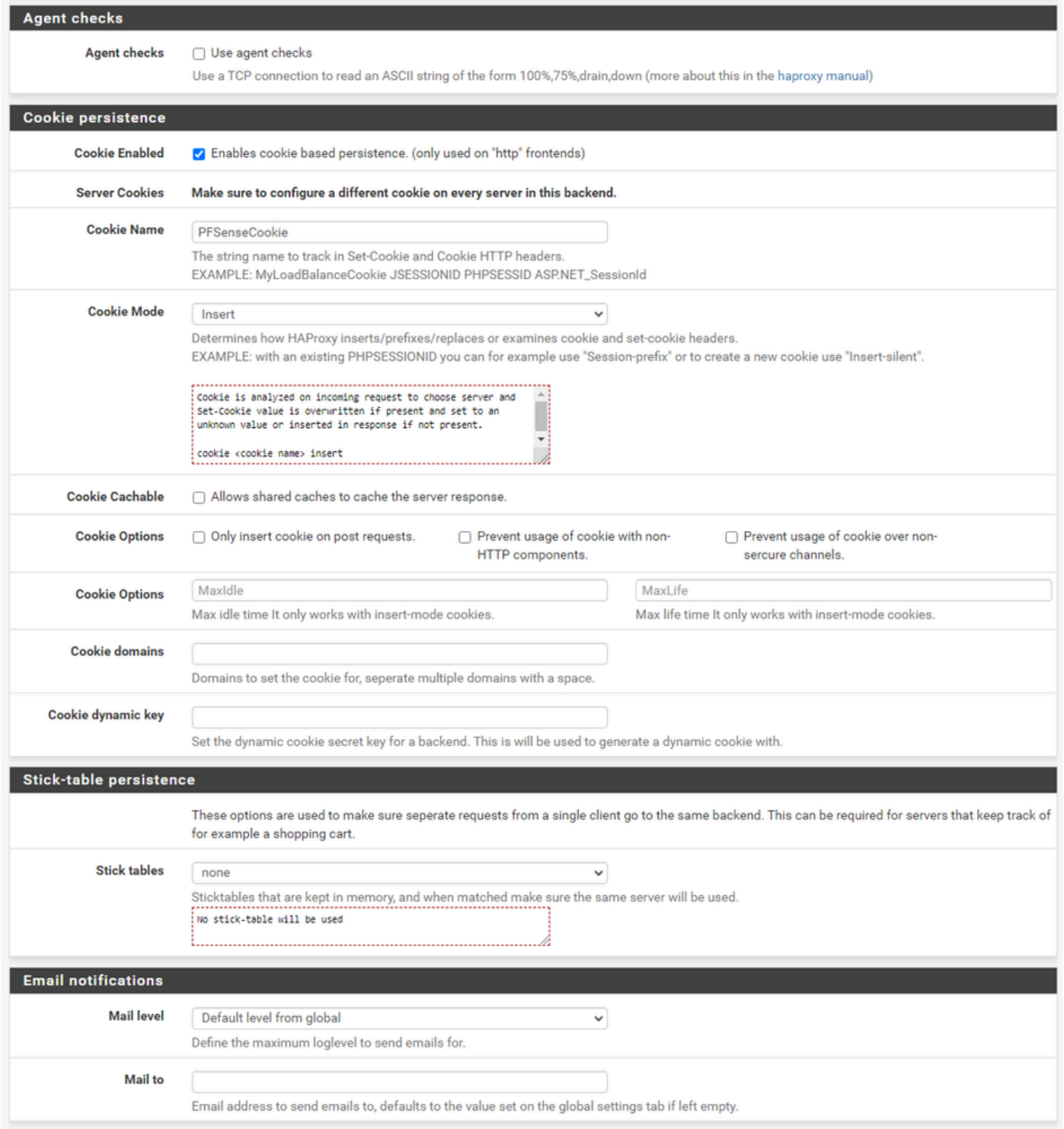
此配置不使用访问控制列表。

超时/重试设置可以保留为其默认配置。

配置运行状况检查部分。

1. 运行状况检查方法：HTTP
2. 检查频率：留空以使用每1秒的默认值。
3. 日志检查：选择此选项可将任何运行状况更改写入日志。
4. Http检查方法：从列表中选择GET。
5. http检查请求使用的URL:对于ECE服务器，请输入 /system/web/view/platform/common/login/root.jsp?partitionId=1
6. HTTP检查版本：输入，HTTP/1.1\r\n\Host:\ {fqdn_of_server}

