为ECE配置pfSense社区负载均衡器

目录

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。

第二步：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安装到虚拟机

第二步：打开VM电源，然后按照提示进行安装。

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：本文档显示的是在单臂模式下配置的设备。

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。

第二步：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。

第三步：分配LAN接口

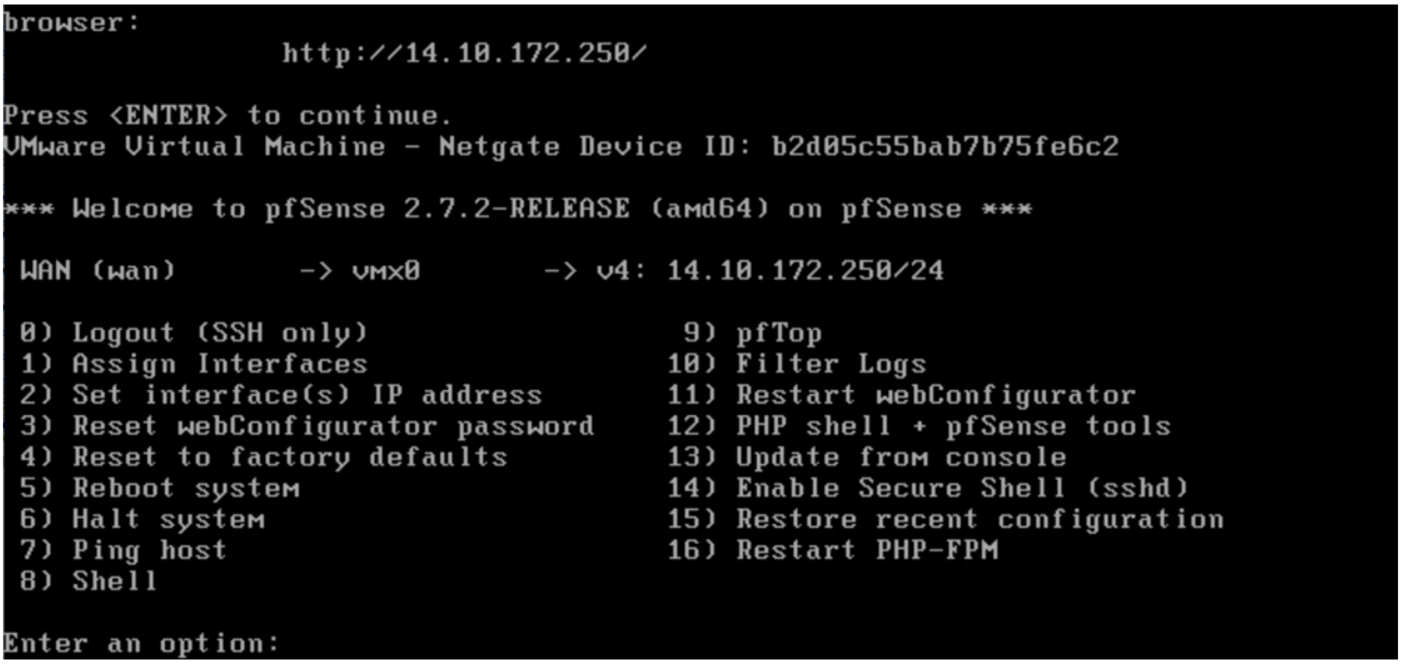
LAN接口是双臂模式下设备的安全端。如果需要，请在提示时输入接口名称。

第四步：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。

第五步：为管理接口分配IP地址

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。



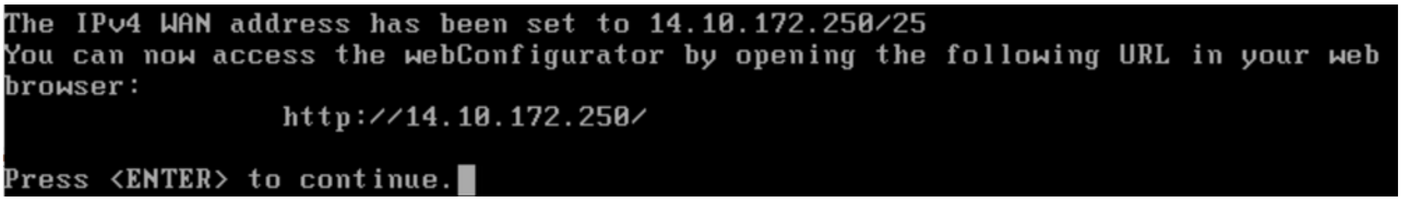
```
browser:
               http://14.10.172.250/

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。



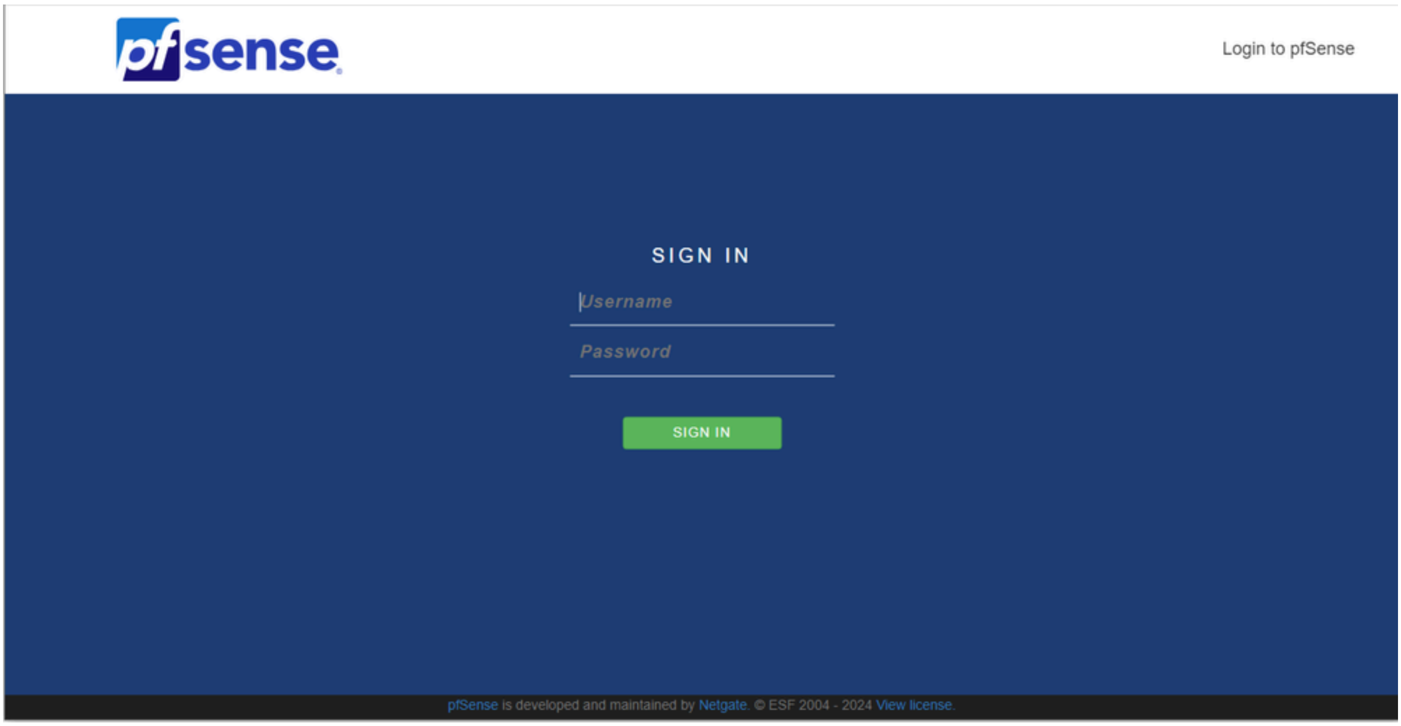
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
               http://14.10.172.250/

Press <ENTER> to continue.
```

pfSense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。



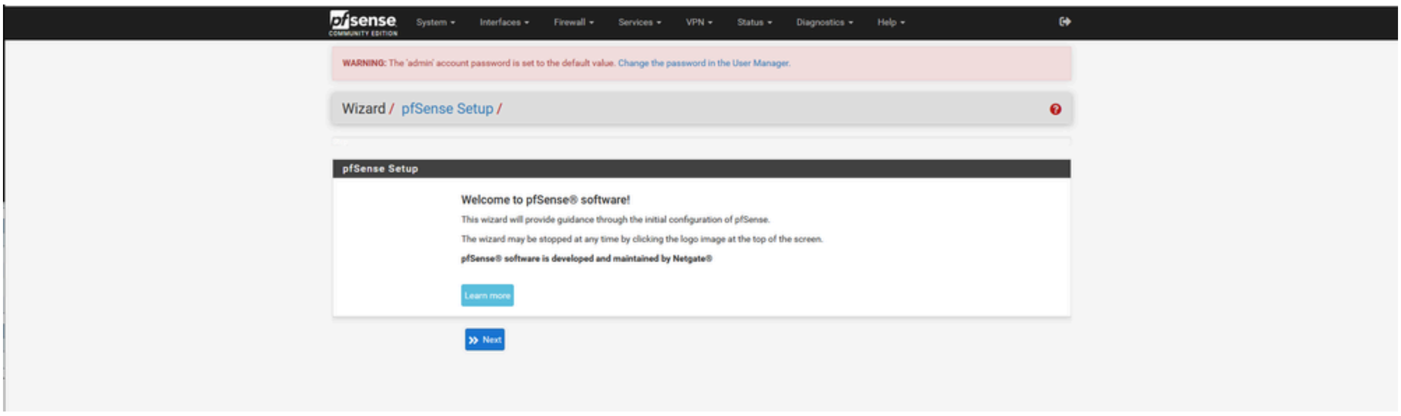
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

pfSense管理员登录

第二步：使用默认登录名admin / pfSense登录

第三步：完成初始设置

单击前两个屏幕中的“下一步”。



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

Wizard / pfSense Setup /

pfSense Setup

Welcome to pfSense® software!

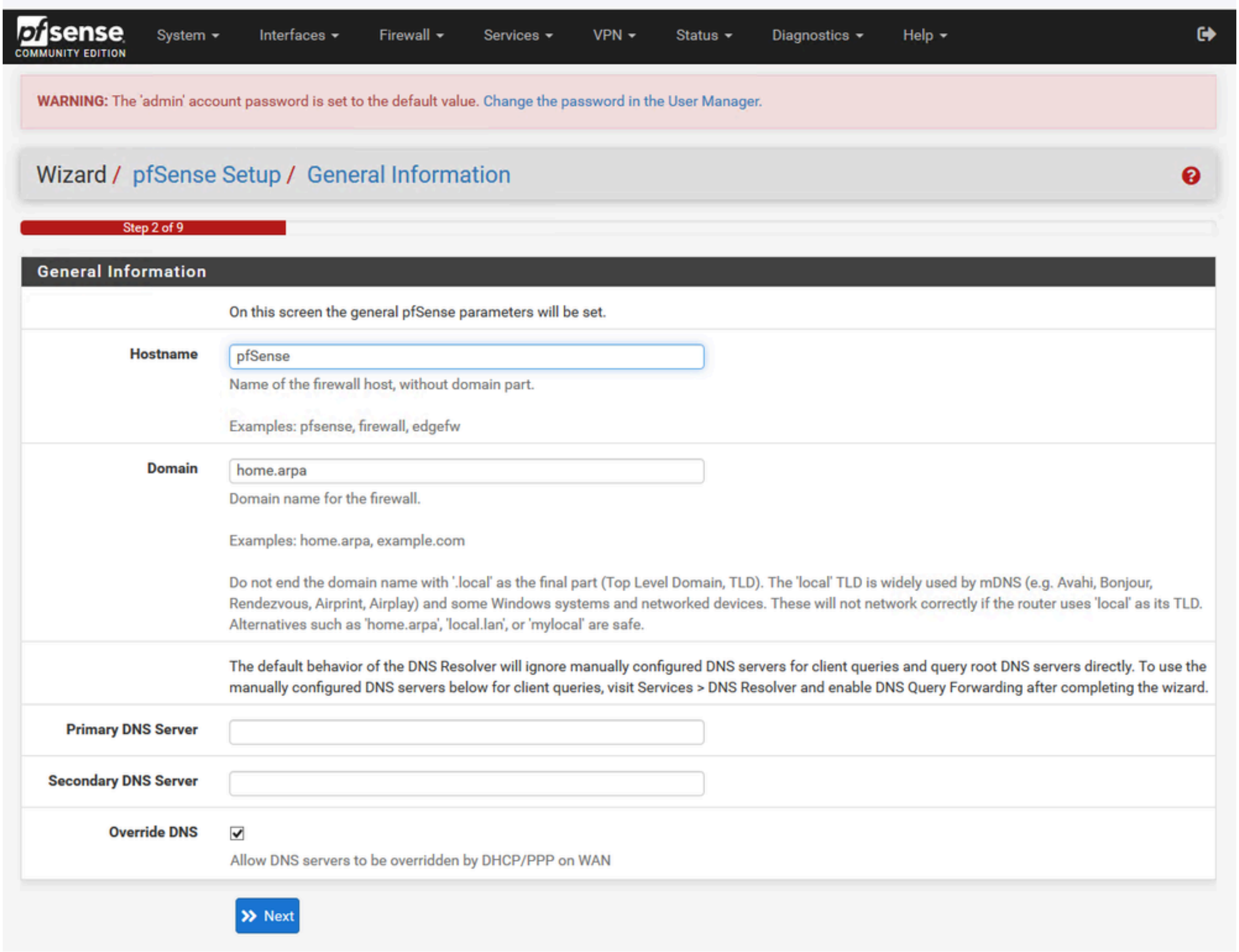
This wizard will provide guidance through the initial configuration of pfSense.

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

pfSense® software is developed and maintained by Netgate®

pfSense安装向导 — 1

提供主机名、域名和DNS服务器信息。



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

Wizard / pfSense Setup / General Information

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain: home.arpa
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:

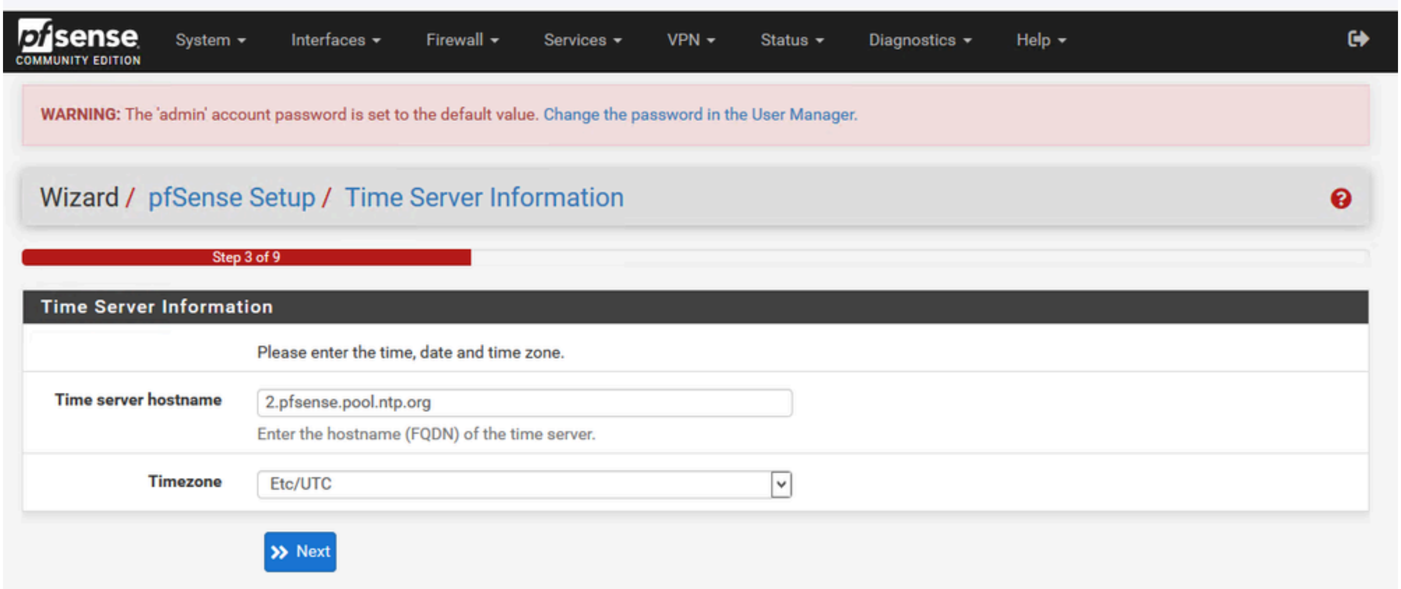
Secondary DNS Server:

Override DNS: ☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

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。



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

Wizard / pfSense Setup / Time Server Information

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Etc/UTC

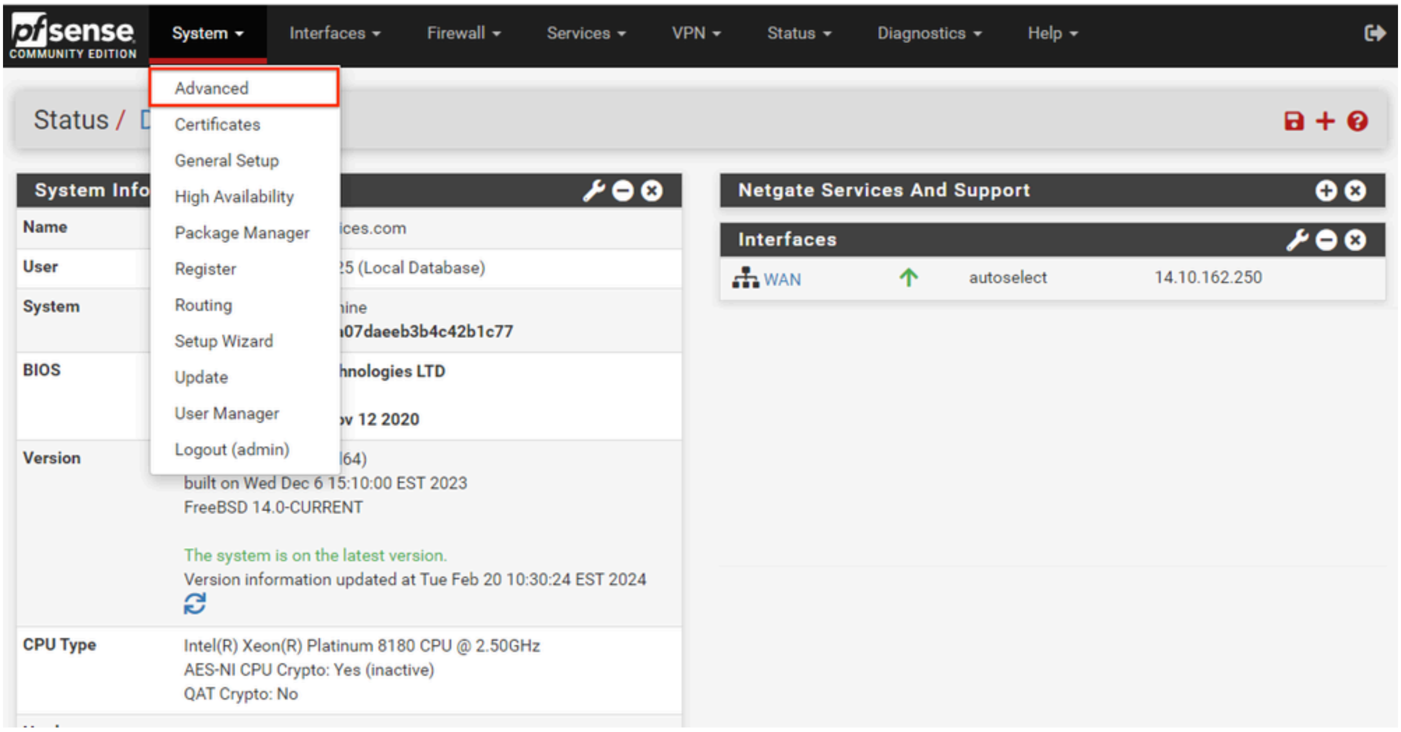
pfSense安装向导 — 3

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

第二步：从系统下拉菜单中选择高级

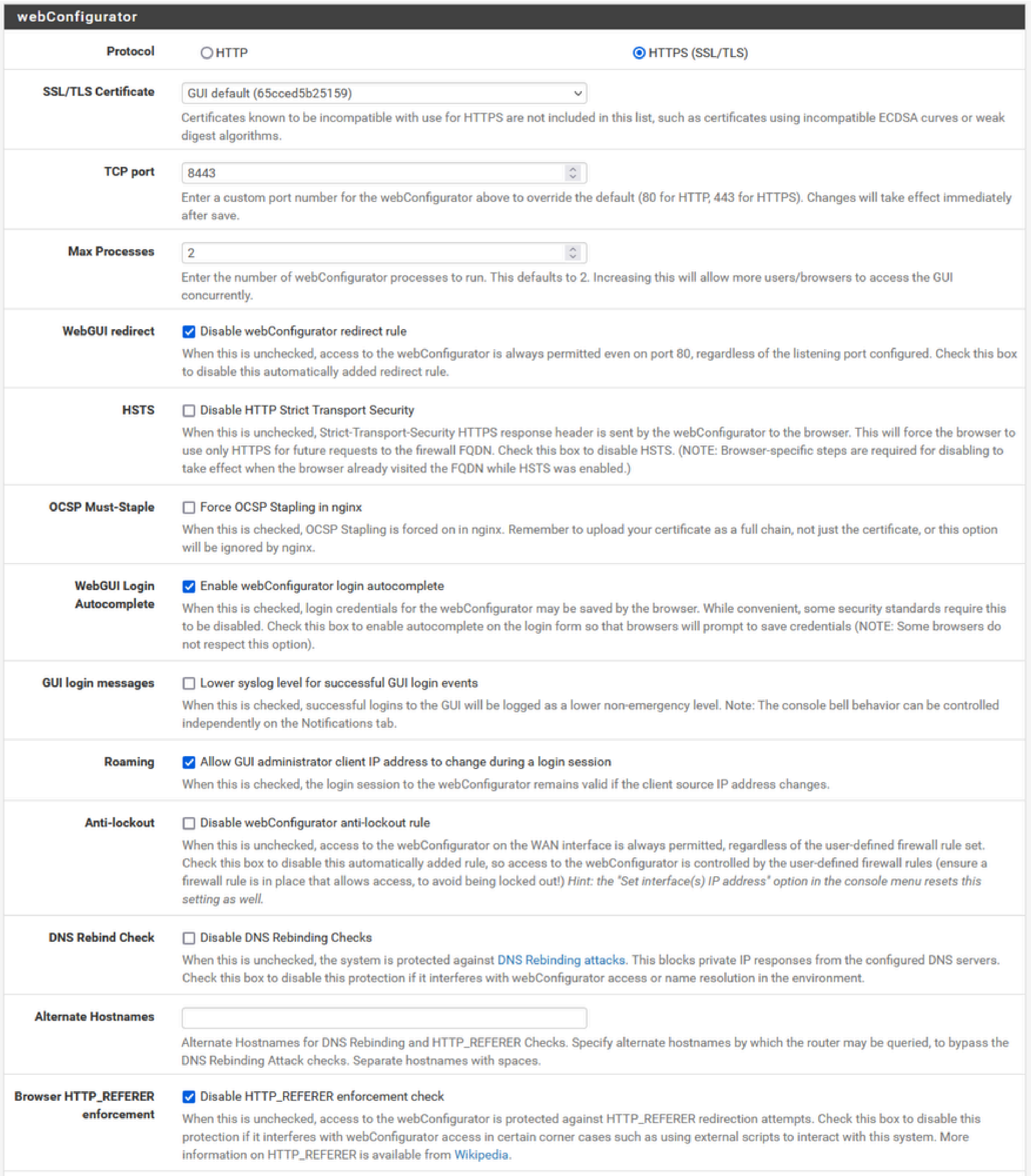


Name	ices.com
User	25 (Local Database)
System	ine 07daeeb3b4c42b1c77
BIOS	hnologies LTD v 12 2020
Version	64) built on Wed Dec 6 15:10:00 EST 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 10:30:24 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180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

