為ECE配置pfSense社群負載平衡器

目錄

簡介

本文檔介紹將pfSense社群版設定為企業聊天和電子郵件(ECE)的負載平衡器的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- ECE 12.x
- pfSense社群版本

採用元件

本檔案中的資訊是根據以下軟體版本：

- 歐洲經委會12.6(1)

- pfSense社群版本2.7.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

安裝pfSense

解決方案概述

pfSense Community Edition是一個多功能產品，可在單個伺服器中提供防火牆、負載平衡器、安全掃描器和許多其他服務。pfSense構建於免費BSD之上，具有最低的硬體要求。負載均衡器是HAProxy的實現，提供了易於使用的GUI來配置產品。

您可以將此負載均衡器用於ECE和聯絡中心管理門戶(CCMP)。本文檔提供了為ECE配置pfSense的步驟。

準備

步驟 1.下載pfSense軟體

使用pfSense網站下載iso安裝程式映像。

步驟 2.配置VM

按照最低要求配置VM:

· 64位amd64(x86-64)相容CPU

· 1GB或更多RAM

· 8 GB或更大的磁碟驅動器（SSD、HDD等）

·一個或多個相容網路介面卡

·用於初始安裝的可啟動USB驅動器或高容量光碟機（DVD或BD）

實驗安裝只需要一個網路介面(NIC)。運行裝置的方法有多種，但最簡單的方法是使用單個NIC（也稱為單臂模式）。在單臂模式下，有一個介面與網路通訊。雖然對於實驗室來說這是一種簡單且充分的方法，但它並不是最安全的方式。

配置裝置的更安全的方法是至少擁有兩個NIC。一個NIC是WAN介面，直接與公共Internet通訊。第二個NIC是LAN介面，與內部公司網路通訊。您還可以新增其他介面，以便與具有不同安全和防火牆規則的網路各個部分通訊。例如，您可以用一個NIC連線到公共網際網路，一個連線到DMZ網路（所有外部可訪問的Web伺服器都連線到該網路），第三個網絡卡連線到公司網路。這樣，您就可以讓內部和外部使用者安全地訪問儲存在DMZ中的同一組Web伺服器。確保在實施前瞭解任何設計的安全影響。與安全工程師協商，確保針對您的具體實施遵循最佳實踐。

安裝

步驟 1.將ISO安裝到VM

步驟 2.開啟VM電源，然後按照提示進行安裝。

請參閱本檔案以瞭解逐步說明。

網路設定

您必須為裝置分配IP地址才能繼續配置。

注意：本文檔顯示的是一個配置在一臂模式下的裝置。

步驟 1.配置VLAN

如果您需要VLAN支援，請回答第一個問題。否則，請回答n。

步驟 2.分配WAN介面

WAN介面是雙臂模式下的裝置的不安全端，也是單臂模式下的唯一介面。出現提示時輸入介面名稱。

步驟 3.分配LAN介面

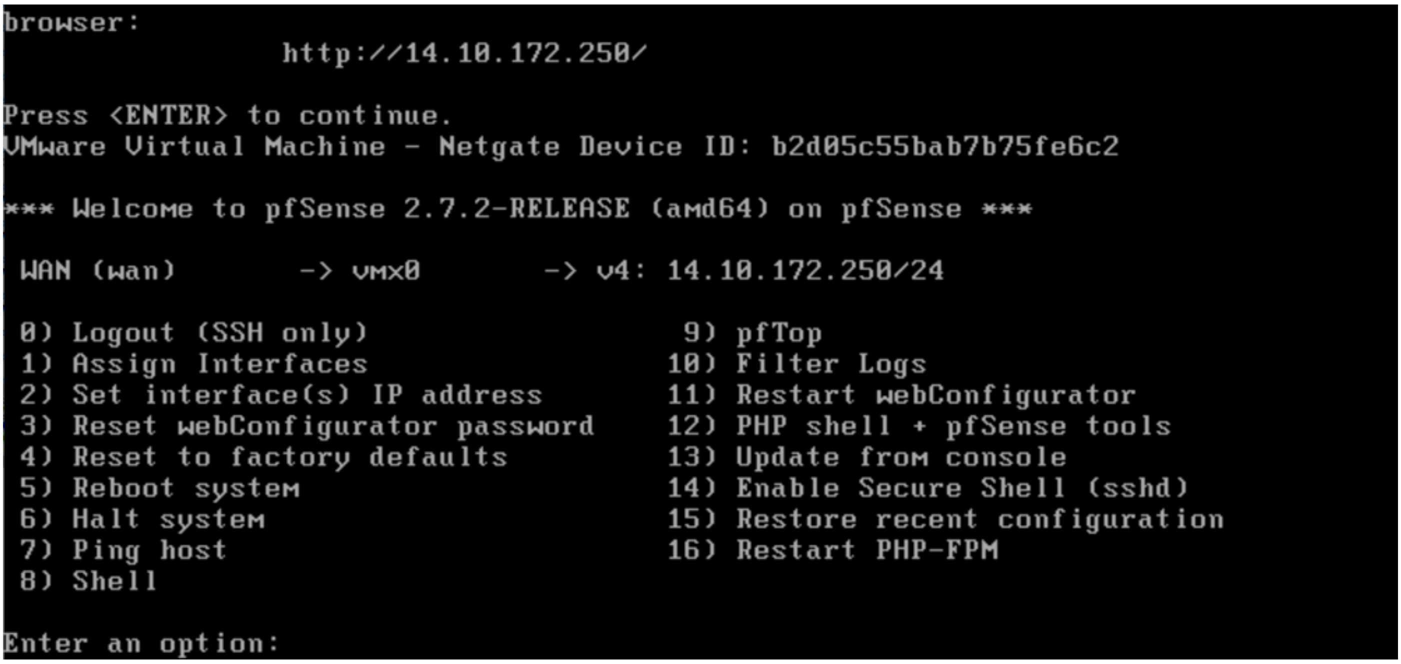
LAN介面是雙臂模式下裝置的安全端。如果需要，請在系統提示時輸入介面名稱。

步驟 4.分配任何其他介面

配置您的特定安裝所需的任何其他介面。這些是可選的，並不常見。

步驟 5.為管理介面分配IP地址

如果您的網路支援DHCP，則分配的IP地址將顯示在控制檯螢幕中。



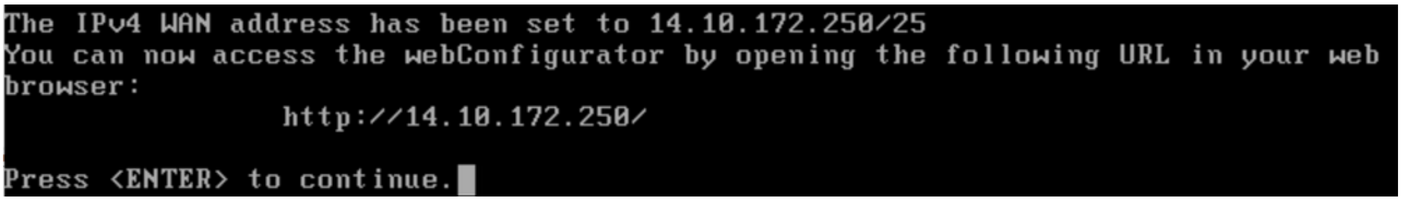
```
browser:
               http://14.10.172.250/

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控制檯

如果沒有分配地址，或者如果您希望分配特定地址，請執行以下步驟。

1. 從控制檯選單中選擇選項2。
2. 回答n以禁用DHCP。
3. 輸入WAN介面的IPv4地址。
4. 輸入位計數中的網路掩碼。(24 = 255.255.255.0,16 = 255.255.0.0,8 = 255.0.0.0)
5. 輸入WAN介面的網關地址。
6. 如果您希望此網關成為裝置的預設網關，請回答y以進入網關提示，否則回答n。
7. 如果需要，配置IPv6的NIC。
8. 禁用介面上的DHCP伺服器。
9. 回答y以在webConfigurator協定上啟用HTTP。這將在後續步驟中使用。

然後，您將收到設定已更新的確認。



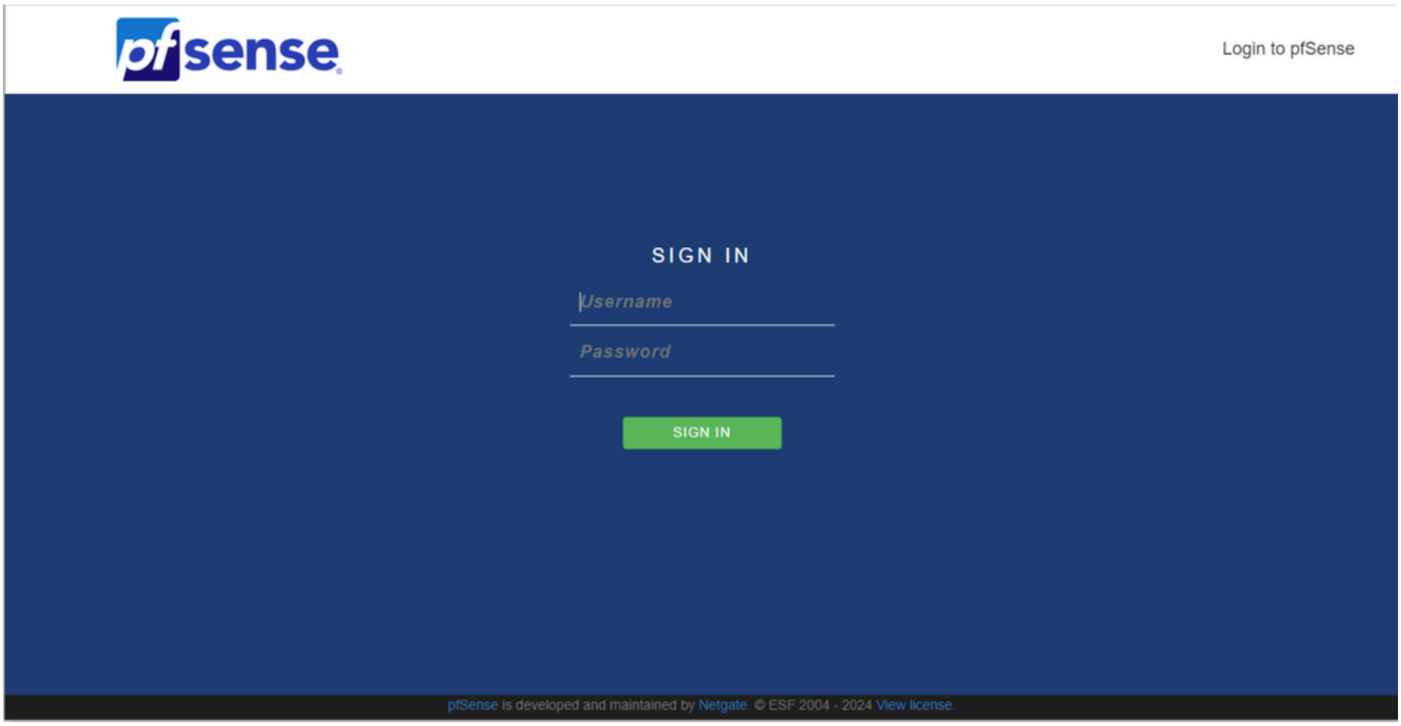
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
               http://14.10.172.250/

Press <ENTER> to continue.
```

pfSense確認

完成初始設定

步驟 1.開啟Web瀏覽器並導航至:http://<ip_address_of_appliance>

注意：您最初必須使用HTTP而不是HTTPS。



Login to pfSense

SIGN IN

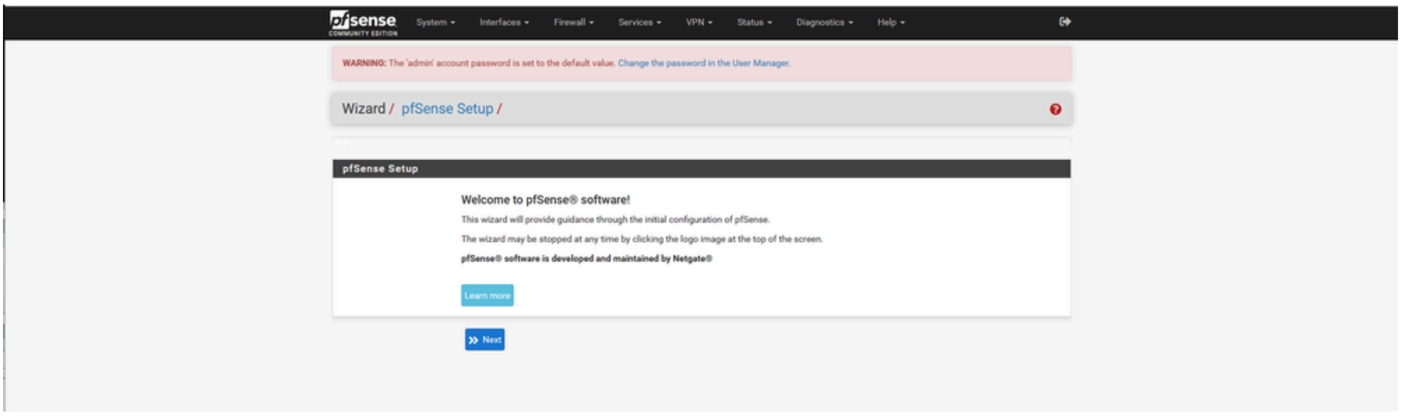
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

pfSense管理員登入

步驟 2.使用預設登入名admin / pfSense登入

步驟 3.完成初始設定

按一下前兩個螢幕中的「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!

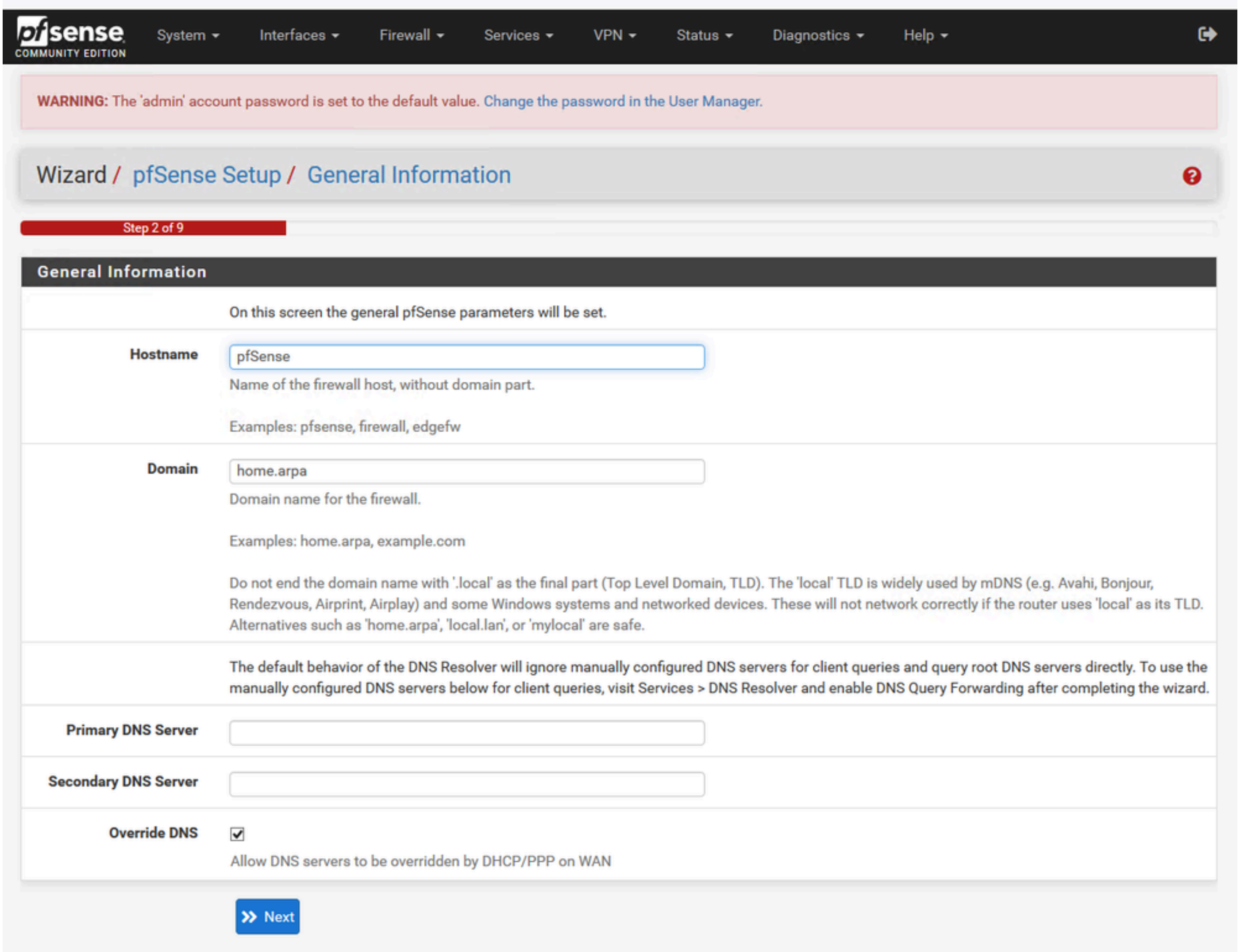
This wizard will provide guidance through the initial configuration of pfSense.

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安裝嚮導 — 1

提供主機名、域名和DNS伺服器資訊。



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

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

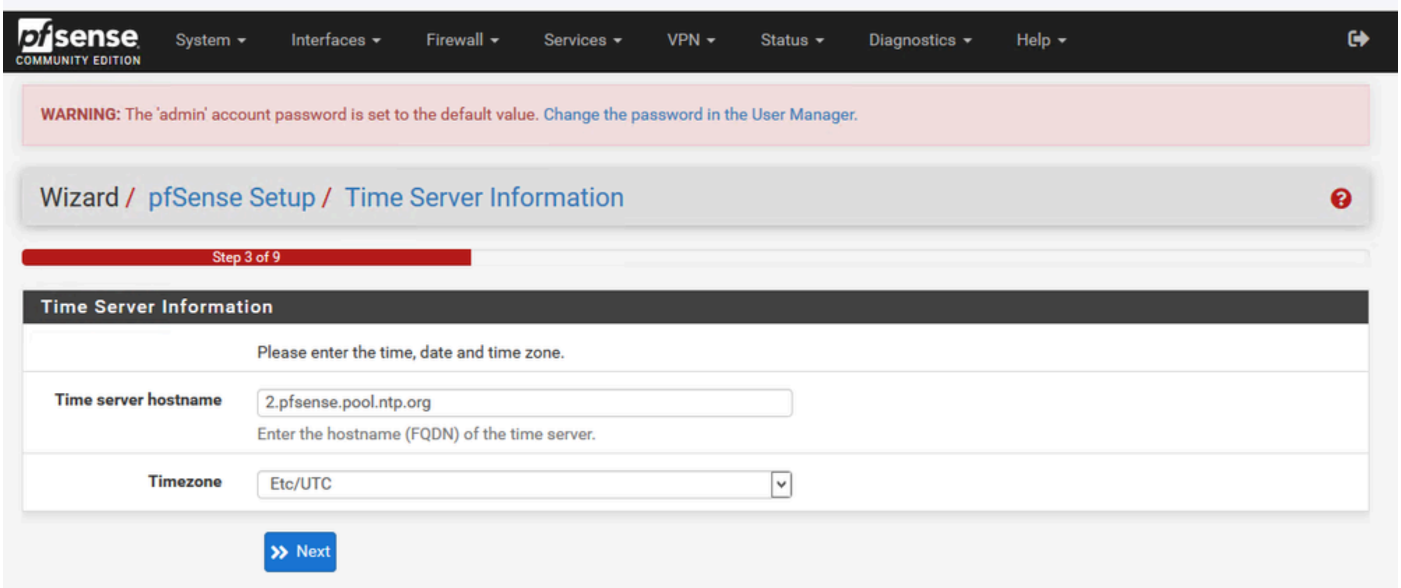
On this screen the general pfSense parameters will be set.