请确保在最终反斜杠之后但在服务器的FQDN之前包含空格。

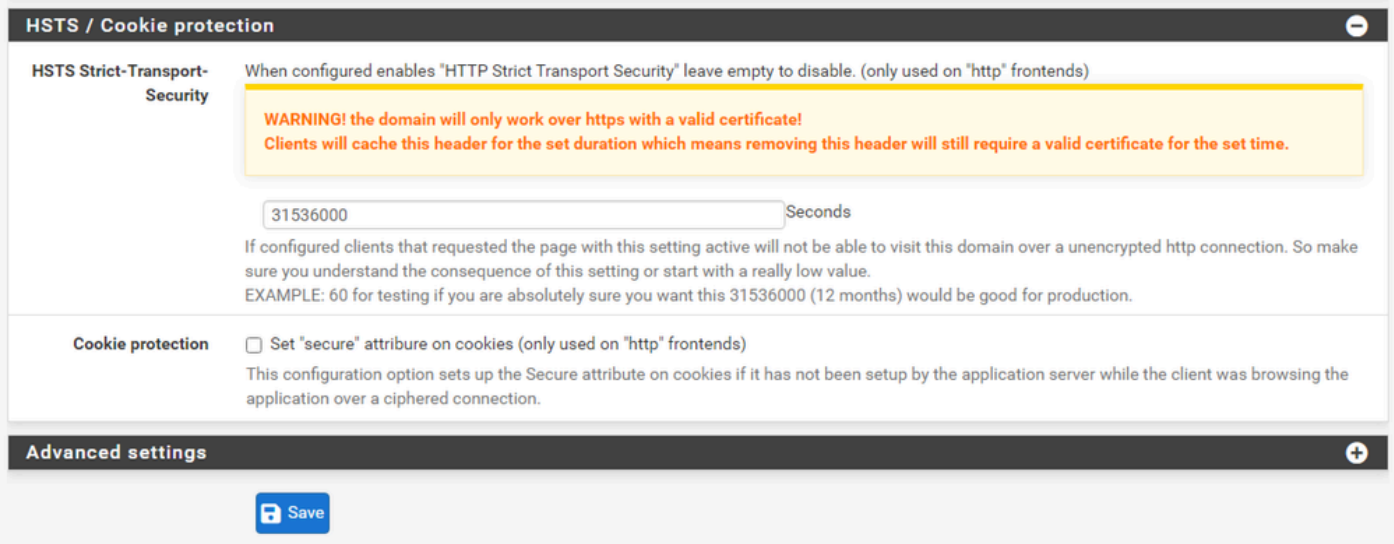


HAProxy后端 — Cookie持久性

取消选中“Agent checks（代理检查）”。

配置Cookie持久性：

1. Cookie已启用：选择以启用基于Cookie的持久性。
2. Cookie名称：为cookie提供名称。
3. Cookie模式：从下拉框中选择“插入”。