WAN	↑	autoselect	14.10.162.250

pfSense GUI — 管理员下拉列表

第三步：更新WebConfigurator设置



webConfigurator

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

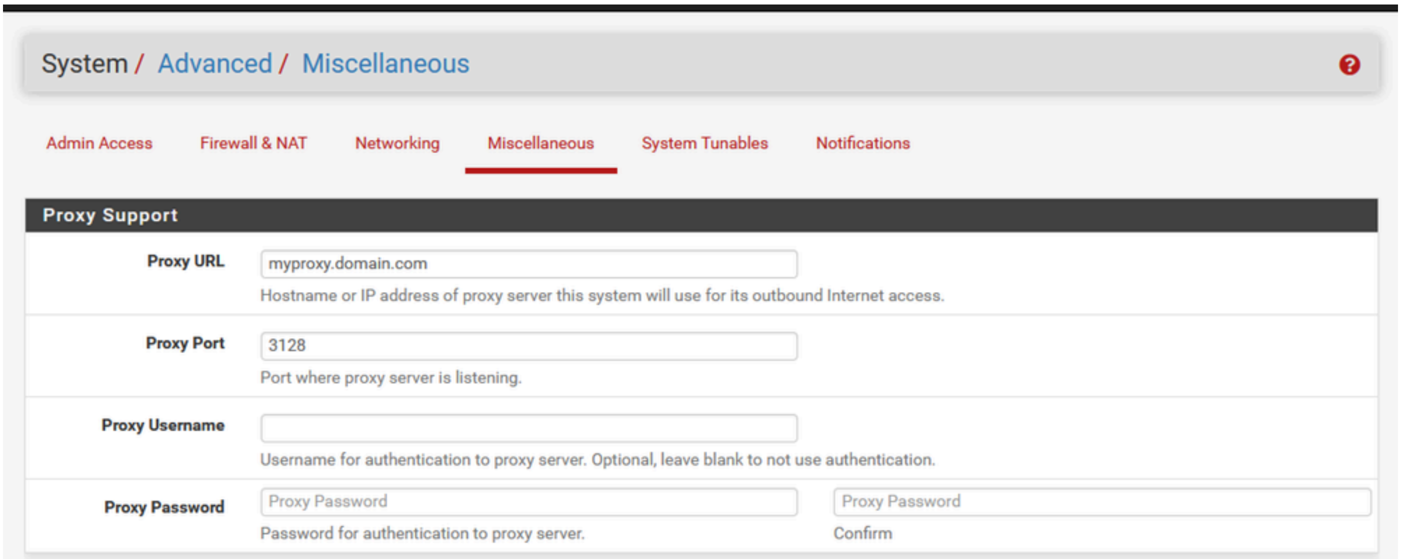
pfSense GUI — 管理员配置

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：请确保在继续操作之前,选择“保存”按钮。然后您将重定向到新的https链接。

第四步：配置代理服务器（如果需要）

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。



Proxy Support

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

Proxy Port: 3128
Port where proxy server is listening.

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

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

pfSense GUI — 代理配置

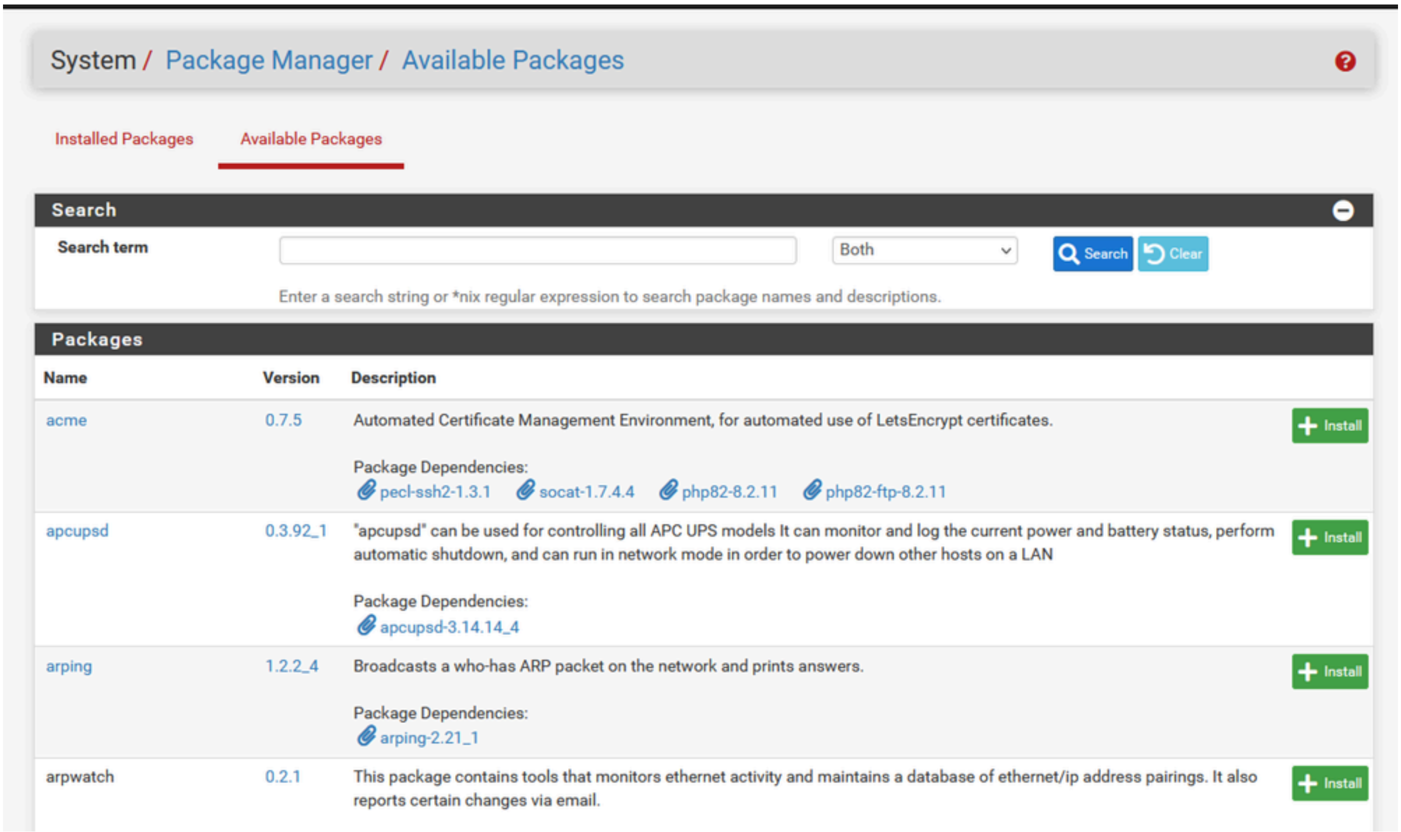
注：请确保在进行更改后选择Save按钮。

添加所需的包

步骤1:选择系统>包管理器

第二步：选择可用包

注：加载所有可用软件包可能需要几分钟的时间。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。



System / Package Manager / Available Packages

Installed Packages | Available Packages

Search

Search term: Both | Search | Clear

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

Packages

Name	Version	Description	
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11	+ Install
apcupsd	0.3.92_1	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Package Dependencies: apcupsd-3.14.14_4	+ Install
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arping-2.21_1	+ Install
arpwatch	0.2.1	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	+ Install

pfSense GUI — 软件包列表

第三步：查找并安装所需的软件包

1. haproxy
2. Open-VM工具

注：请勿选择haproxy-level包。

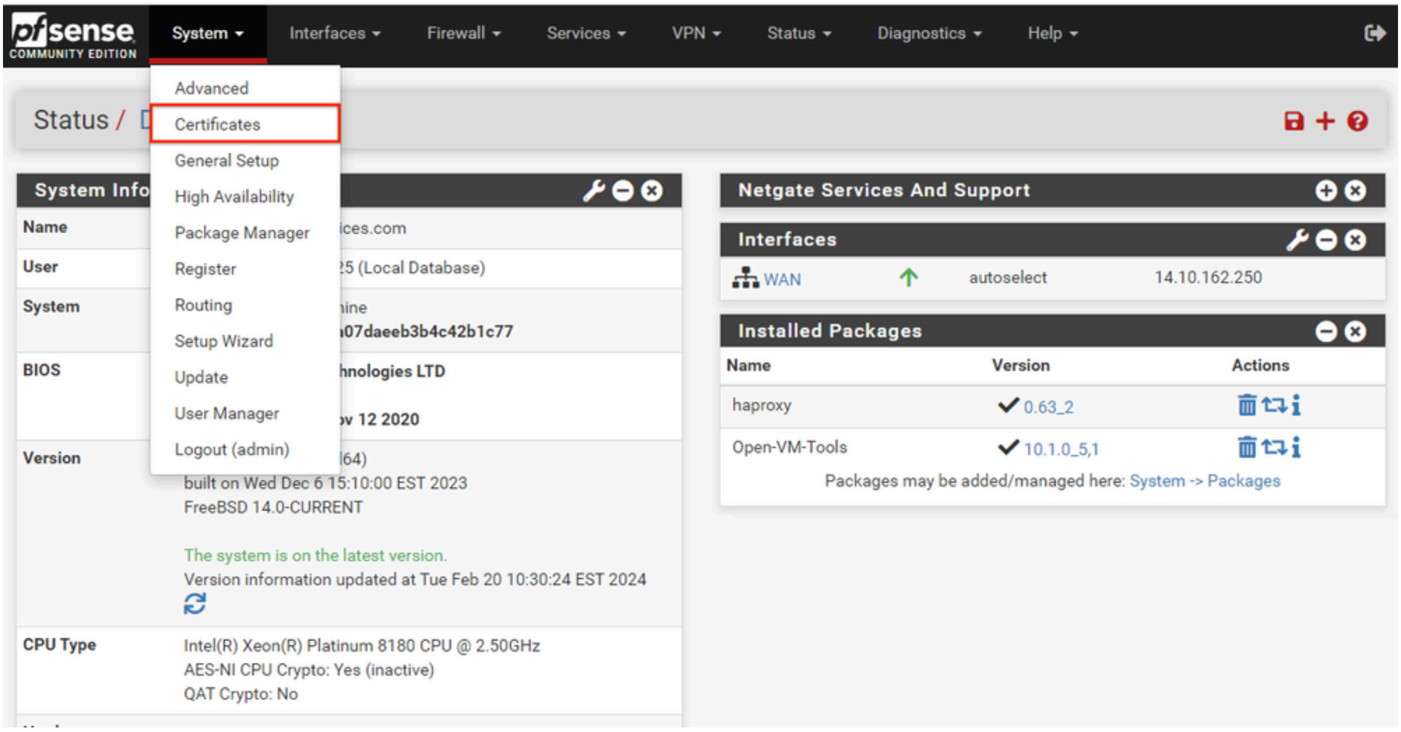
配置证书

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:从系统下拉菜单中选择证书



System Info

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

Netgate Services And Support

Interfaces

WAN	↑	autoselect	14.10.162.250

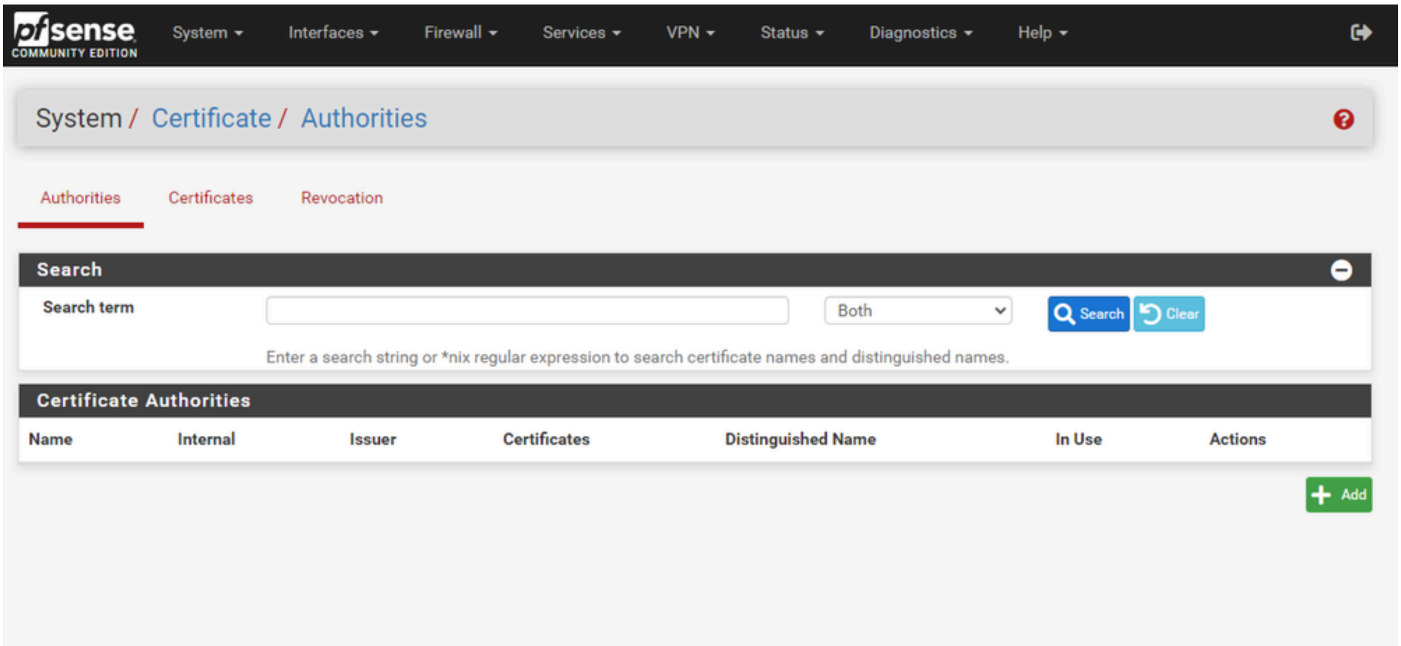
Installed Packages

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

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

pfSense GUI — 证书下拉列表

第二步：导入CA根证书



System / Certificate / Authorities

Search

Search term [ ] Both

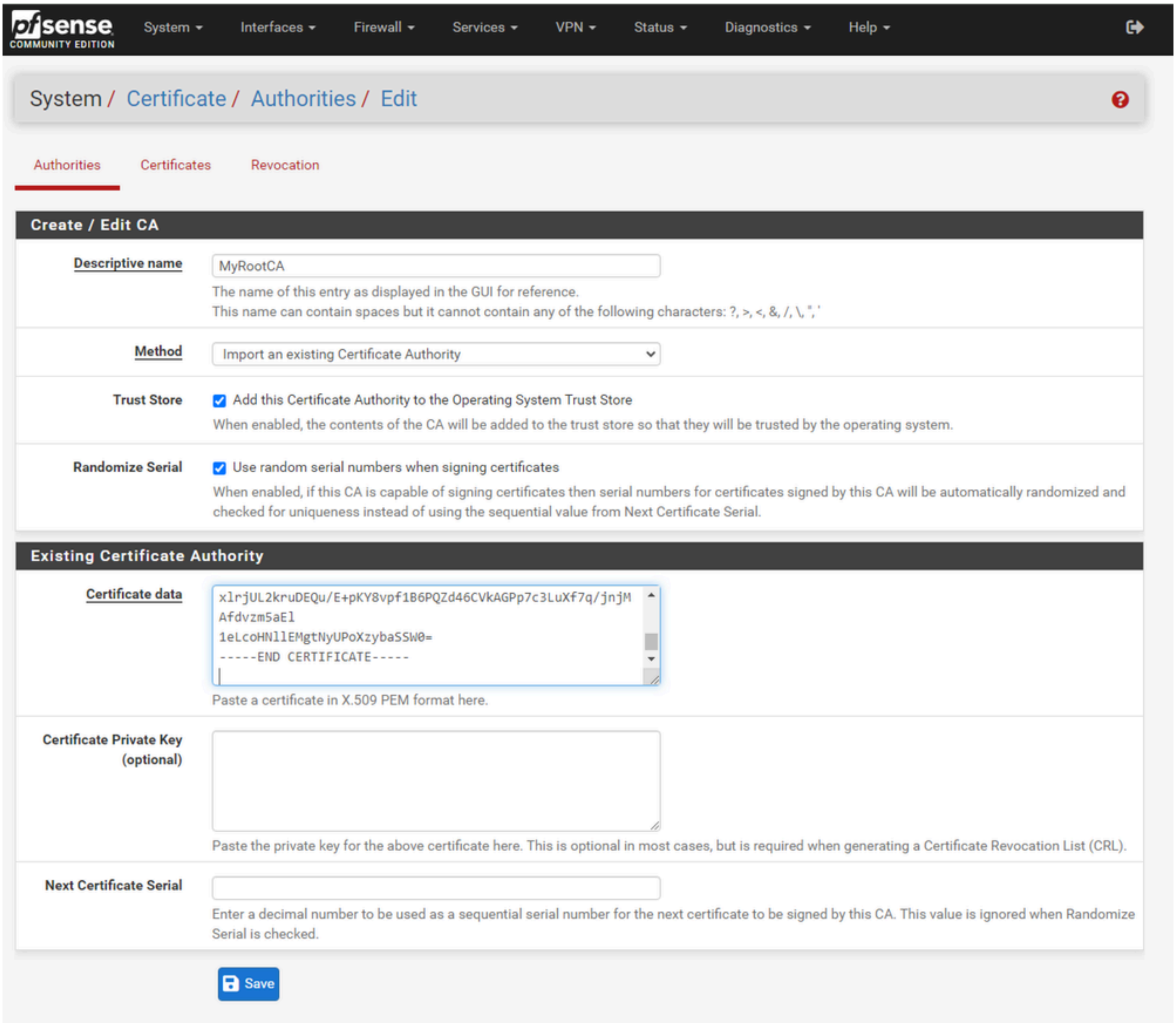
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

pfSense GUI - CA证书列表

选择Add按钮。



System / Certificate / Authorities / Edit

Create / Edit CA

Descriptive name: MyRootCA

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

Method: Import an existing Certificate Authority

Trust Store: ☑ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: ☑ Use random serial numbers when signing certificates

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

Existing Certificate Authority

Certificate data:

```
xlrjUL2kruDEQu/E+pKY8vpf1B6PQZd46CVkAGPp7c3LuXf7q/jnjM
Afdvzm5aEl
1eLcoHNllEMgtNyUPoXzybaSSW0=
-----END CERTIFICATE-----
```

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional):

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

Next Certificate Serial:

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

pfSense GUI - CA导入

如图所示:

1.提供唯一的描述性名称

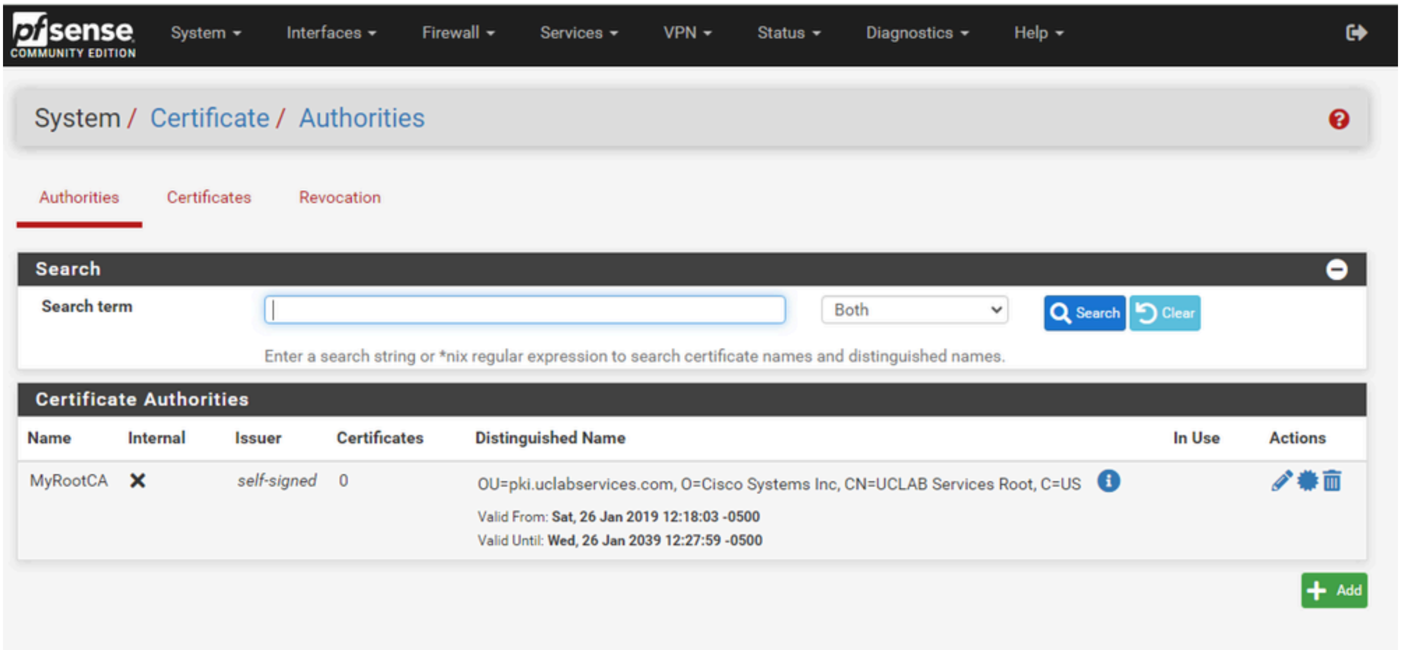
2.从“方法”下拉列表中选择“导入现有证书颁发机构”。

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。



System / Certificate / Authorities

Search

Search term: Both

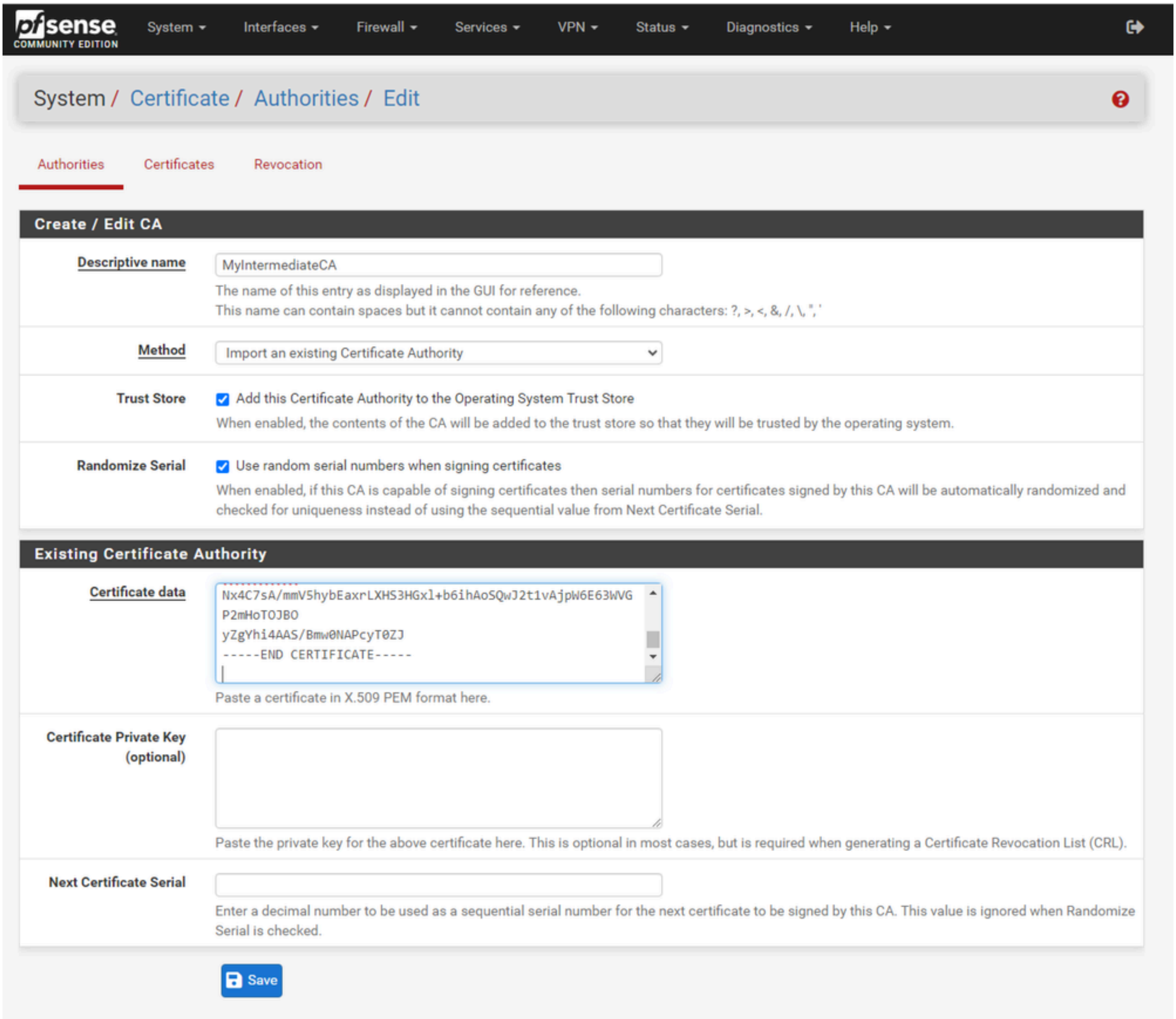
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

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

pfSense GUI - CA列表

第三步：导入CA中间证书



System / Certificate / Authorities / Edit

Create / Edit CA

Descriptive name: MyIntermediateCA

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

Method: Import an existing Certificate Authority

Trust Store: ☑ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: ☑ Use random serial numbers when signing certificates

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

Existing Certificate Authority

Certificate data:

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

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional):

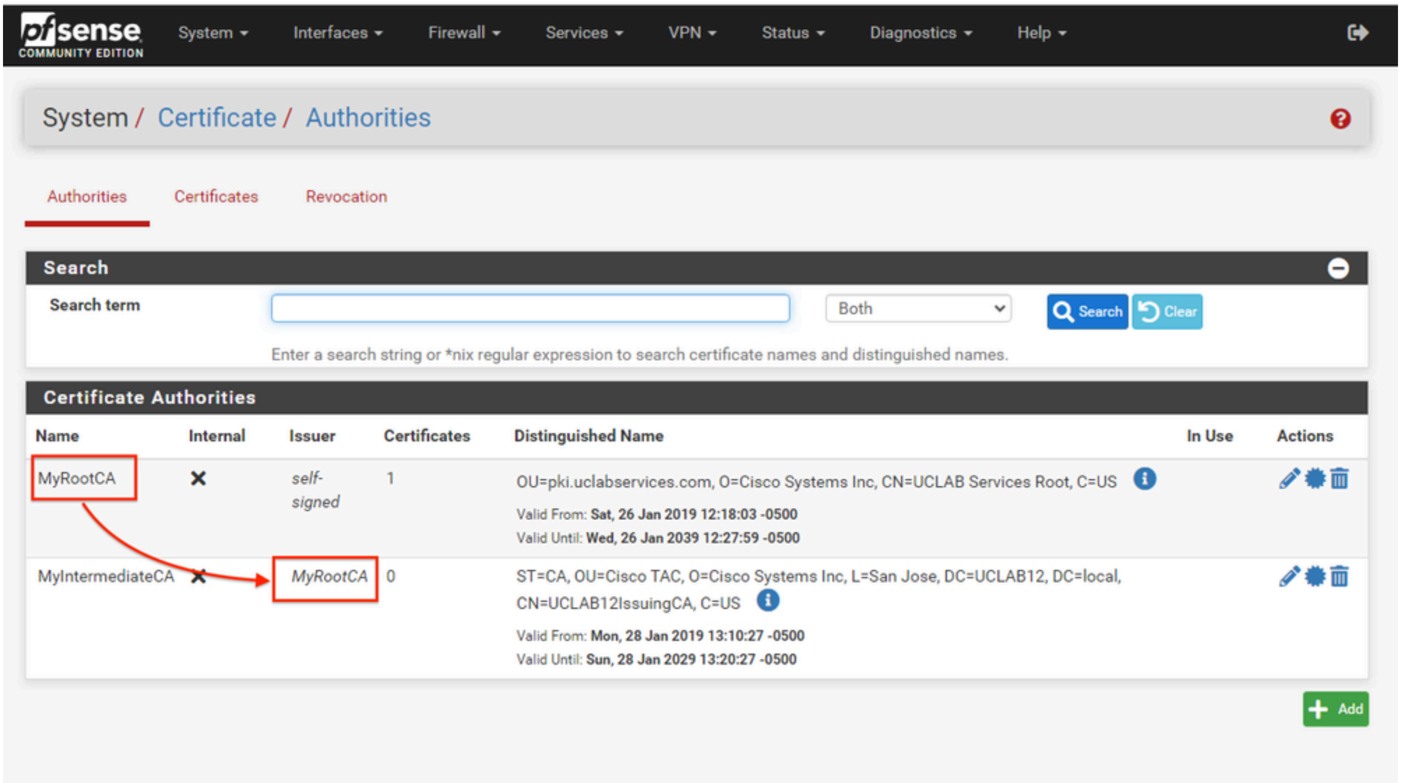
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial:

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

pfSense GUI - CA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。



System / Certificate / Authorities

Search term

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

Certificate Authorities

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

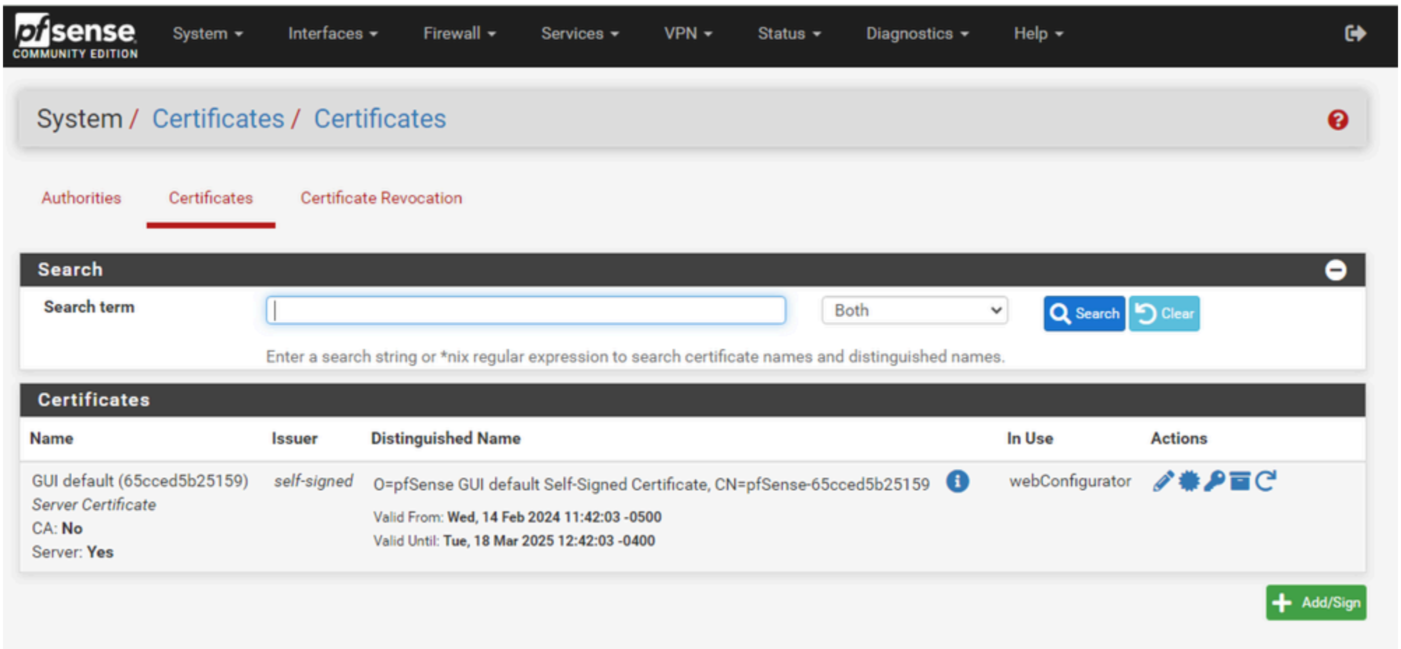
pfSense GUI - CA链接

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。

第四步：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。



System / Certificates / Certificates

Search term

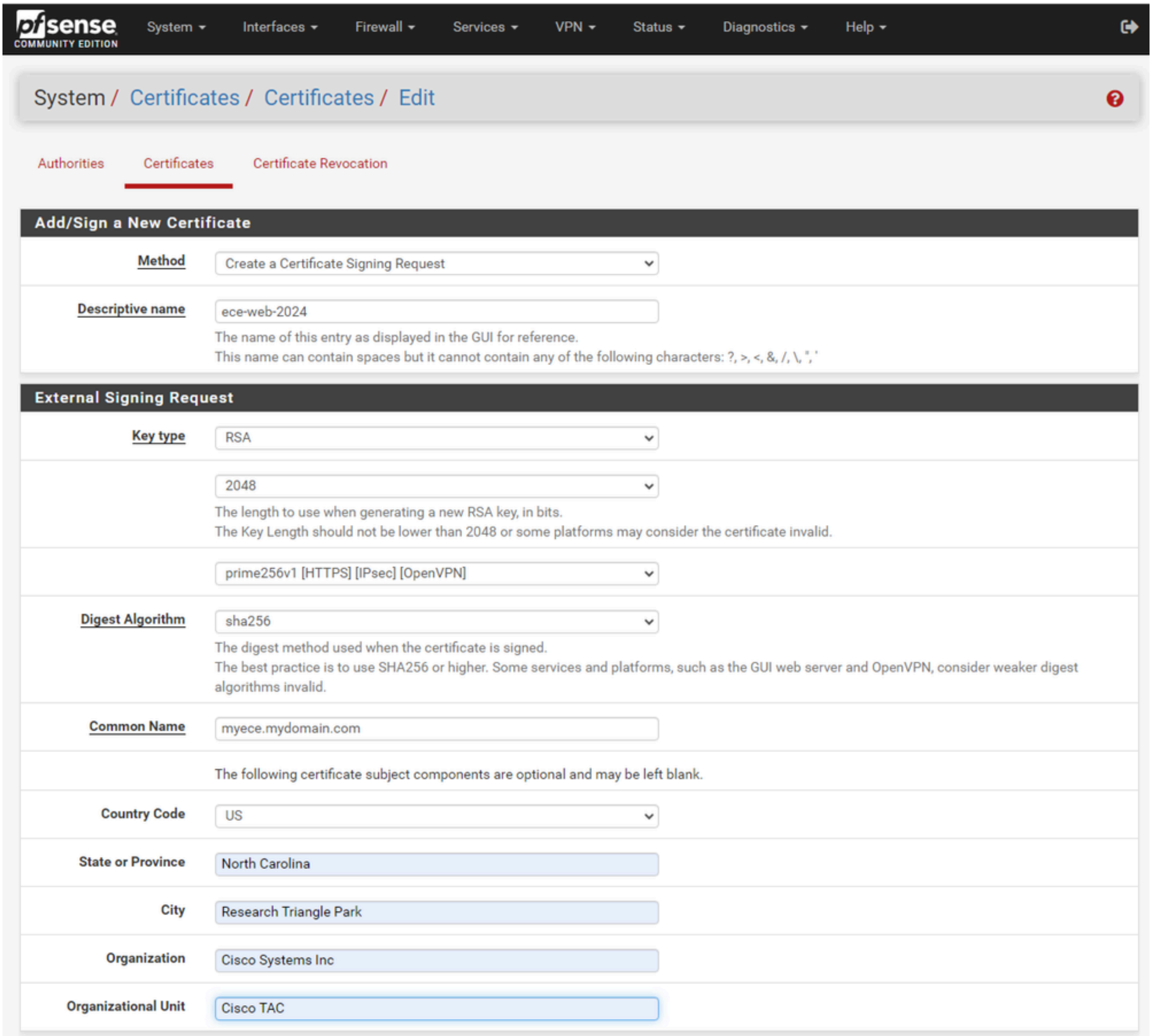
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

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

pfSense GUI — 证书列表

2.填写证书签名请求表。



System / Certificates / Certificates / Edit

Authorities | Certificates | Certificate Revocation

Add/Sign a New Certificate

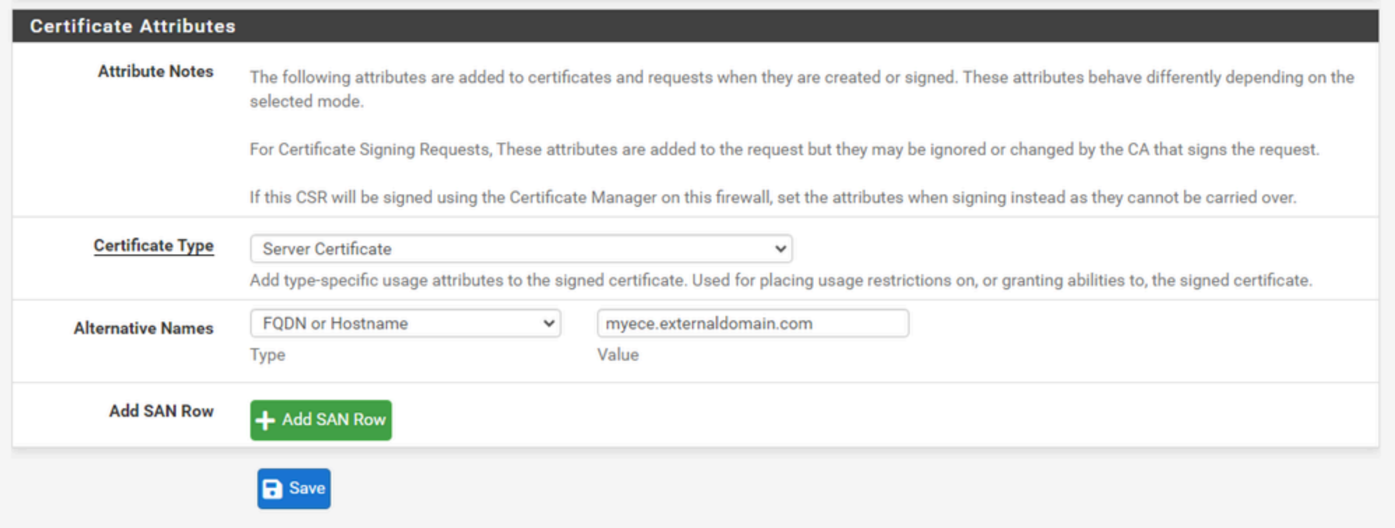
Method	Create a Certificate Signing Request
Descriptive name	ece-web-2024 The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

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创建

- 方法：从下拉列表中选择创建证书签名请求
- 描述性名称：为证书提供一个名称
- 密钥类型和摘要算法：查看以确保它们符合您的要求
- Common Name：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