Hostname	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安裝嚮導 — 2

驗證IP地址資訊。如果您最初選擇了DHCP，現在您可以更改它。

提供NTP時間伺服器主機名並在下拉選單中選擇正確的時區。



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

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname	2.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone	Etc/UTC

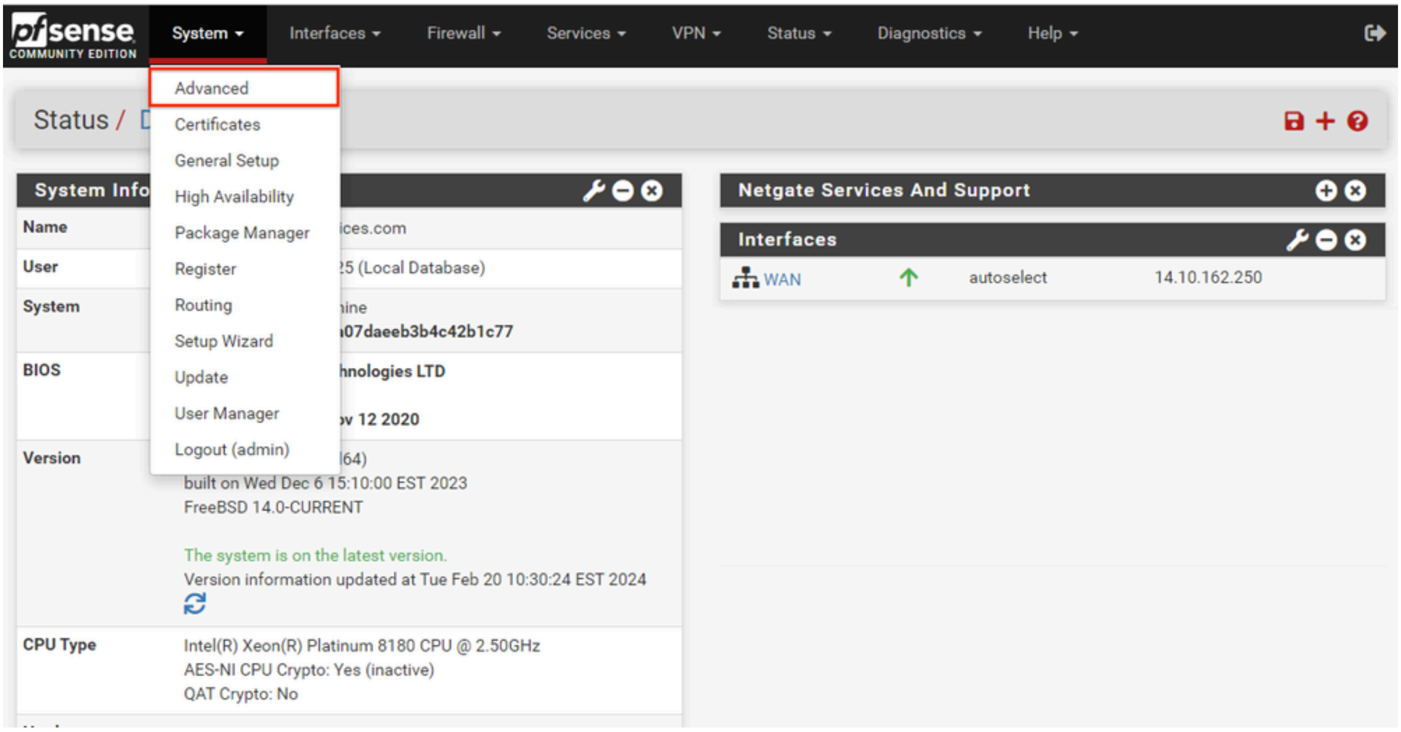
pfSense安裝嚮導 — 3

繼續通過安裝嚮導直到結束。介面GUI會重新啟動，完成後，系統會將您重新導向到新URL。

配置基本管理員設定

步驟 1.登入到管理介面

步驟 2.從「系統」下拉選單中選擇「高級」

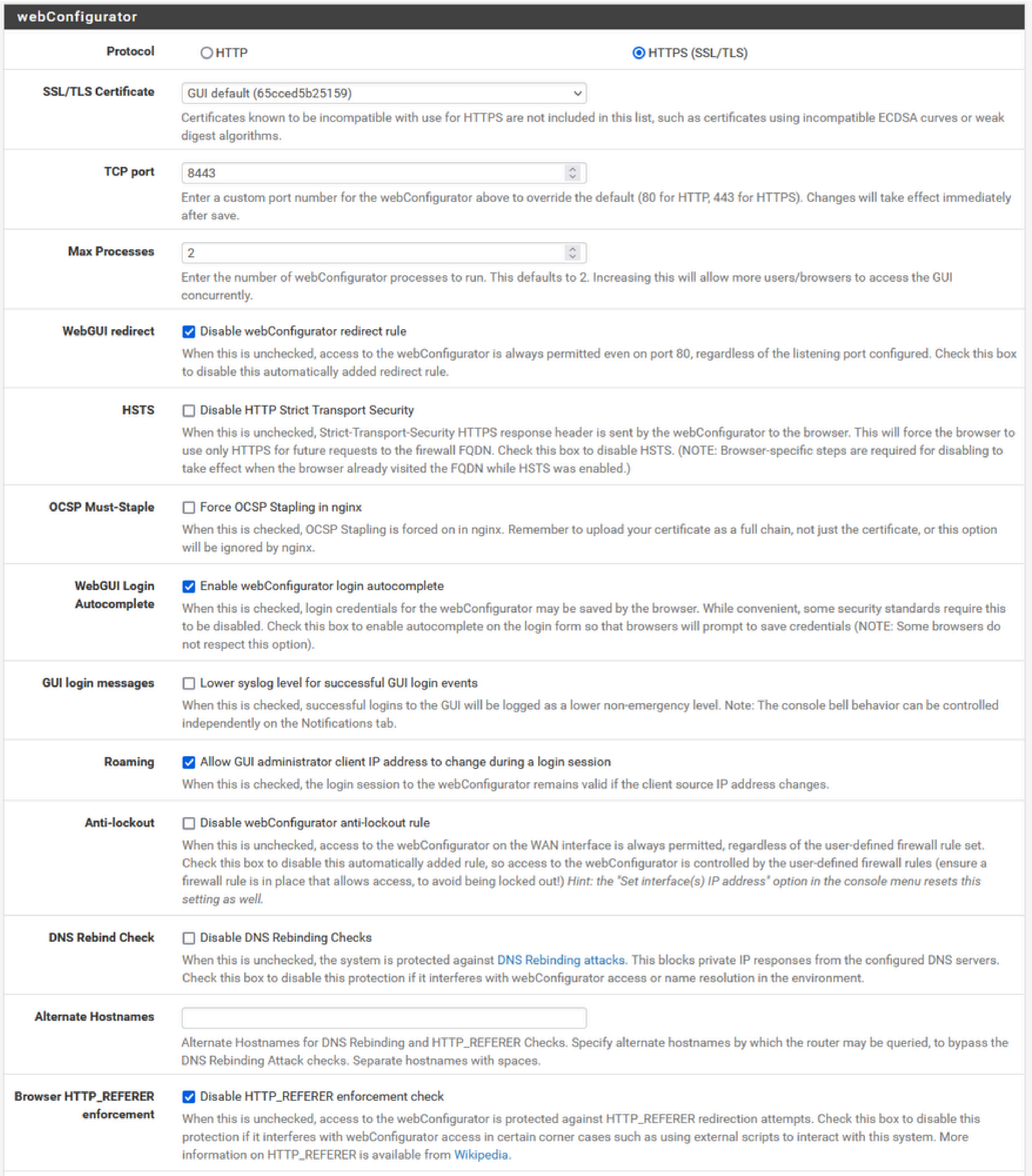


Name	ices.com
User	25 (Local Database)
System	hine a07daeeb3b4c42b1c77
BIOS	hnologies LTD ov 12 2020
Version	64) built on Wed Dec 6 15:10:00 EST 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 10:30:24 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

WAN	↑	autoselect	14.10.162.250

pfSense GUI - Admin下拉選單

步驟 3.更新WebConfigurator設定



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.

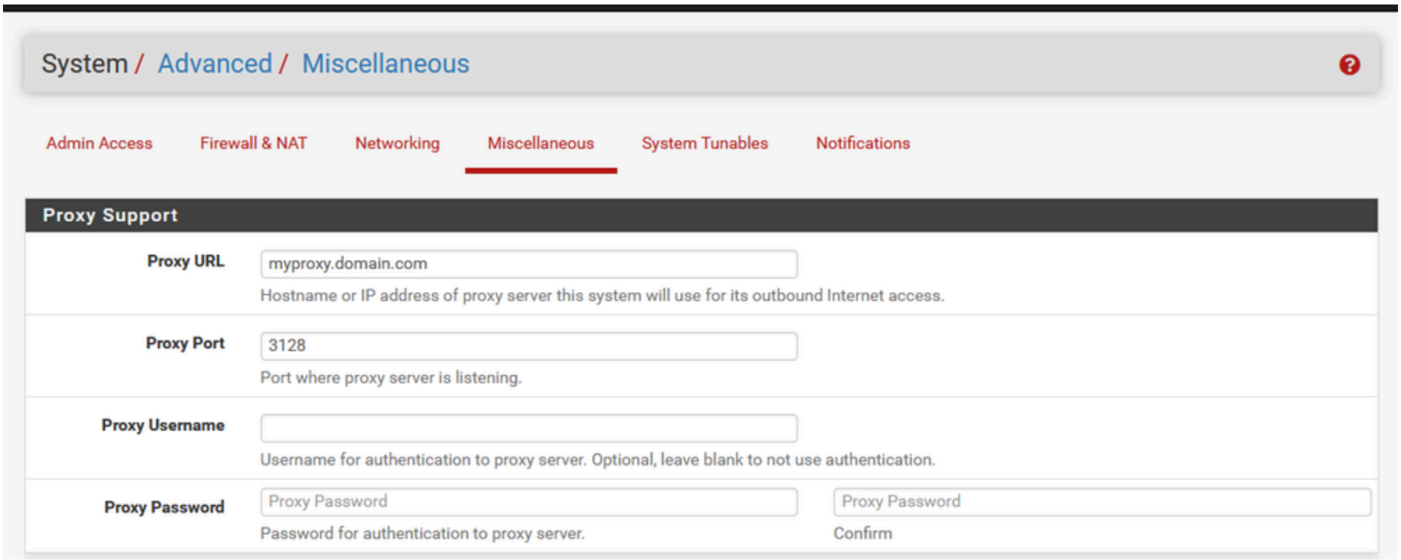
pfSense GUI — 管理員配置

1. 選擇HTTPS(SSL/TLS)協定。
2. 此時將SSL/TLS證書保留為自簽名證書。
3. 將TCP埠更改為443以外的埠，以更好地保護介面並防止埠重疊問題。
4. 選擇WebGUI重定向選項以禁用埠80上的管理介面。
5. 選擇Browser HTTP_REFERER enforcement選項。
6. 通過選擇啟用安全外殼選項啟用安全外殼。

✎ 註：請確保在繼續操作之前,選擇「儲存」按鈕。然後您將重定向到新的https連結。

步驟 4.配置代理伺服器（如果需要）

如果需要，請在「其他」頁籤上配置代理資訊。要完成設定和配置，裝置必須能夠訪問Internet。



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 Password for authentication to proxy server.
	Proxy Password Confirm

pfSense GUI — 代理配置

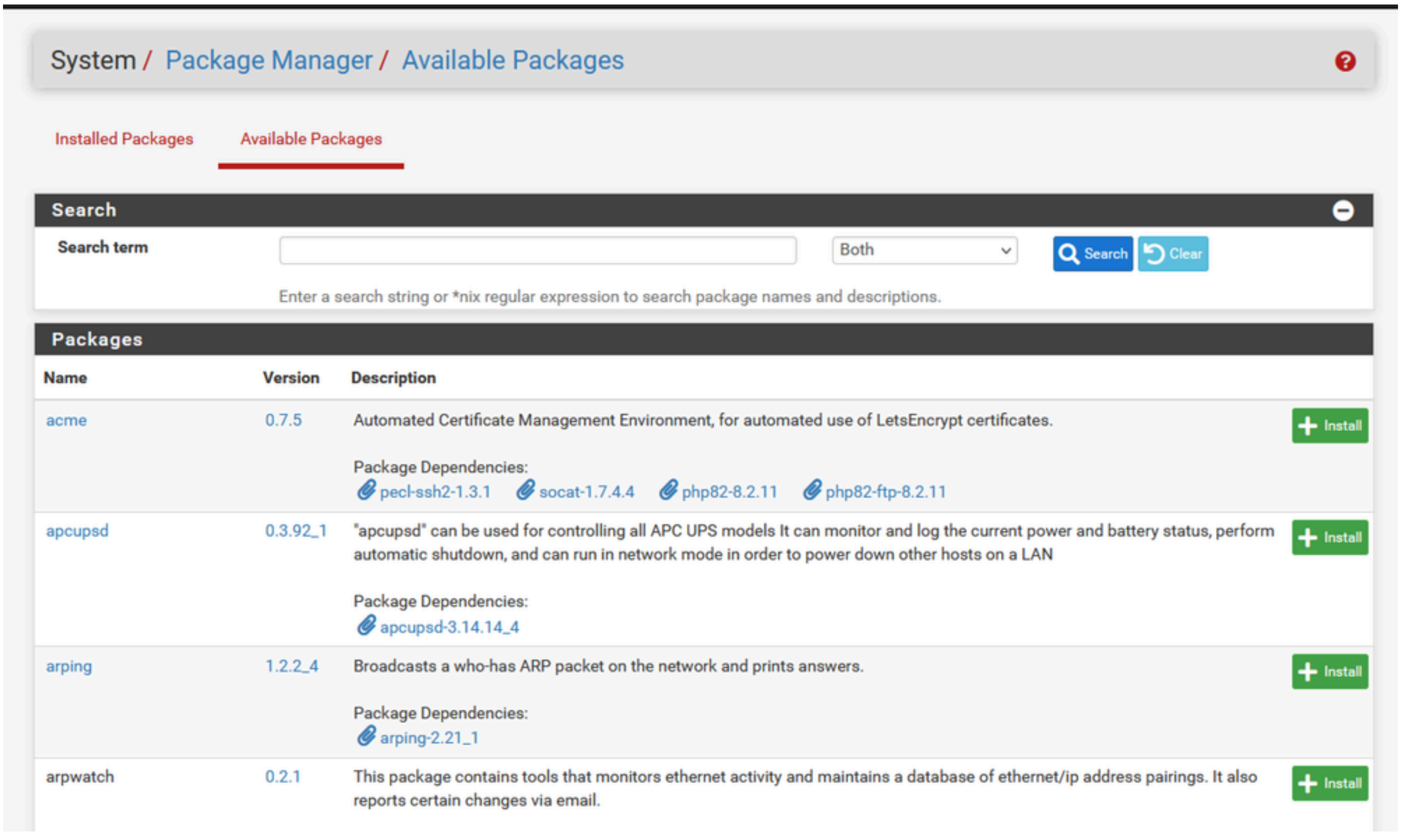
✎ 註：請確保在進行更改後選擇「儲存」按鈕。

新增所需的包

步驟 1.選擇「系統」>「包管理器」

步驟 2.選擇可用包

✎ 註：載入所有可用的軟體包可能需要幾分鐘的時間。如果超時，請確認DNS伺服器配置正確。通常，裝置的重新啟動會修復Internet連線。



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 — 包清單

步驟 3.查詢並安裝所需的軟體包

1. haproxy
2. Open-VM工具

註：請勿選擇haproxy級包。

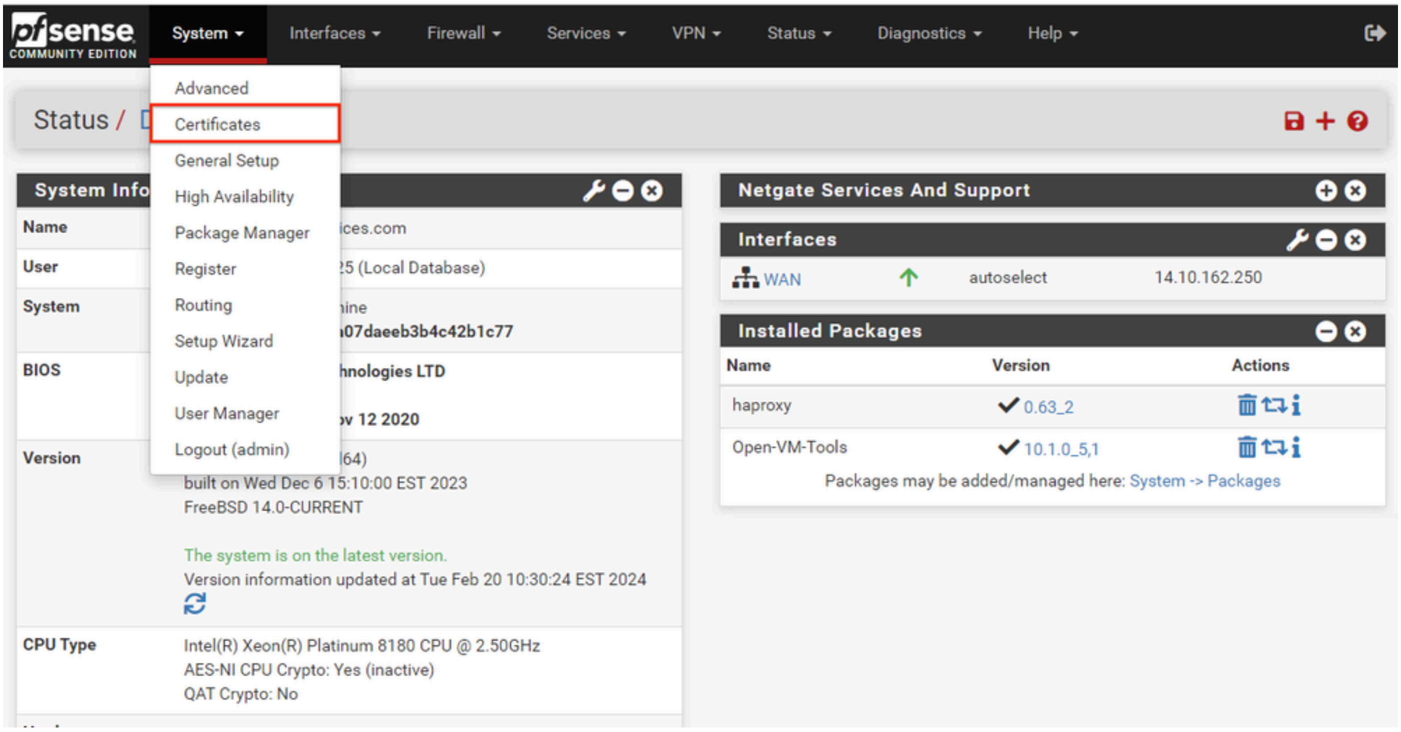
配置證書

pfSense可以建立自簽名證書，也可以與公共CA（內部CA）整合，或者可以充當CA並頒發CA簽名證書。本指南說明與內部CA整合的步驟。

開始此部分之前，請確保這些專案可用。

1. CA的根證書儲存為PEM或Base-64編碼格式。
2. CA的所有中繼（有時稱為簽發）憑證儲存為PEM或Base-64編碼格式。

步驟 1.從「系統」下拉選單中選擇「證書」



System Info

Name	ices.com
User	25 (Local Database)
System	hine 07daeeb3b4c42b1c77
BIOS	hnologies LTD ov 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

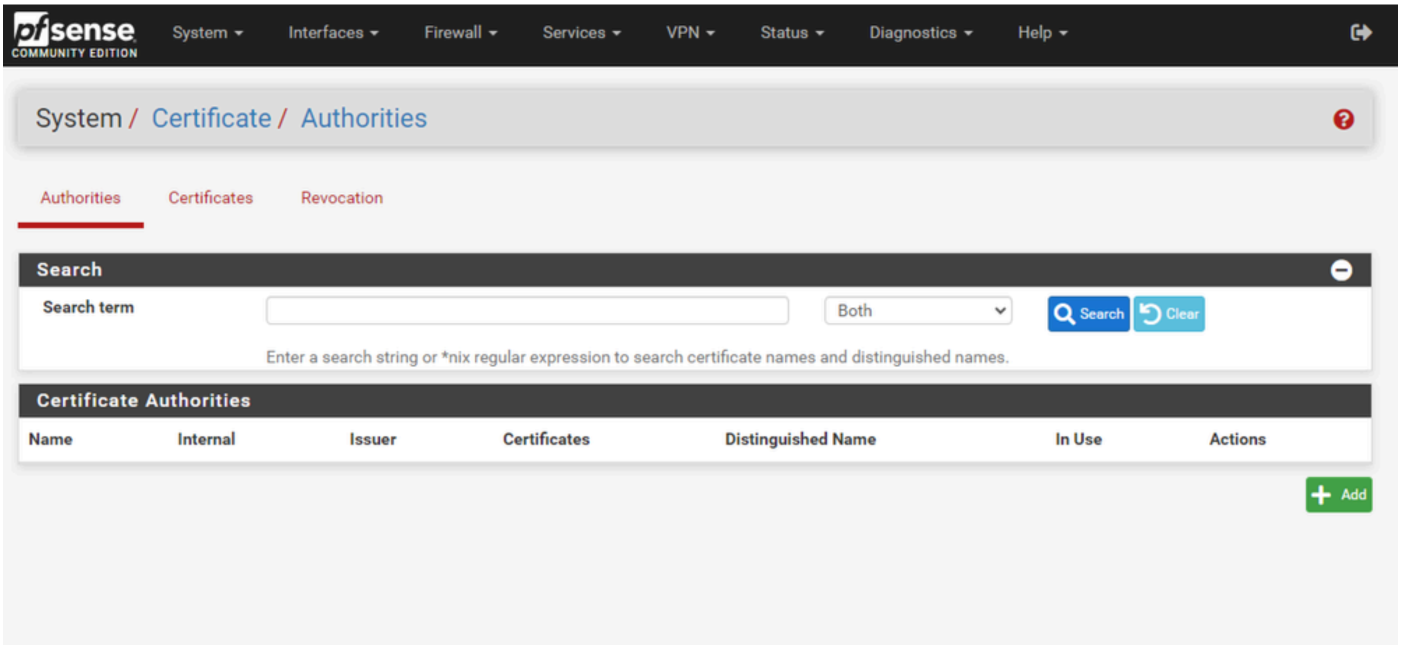
Installed Packages

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 - Certificates下拉選單

步驟 2.匯入CA根證書



System / Certificate / Authorities

Search

Search term

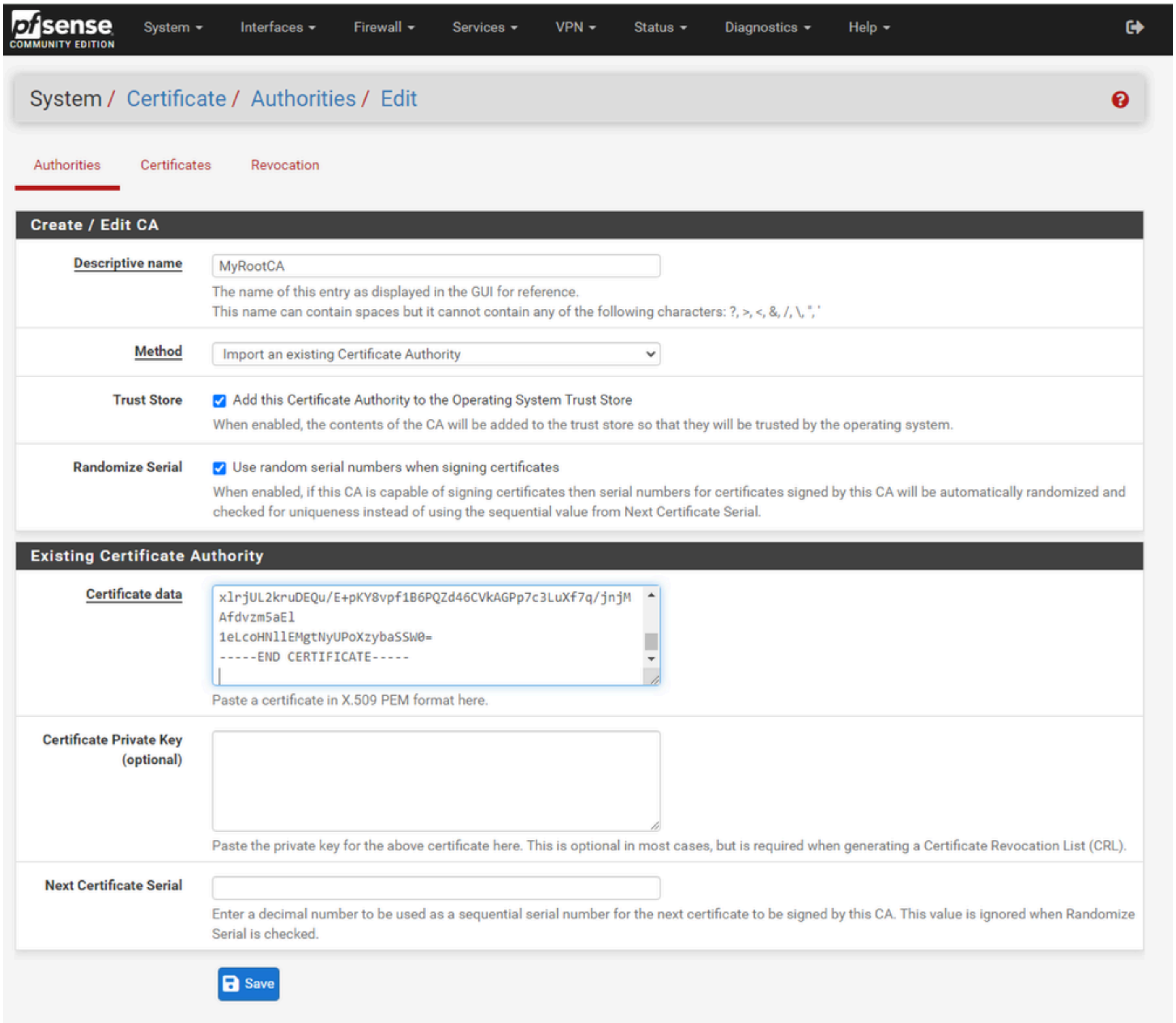
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