4. 取消设置其余选项。



HAProxy后端 — HSTS

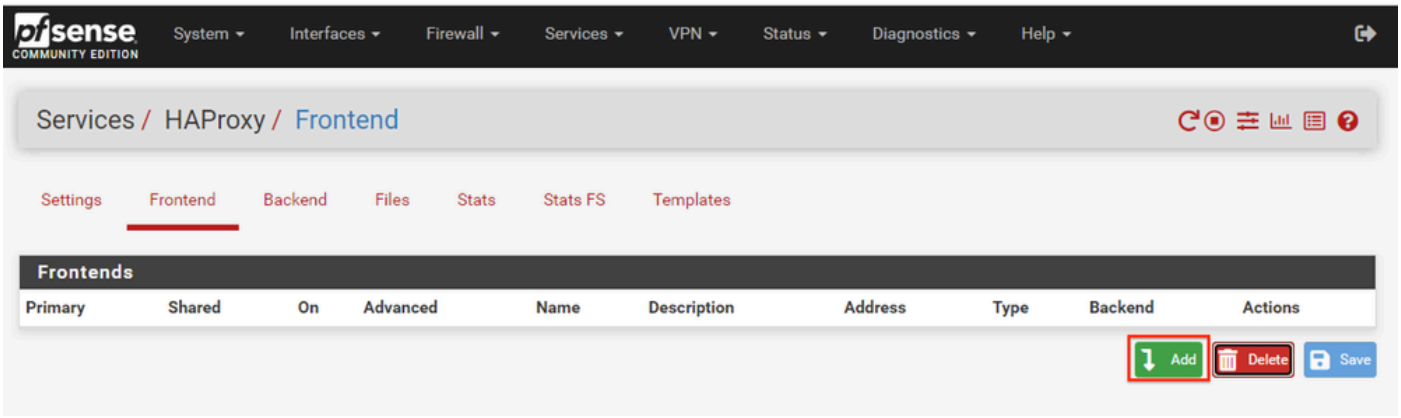
后端配置表单的其余部分可以保留默认设置。

如果要配置HSTS，请在此部分中配置超时值。ECE也插入HSTS Cookie，因此此配置是冗余的。

选择Save。

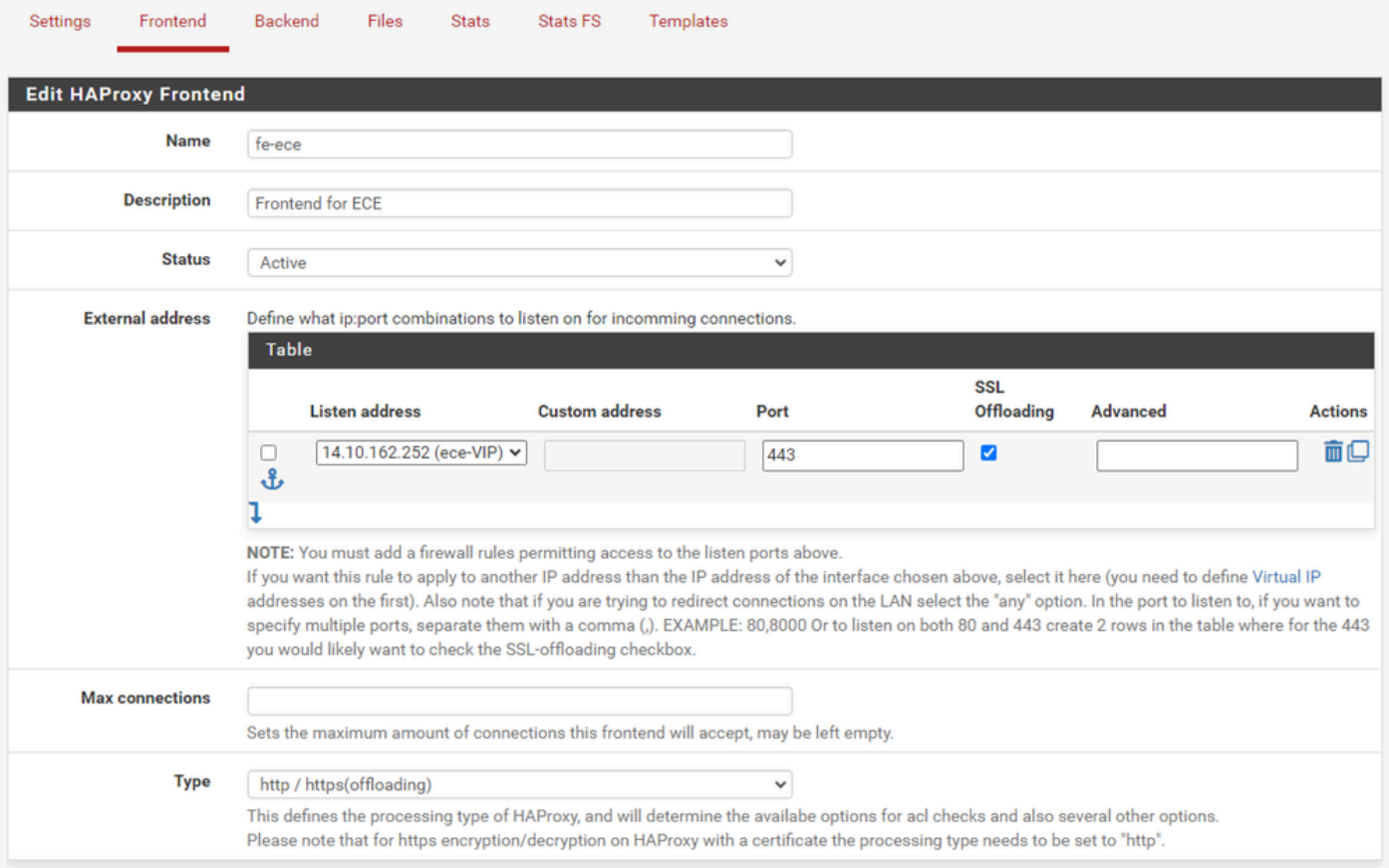
配置HAProxy前端