Certificate Attributes

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

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

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

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

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

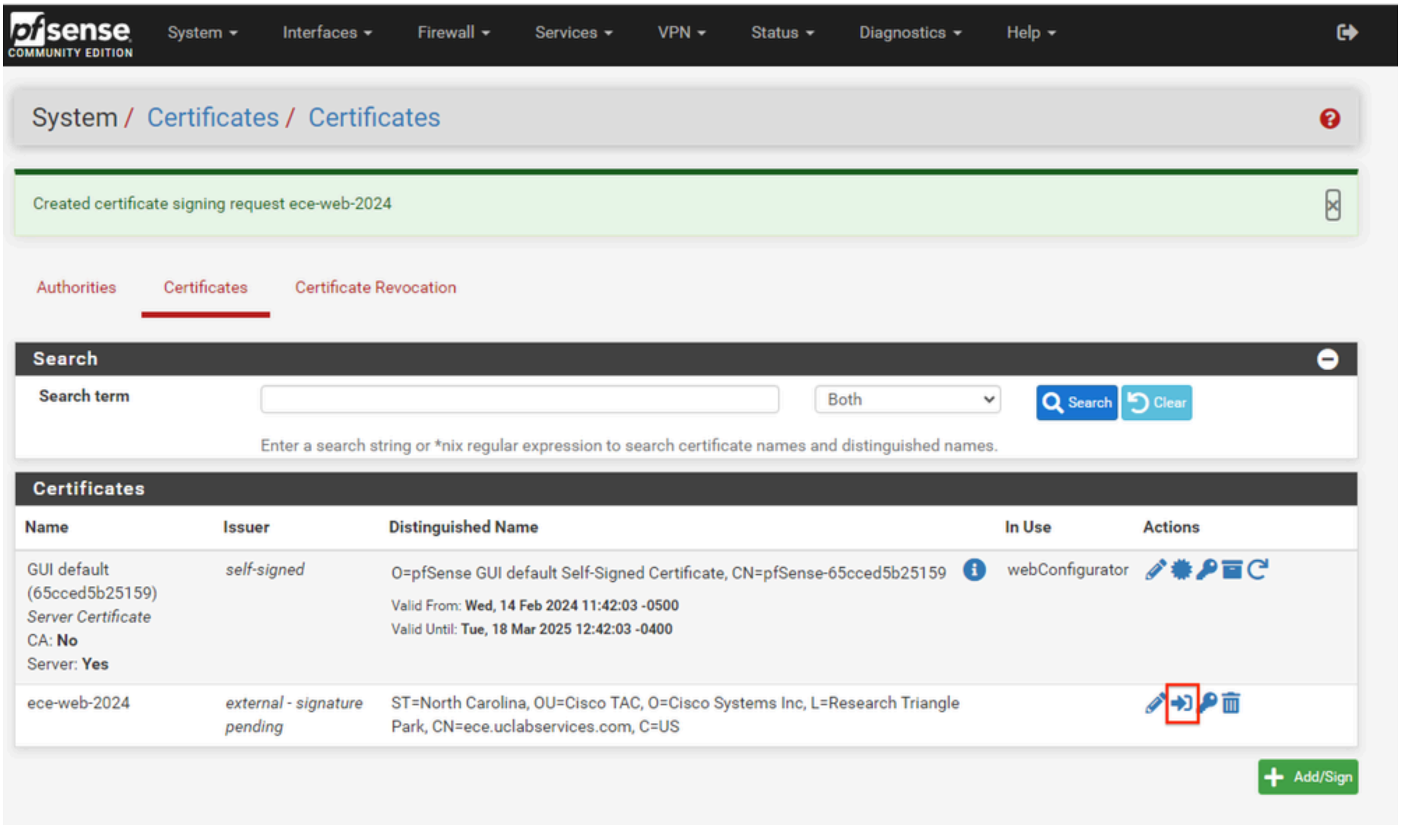
pfSense GUI - CSR高级

- Certificate Type：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：公用名会自动添加到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。



System / Certificates / Certificates

Created certificate signing request ece-web-2024

Search

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

Certificates

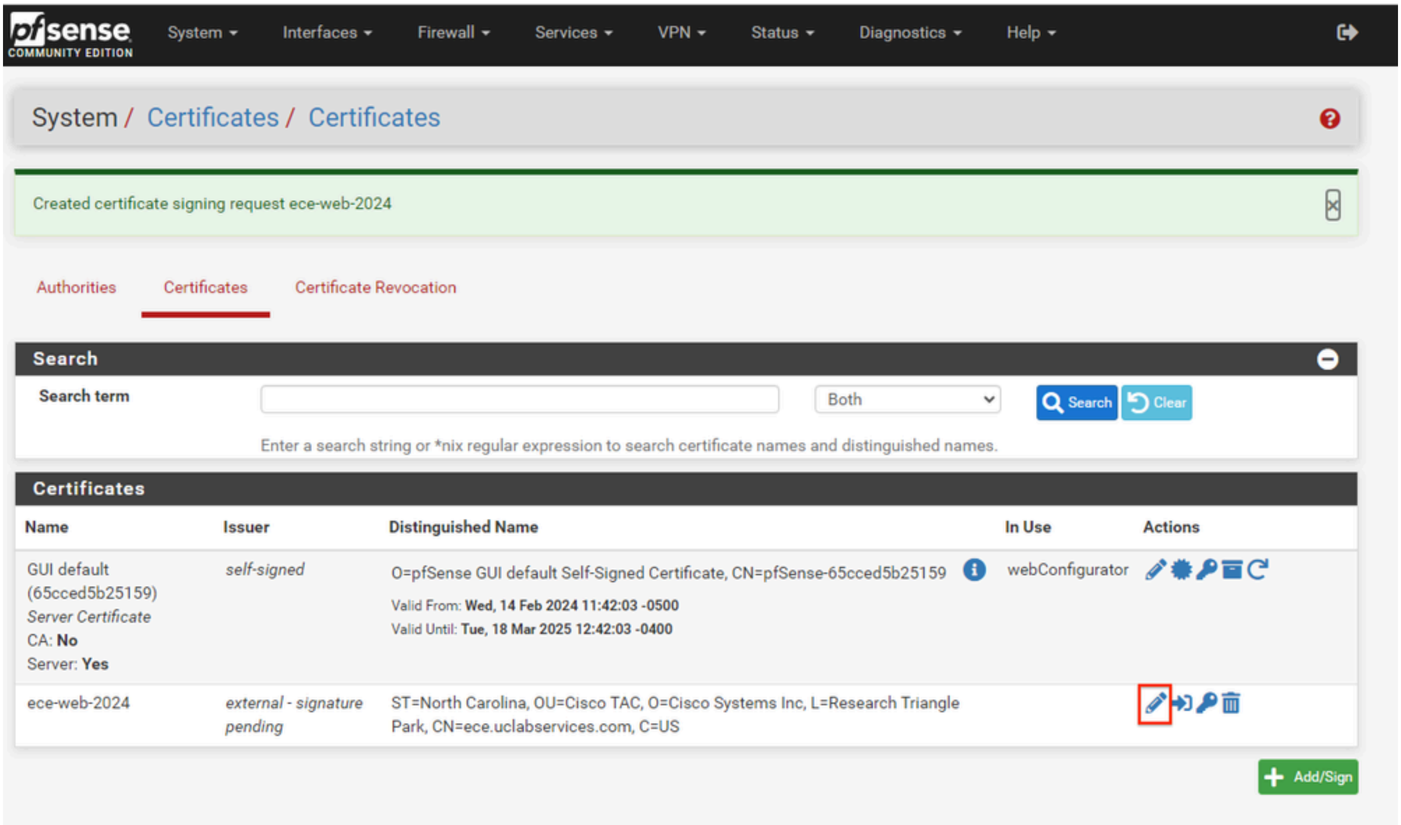
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: **Wed, 14 Feb 2024 11:42:03 -0500** Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400**	webConfigurator	
ece-web-2024	*external - signature pending*	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US		

pfSense GUI - CSR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。



Created certificate signing request ece-web-2024

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

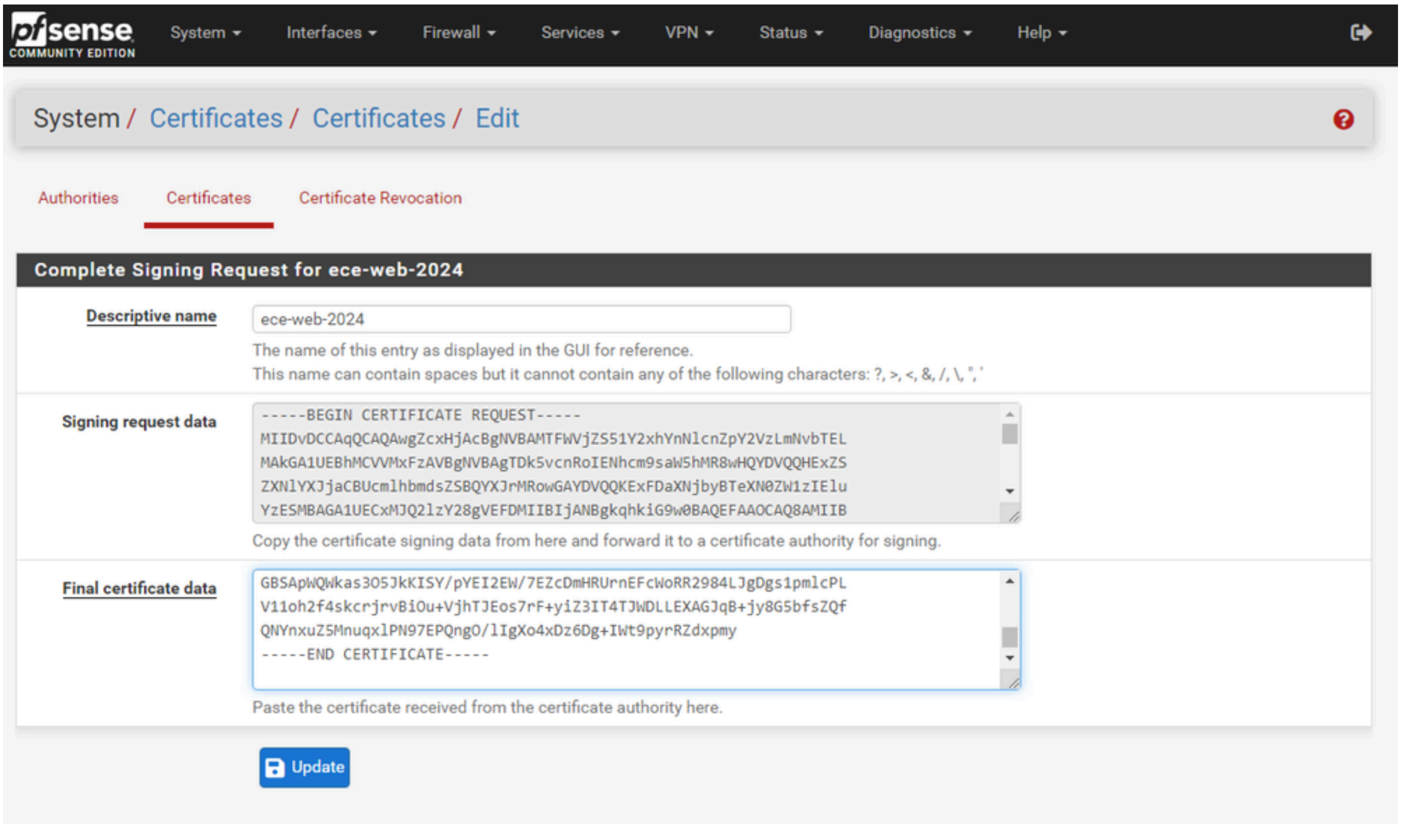
Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: **Wed, 14 Feb 2024 11:42:03 -0500** Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400**	webConfigurator	
ece-web-2024	*external - signature pending*	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US		

pfSense GUI — 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。



System / Certificates / Certificates / Edit

Authorities | Certificates | Certificate Revocation

Complete Signing Request for ece-web-2024

Descriptive name: ece-web-2024

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

Signing request data

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

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

Final certificate data

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

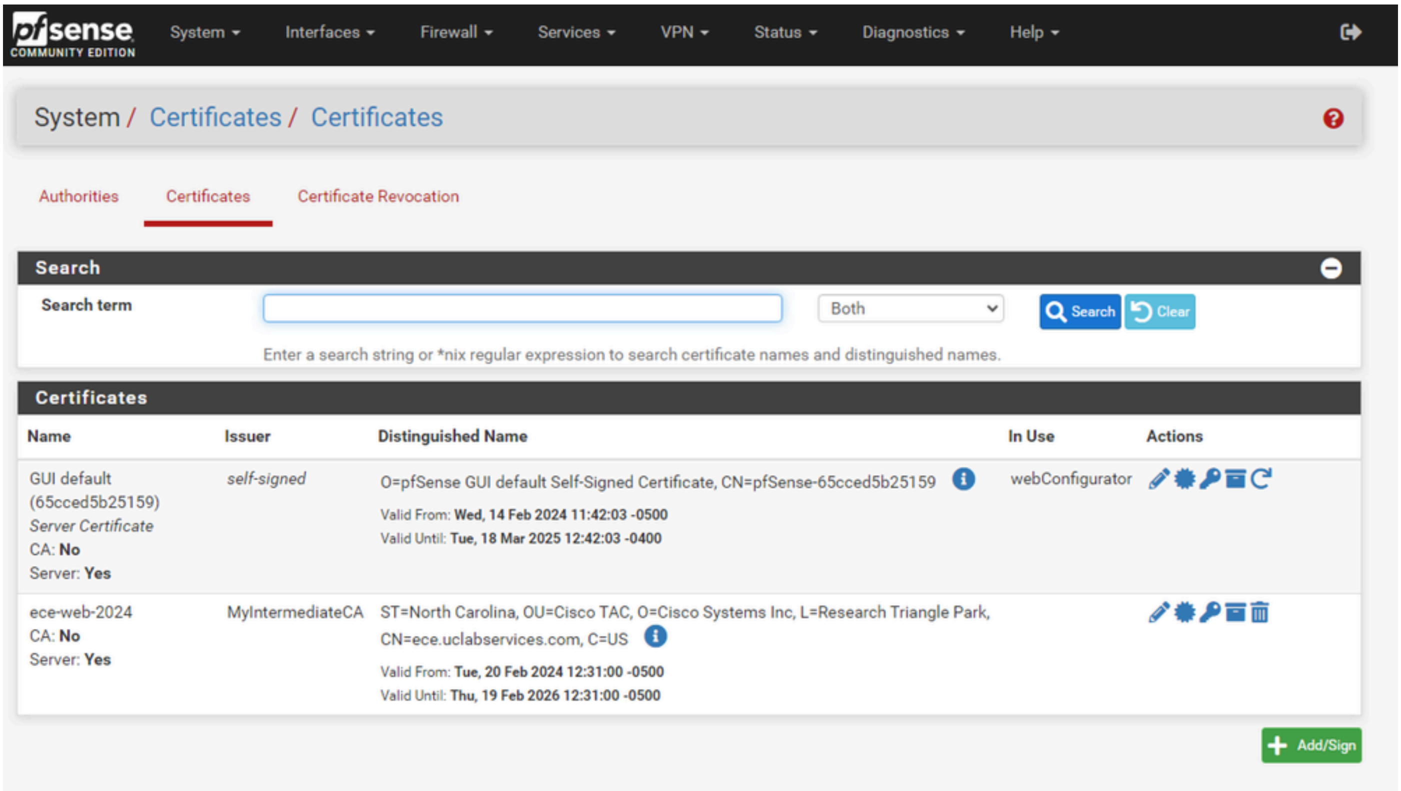
Paste the certificate received from the certificate authority here.

Update

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。



System / Certificates / Certificates

Authorities | Certificates | Certificate Revocation

Search

Search term: Both | Search | Clear

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

Certificates

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

Add/Sign

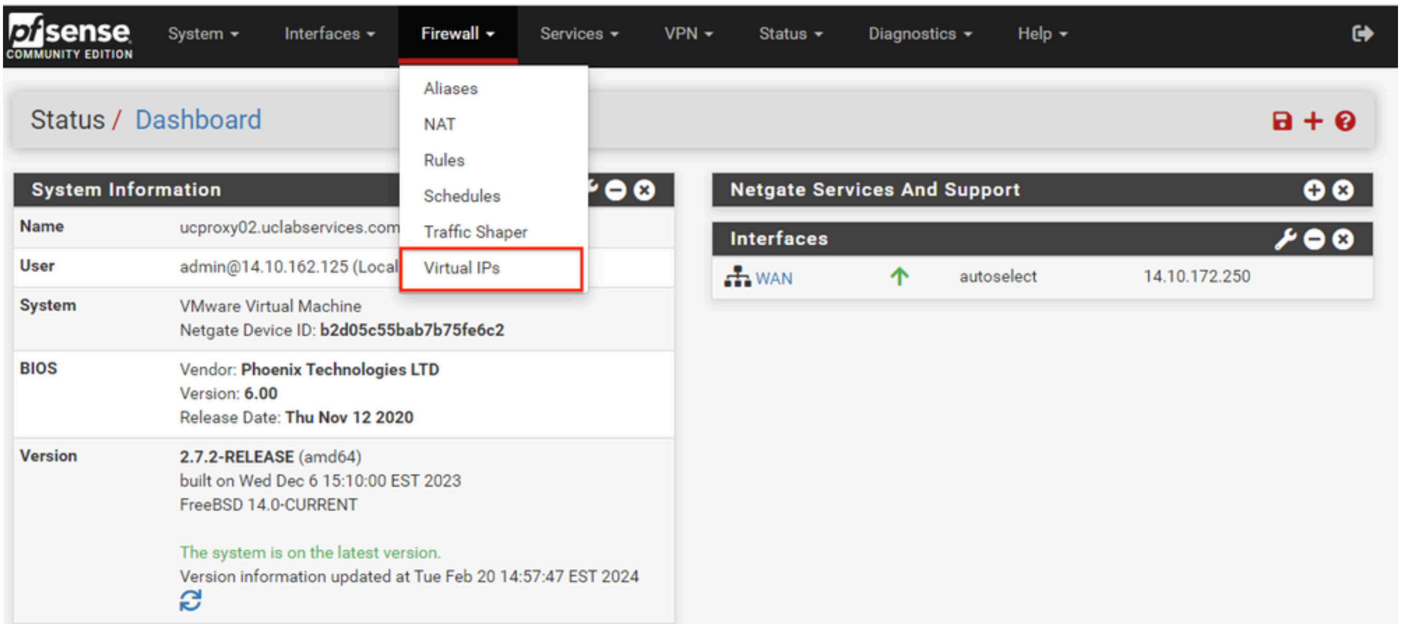
pfSense GUI — 证书列表

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

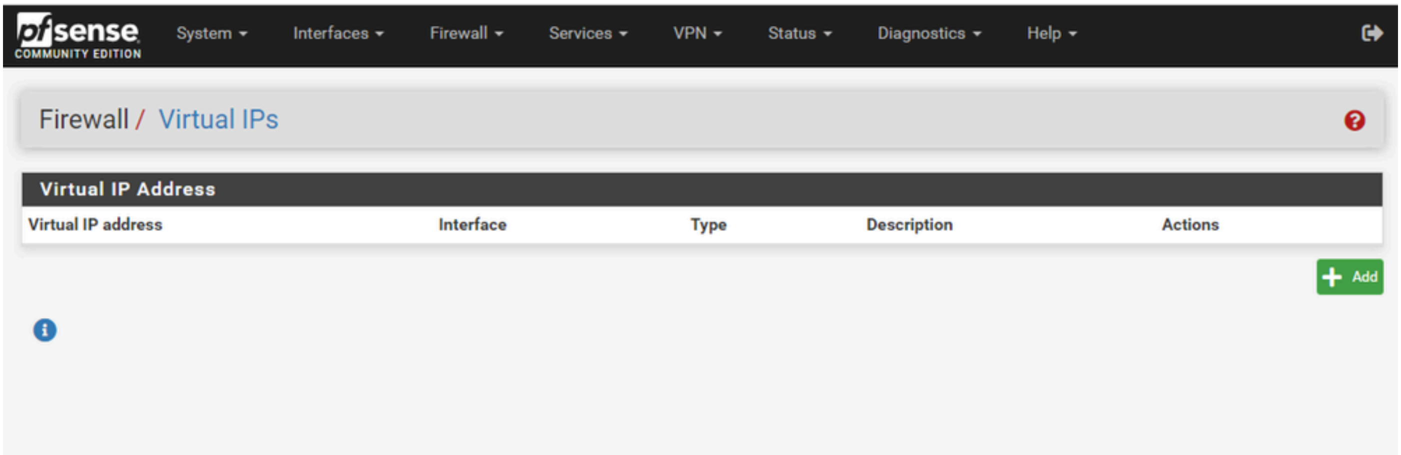


Name	ucproxy02.uclabservices.com
User	admin@14.10.162.125 (Local
System	VMware Virtual Machine Netgate Device ID: **b2d05c55bab7b75fe6c2**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.7.2-RELEASE** (amd64) built on Wed Dec 6 15:10:00 EST 2023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

WAN	↑	autoselect	14.10.172.250

pfSense GUI - VIP下拉列表

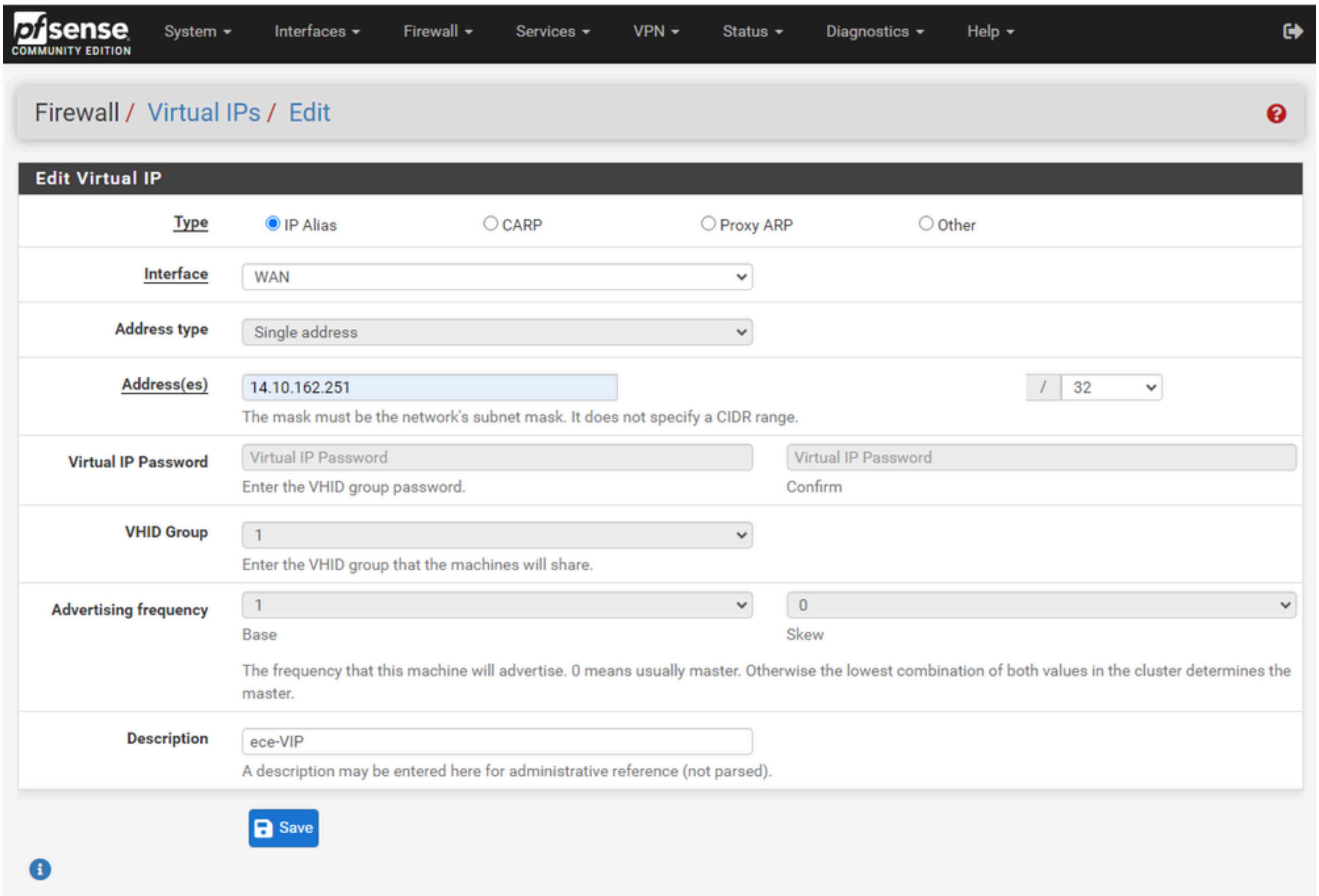
第二步：选择Add按钮



Virtual IP address	Interface	Type	Description	Actions

pfSense GUI - VIP登录页

第三步：提供地址信息



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 | Virtual IP Password

Enter the VHID group password. | Confirm

VHID Group: 1

Enter the VHID group that the machines will share.