pfSense GUI - CA證書清單

選擇Add按鈕。



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
1eLcoHNl1EMgtNyUPoXzybaSSW0=
-----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匯入

如下圖所示：

1.提供一個唯一的描述性名稱

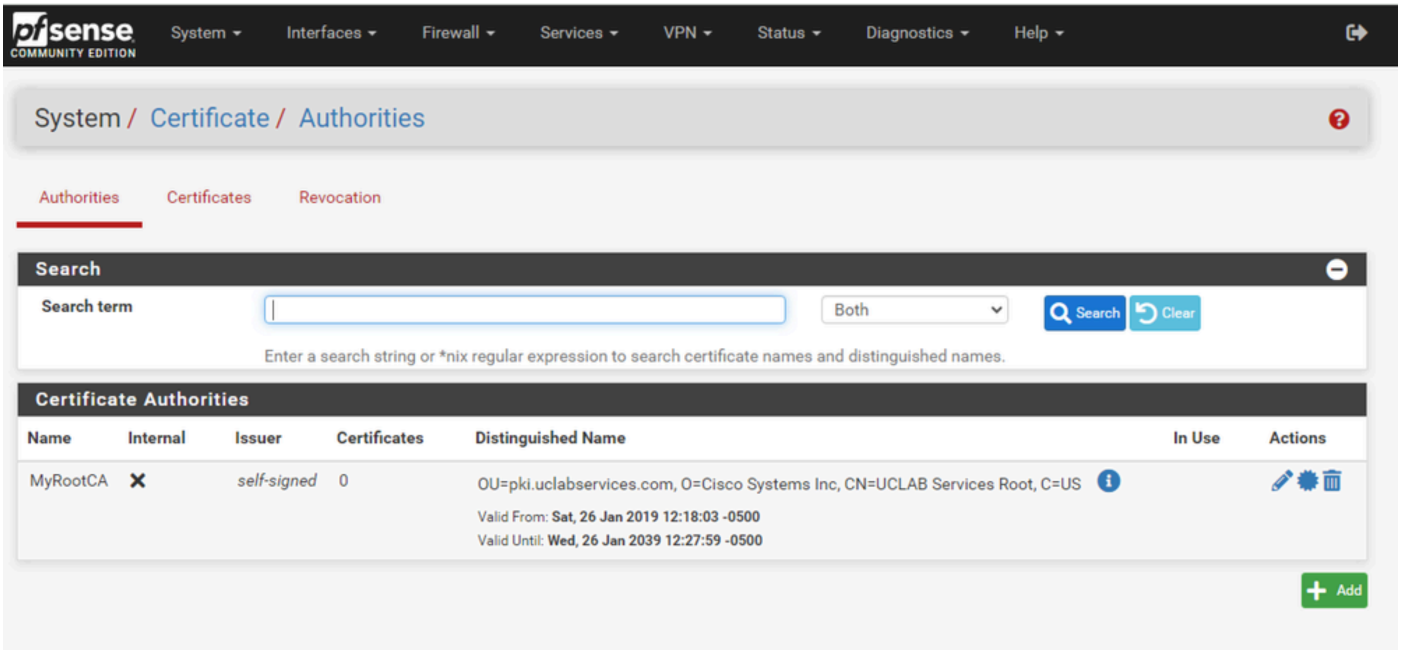
2.從「方法」下拉選單中選擇「匯入現有證書頒發機構」。

3.確保選中「信任儲存」和「隨機序列」覈取方塊。

4.將整個證書貼上到「證書資料」文本框中。確保包括-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----行。

5.選擇儲存。

6.驗證是否已匯入證書，如下圖所示。



Search term: Both

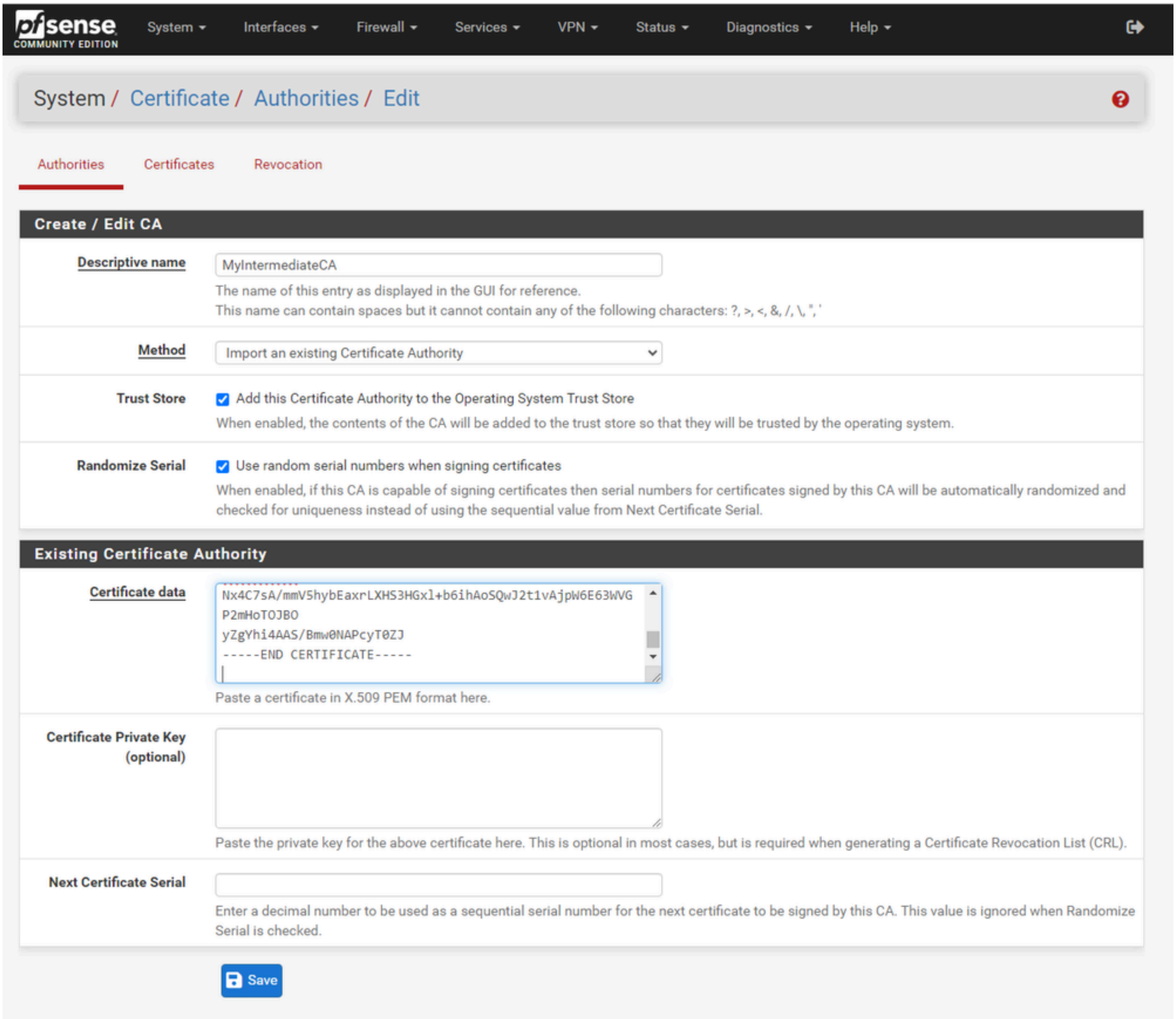
Enter a search string or *nix regular expression to search certificate names and distinguished names.

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清單

步驟 3.匯入CA中間證書



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):

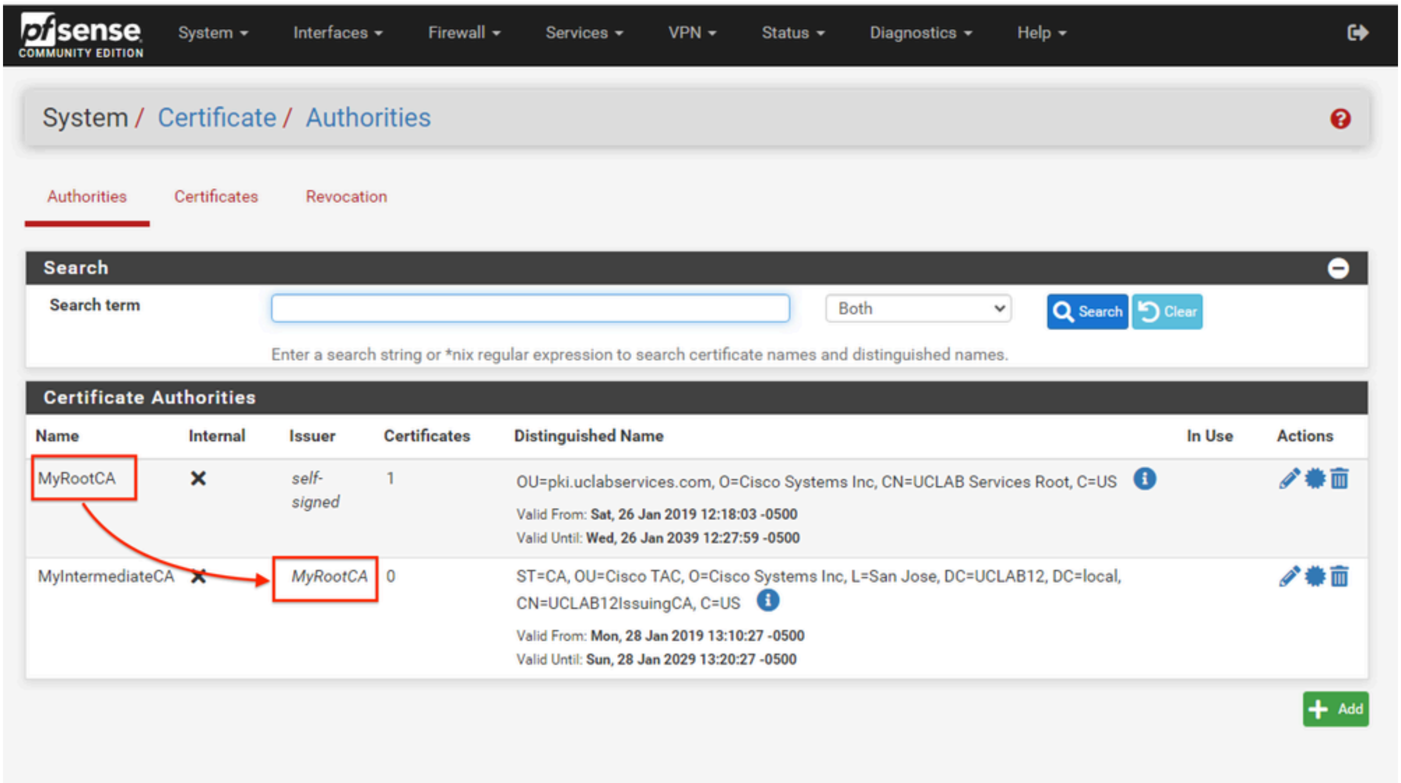
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

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中間匯入

重複這些步驟以匯入根CA證書以匯入中間CA證書。



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**		

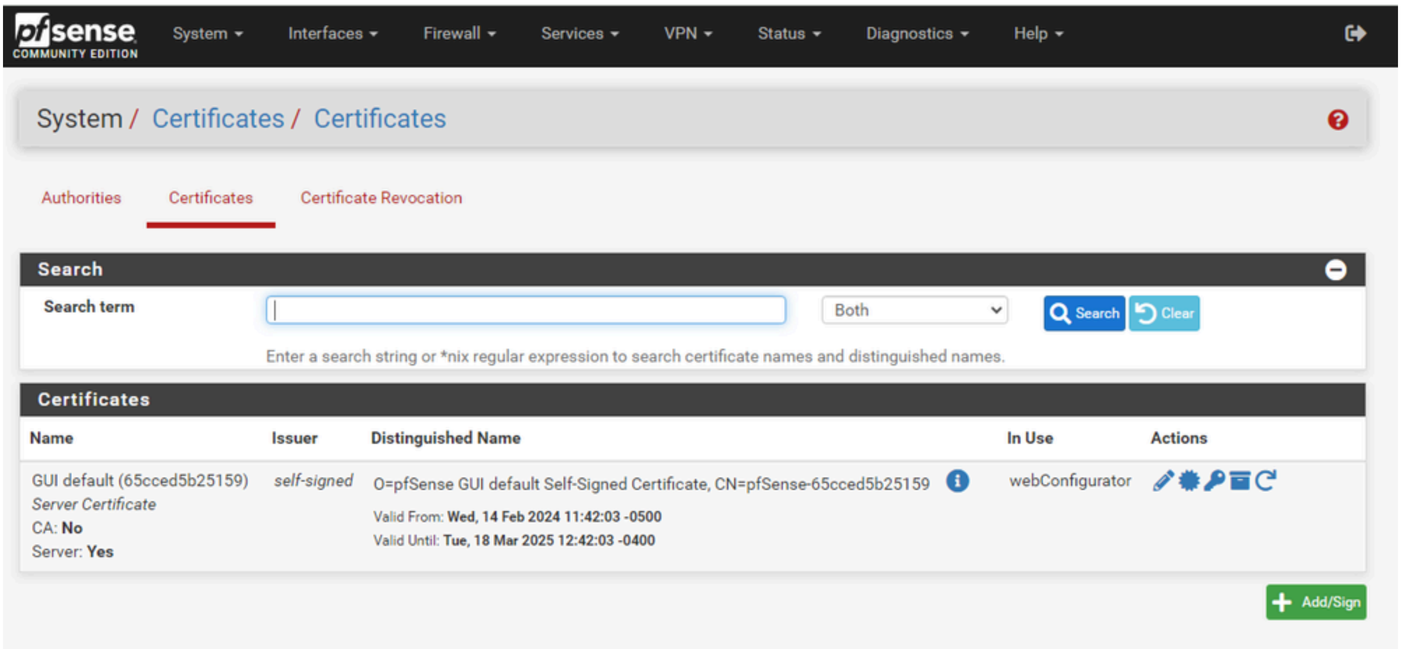
pfSense GUI - CA連結

檢視「Certificate Authorities（證書頒發機構）」，確保已正確將中間證書連結到根證書，如下圖所示。

步驟 4.為負載平衡網站建立和匯出CSR

以下說明建立CSR、匯出CSR，然後匯入簽署憑證的步驟。如果已經具有PFX格式的現有證書，則可以匯入此證書。有關這些步驟，請參閱pfSense文檔。

1.選擇「證書」選單，然後選擇新增/簽名按鈕。



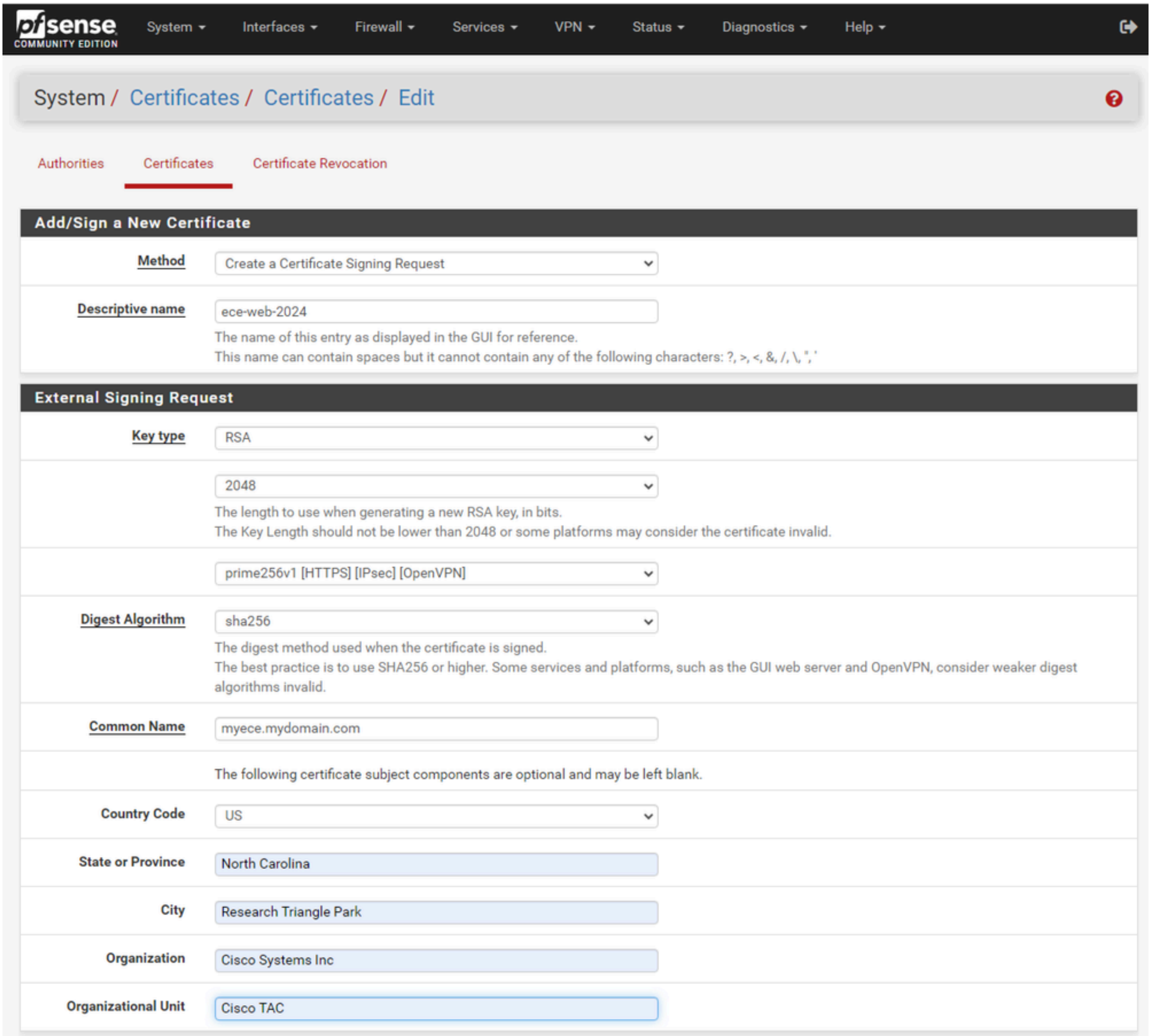
Enter a search string or *nix regular expression to search certificate names and distinguished names.