切换到Frontend菜单。



pfSense GUI - HAProxy添加前端

选择，添加按钮



HAProxy — 前端报头

为前端提供一个名称。

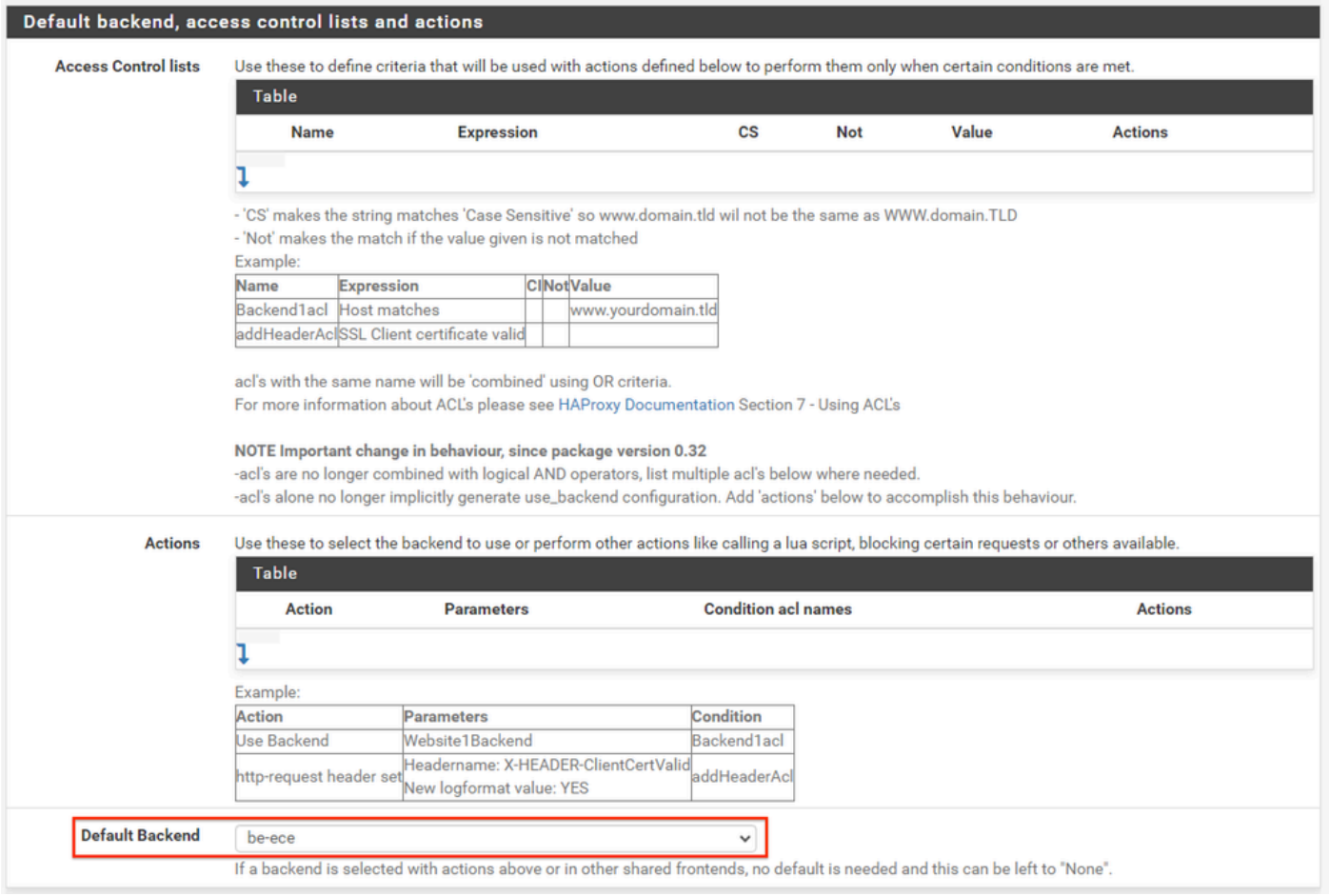
提供说明，以帮助稍后确定前端。

在External address表中：

1. 侦听地址：选择您为此网站创建的VIP。
2. 端口：输入 443。
3. SSL卸载：选择此选项，以便可以插入会话cookie。