Advertising frequency: 1 | 0

Base | 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配置

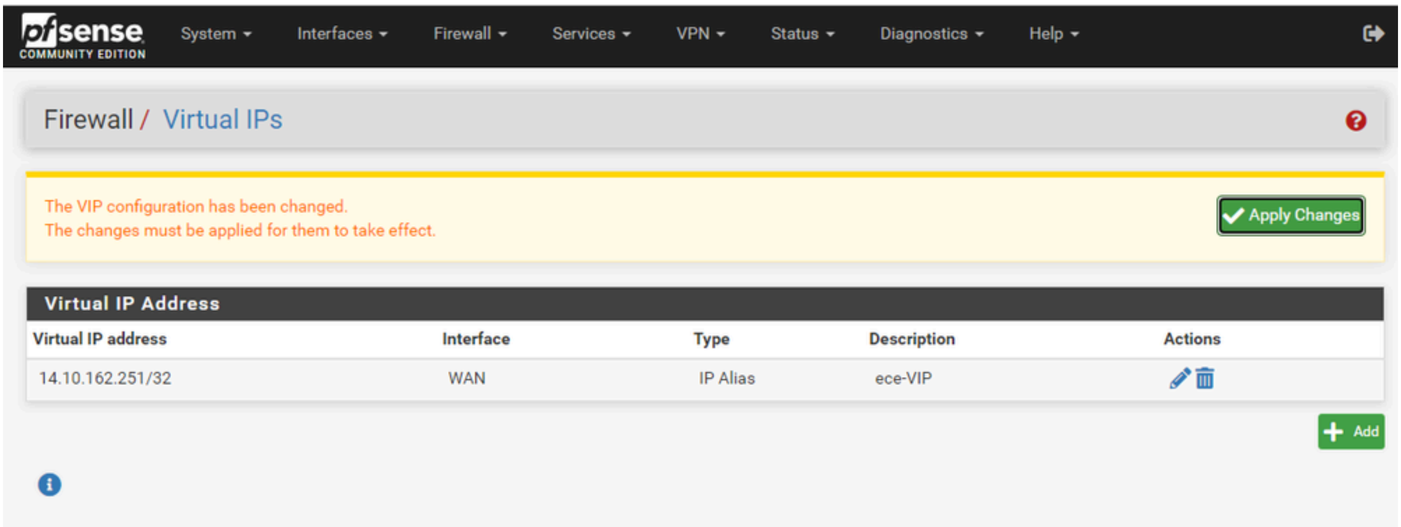
使用这些信息添加VIP。

- 类型：选择IP别名
- Interface：选择要广播的此IP地址的接口
- Address(es)：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
- 说明：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。

第四步：应用配置



Firewall / Virtual IPs

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

Virtual IP Address

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

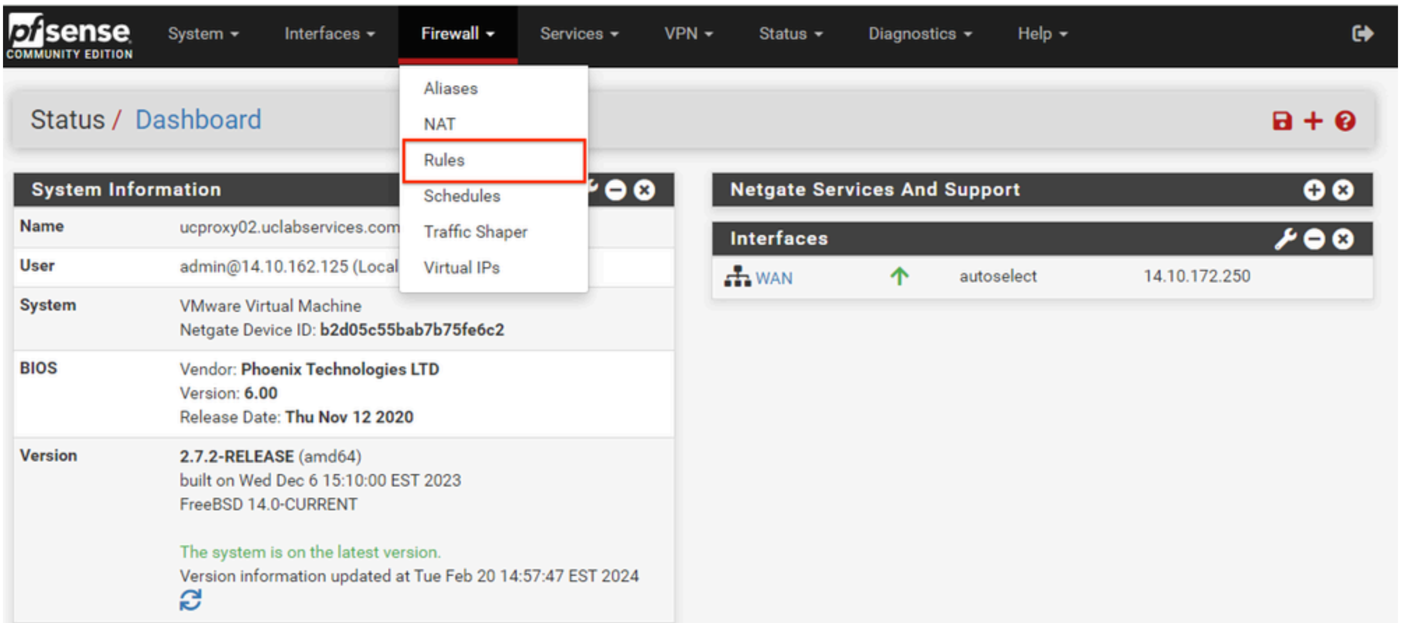
pfSense GUI - VIP列表

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



Status / Dashboard

System Information

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

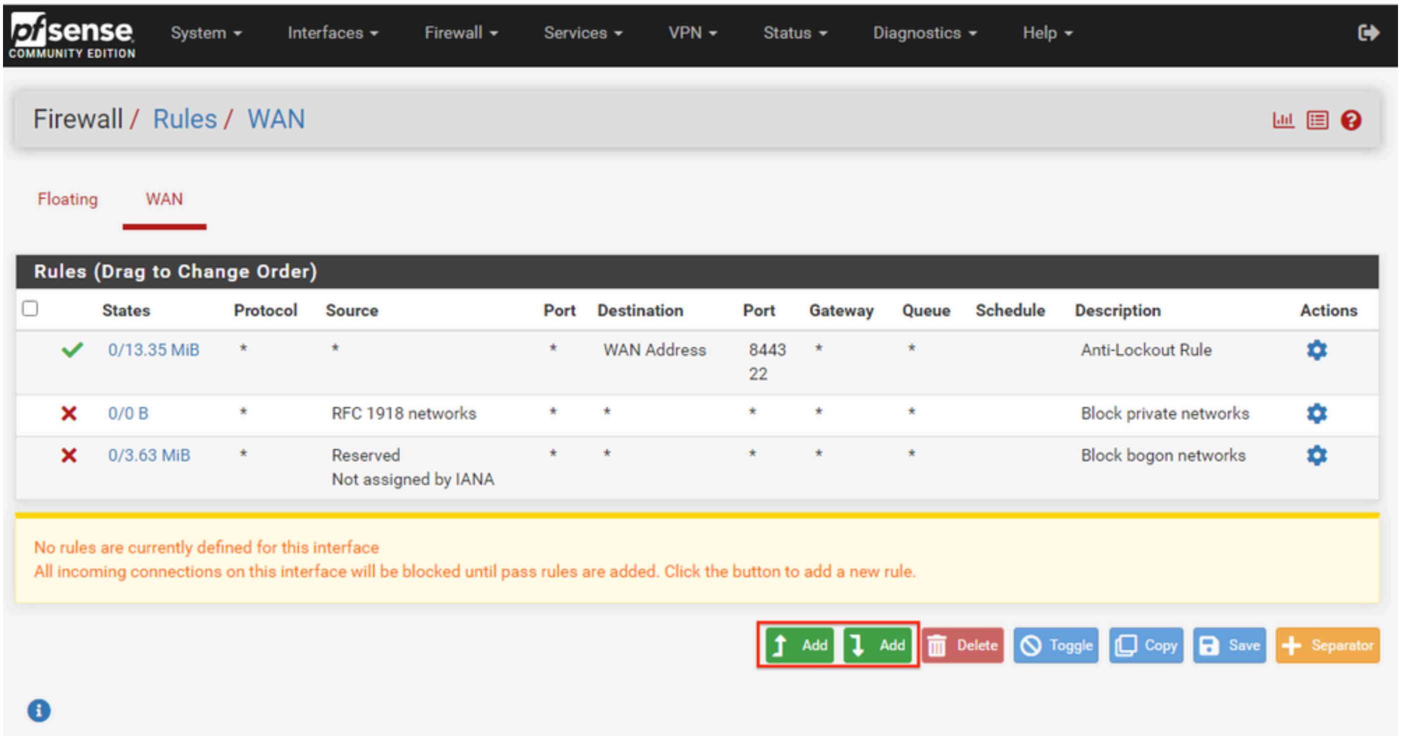
Netgate Services And Support

Interfaces

WAN	↑	autoselect	14.10.172.250

pfSense GUI — 防火墙规则下拉列表

第二步：选择其中一个Add按钮



Firewall / Rules / WAN

Rules (Drag to Change Order)

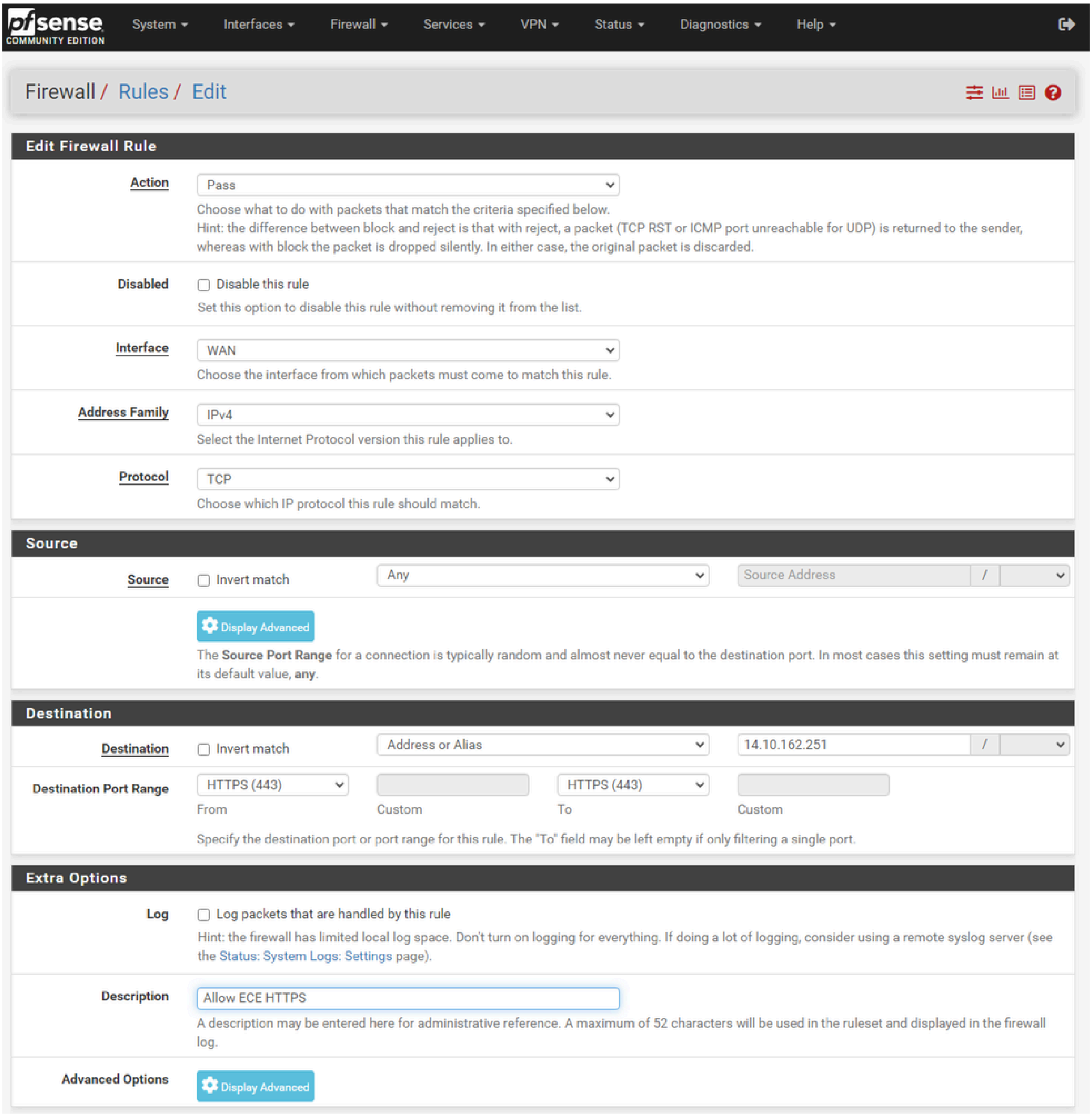
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/13.35 MiB	*	*	*	WAN Address	8443 22	*	*		Anti-Lockout Rule	⚙
	✗	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0/3.63 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

pfSense GUI — 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。

第三步：创建防火墙规则，以允许流量传输到IP地址的端口443



Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

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

Disabled: □ Disable this rule

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

Interface: WAN

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

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

Source

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

Display Advanced

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

Destination

Destination: □ Invert match | Address or Alias | 14.10.162.251 | /

Destination Port Range: HTTPS (443) From | Custom | HTTPS (443) To | Custom

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

Extra Options

Log: □ Log packets that are handled by this rule

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

Description: Allow ECE HTTPS

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

Advanced Options: Display Advanced

pfSense GUI — 防火墙通过规则配置

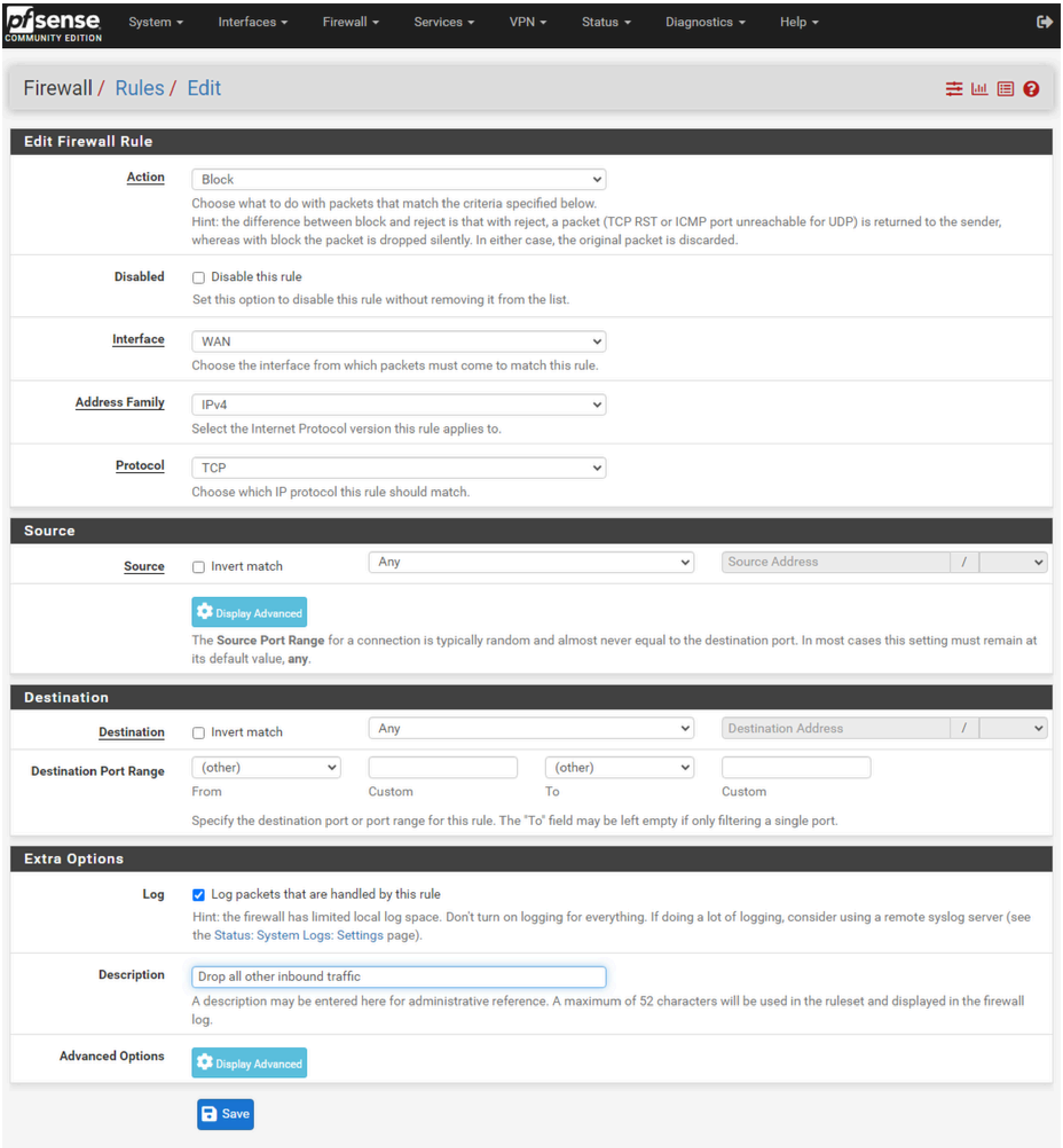
使用信息创建规则。

- 操作：选择通过
- Interface：选择规则应用于的接口
- 地址系列和协议：选择适当选项
- 来源：保持选定为任意(Any)
- Destination：从Destination下拉列表中选择Address或Alias，然后输入应用规则的IP地址
- Destination Port Range：选择，在From和To下拉列表中的HTTPS(443)
- Log：选中此复选框可记录与此规则匹配的任何计帐数据包
- 说明：提供文本供以后参考规则

选择Save。

第四步：创建防火墙规则以丢弃所有其它到pfSense的流量

选择Add按钮将规则插入到新创建的规则下方。



Firewall / Rules / Edit

Edit Firewall Rule

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

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

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

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Source: □ Invert match Any Source Address /

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

Destination

Destination: □ Invert match Any Destination Address /

Destination Port Range: (other) From Custom (other) To Custom

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

Extra Options

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

Description: Drop all other inbound traffic
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options:

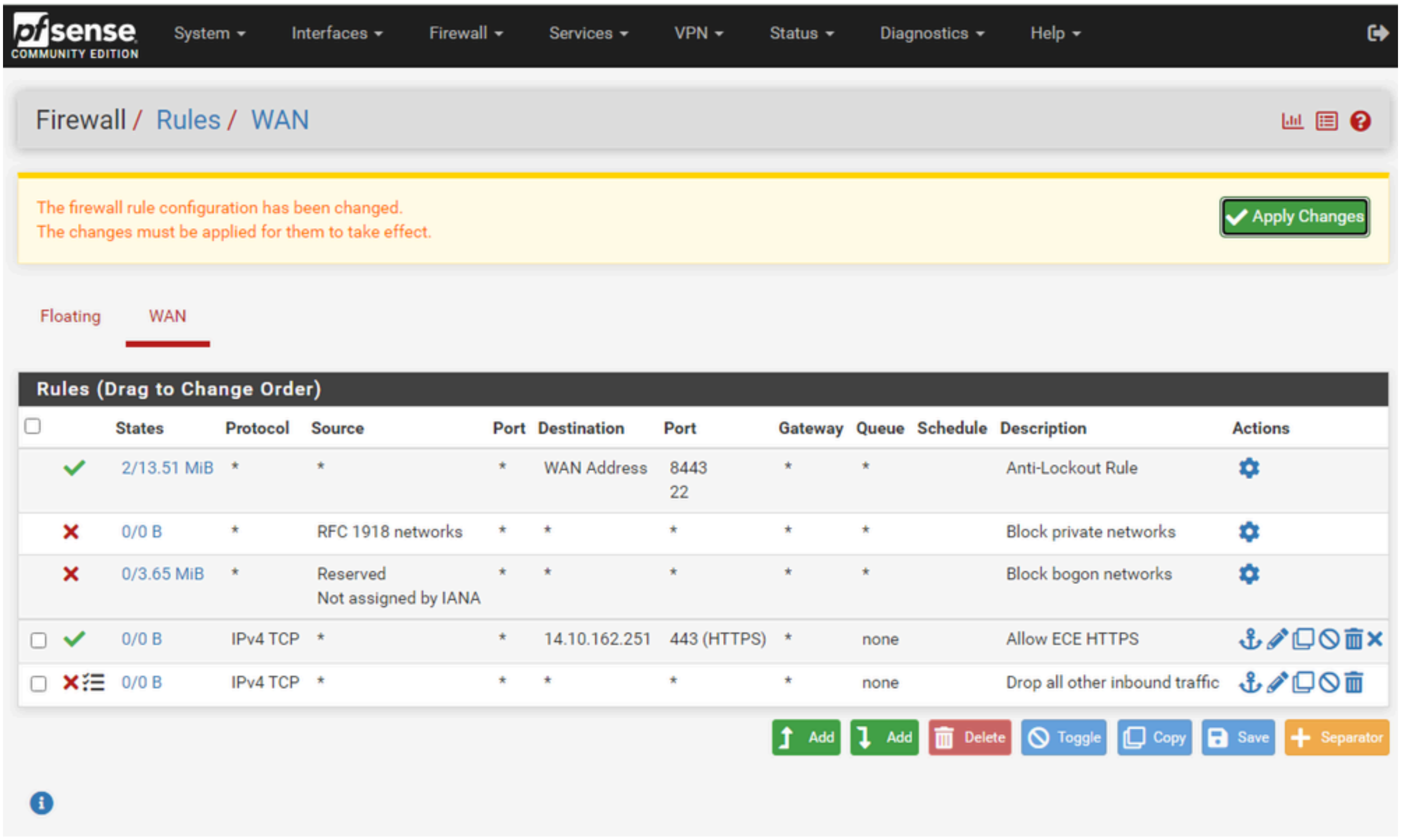
pfSense GUI — 防火墙丢弃规则配置

- 操作：选择阻止(Block)
- Interface：选择规则应用于的接口
- 地址系列和协议：选择适当选项

- 来源：保持选定为任意(Any)
- 目标：保持选定为任意(Any)
- Log：选中此复选框可记录与此规则匹配的任何计帐数据包
- 说明：提供文本供以后参考规则

选择Save。

第五步：检查规则并确保阻止规则位于底部



Firewall / Rules / WAN

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

Rules (Drag to Change Order)

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

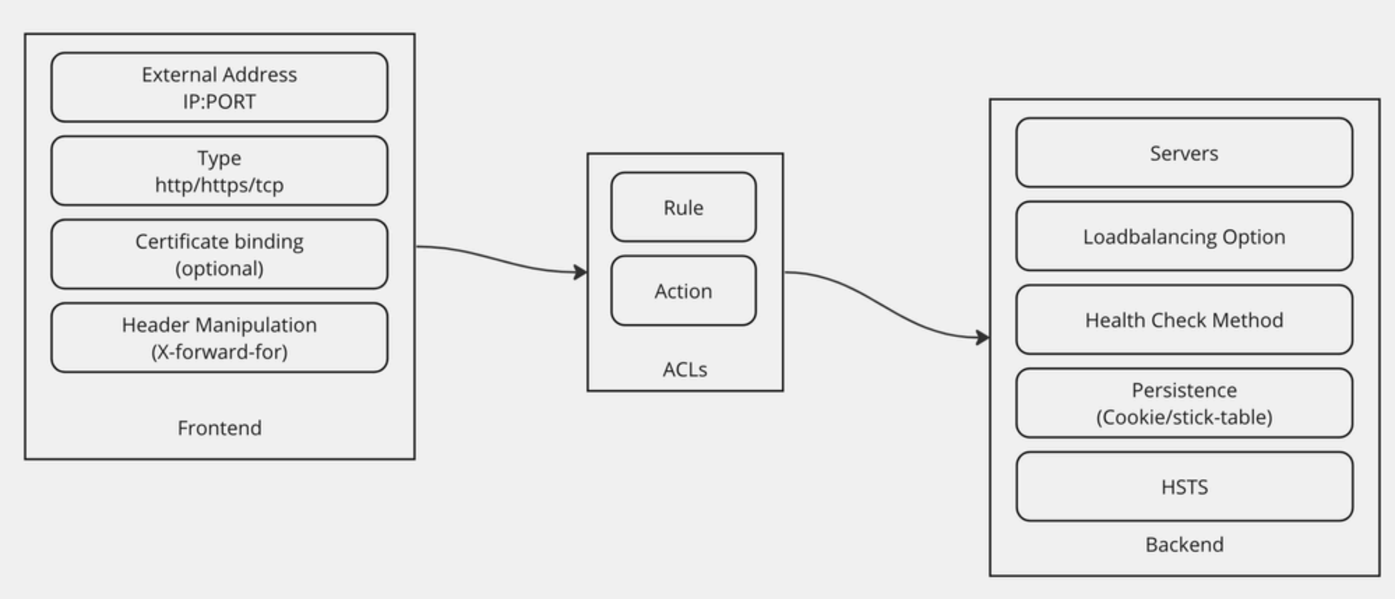
pfSense GUI — 防火墙规则列表

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。

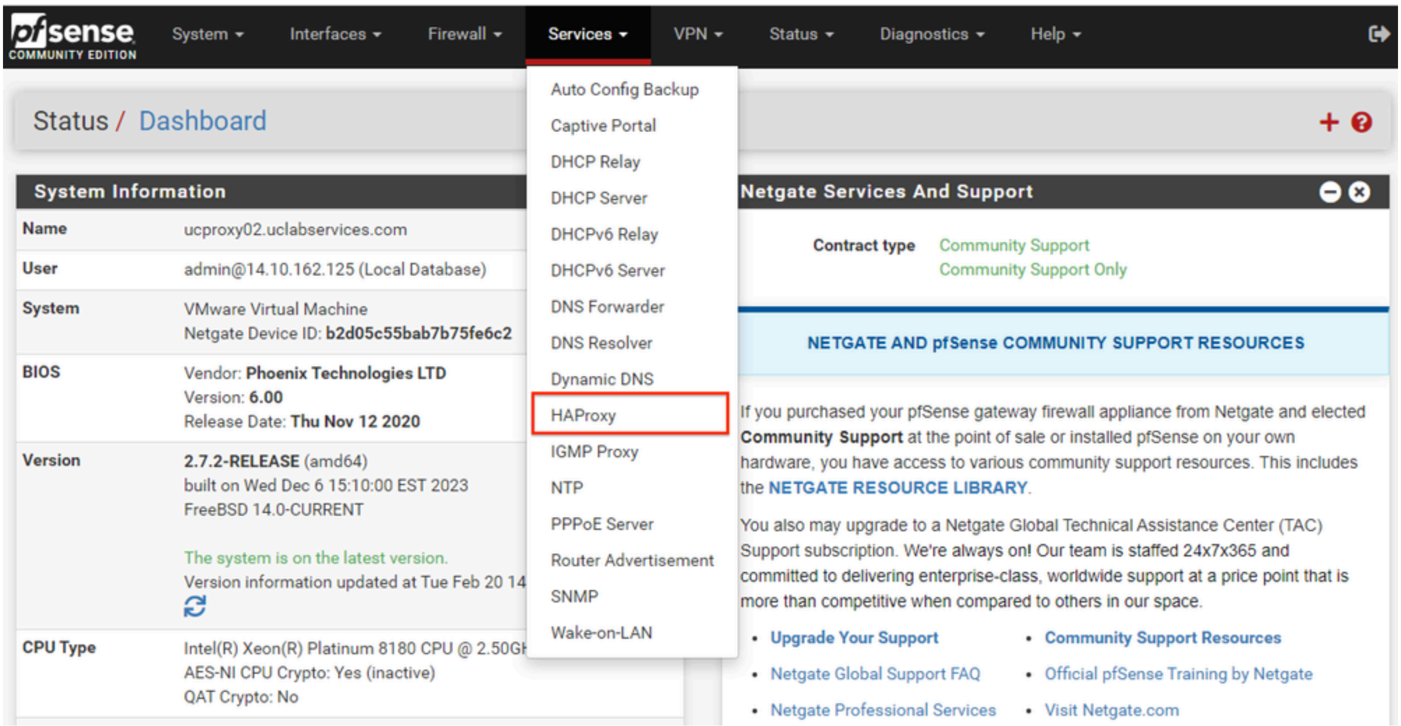
后端定义实际服务器和端口、初始分配的负载均衡方法、运行状况检查和持久性。

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



System Information

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

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

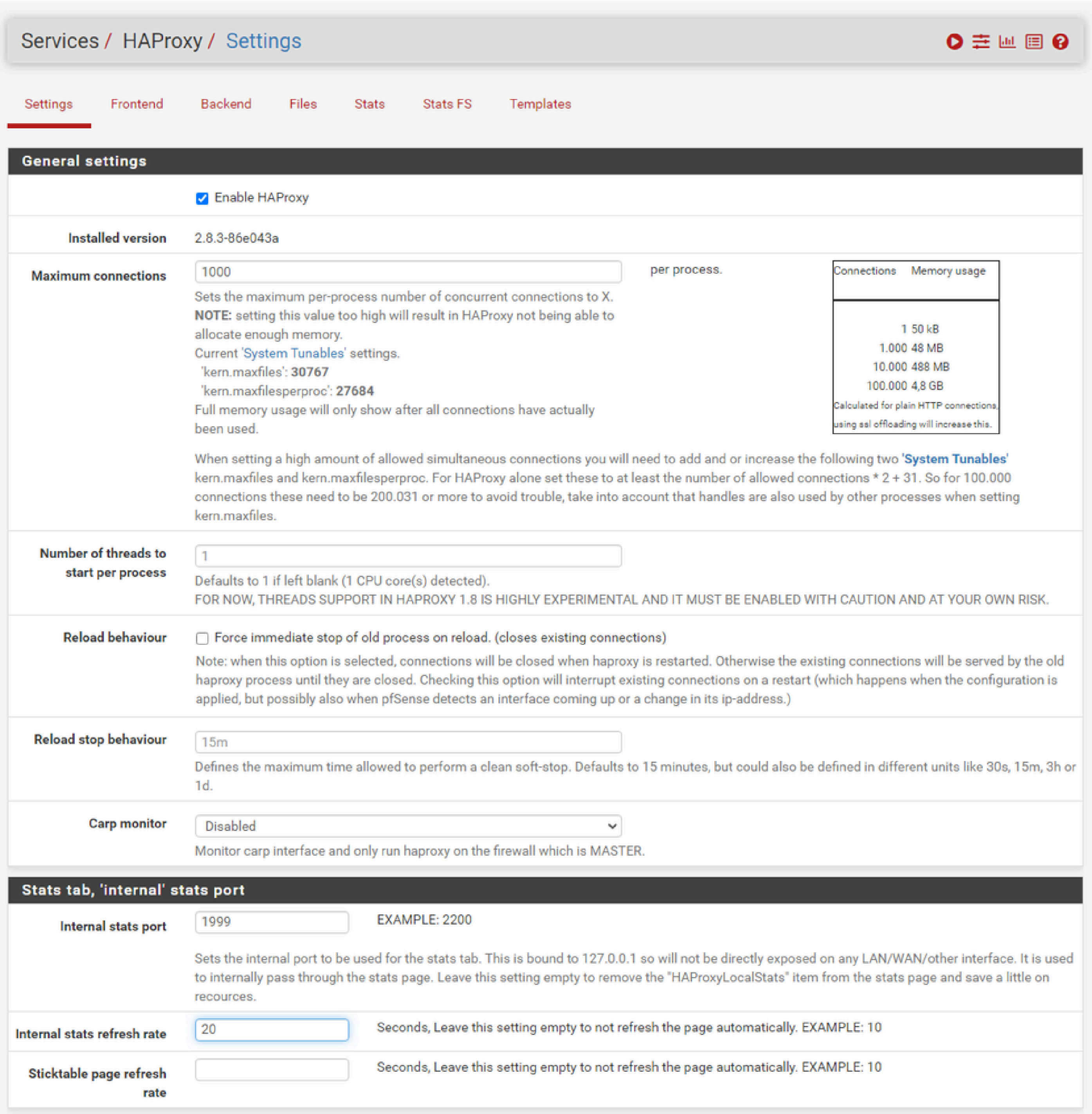
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

pfSense GUI - HAProxy下拉列表

第二步：配置基本设置



Services / HAProxy / Settings

General settings

☑ Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections 1000 per process.

Sets the maximum per-process number of concurrent connections to X.
NOTE: setting this value too high will result in HAProxy not being able to allocate enough memory.
Current 'System Tunables' settings.
'kern.maxfiles': **30767**
'kern.maxfilesperproc': **27684**
Full memory usage will only show after all connections have actually been used.

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

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

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

Number of threads to start per process 1

Defaults to 1 if left blank (1 CPU core(s) detected).
FOR NOW, THREADS SUPPORT IN HAPROXY 1.8 IS HIGHLY EXPERIMENTAL AND IT MUST BE ENABLED WITH CAUTION AND AT YOUR OWN RISK.

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

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

Reload stop behaviour 15m

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

Carp monitor Disabled

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

Stats tab, 'internal' stats port

Internal stats port 1999 EXAMPLE: 2200

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

Internal stats refresh rate 20 Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

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

pfSense GUI - HAProxy主设置

选中Enable HAProxy复选框。

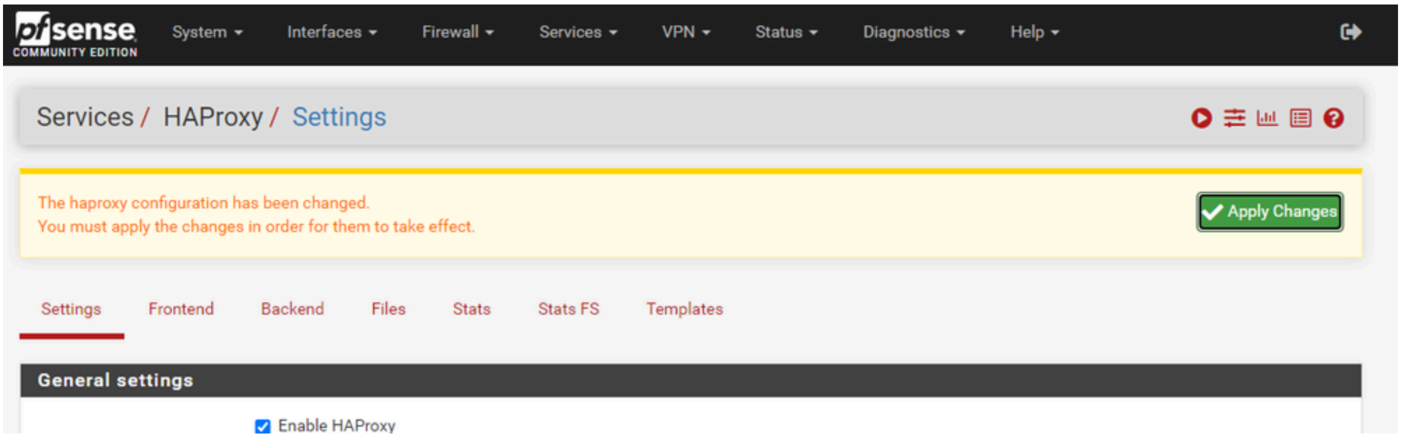
输入最大连接数(Maximum Connections)的值。请参阅本节中的图表以获取有关所需内存的详细信息。