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 — 證書清單

2.完成「證書簽名請求」表單。



System / Certificates / Certificates / Edit

Authorities | Certificates | Certificate Revocation

Add/Sign a New Certificate

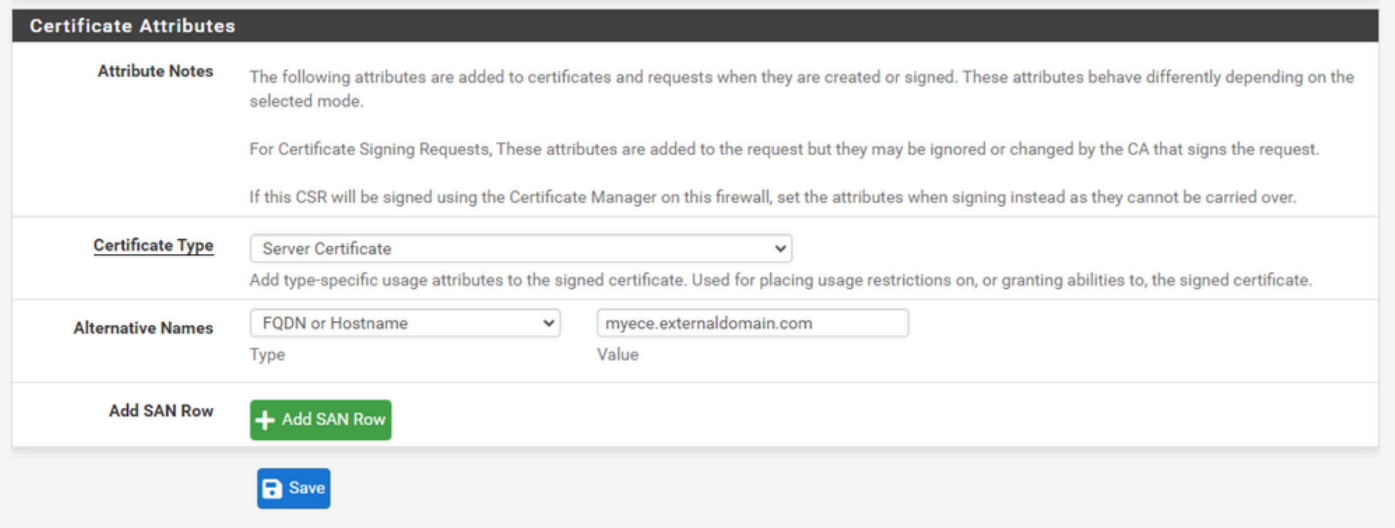
Method	Create a Certificate Signing Request
Descriptive name	ece-web-2024 The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

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建立

- 方法：從下拉選單中選擇「建立證書簽名請求」
- 描述性名稱：提供證書的名稱
- 金鑰型別和摘要演算法：檢視以確保它們符合您的要求
- 通用名稱：提供完全限定的域名網站
- 根據您的環境要求提供其餘證書資訊



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: FQDN or Hostname (Type) — myece.externaldomain.com (Value)

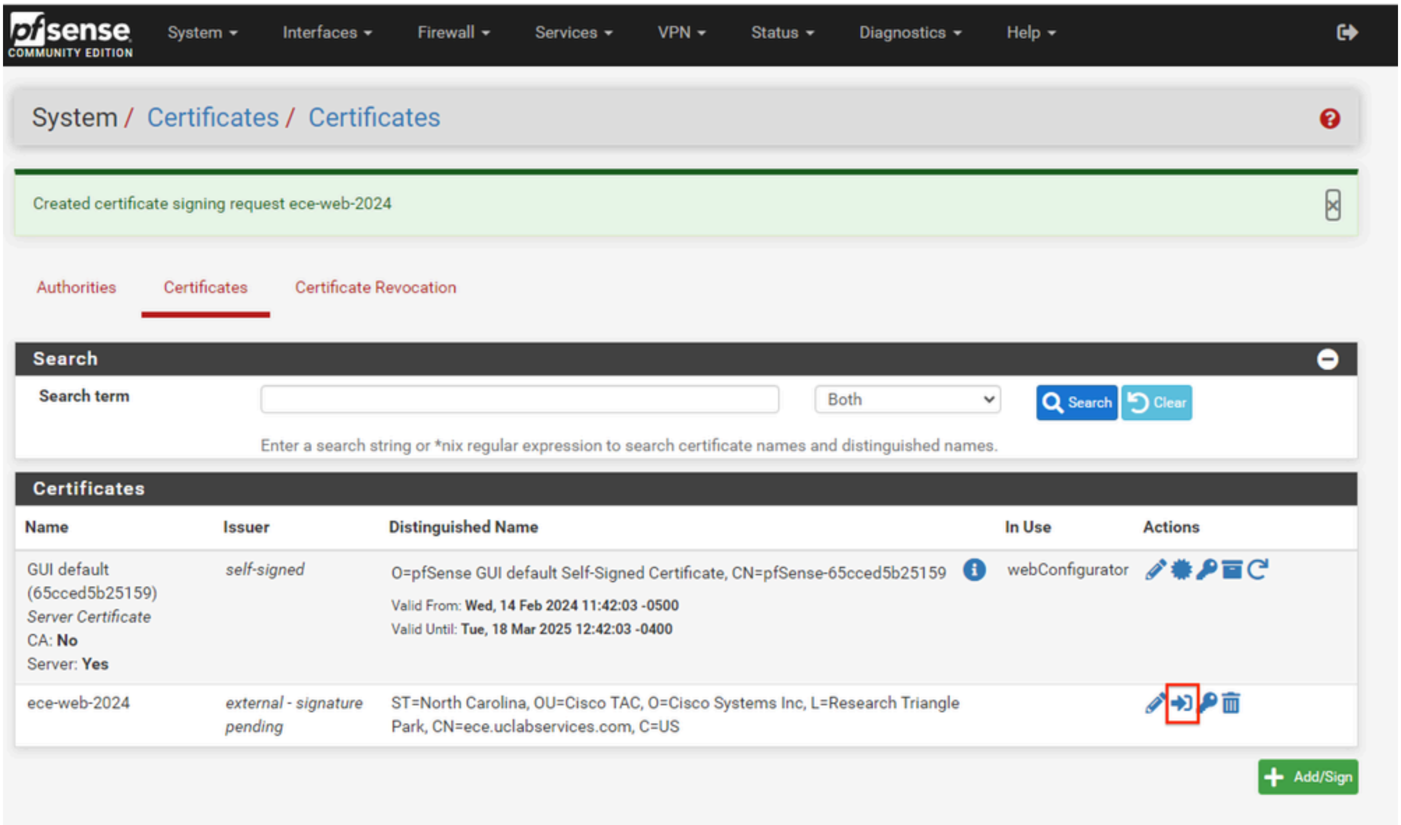
pfSense GUI - CSR高級

- Certificate Type：在下拉選單中選擇Server Certificate。
- 備用名稱：提供實施所需的任何主題備用名稱(SAN)。

✎ 注意：公用名會自動新增到SAN欄位中。您只需要新增其他所需名稱。

所有欄位都正確後，選擇Save。

3.將CSR匯出到檔案。



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

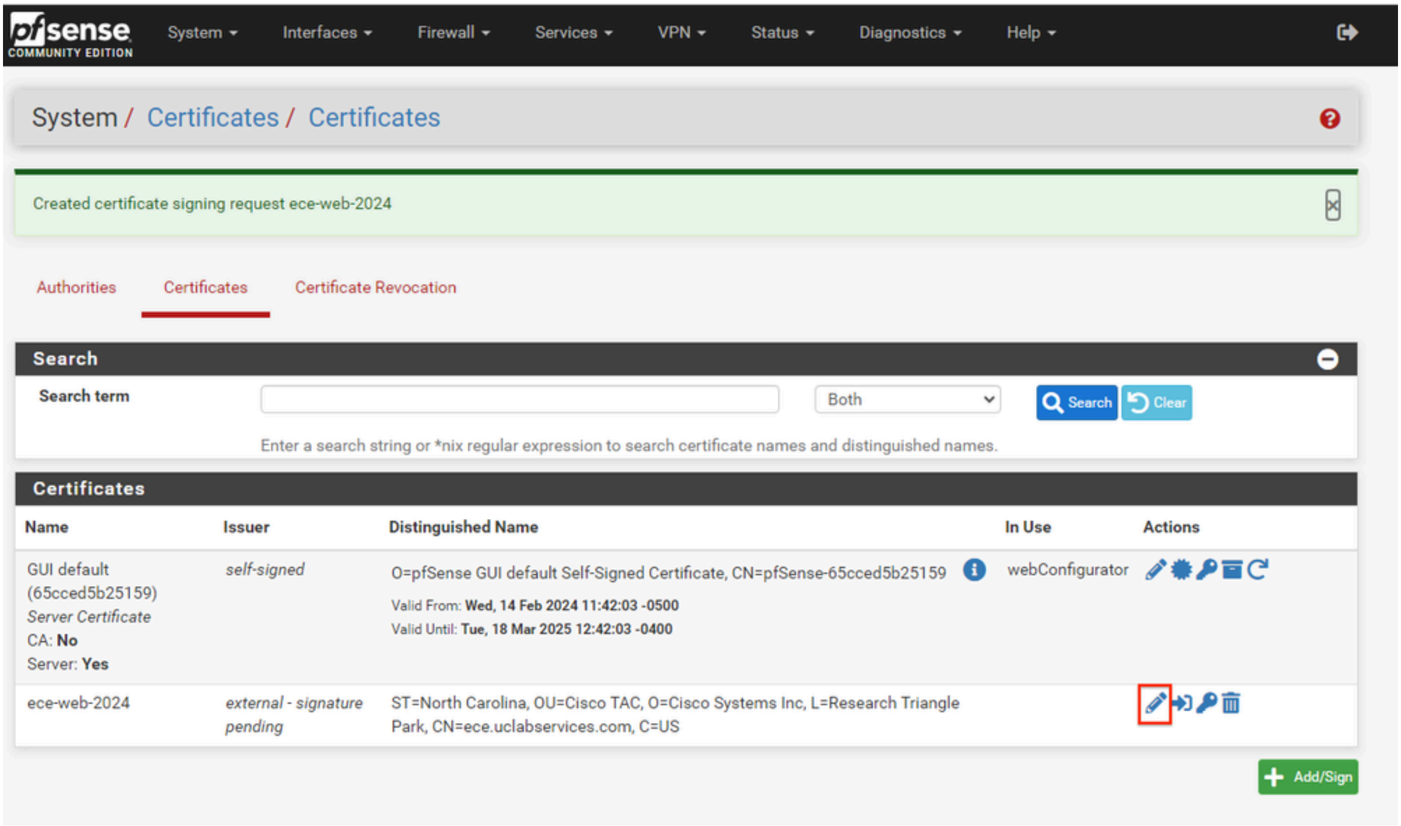
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: **Wed, 14 Feb 2024 11:42:03 -0500** Valid Until: **Tue, 18 Mar 2025 12:42:03 -0400**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