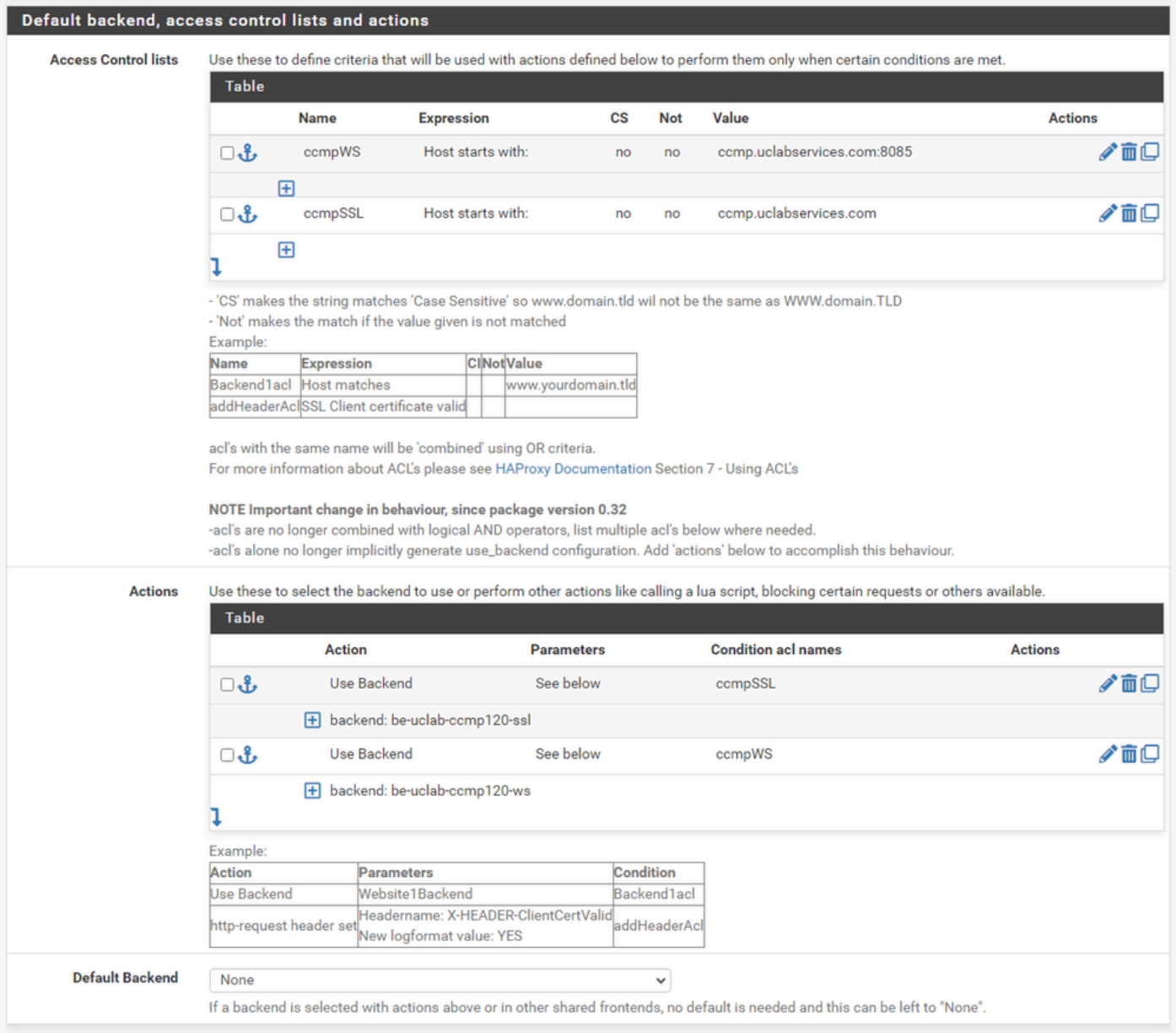
将Max connections留空。

确保Type选择为http / https（卸载）。



HAProxy后端 — 默认后端选择

最简单的配置是从下拉列表中选择默认后端。当VIP托管一个网站时，可以选择此选项。

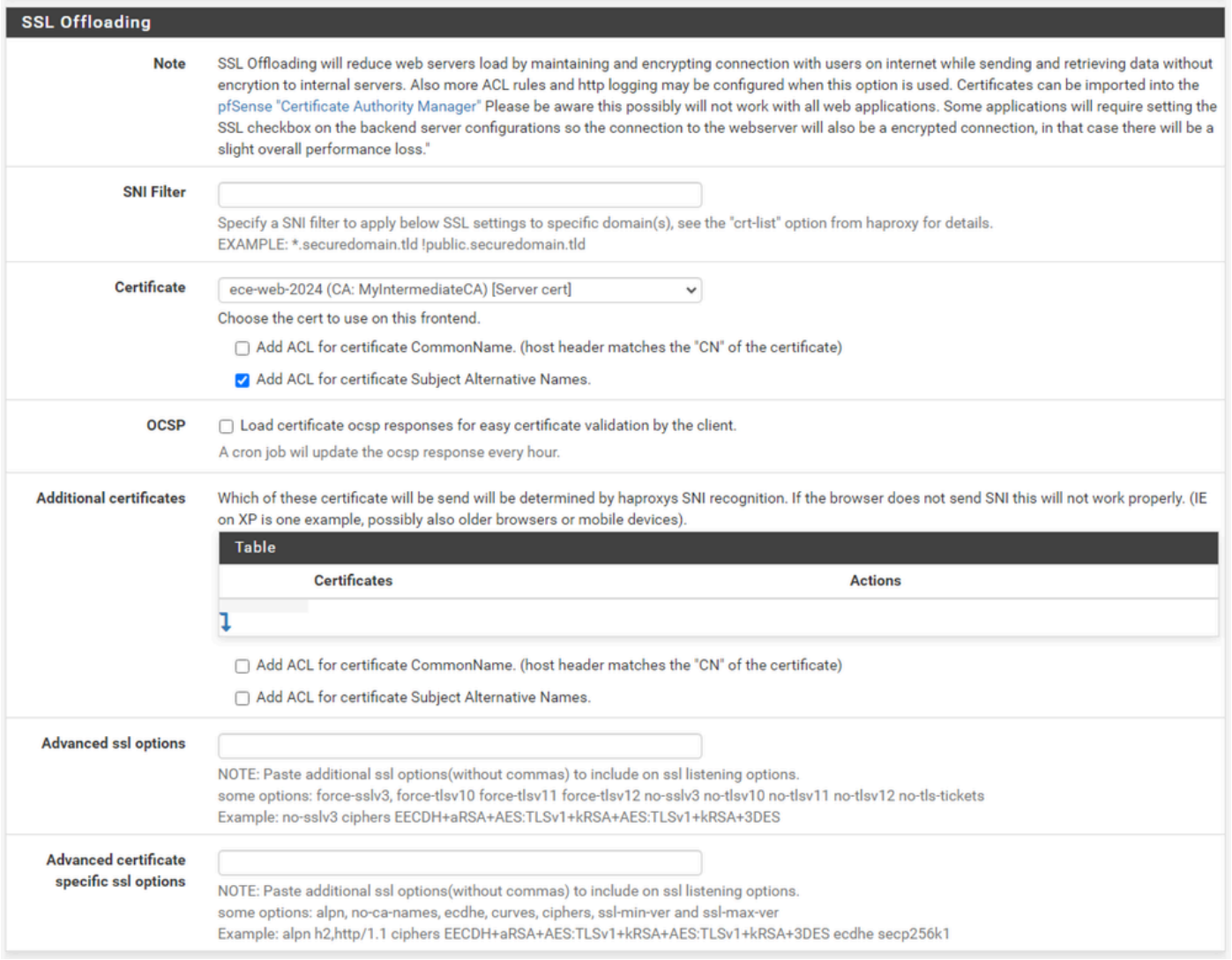