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。



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

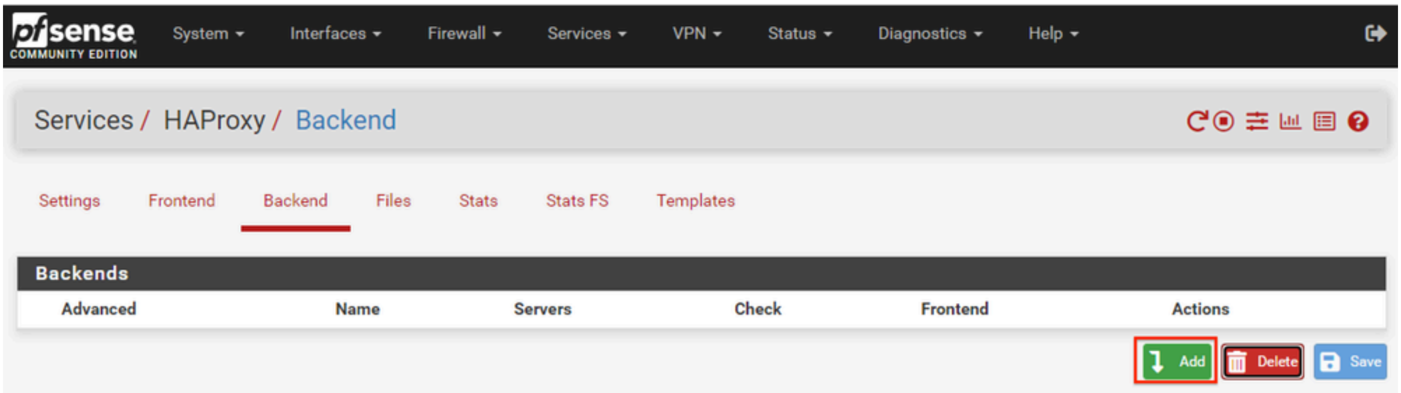
☑ Enable HAProxy

pfSense GUI - HAProxy应用更改

注意：只有选择“应用更改”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

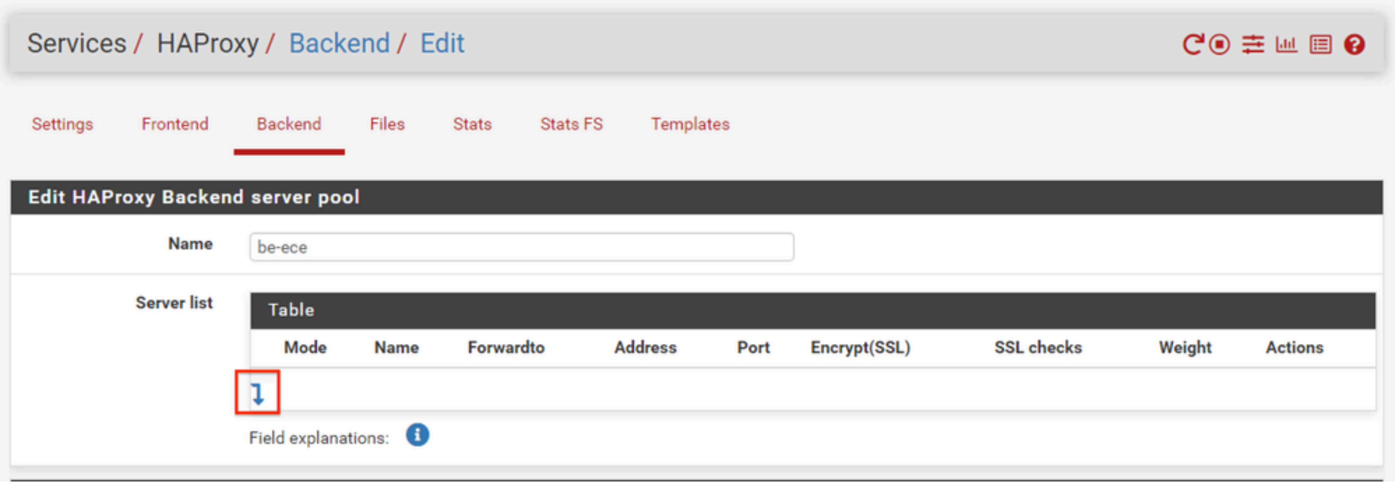
从后端开始。原因是前端必须引用后端。确保您已选择“后端”菜单。



Advanced	Name	Servers	Check	Frontend	Actions

pfSense GUI - HAProxy添加后端

选择Add按钮。



Name: be-ece

Server list

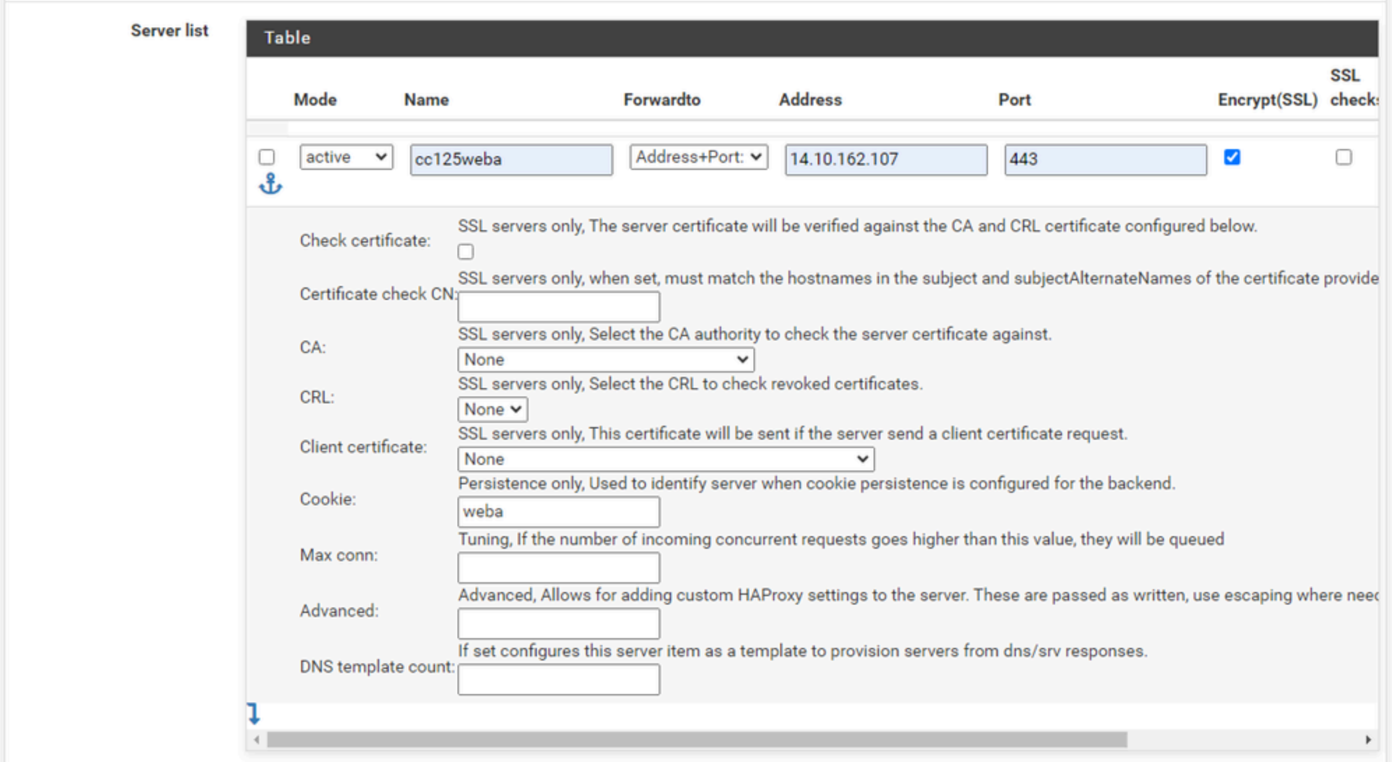
Table

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

pfSense GUI - HAProxy后端启动

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



Server list

Table

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

Check certificate:	SSL servers only, The server certificate will be verified against the CA and CRL certificate configured below. □
Certificate check CN:	SSL servers only, when set, must match the hostnames in the subject and subjectAlternateNames of the certificate provide
CA:	SSL servers only, Select the CA authority to check the server certificate against. None
CRL:	SSL servers only, Select the CRL to check revoked certificates. None
Client certificate:	SSL servers only, This certificate will be sent if the server send a client certificate request. None
Cookie:	Persistence only, Used to identify server when cookie persistence is configured for the backend. weba
Max conn:	Tuning, If the number of incoming concurrent requests goes higher than this value, they will be queued
Advanced:	Advanced, Allows for adding custom HAProxy settings to the server. These are passed as written, use escaping where need
DNS template count:	If set configures this server item as a template to provision servers from dns/srv responses.

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。

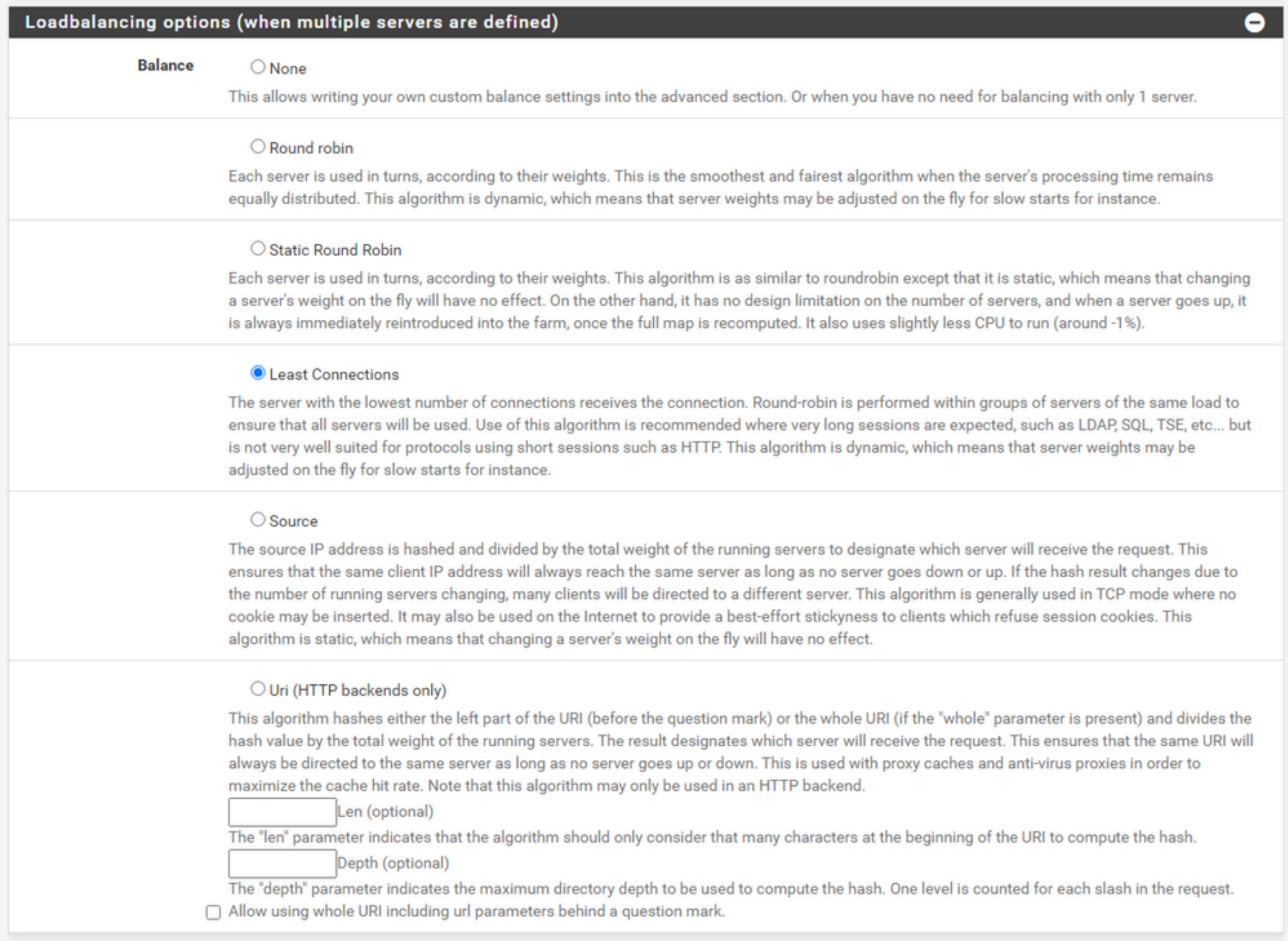
提供服务器的地址。这可以配置为FQDN的IP地址。

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。



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)

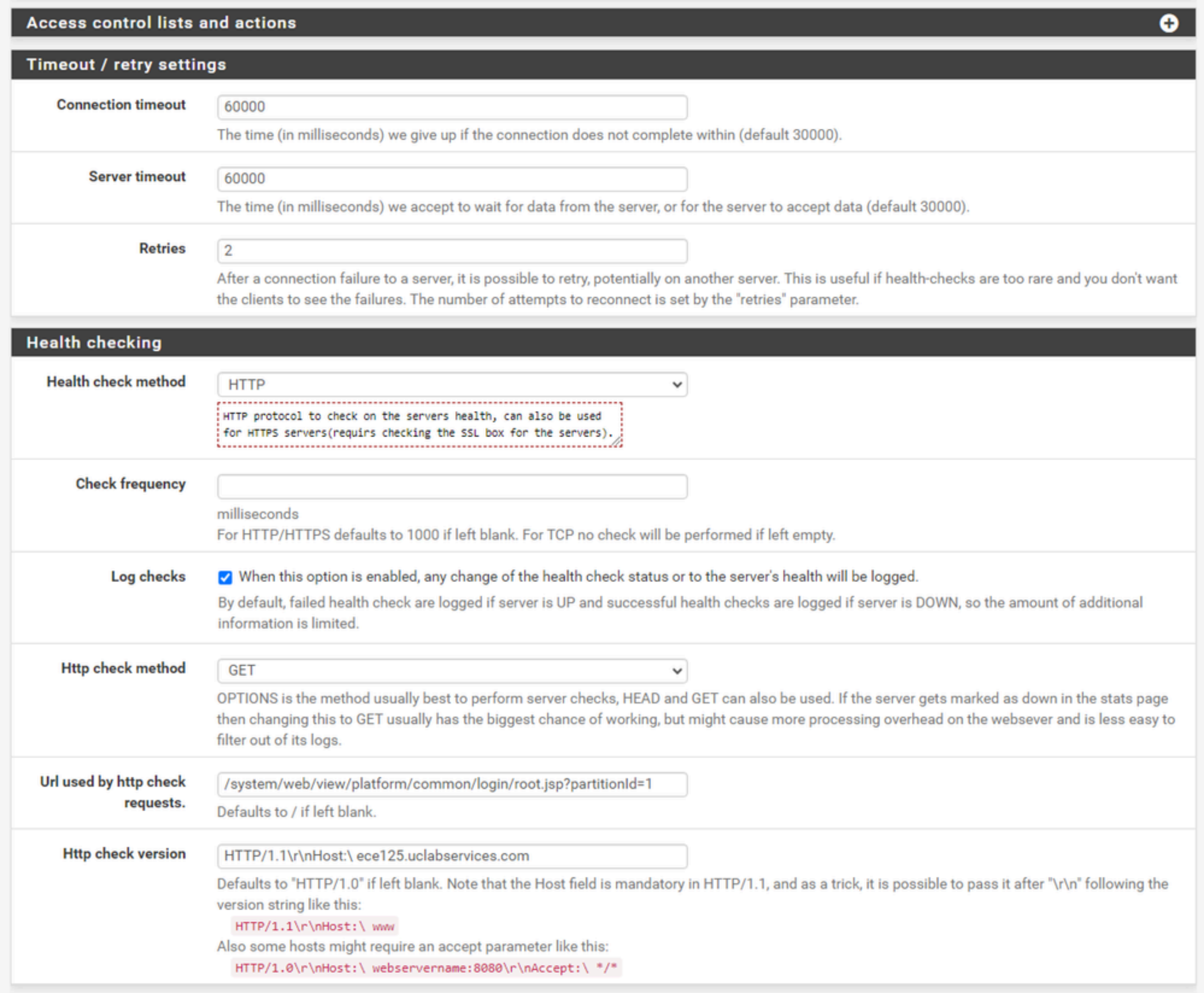
The "depth" parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request.

□ 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”。



Access control lists and actions

Timeout / retry settings

Connection timeout: 60000
The time (in milliseconds) we give up if the connection does not complete within (default 30000).

Server timeout: 60000
The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).

Retries: 2
After a connection failure to a server, it is possible to retry, potentially on another server. This is useful if health-checks are too rare and you don't want the clients to see the failures. The number of attempts to reconnect is set by the "retries" parameter.

Health checking

Health check method: HTTP

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

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

Log checks: ☑ When this option is enabled, any change of the health check status or to the server's health will be logged.
By default, failed health check are logged if server is UP and successful health checks are logged if server is DOWN, so the amount of additional information is limited.

Http check method: GET
OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the websever and is less easy to filter out of its logs.

Url used by http check requests.: /system/web/view/platform/common/login/root.jsp?partitionId=1
Defaults to / if left blank.

Http check version: HTTP/1.1\r\nHost:\ ece125.uclabservices.com
Defaults to "HTTP/1.0" if left blank. Note that the Host field is mandatory in HTTP/1.1, and as a trick, it is possible to pass it after "\r\n" following the version string like this:
`HTTP/1.1\r\nHost:\ www`
Also some hosts might require an accept parameter like this:
`HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*`

HAProxy后端 — 运行状况检查

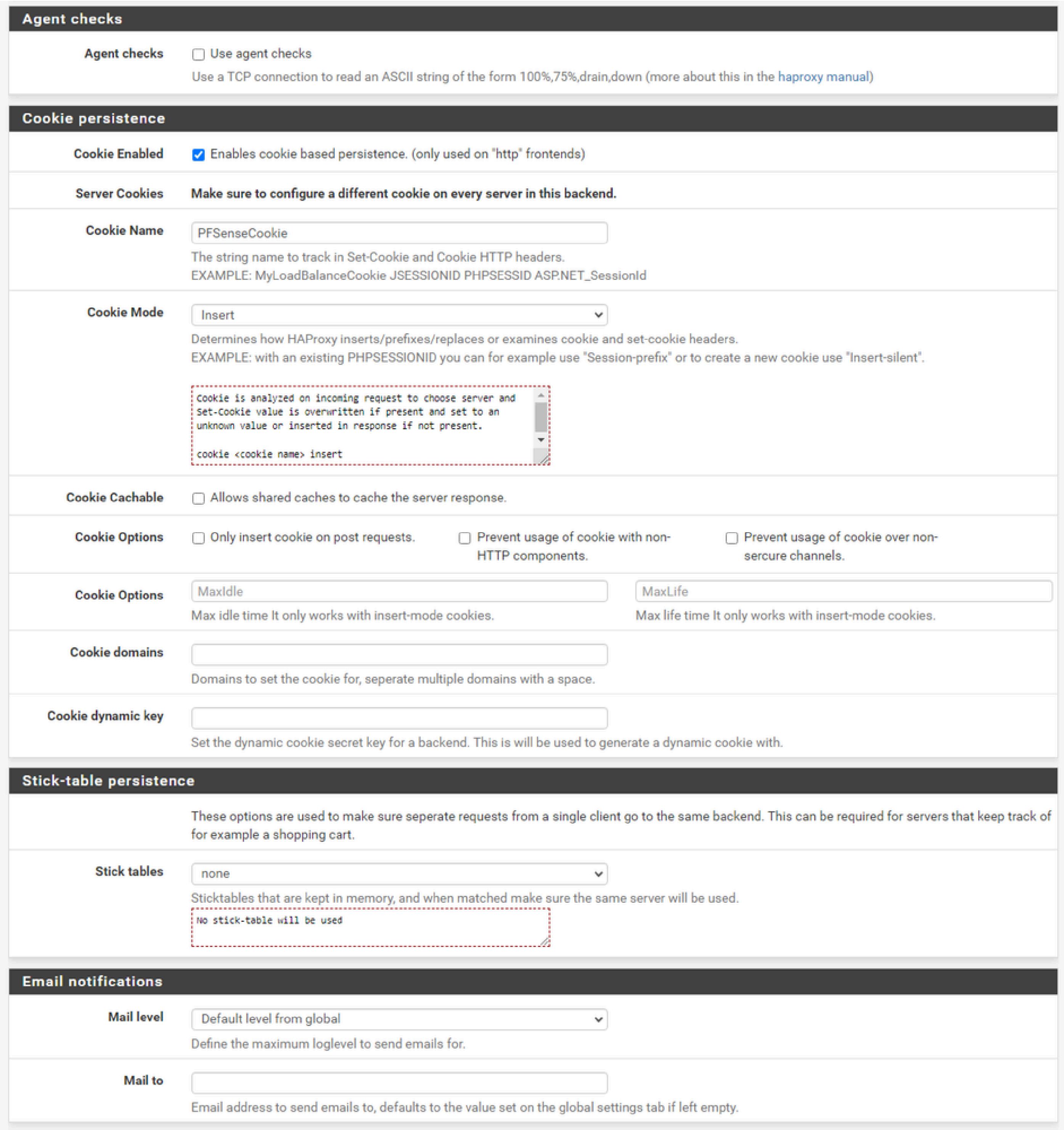
此配置不使用访问控制列表。

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。



Agent checks

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

Cookie persistence

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

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

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

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

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

cookie <cookie name> insert
```

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

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

Cookie Options MaxIdle MaxLife
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 none
Sticktables that are kept in memory, and when matched make sure the same server will be used.