選擇「匯出」按鈕儲存CSR，然後與CA進行簽名。獲得簽名證書後，將其另存為PEM或Base-64檔

案以完成該過程。

4.匯入簽名證書。



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

System / Certificates / Certificates

Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

Search

Search term

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

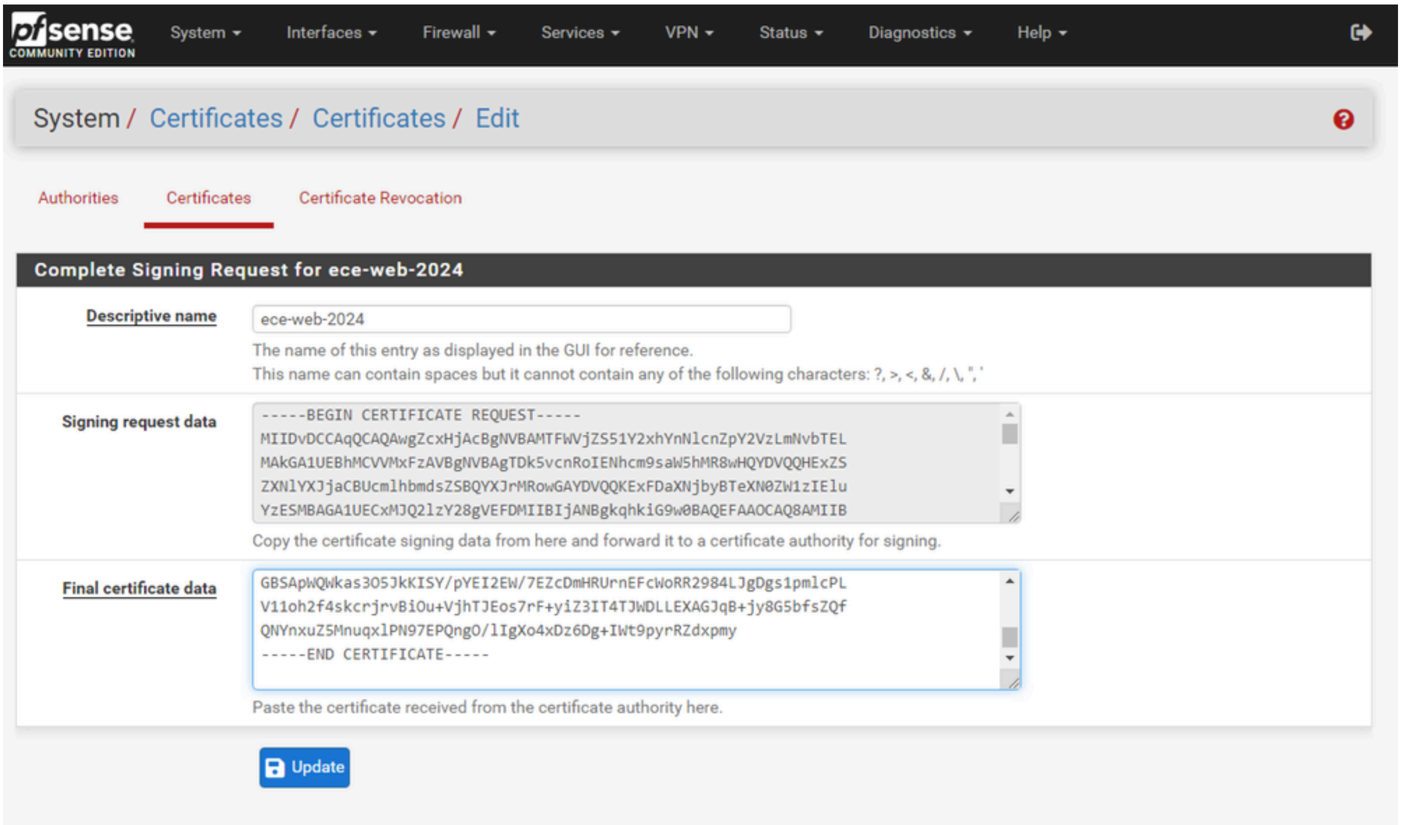
Certificates

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 — 憑證匯入

選擇鉛筆圖示以匯入簽名證書。

5.在表單中貼上證書資料。



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-----
```

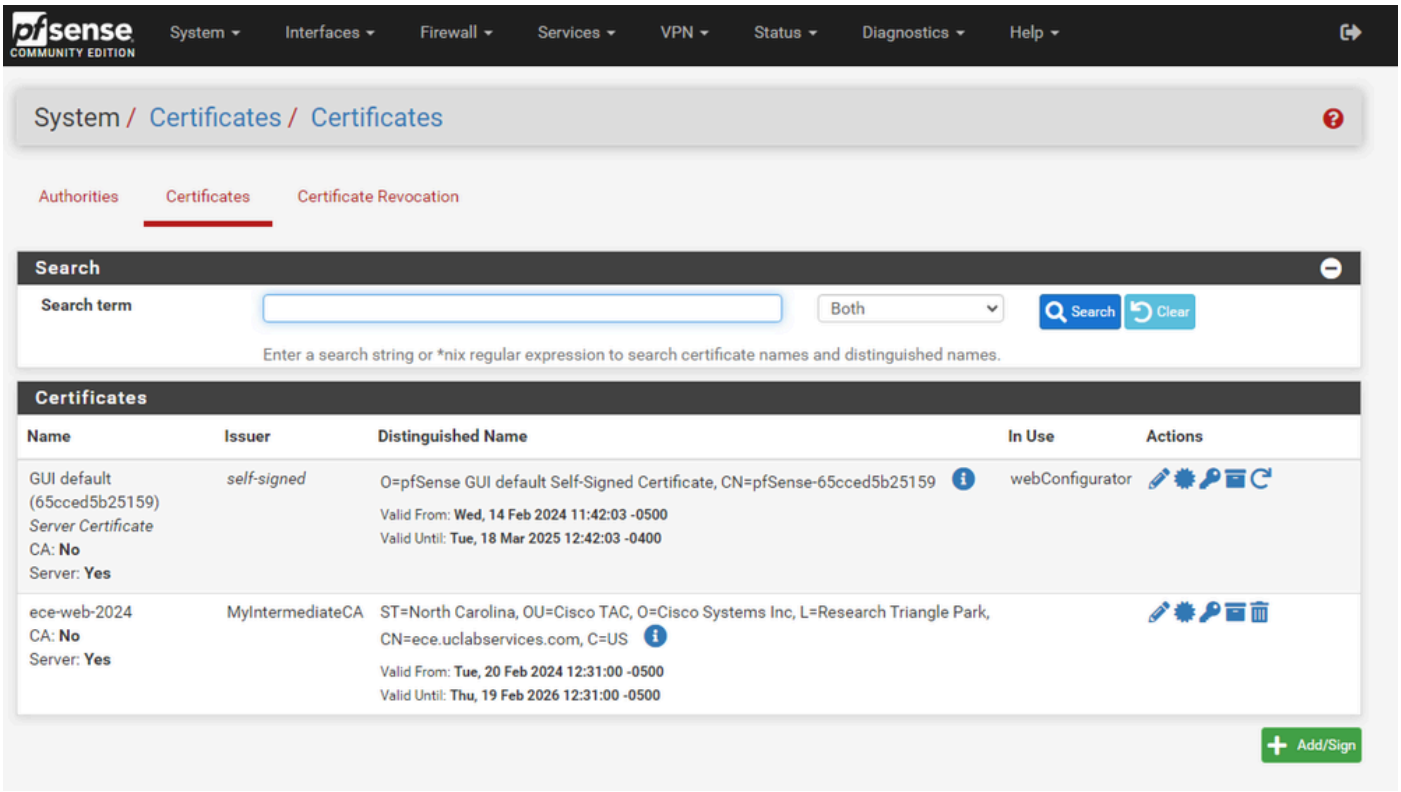
Paste the certificate received from the certificate authority here.

Update

pfSense GUI — 憑證匯入

選擇Update以儲存證書。

6.檢查證書資料以確保其正確。



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

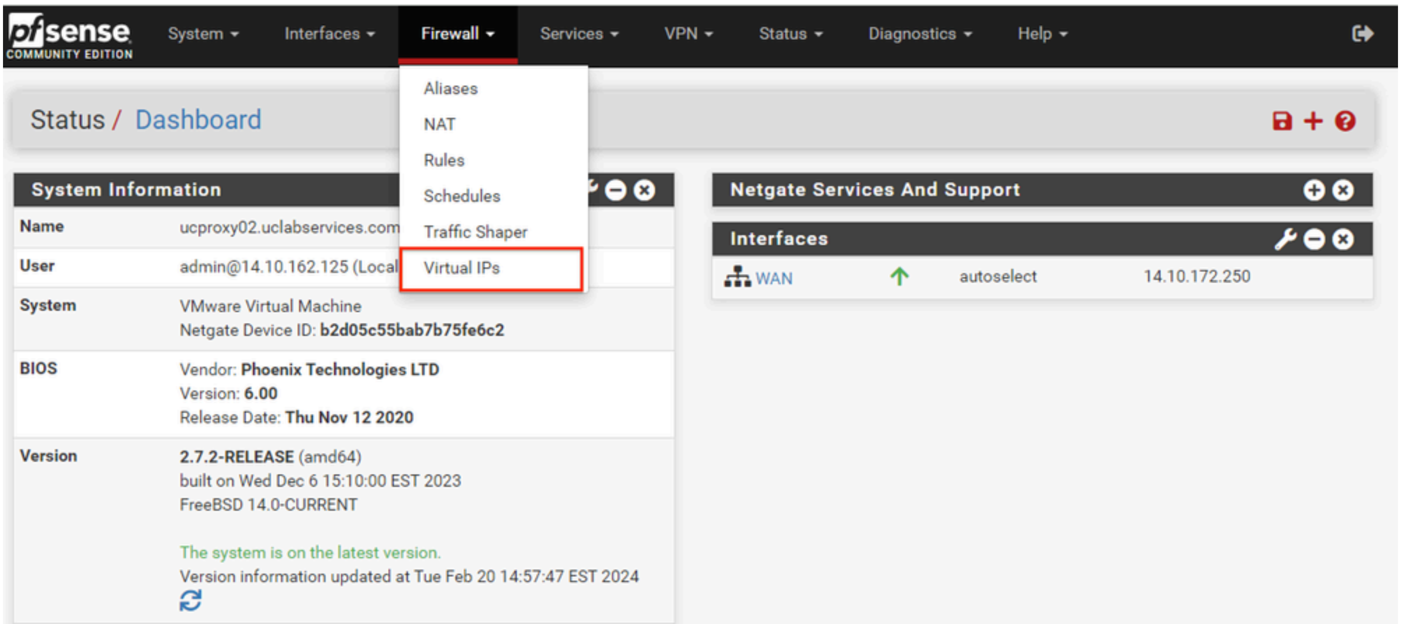
pfSense GUI — 證書清單

7.如果希望在此pfSense上託管多個站點，請重複此過程。

新增虛擬IP

在pfSense上託管網站至少需要一個IP。在pfSense中，這可通過虛擬IP(VIP)完成。

步驟 1.從Firewall下拉選單中選擇Virtual IPs



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

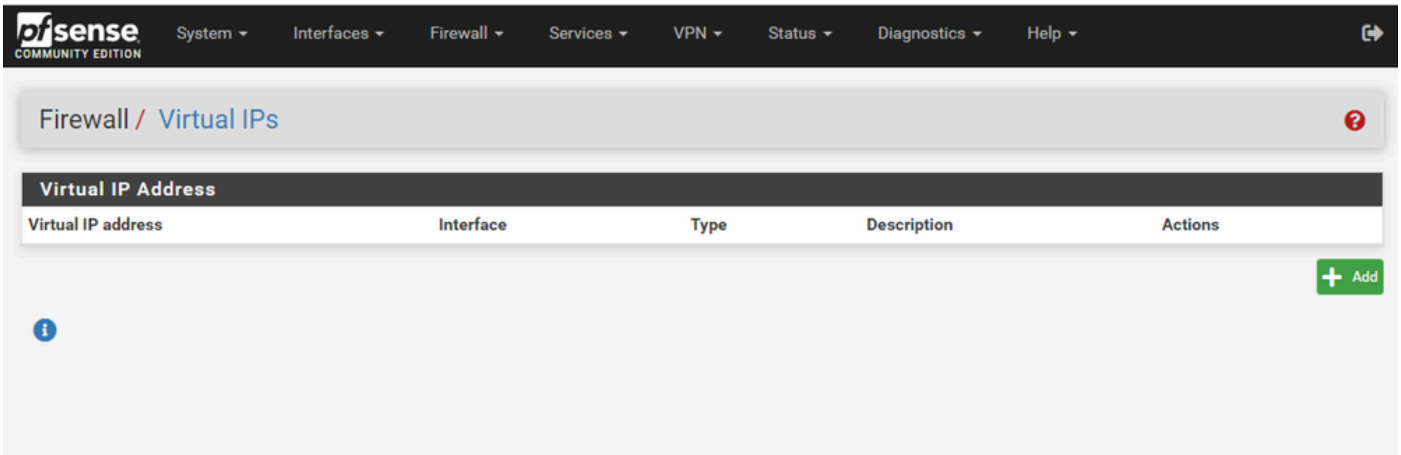
Netgate Services And Support

Interfaces

WAN	↑	autoselect	14.10.172.250

pfSense GUI - VIP下拉選單

步驟 2.選擇「新增」按鈕

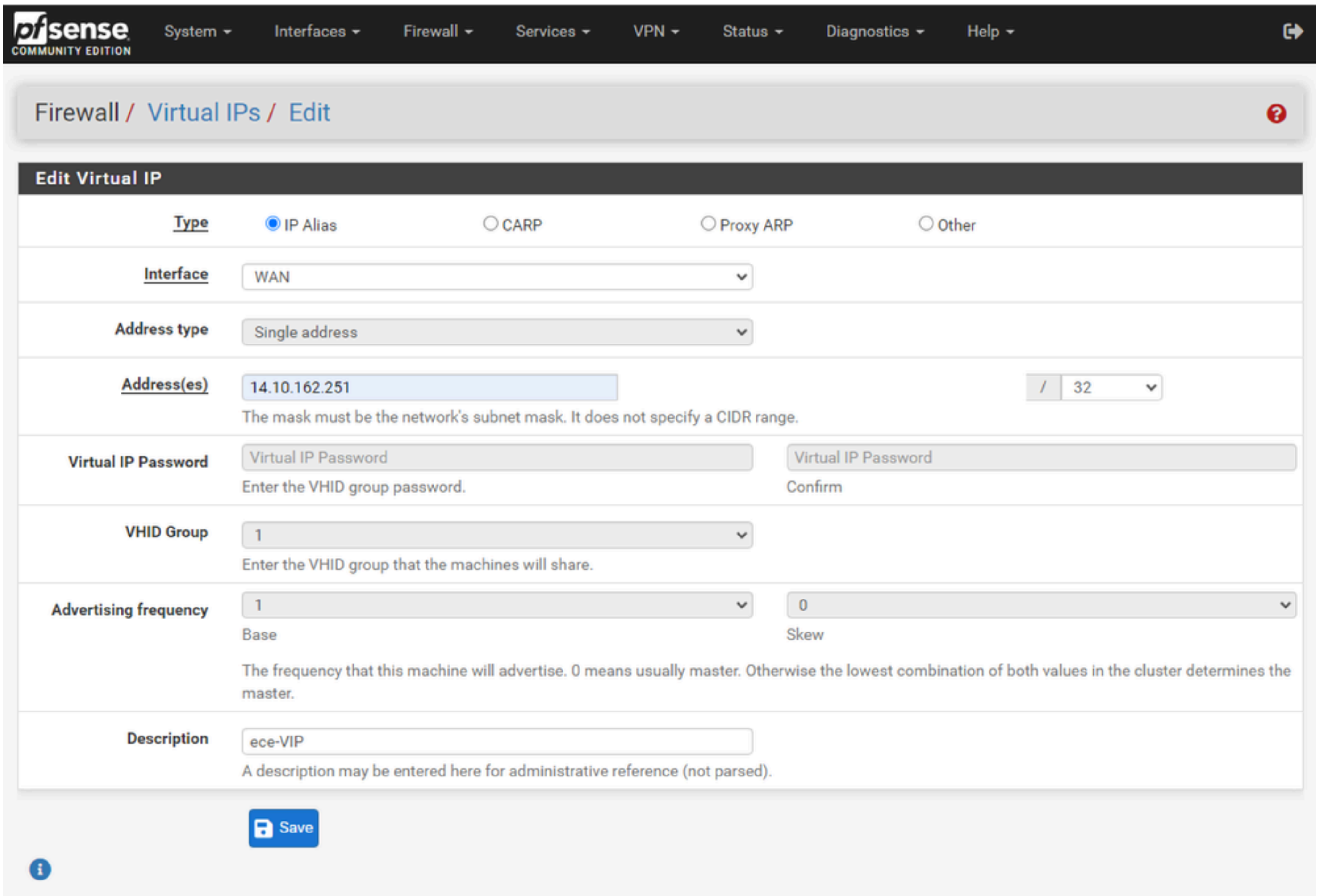


Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions

pfSense GUI - VIP登入頁

步驟 3.提供地址資訊



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).

Save

pfSense GUI - VIP配置

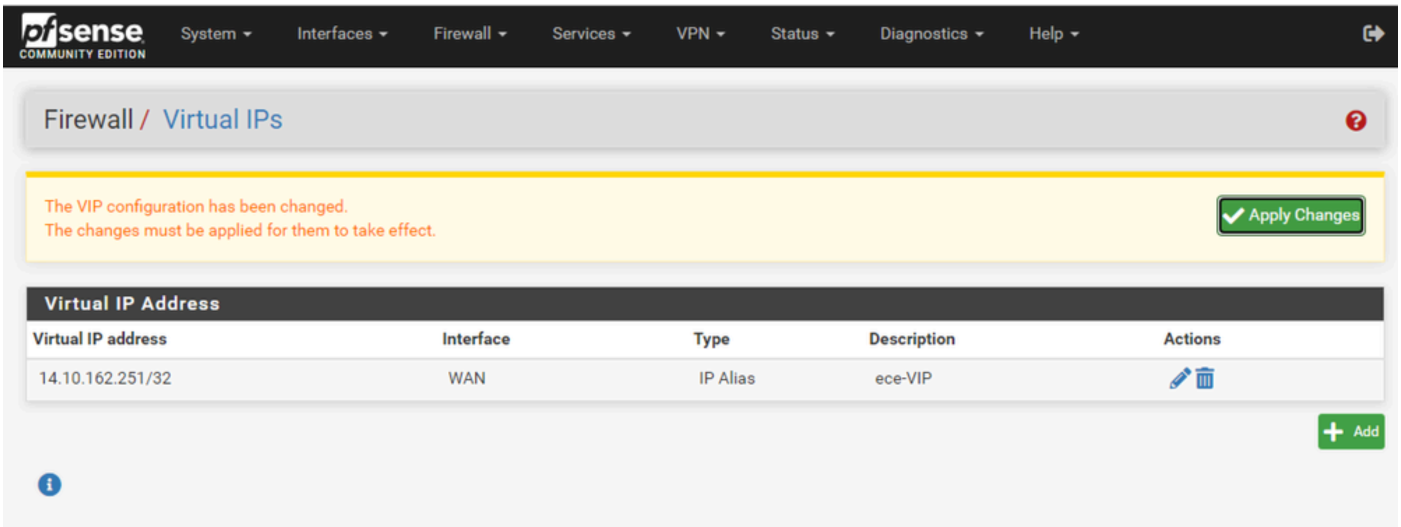
使用這些資訊新增VIP。

- 型別：選擇IP別名
- Interface：選擇要廣播的此IP地址的介面
- 地址：輸入IP地址
- 地址掩碼：對於用於負載平衡的IP地址，掩碼必須為/32
- 說明：提供簡短文本，以便以後更容易理解配置

選擇Save以提交更改。

對您的配置所需的每個IP地址重複此步驟。

步驟 4.應用配置



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	

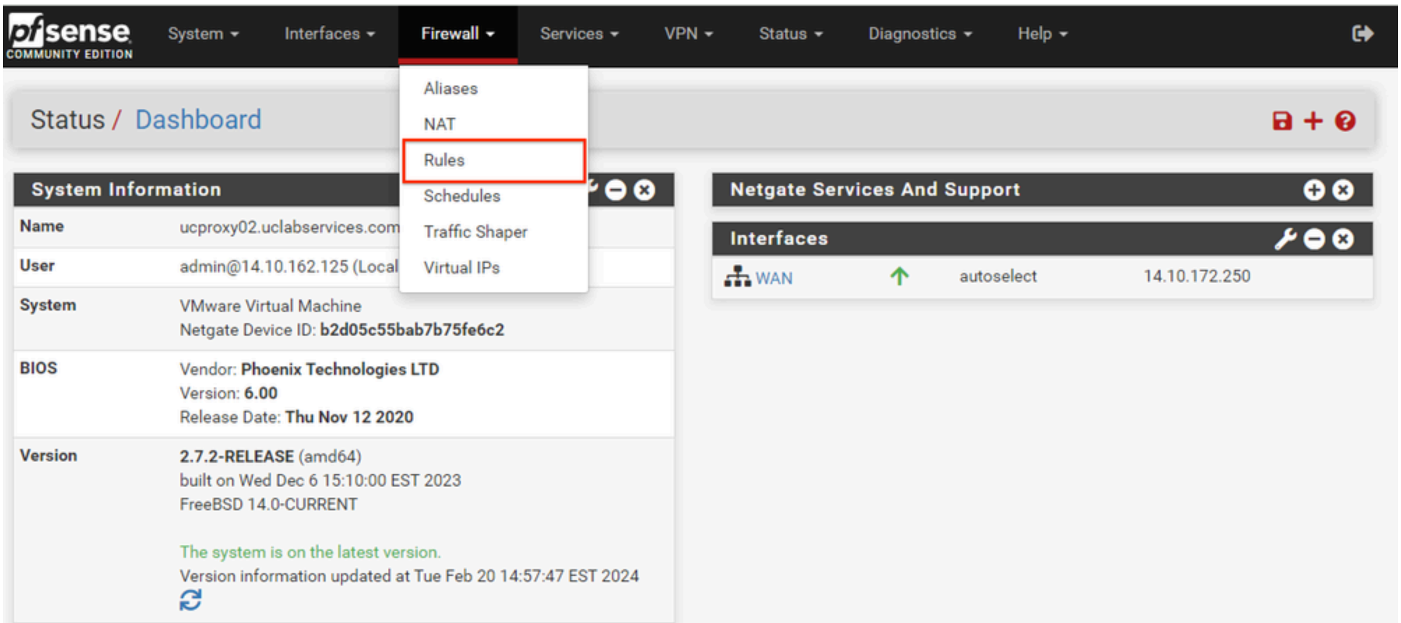
pfSense GUI - VIP清單

新增所有VIP後，選擇Apply Changes按鈕。

配置防火牆

pfSense具有內建防火牆。預設規則集非常有限。在裝置投入生產之前，請確保構建全面的防火牆策略。

步驟 1.從Firewall下拉選單中選擇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

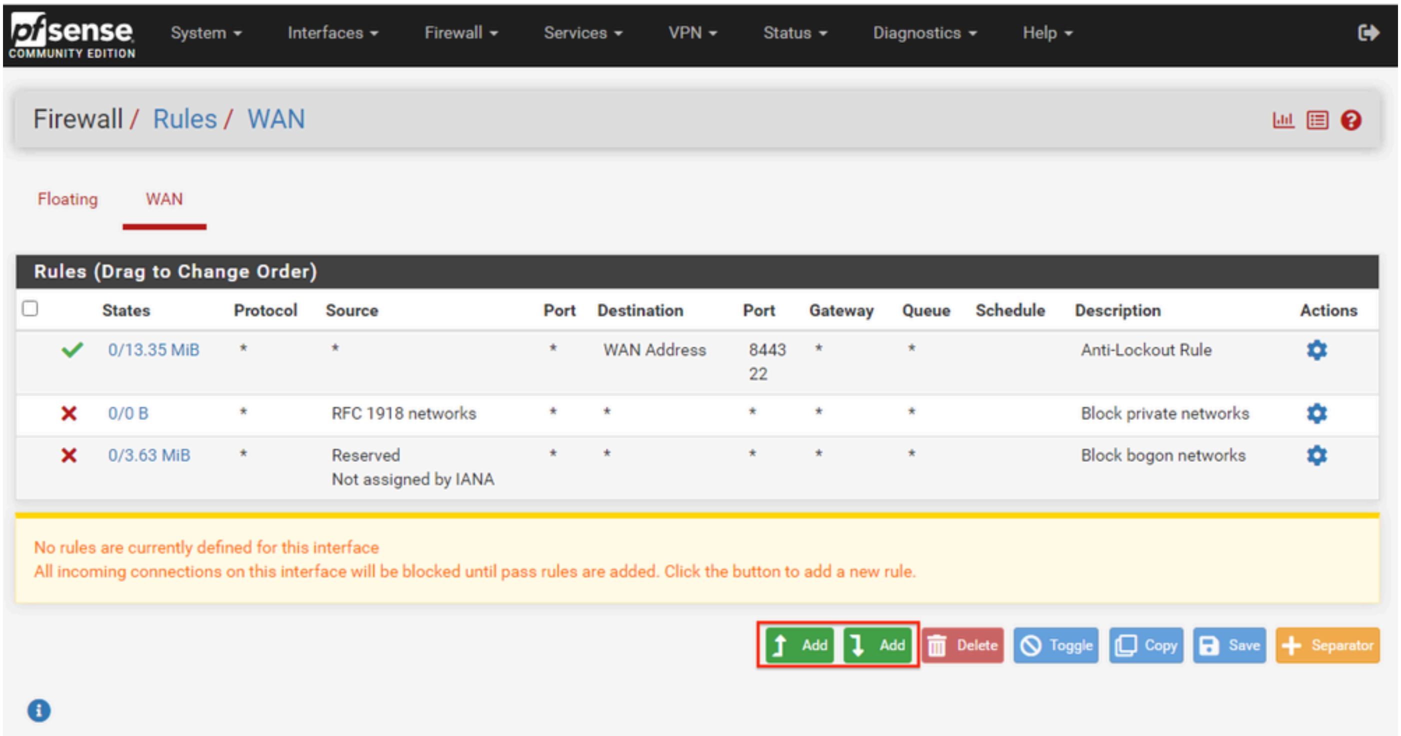
Netgate Services And Support

Interfaces

WAN	↑	autoselect	14.10.172.250

pfSense GUI - Firewall Rules下拉選單

步驟 2.選擇其中一個Add按鈕



Firewall / Rules / WAN