HAProxy后端 — ACL高级

如图所示，ACL可用于根据情况将单个前端重定向到多个后端。

您可以看到ACL会检查请求中的主机是否以名称和端口号开头。或者只是名字。基于此，使用特定的后端。

这在欧洲经委会中并不常见。



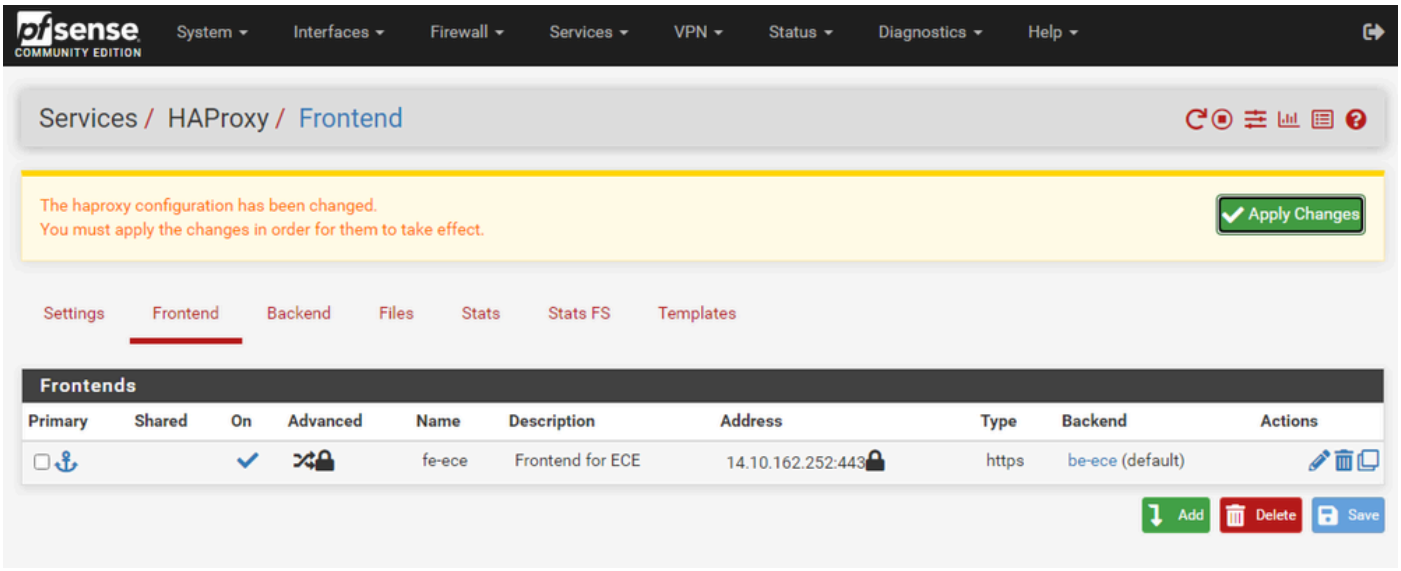
HAProxy前端 — 证书绑定

在SSL Offloading部分中，选择要用于此站点的证书。此证书必须是服务器证书。

选择选项Add ACL for certificate Subject Alternative Names。

您可以将其余选项保留为其默认值。

选择保存，在此表单的末尾。



HAProxy — 应用配置

选择Apply Changes将前端和后端更改提交到运行配置。

祝贺您，您已完成pfSense的设置和配置。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。