```
No stick-table will be used
```

Email notifications

Mail level Default level from global
Define the maximum loglevel to send emails for.

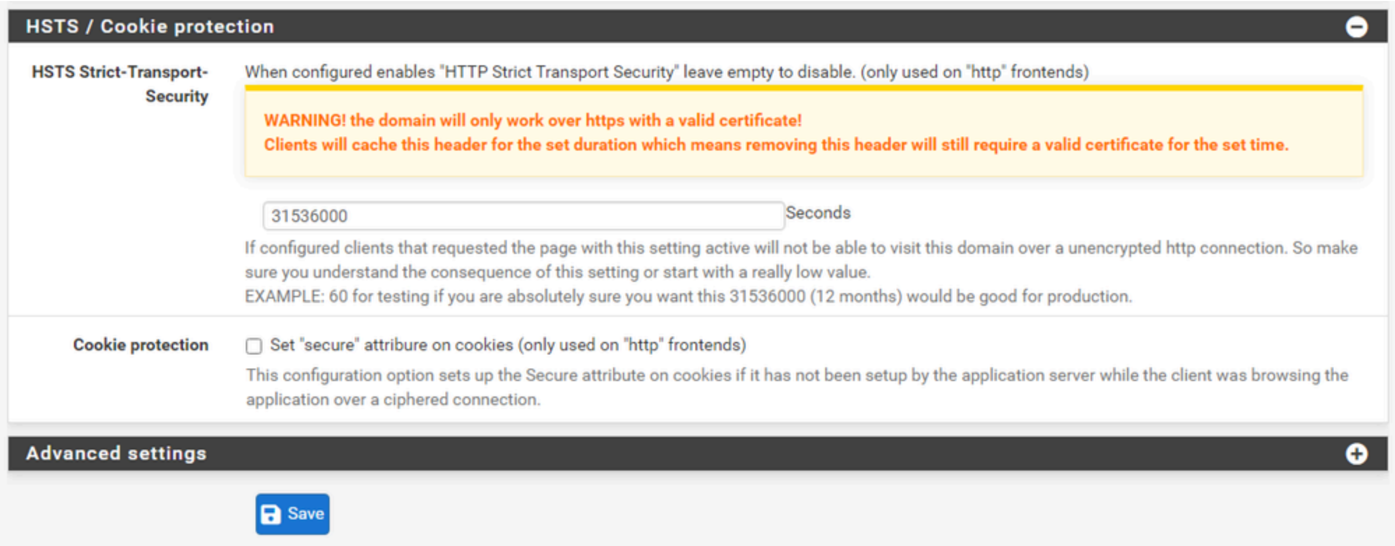
Mail to
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

HAProxy后端 — Cookie持久性

取消选中“Agent checks（代理检查）”。

配置Cookie持久性：

1. Cookie Enabled：选择以启用基于Cookie的持久性。
2. Cookie Name：提供Cookie的名称。
3. Cookie Mode：从下拉框中选择Insert。
4. 取消设置其余选项。



HSTS Strict-Transport-Security

When configured enables "HTTP Strict Transport Security" leave empty to disable. (only used on "http" frontends)

WARNING! the domain will only work over https with a valid certificate!
Clients will cache this header for the set duration which means removing this header will still require a valid certificate for the set time.

31536000 Seconds

If configured clients that requested the page with this setting active will not be able to visit this domain over a unencrypted http connection. So make sure you understand the consequence of this setting or start with a really low value.
EXAMPLE: 60 for testing if you are absolutely sure you want this 31536000 (12 months) would be good for production.

Cookie protection

□ Set "secure" attribure on cookies (only used on "http" frontends)

This configuration option sets up the Secure attribute on cookies if it has not been setup by the application server while the client was browsing the application over a ciphered connection.

HAProxy后端 — HSTS

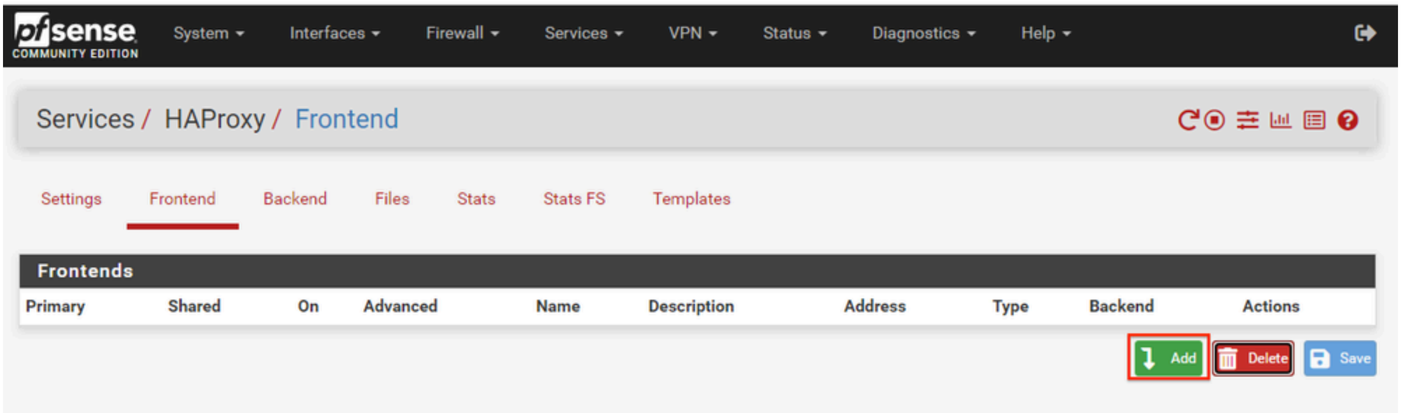
后端配置表单的其余部分可以保留默认设置。

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。

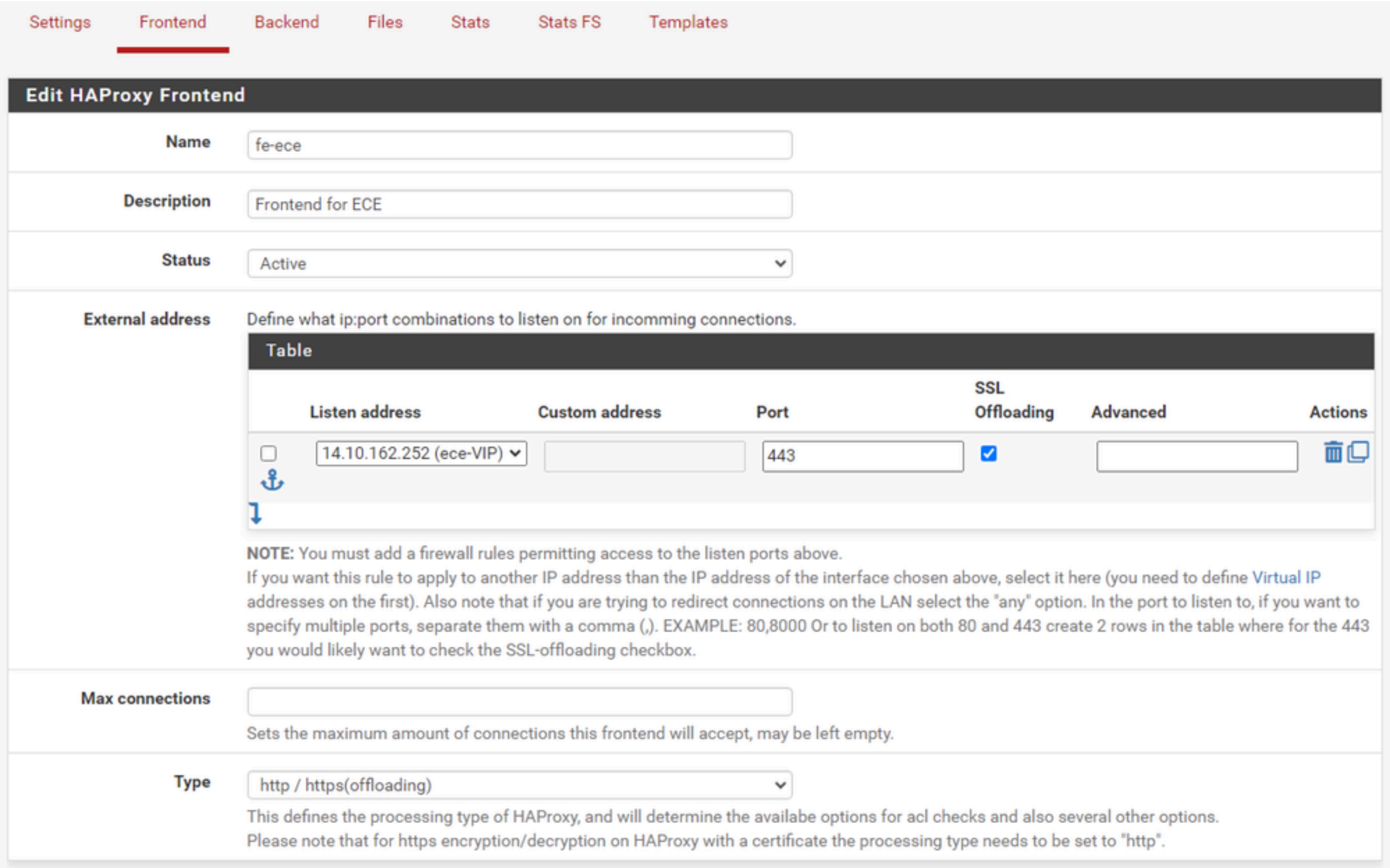


Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions

pfSense GUI - HAProxy添加前端

选择，添加按钮



Edit HAProxy Frontend

Name	fe-ece
Description	Frontend for ECE
Status	Active

External address

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

Table

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

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

Max connections

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

Type: http / https(offloading)

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

HAProxy — 前端报头

为前端提供一个名称。

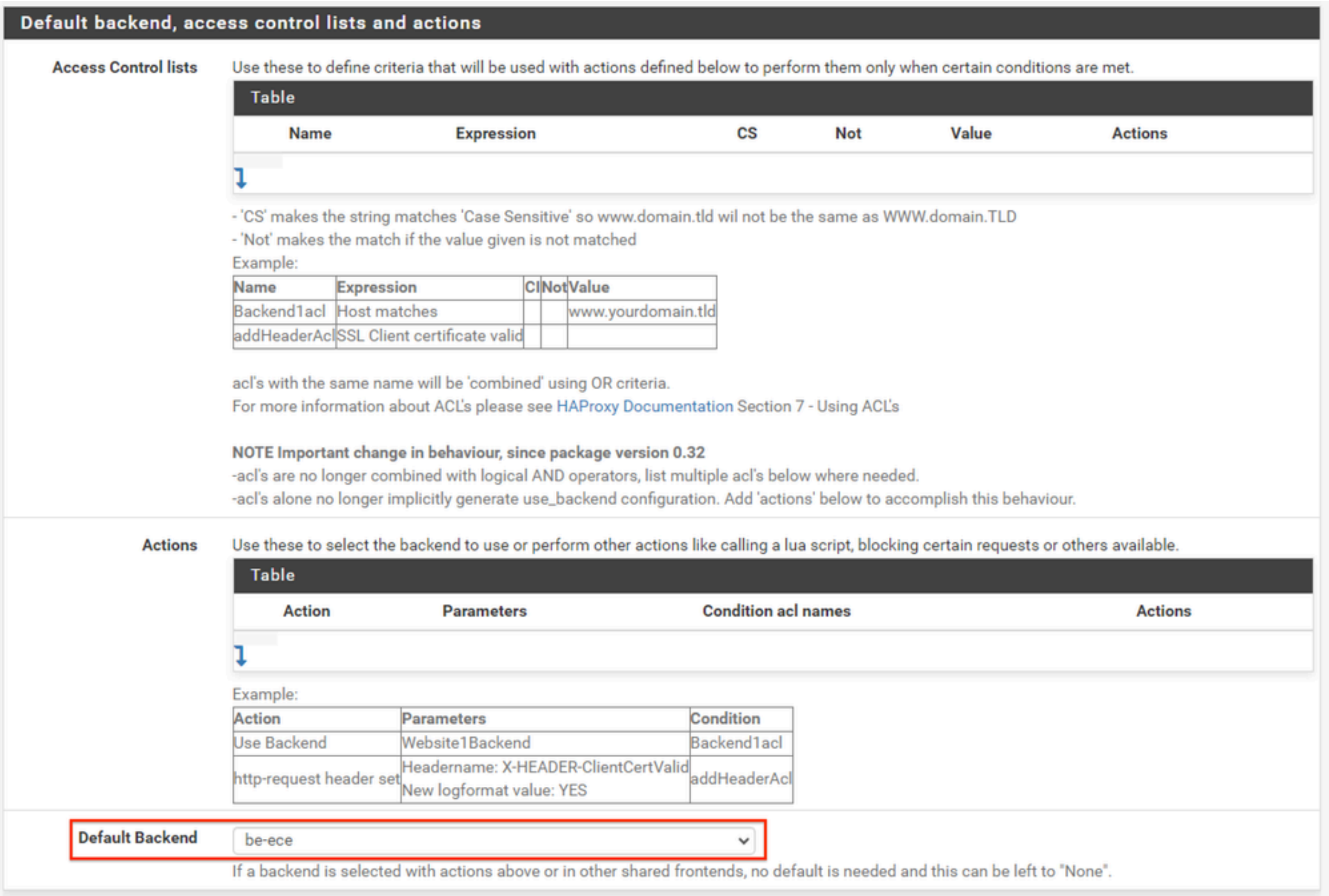
提供说明，以帮助稍后确定前端。

在External address表中：

1. 倾听地址：选择您为此网站创建的VIP。
2. 端口：输入443。
3. SSL卸载：选择此选项可插入会话cookie。

将Max connections留空。

确保Type选择为http / https（卸载）。



Default backend, access control lists and actions

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

Table

Name	Expression	CS	Not	Value	Actions
⤵					

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

Example:

Name	Expression	CI	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAcl	SSL Client certificate valid			

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

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

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

Table

Action	Parameters	Condition acl names	Actions
⤵			

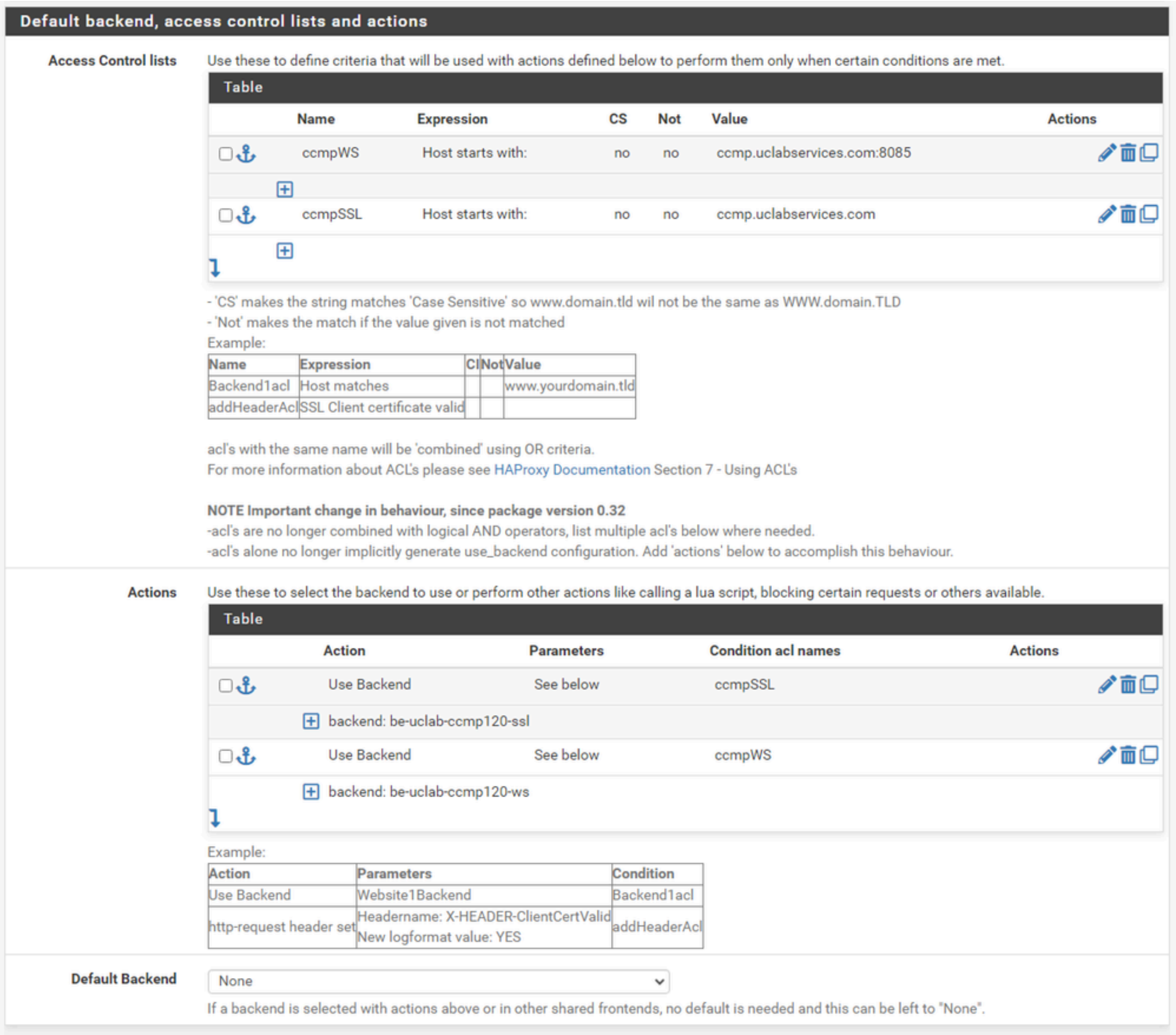
Example:

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

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

HAProxy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。



Default backend, access control lists and actions

Access Control lists

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

Table

	Name	Expression	CS	Not	Value	Actions
□ ⚓	ccmpWS	Host starts with:	no	no	ccmp.uclabservices.com:8085	✎ 🗑 ⧉
⊞						
□ ⚓	ccmpSSL	Host starts with:	no	no	ccmp.uclabservices.com	✎ 🗑 ⧉
⊞						

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

Example:

Name	Expression	CI	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAcl	SSL Client certificate valid			

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

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

Actions

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

Table

	Action	Parameters	Condition acl names	Actions
□ ⚓	Use Backend	See below	ccmpSSL	✎ 🗑 ⧉
	⊞ backend: be-uclab-ccmp120-ssl			
□ ⚓	Use Backend	See below	ccmpWS	✎ 🗑 ⧉
	⊞ backend: be-uclab-ccmp120-ws			

Example:

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

Default Backend

None ⌄

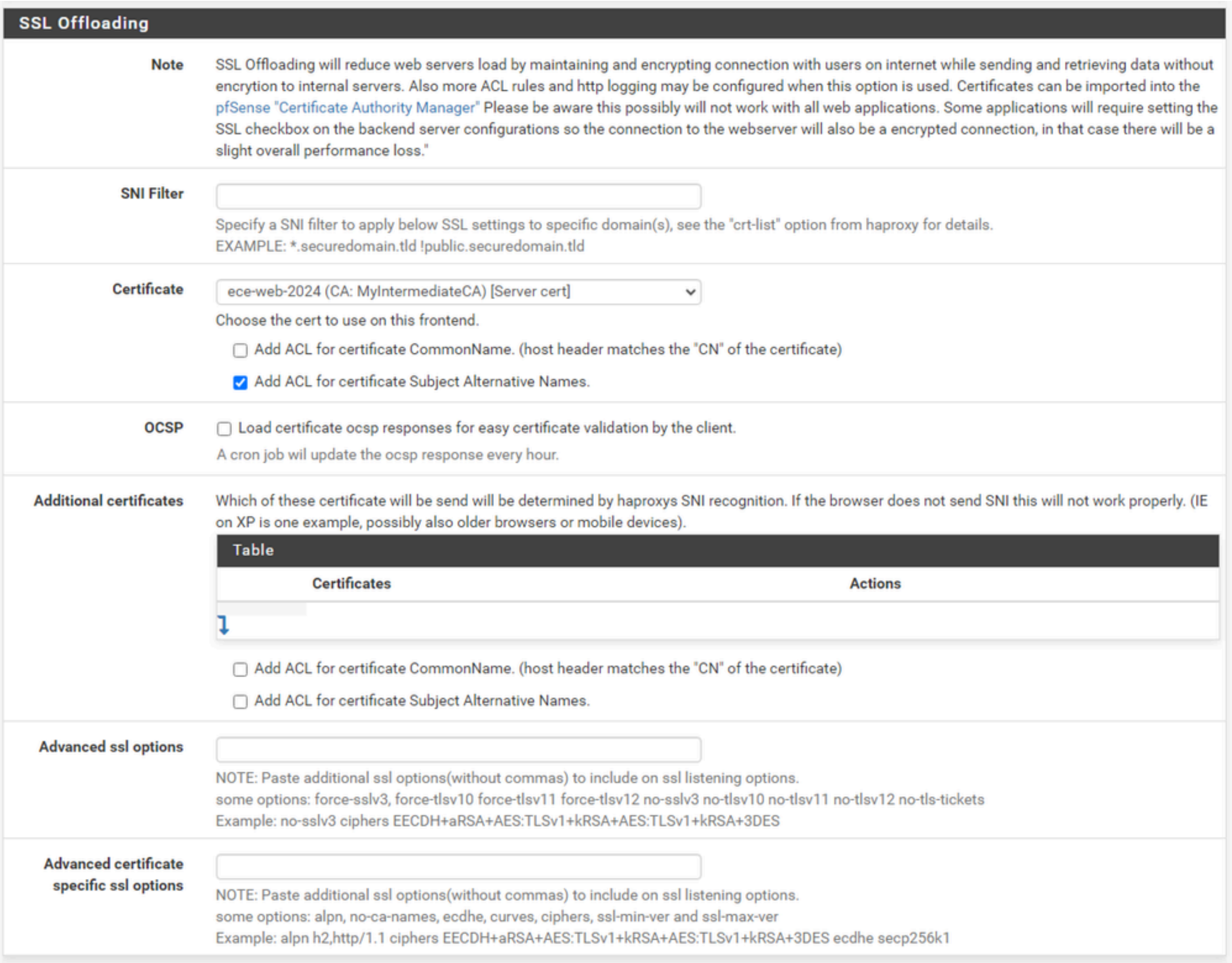
If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

HAProxy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，或者只是以名称开头。基于此，使用特定的后端。

这在欧洲经委会中并不常见。



SSL Offloading

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

SNI Filter

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

Certificate ece-web-2024 (CA: MyIntermediateCA) [Server cert]

Choose the cert to use on this frontend.

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

☑ Add ACL for certificate Subject Alternative Names.

OCSP □ Load certificate ocsp responses for easy certificate validation by the client.

A cron job wil update the ocsp response every hour.

Additional certificates Which of these certificate will be send will be determined by haproxys SNI recognition. If the browser does not send SNI this will not work properly. (IE on XP is one example, possibly also older browsers or mobile devices).

Table

Certificates	Actions

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

□ Add ACL for certificate Subject Alternative Names.

Advanced ssl options

NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: force-sslv3, force-tlsv10 force-tlsv11 force-tlsv12 no-sslv3 no-tlsv10 no-tlsv11 no-tlsv12 no-tls-tickets
Example: no-sslv3 ciphers EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES

Advanced certificate specific ssl options

NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: alpn, no-ca-names, ecdhe, curves, ciphers, ssl-min-ver and ssl-max-ver
Example: alpn h2,http/1.1 ciphers EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecdhe secp256k1

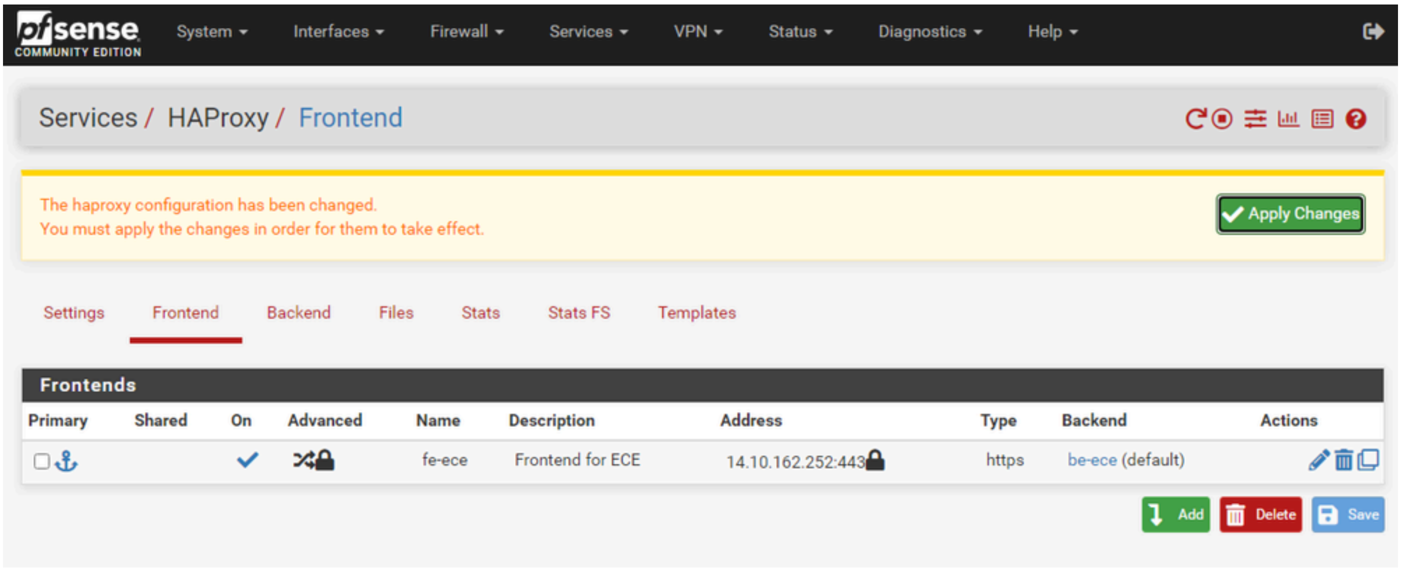
HAProxy前端 — 证书绑定

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。



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

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
□ ⚓		✓	⤮🔒	fe-ece	Frontend for ECE	14.10.162.252:443🔒	https	be-ece (default)	

HAProxy — 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）。