Rules (Drag to Change Order)

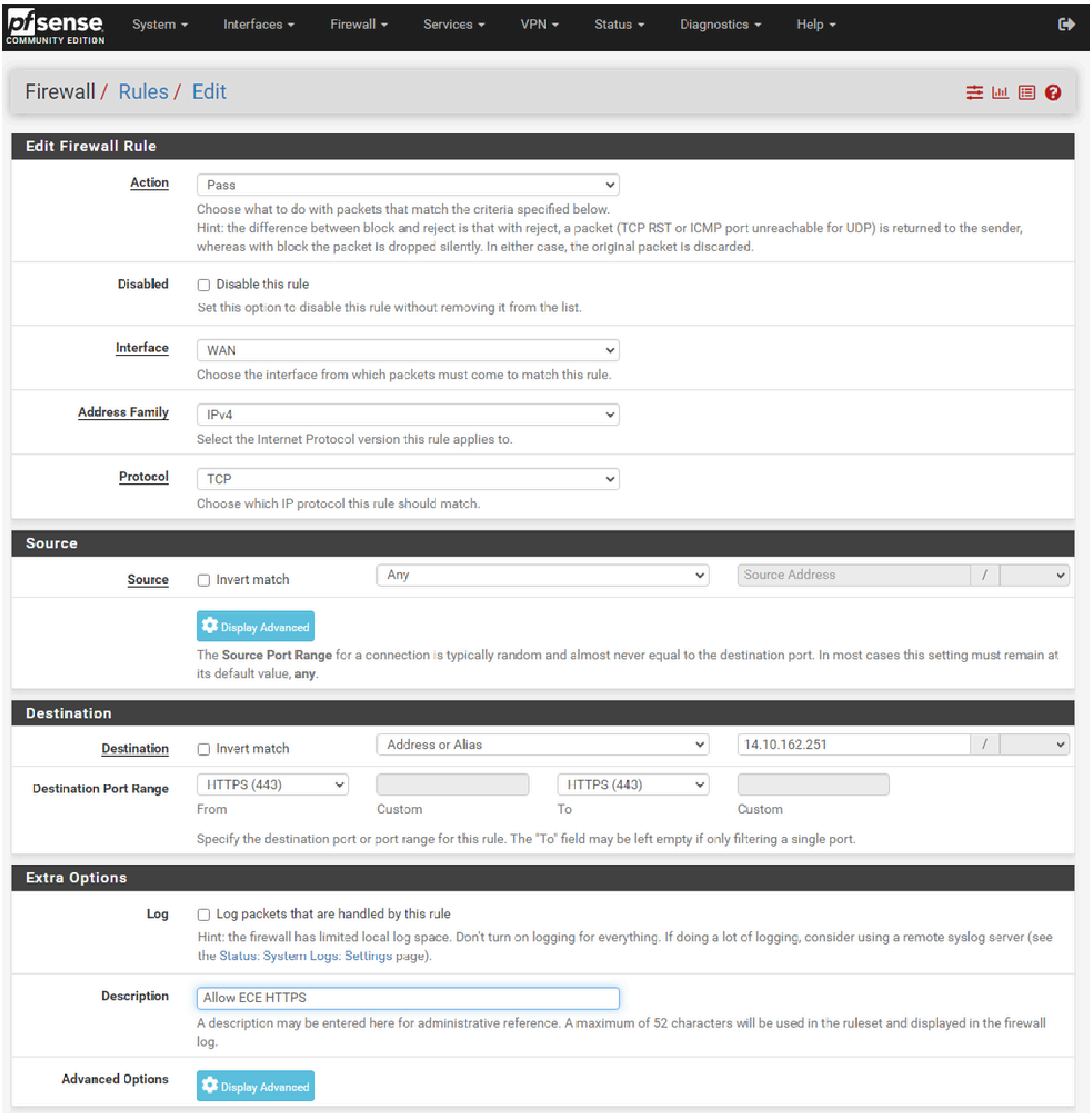
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/13.35 MiB	*	*	*	WAN Address	8443 22	*	*		Anti-Lockout Rule	⚙
	✗	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0/3.63 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

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 — 防火牆規則清單

請注意，一個按鈕將新規則新增到所選行上方，而另一個按鈕將規則新增到所選規則下方。任一按鈕都可用於第一條規則。

步驟 3.建立防火牆規則以允許流量通過IP地址到埠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 — 防火牆通過規則配置

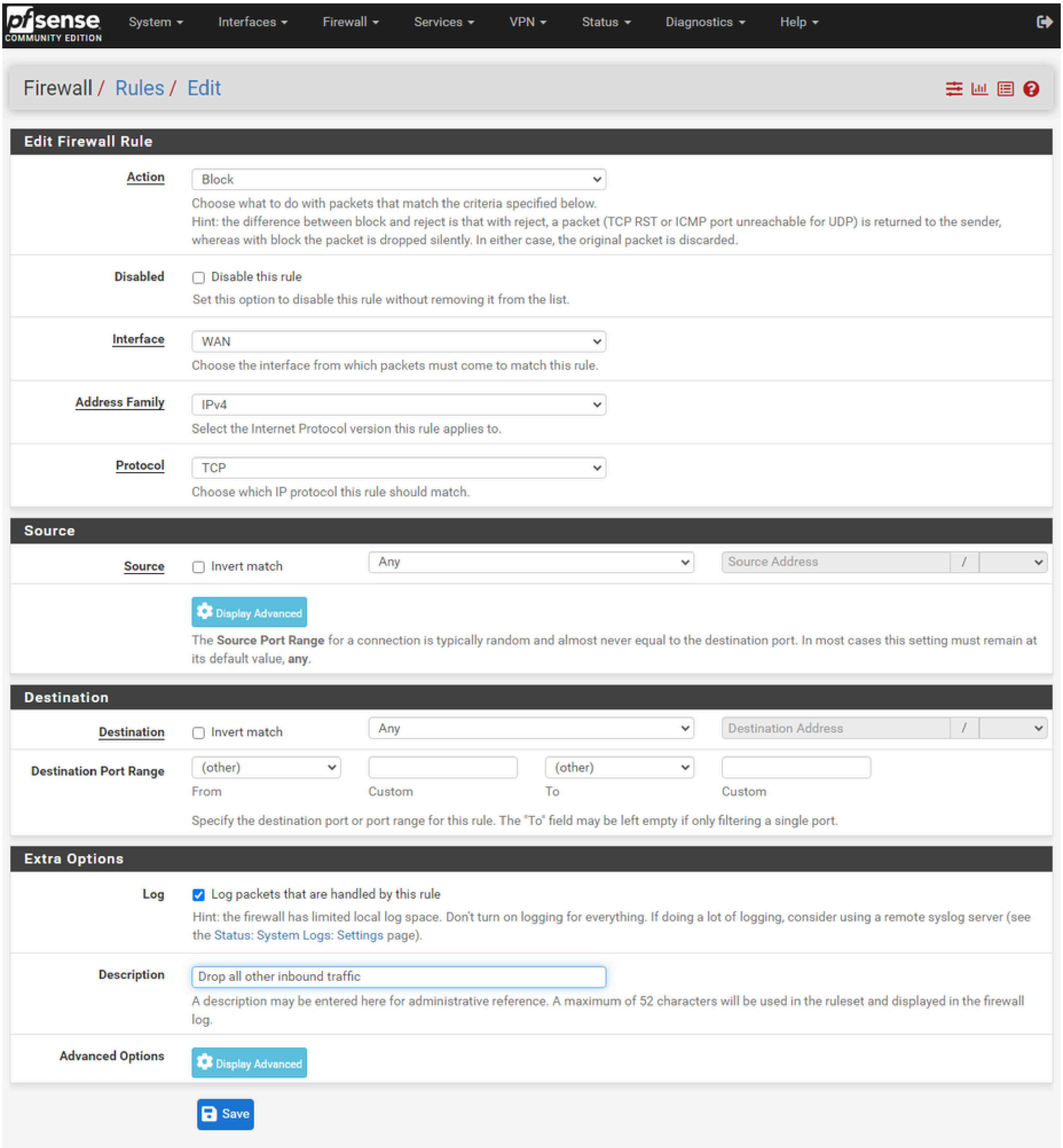
使用該資訊建立規則。

- 操作：選擇通過
- Interface：選擇應用規則的介面
- 地址系列和協定：根據情況選擇
- 來源：將選定內容保留為任意
- 目標：從「目標」下拉選單中選擇「地址」或「別名」，然後輸入應用規則的IP地址
- 目的地連線埠範圍：選擇，在「自」和「至」下拉選單中的HTTPS(443)
- Log：選中此覈取方塊可記錄與此規則匹配的任何資料包進行記帳
- 說明：提供文本以稍後引用規則

選擇Save。

步驟 4.建立防火牆規則以丟棄到pfSense的所有其他流量

選擇Add按鈕將規則插入到新建立的規則下方。


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

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 /

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 | 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: Display Advanced

Save

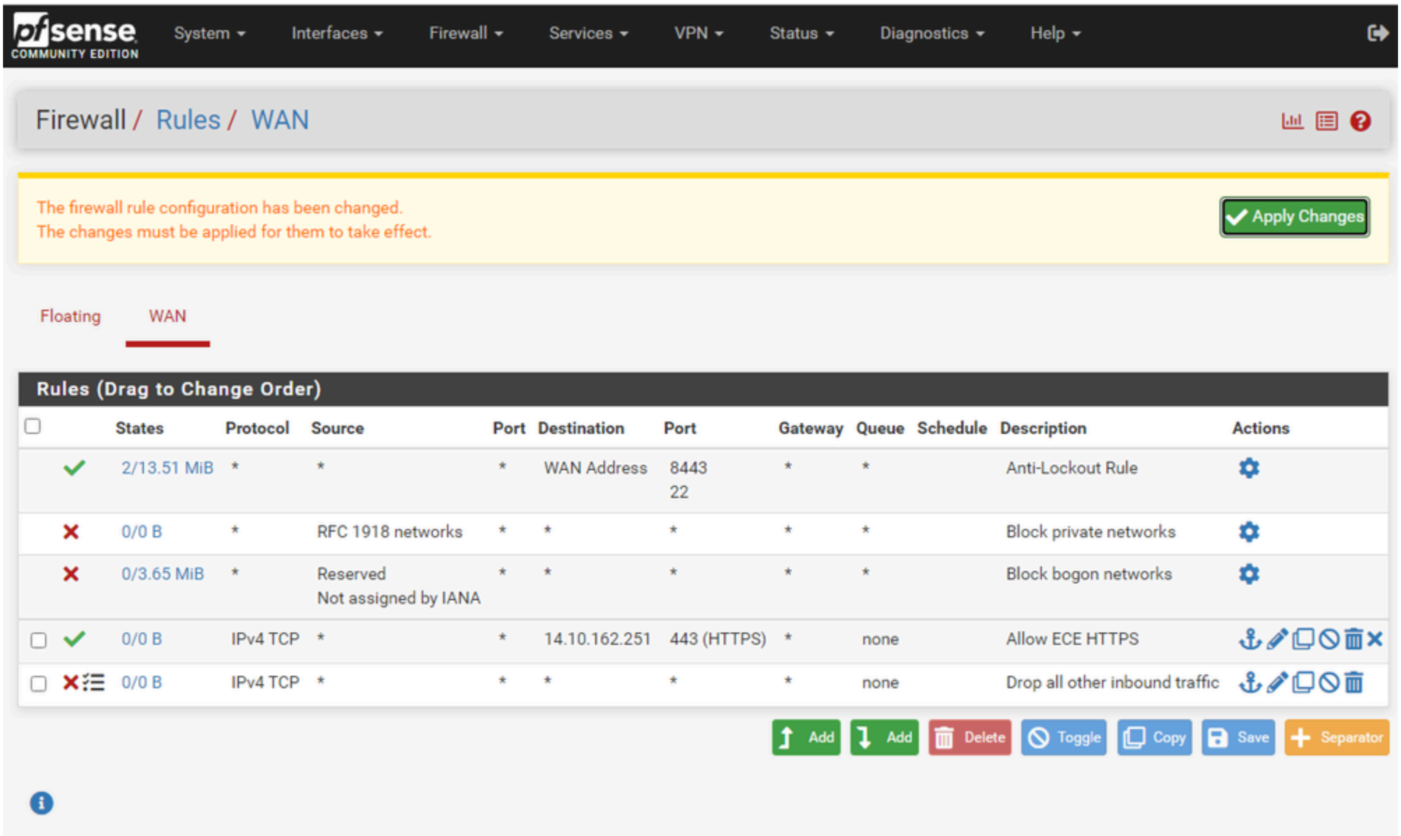
pfSense GUI — 防火牆丟棄規則配置

- 操作：選擇塊
- Interface：選擇應用規則的介面
- 地址系列和協定：根據情況選擇

- 來源：將選定內容保留為任意
- 目標：將選定內容保留為任意
- Log：選中此覈取方塊可記錄與此規則匹配的任何資料包進行記帳
- 說明：提供文本以稍後引用規則

選擇Save。

步驟 5.檢查規則並確保阻止規則位於底部



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	

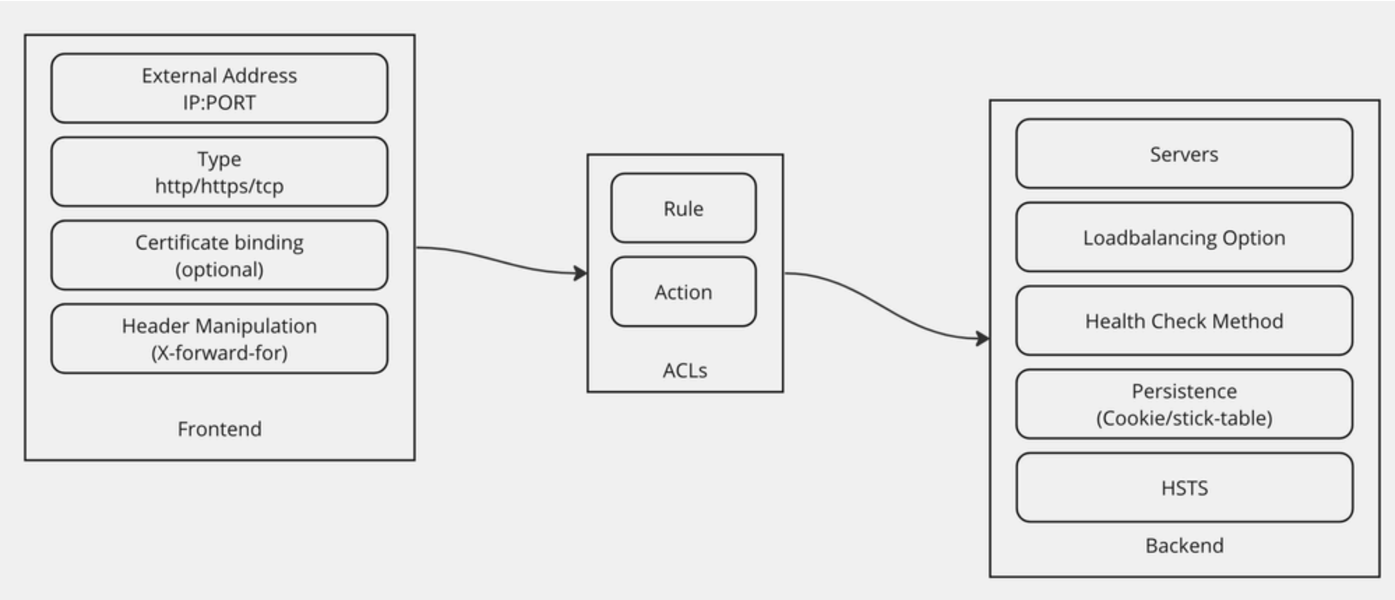
pfSense GUI — 防火牆規則清單

如果需要，請拖動規則對它們進行排序。

選擇Apply Changes（在防火牆規則符合您的環境所需的順序後應用更改）。

配置HAProxy

HAProxy概念



HAProxy概念

HAProxy是使用Frontend/Backend模型實現的。

前端定義客戶與之通訊的代理端。

前端包括IP和埠組合、證書繫結，並且可以實施某些報頭操作。

後端定義代理與物理Web伺服器通訊的一端。

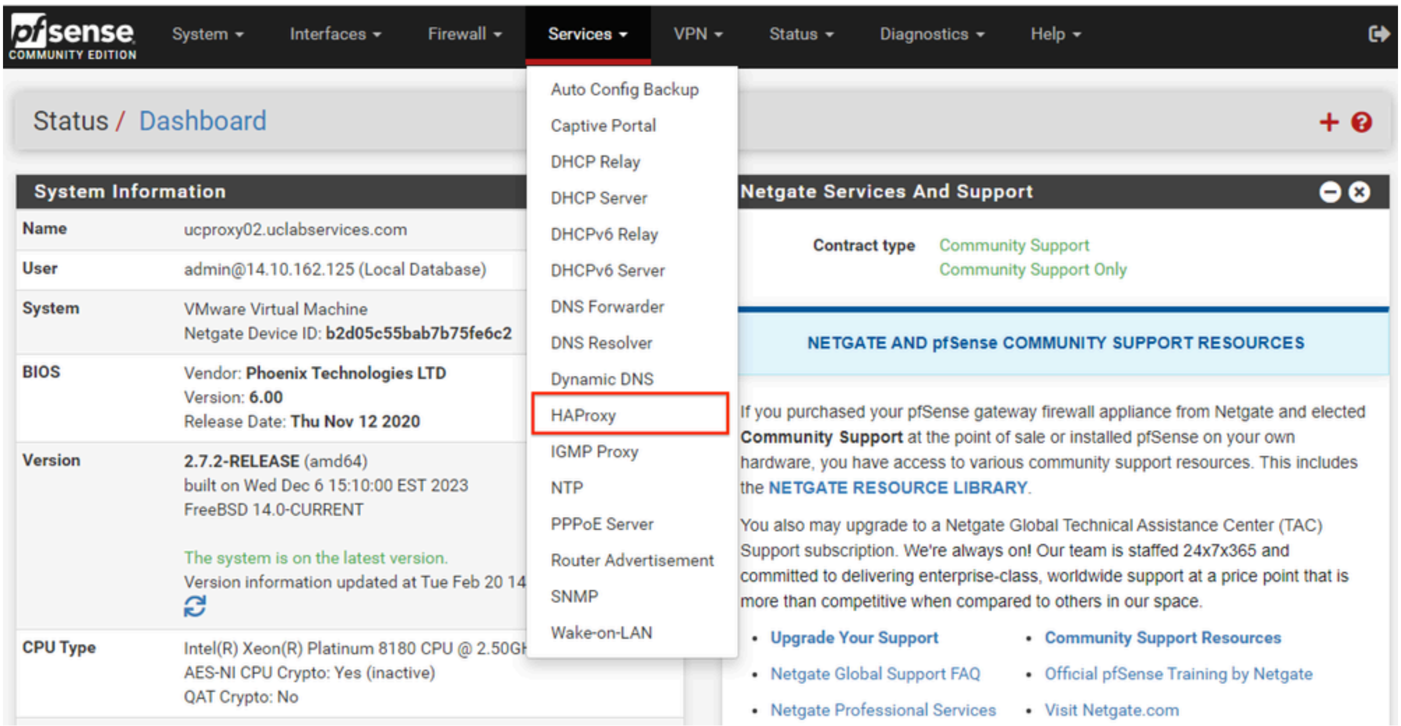
後端定義實際的伺服器和埠、用於初始分配的負載均衡方法、運行狀況檢查和永續性。

前端知道通過專用後端或使用ACL與哪些後端通訊。

ACL可以建立不同的規則，以便給定前端可以根據各種情況與不同的後端通訊。

初始HAProxy設定

步驟 1.從Services下拉選單中選擇HAProxy



Status / Dashboard

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

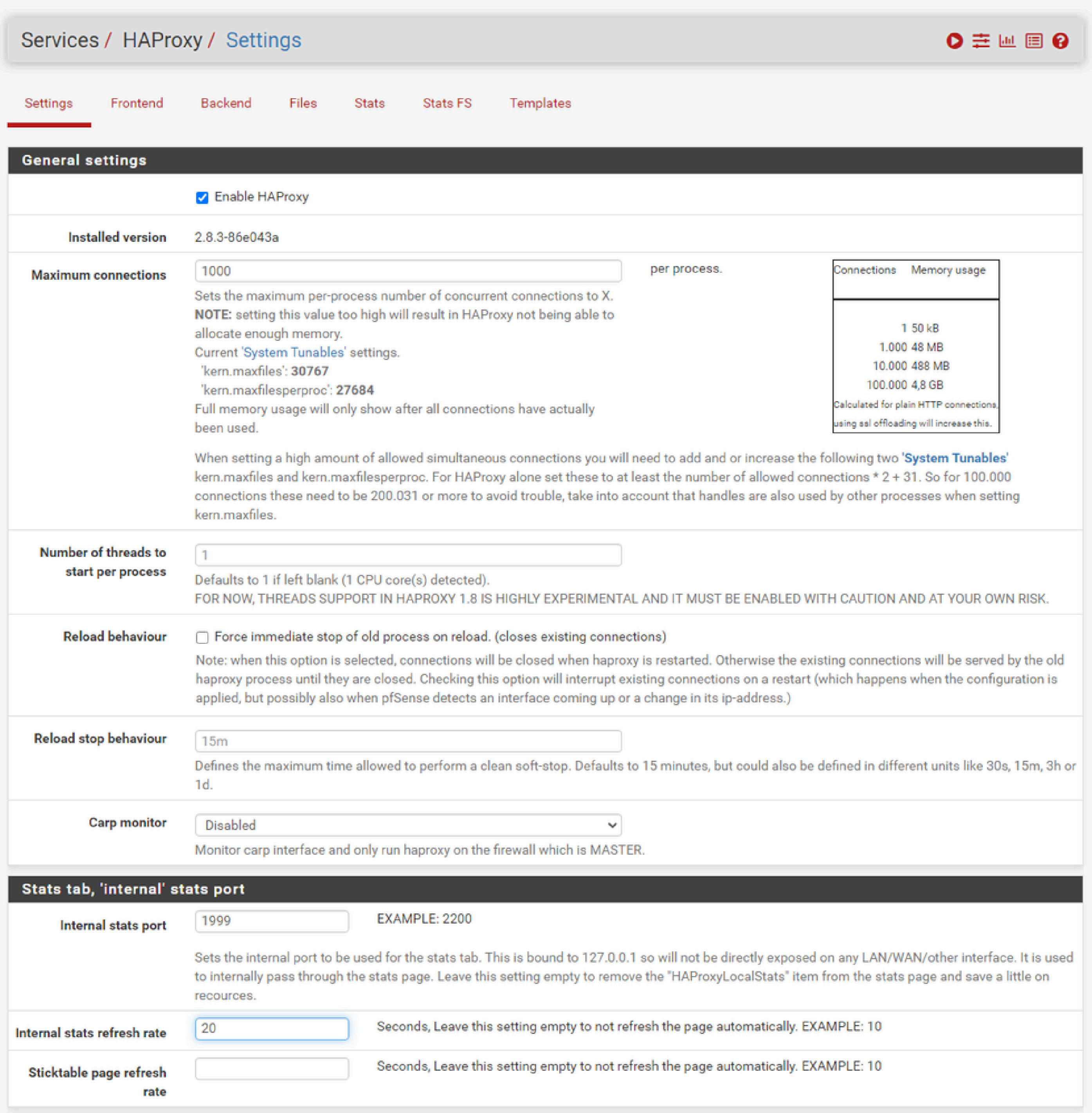
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

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下拉選單

步驟 2.配置基本設定



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主設定

選中Enable HAProxy覈取方塊。

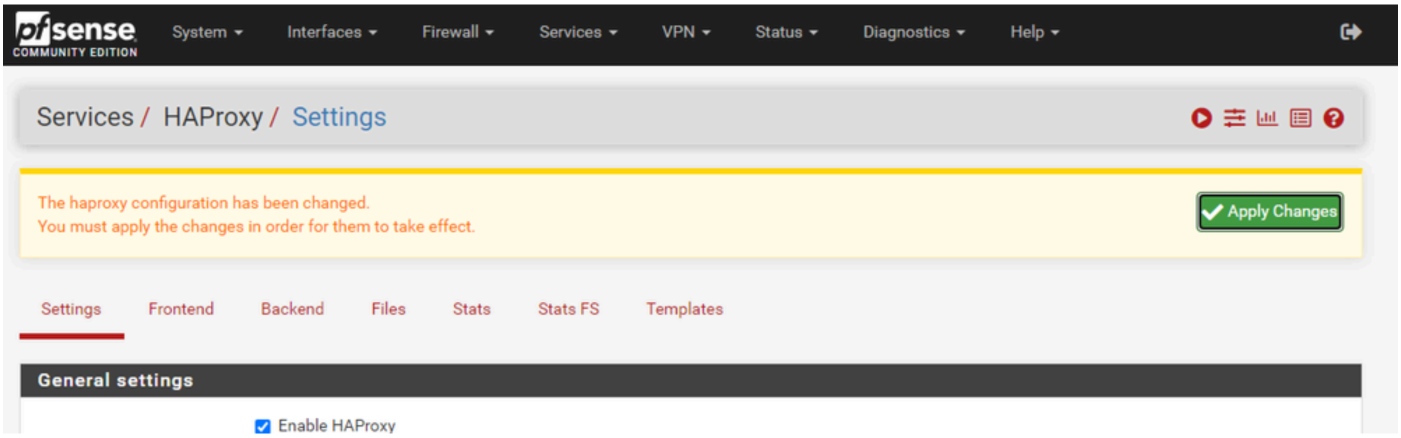
輸入最大連線數的值。有關所需記憶體的詳細資訊，請參閱本節中的圖表。

為Internal stats埠輸入一個值。此埠用於顯示裝置上的HAProxy統計資訊，但不會在裝置外部顯示。

輸入內部統計刷新率的值。

檢查其餘配置，並根據您的環境需要進行更新。

選擇Save。


Services / HAProxy / Settings

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

General settings

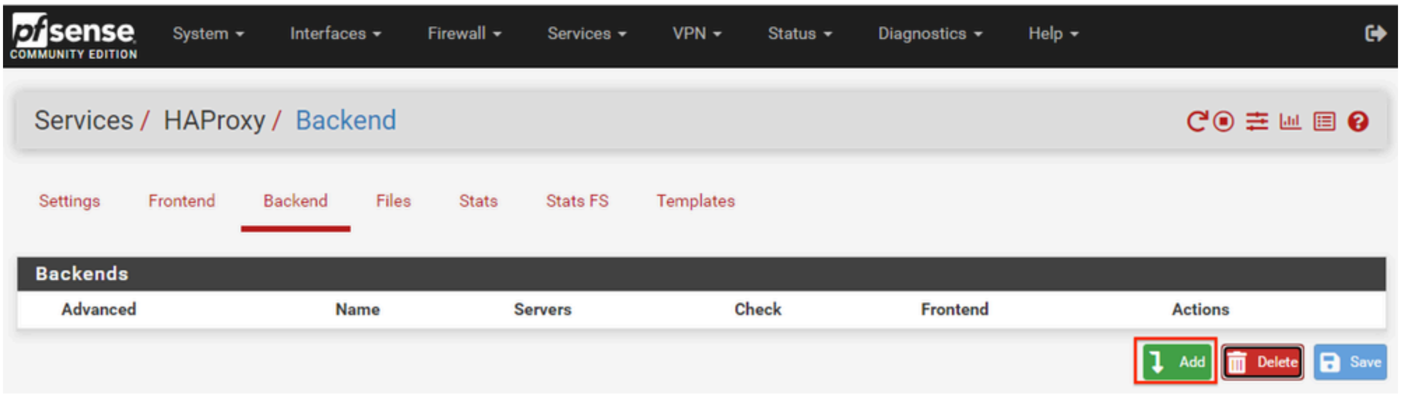
☑ Enable HAProxy

pfSense GUI - HAProxy應用更改

注意：只有選擇「應用更改」按鈕後，配置更改才會變為活動狀態。您可以進行多項配置更改並同時應用所有更改。配置無需應用於其他部分即可使用。

配置HAProxy後端

從後端開始。原因是前端必須引用後端。確保已選擇「Backend（後端）」選單。

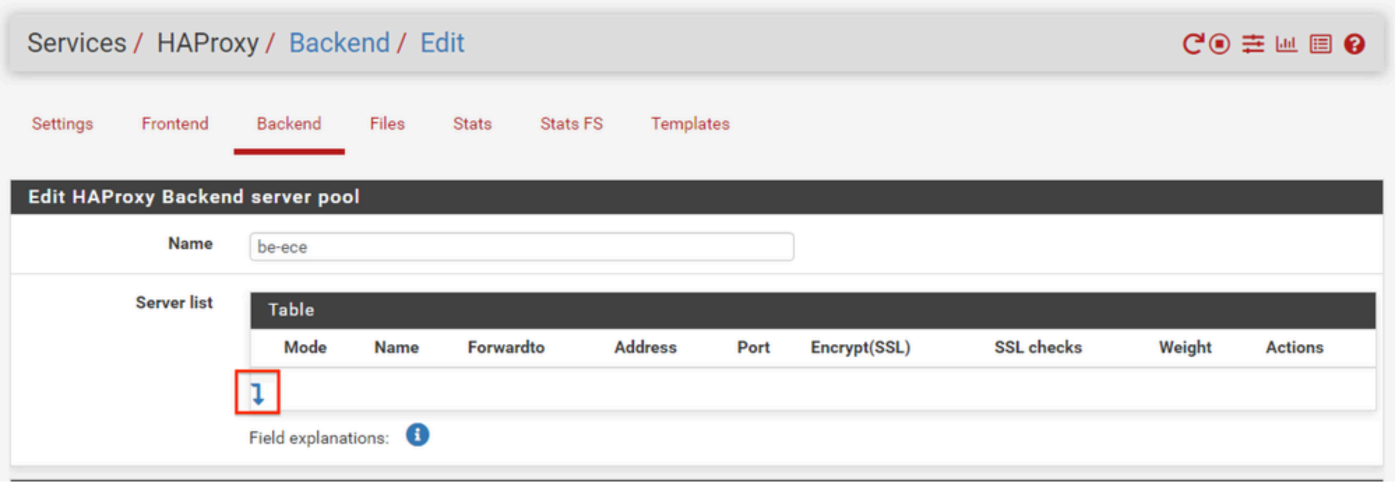

Services / HAProxy / Backend

Backends

Advanced	Name	Servers	Check	Frontend	Actions

pfSense GUI - HAProxy新增後端

選擇Add按鈕。


Services / HAProxy / Backend / Edit

Edit HAProxy Backend server pool

Name: be-ece

Server list

Table

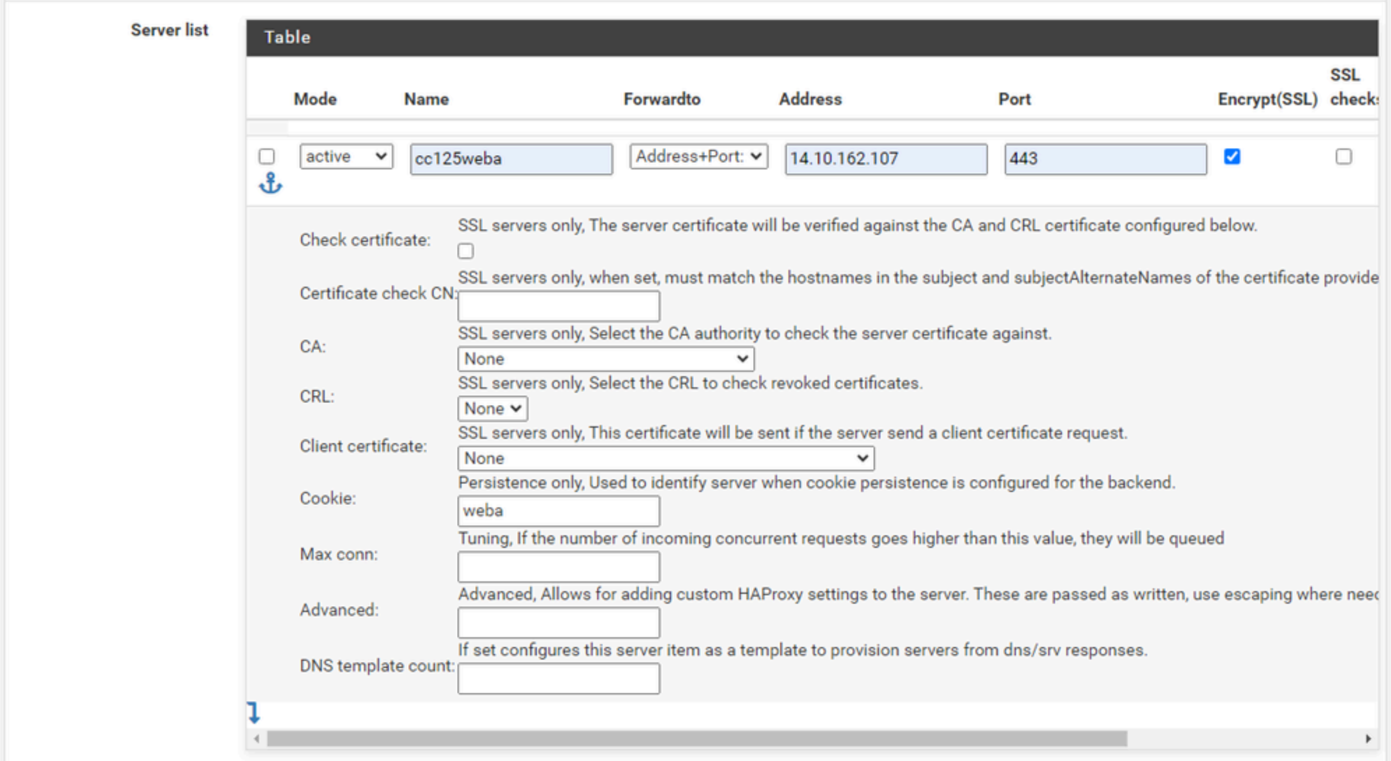
Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions

Field explanations:

pfSense GUI - HAProxy後端啟動

為後端提供名稱。

選擇向下箭頭，將第一個伺服器新增到「伺服器」清單中



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.

後端 — 伺服器清單

提供引用伺服器的名稱。這不需要與實際的伺服器名稱匹配。這是顯示在統計資訊頁面上的名稱。

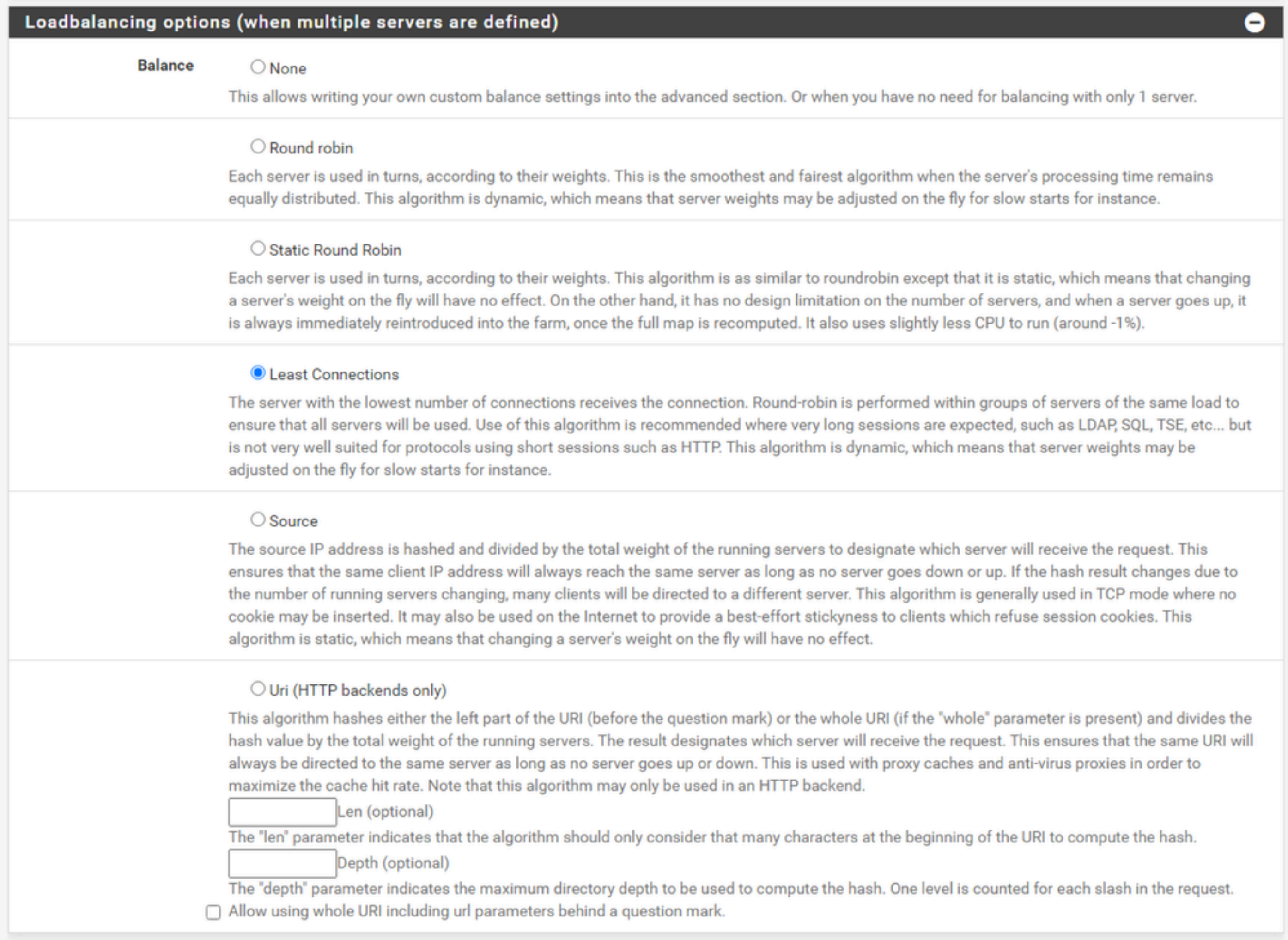
提供伺服器的地址。可以將其配置為FQDN的IP地址。

提供要連線的埠。這是ECE的埠443。

選中Encrypt(SSL)覈取方塊。

在Cookie欄位中提供一個值。這是會話粘性Cookie的內容，並且在後端內必須是唯一的。

配置第一個伺服器後，選擇向下箭頭以配置環境中的任何其他Web伺服器。



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)

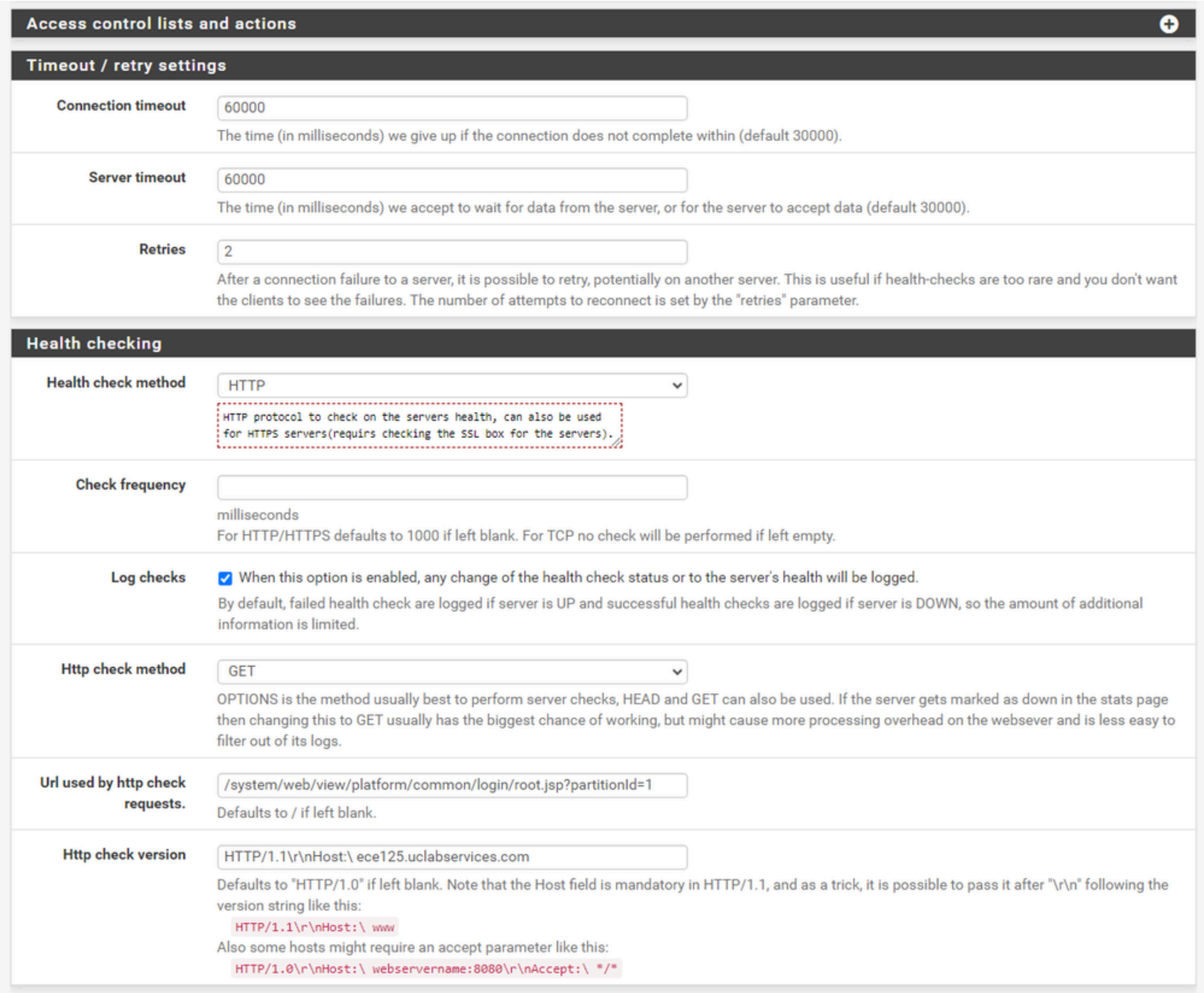
The "depth" parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request.

□ Allow using whole URI including url parameters behind a question mark.

HAProxy後端 — 負載平衡

配置負載均衡選項。

對於ECE伺服器，必須將其設定為「最少連線」。



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後端 — 運行狀況檢查

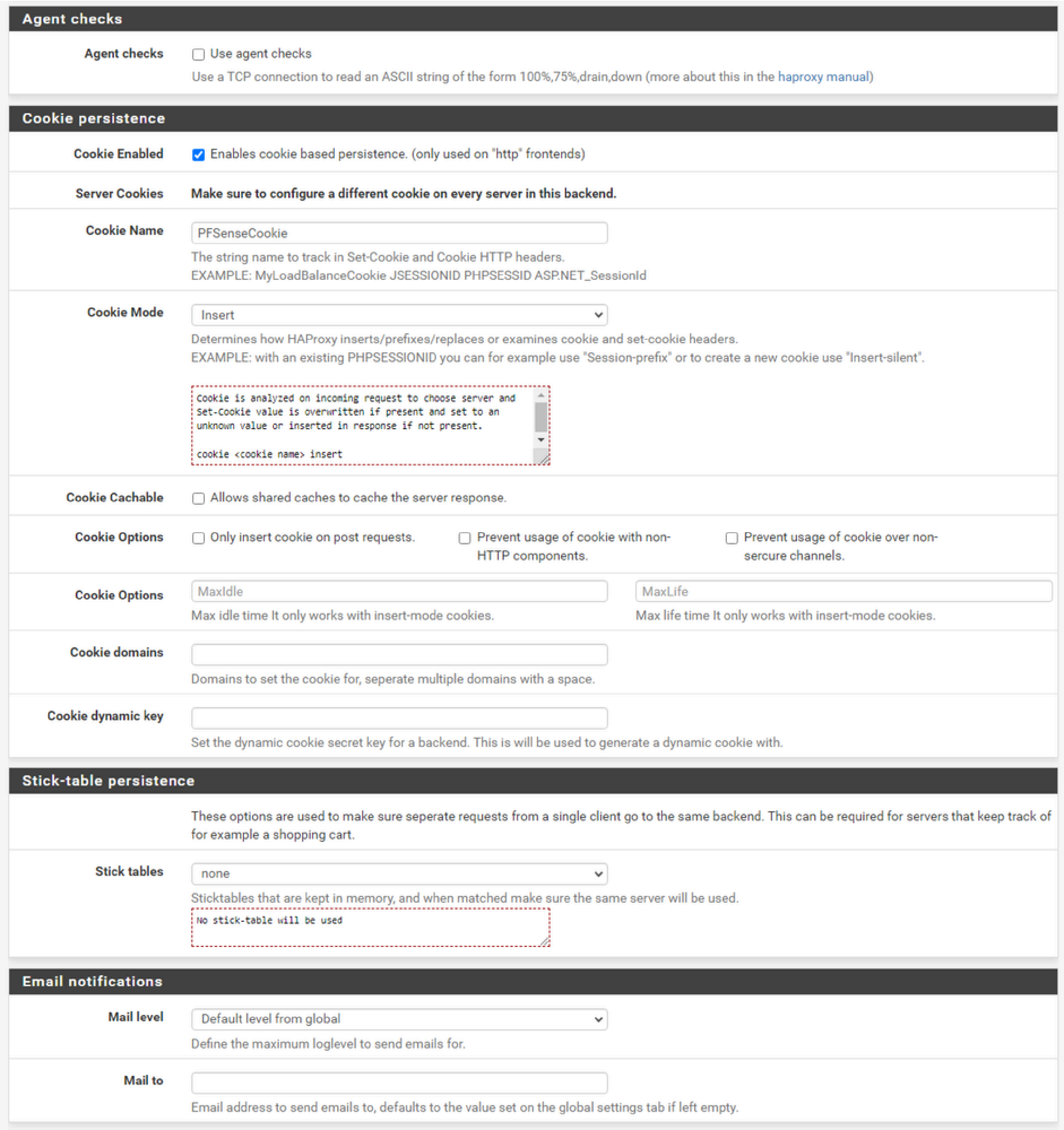
此配置中未使用訪問控制清單。

超時/重試設定可以保留為其預設配置。

配置健康檢查部分。

1. 運行狀況檢查方法：HTTP
2. 檢查頻率：留空以使用每1秒的預設值。
3. 日誌檢查：選擇此選項可將任何運行狀況更改寫入日誌。
4. Http檢查方法：從清單中選擇GET。
5. http檢查請求使用的URL。提示：對於ECE伺服器，請輸入 /system/web/view/platform/common/login/root.jsp?partitionId=1
6. HTTP檢查版本： Enter，HTTP/1.1\r\n\Host:\ {fqdn_of_server}

請確保在最後反斜線之後但在伺服器的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.

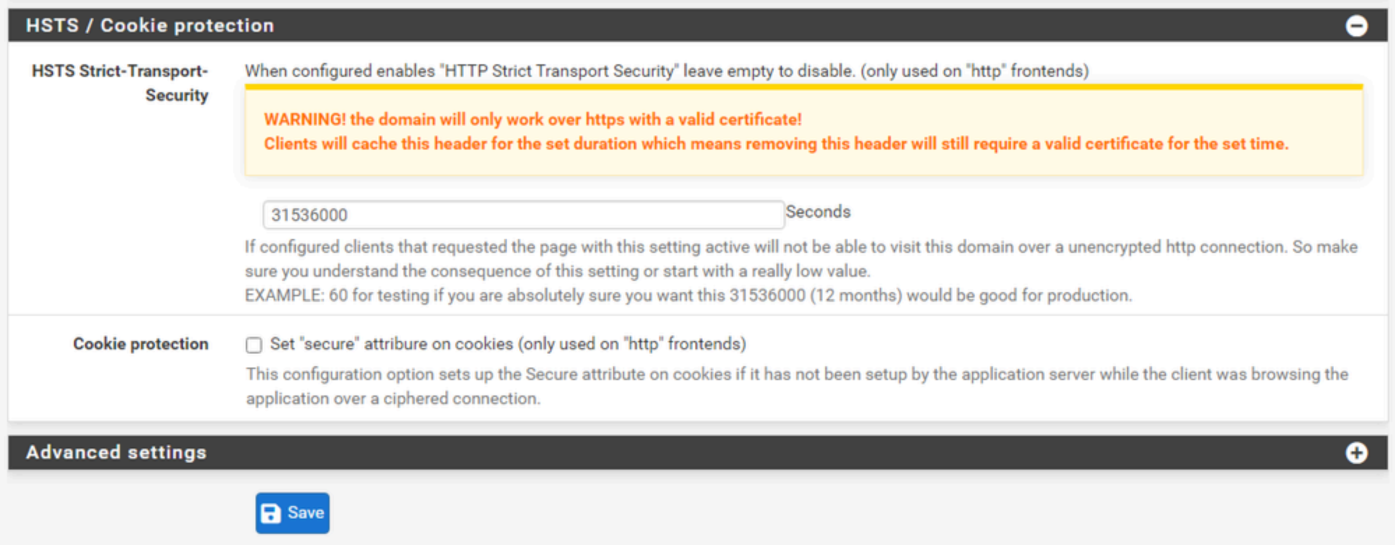
Mail to
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

HAProxy後端 — Cookie持續性

保持未選中代理檢查。

配置Cookie永續性：

1. Cookie Enabled：選擇以啟用基於Cookie的永續性。
2. Cookie名稱：提供cookie的名稱。
3. Cookie模式：從下拉框中選擇插入。
4. 不設定其餘選項。



HSTS / Cookie protection

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.

Advanced settings

HAProxy後端 — HST

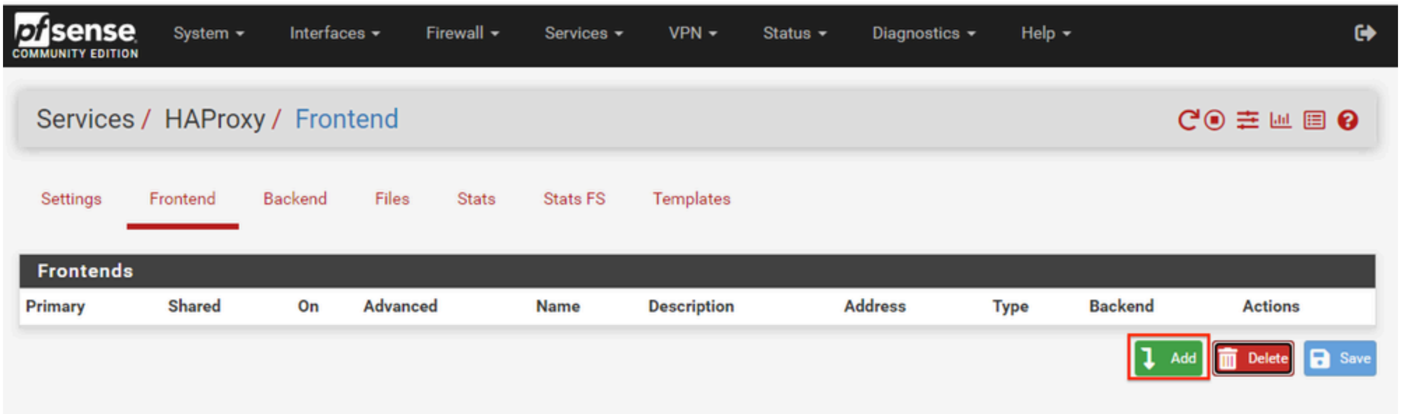
後端配置表單的其餘部分可以保留其預設設定。

如果要配置HSTS，請在此部分中配置超時值。ECE也插入HSTS cookie，因此此配置是冗餘的。

選擇，儲存。

配置HAProxy前端

轉到「前端」選單。

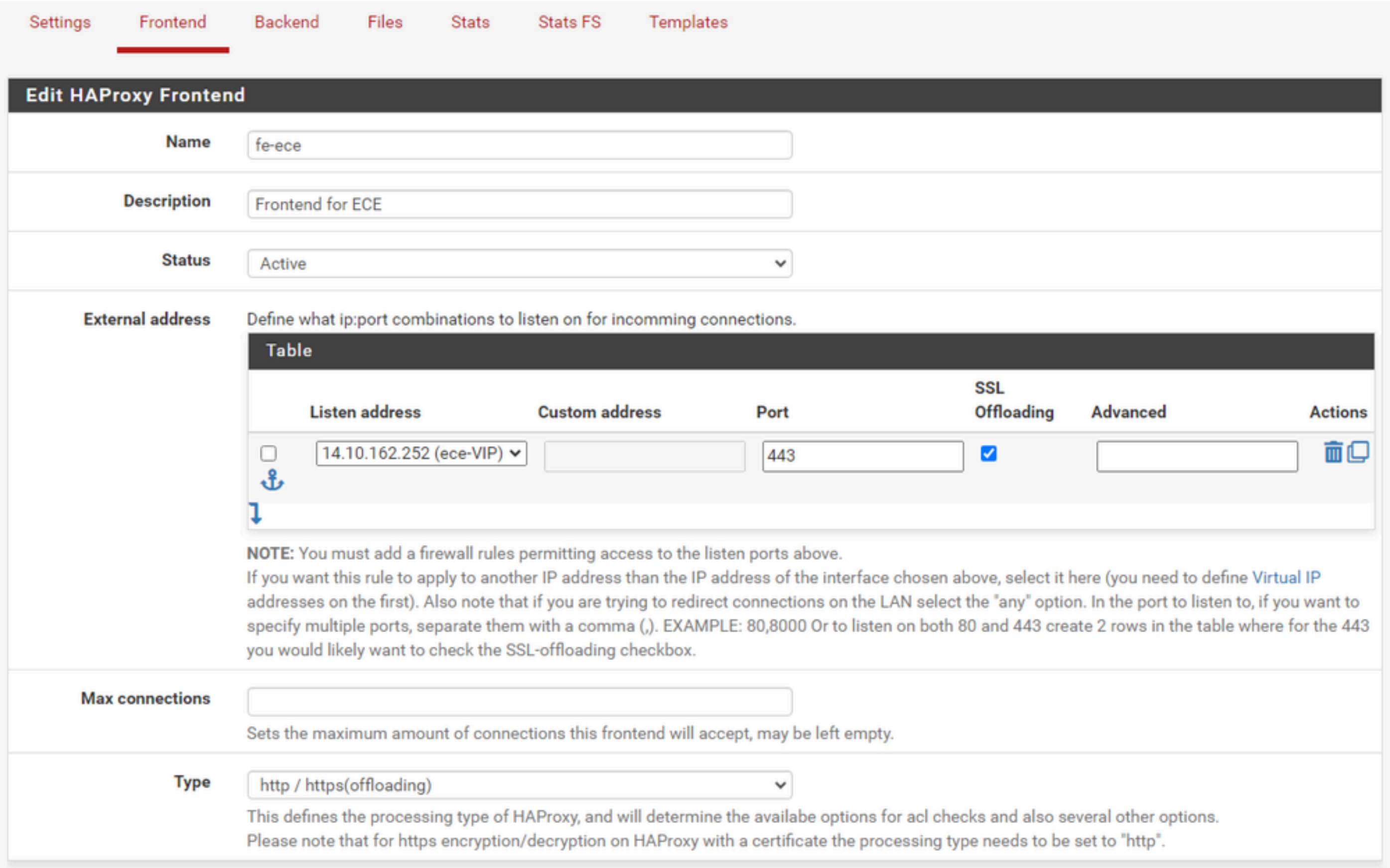


Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions

pfSense GUI - HAProxy新增前端

選擇「新增」按鈕



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 — 前端標頭

為前端提供一個名稱。

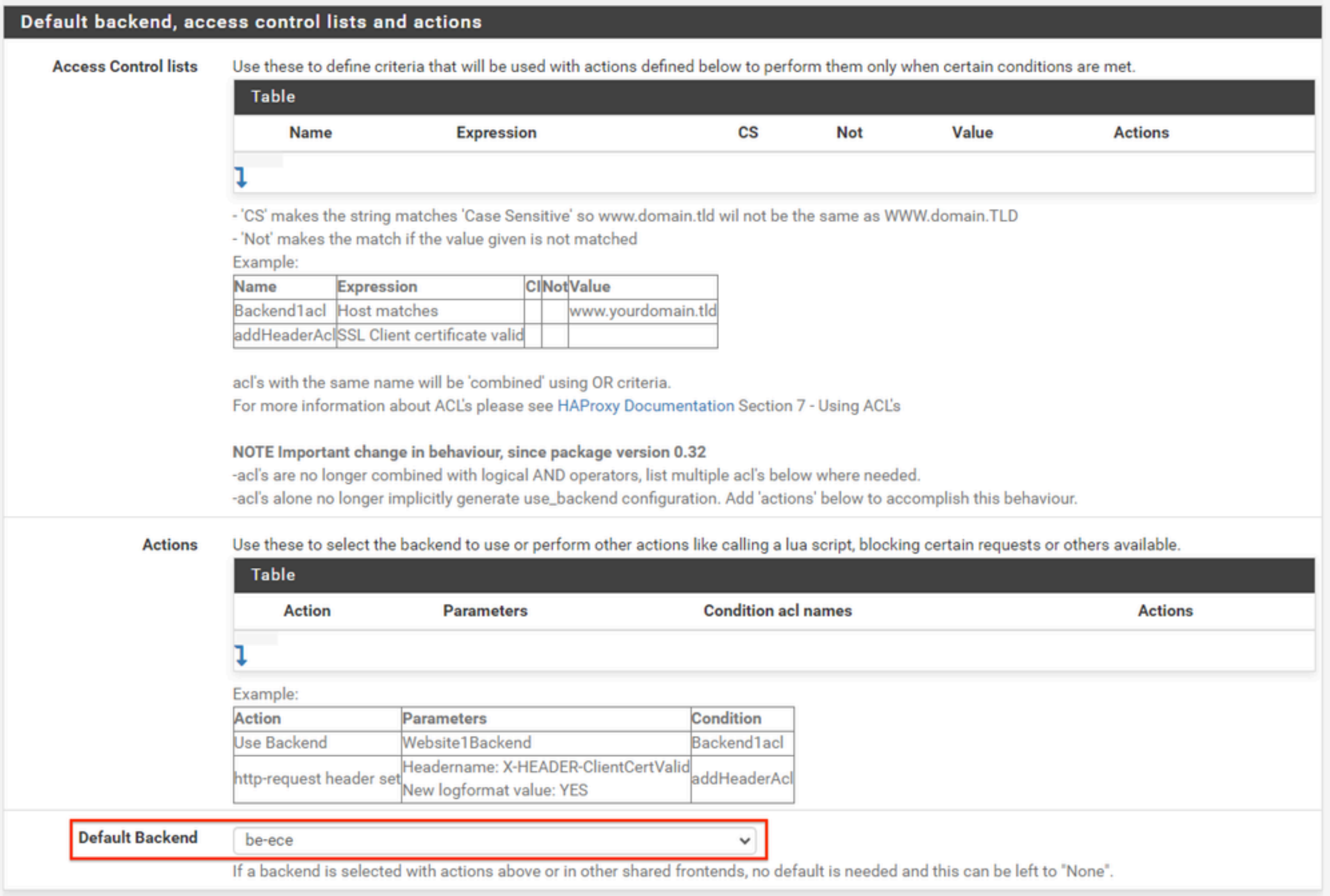
提供說明，以便稍後幫助識別前端。

在External address表中：

1. 收聽地址：選擇您為此網站建立的VIP。
2. 埠：輸入443。
3. SSL解除安裝：選擇此選項可插入會話cookie。

將Max連線留空。

確保「Type（型別）」選擇為「http / https（解除安裝）」。



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:

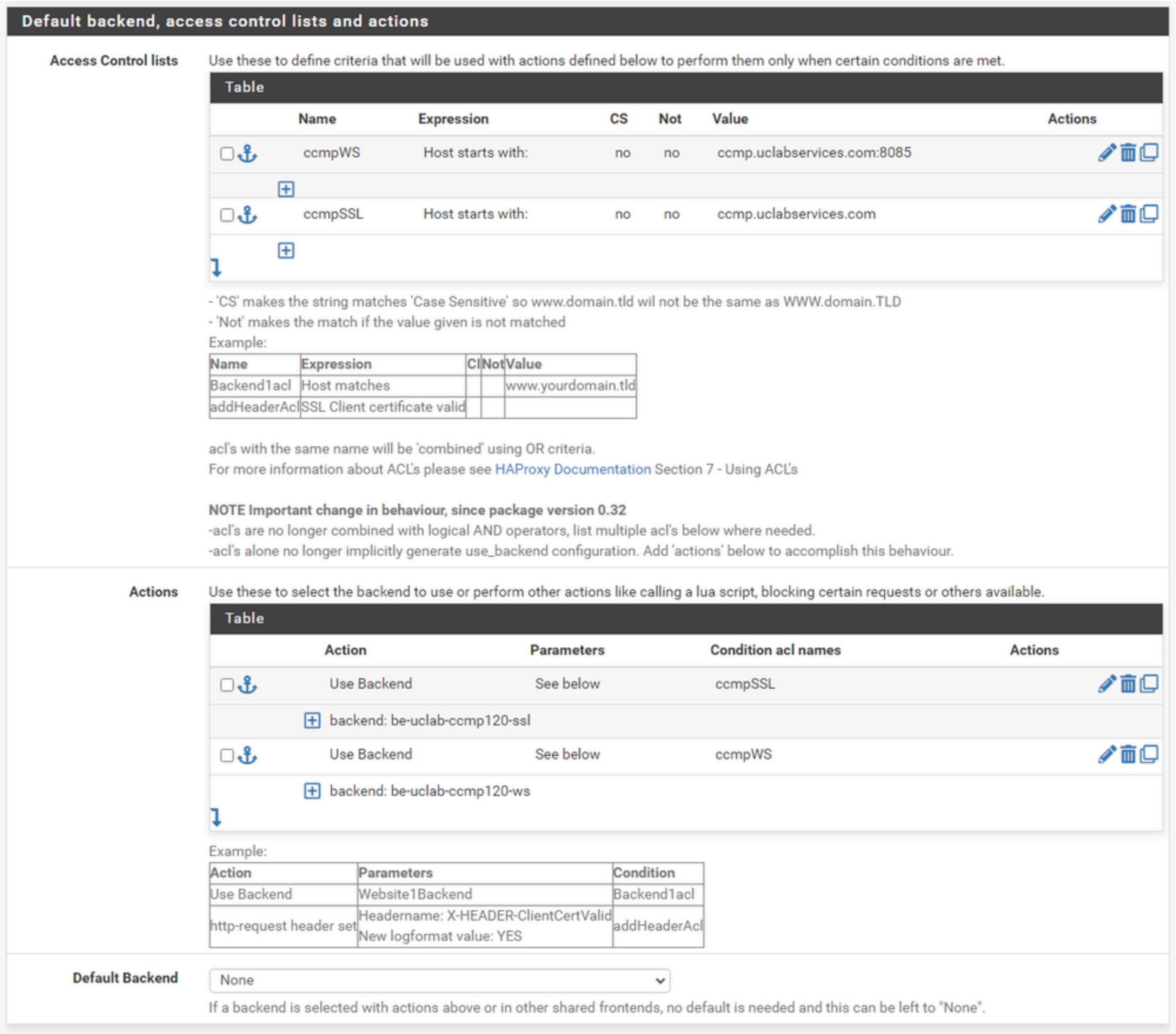
Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAcl

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後端 — 預設後端選擇

最簡單的配置是從下拉選單中選擇預設後端。當VIP託管單個網站時可以選擇此選項。



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

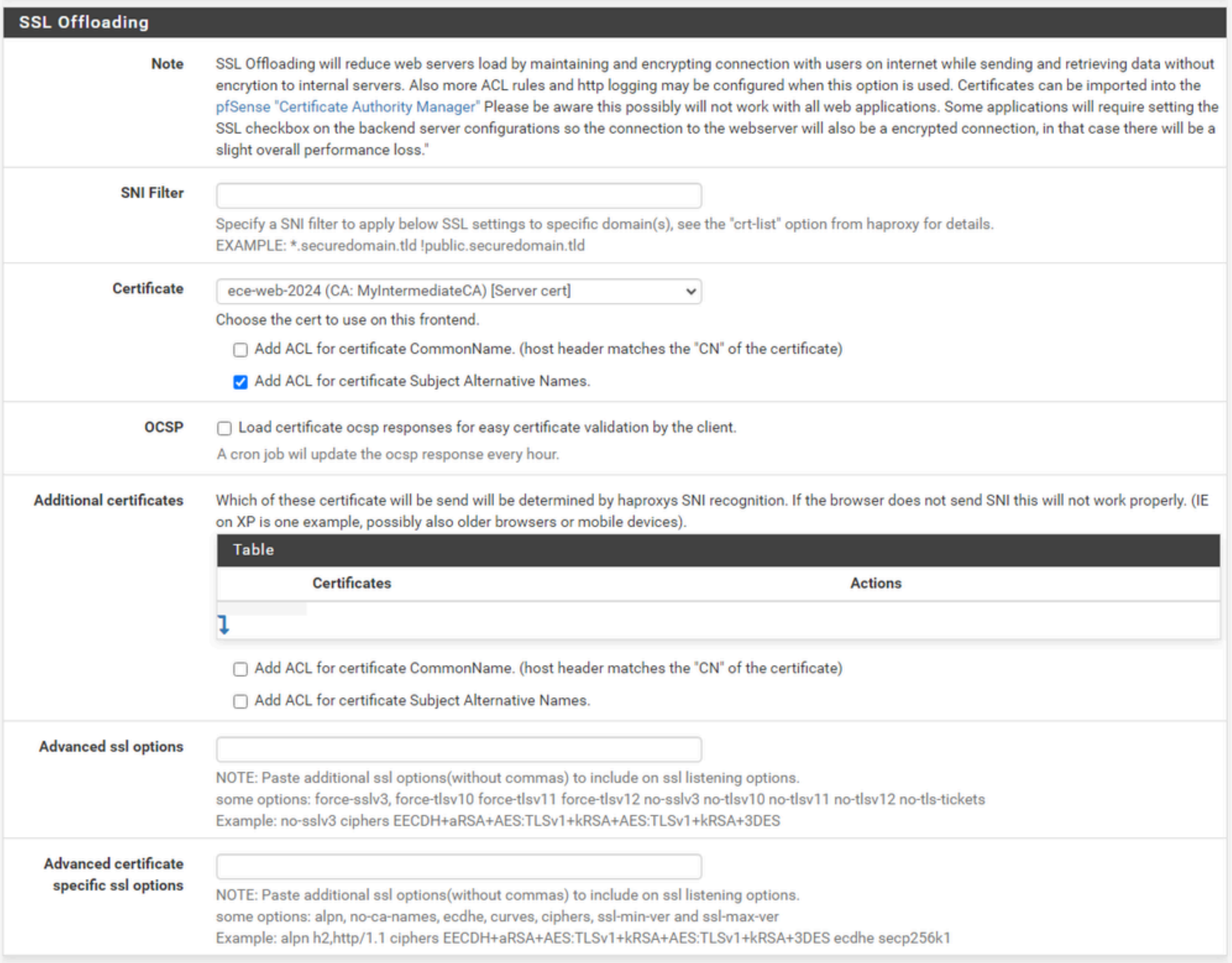
If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

HAProxy後端 — ACL高級

如圖所示，ACL可用於根據情況將單一前端重新導向多個後端。

您可以看到ACL會檢查請求中的主機是否以名稱和埠號開頭，或者只是以名稱開頭。基於此，使用特定後端。

這在歐洲經委會中並不常見。



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

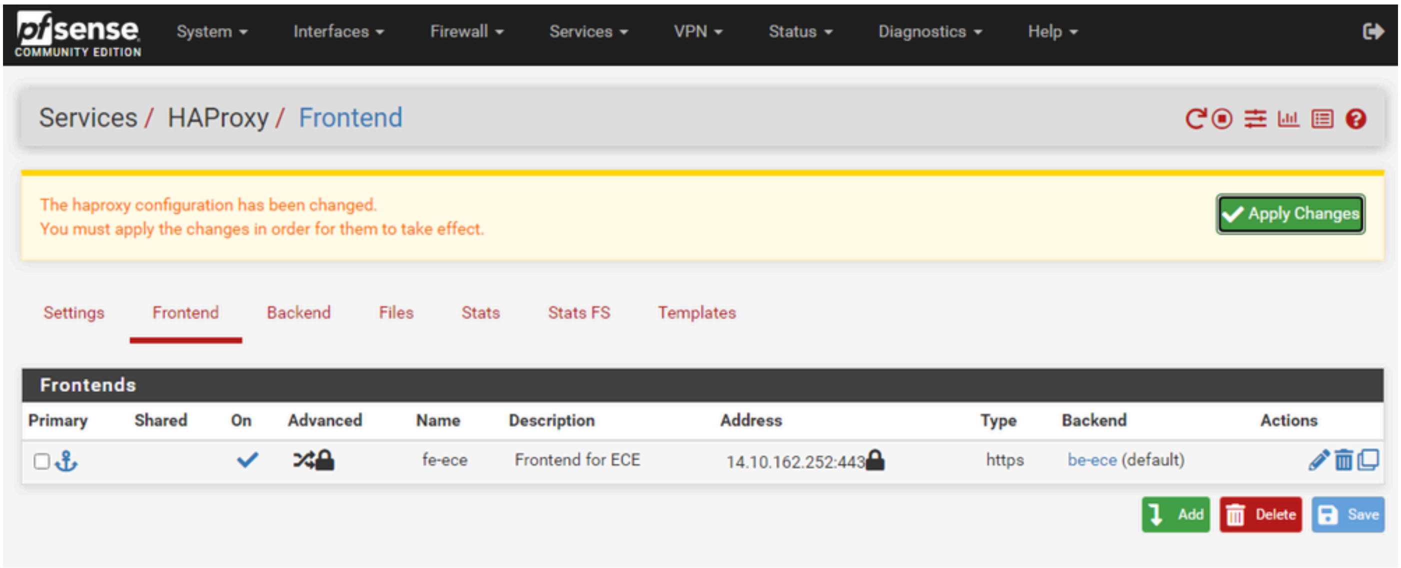
HAProxy前端 — 憑證繫結

在SSL Offloading部分，選擇要用於此站點的證書。此證書必須是伺服器證書。

選擇選項Add ACL for certificate Subject Alternative Names。

可將其餘選項保留為預設值。

選擇此表單末尾的Save。



Services / HAProxy / Frontend

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 — 應用配置

選擇Apply Changes以將前端和後端更改提交到運行配置。

恭喜，您已完成pfSense的設定和配置。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。