

# Configuración del balanceador de carga de comunidad pfSense para ECE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Instalar pfSense](#)

[Descripción general de soluciones](#)

[Preparación](#)

[Instalación](#)

[Configuración de la red](#)

[Completar configuración inicial](#)

[Configuración de los parámetros básicos de administración](#)

[Agregar paquetes requeridos](#)

[Configurar certificados](#)

[Agregar IP virtuales](#)

[Configurar firewall](#)

[Configurar HAProxy](#)

[Conceptos de HAProxy](#)

[Configuración inicial de HAProxy](#)

[Configuración del servidor HAProxy](#)

[Configuración de HAProxy Frontend](#)

---

## Introducción

Este documento describe los pasos para configurar pfSense Community Edition como un equilibrador de carga para Enterprise Chat and Email (ECE).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ECE 12.x
- pfSense Community Edition

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CEPE 12.6(1)
- pfSense Community Edition 2.7.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Instalar pfSense

### Descripción general de soluciones

pfSense Community Edition es un producto multifunción que proporciona un firewall, un equilibrador de carga, un analizador de seguridad y muchos otros servicios en un único servidor. pfSense está basado en BSD libre y tiene unos requisitos de hardware mínimos. El equilibrador de carga es una implementación de HAProxy y se proporciona una GUI fácil de usar para configurar el producto.

Puede utilizar este equilibrador de carga tanto con ECE como con el portal de gestión del centro de contacto (CCMP). Este documento proporciona los pasos para configurar pfSense para ECE.

### Preparación

#### Paso 1. Descargar el software pfSense

Utilice el [sitio web de pfSense](#) para descargar la imagen del instalador iso.

#### Paso 2. Configurar VM

Configure una VM con los requisitos mínimos:

- CPU compatible con amd64 (x86-64) de 64 bits
- 1 GB o más de RAM
- Unidad de disco de 8 GB o más (SSD, HDD, etc.)
- Una o más tarjetas de interfaz de red compatibles
- Unidad USB de arranque o unidad óptica de alta capacidad (DVD o BD) para la instalación inicial

Para una instalación en laboratorio, solo se necesita una interfaz de red (NIC). Hay varias formas de ejecutar el dispositivo, pero la más sencilla es con una única NIC, también denominada modo de brazo único. En el modo de brazo único, existe una única interfaz que se comunica con la red. Aunque esta es una manera fácil y adecuada para un laboratorio, no es la manera más segura.

Una forma más segura de configurar el dispositivo es tener al menos dos NIC. Una NIC es la interfaz WAN y se comunica directamente con la red pública de Internet. La segunda NIC es la interfaz LAN y se comunica con la red corporativa interna. También puede agregar interfaces adicionales para comunicarse con diversas partes de la red que tienen diferentes reglas de seguridad y firewall. Por ejemplo, puede tener una conexión NIC a la red pública de Internet, una conexión a la red DMZ donde se encuentran todos los servidores web accesibles externamente y una tercera conexión NIC a la red corporativa. Esto permite que los usuarios internos y externos accedan de forma segura al mismo conjunto de servidores web que se mantienen en una DMZ. Asegúrese de comprender las implicaciones de seguridad de cualquier diseño antes de la implementación. Póngase en contacto con un ingeniero de seguridad para asegurarse de que se siguen las prácticas recomendadas para su implementación específica.

## Instalación

Paso 1. Montar el ISO en la máquina virtual

Paso 2. Encienda la máquina virtual y siga las indicaciones para instalar.

Consulte este [documento](#) para obtener instrucciones paso a paso.

## Configuración de la red

Debe asignar direcciones IP al dispositivo para continuar con la configuración.



Nota: Este documento muestra un dispositivo configurado en modo de brazo único.

---

Paso 1. Configuración de VLAN

Si necesita compatibilidad con VLAN, responda y a la primera pregunta. De lo contrario, conteste n.

Paso 2. Asignar interfaz WAN

La interfaz WAN es el lado no seguro del dispositivo en modo de dos brazos y la única interfaz en modo de un brazo. Introduzca el nombre de la interfaz cuando se le solicite.

Paso 3. Asignar la interfaz LAN

La interfaz LAN es el lado seguro del dispositivo en modo de dos brazos. Si es necesario, introduzca el nombre de la interfaz cuando se le solicite.

Paso 4. Asignar cualquier otra interfaz

Configure cualquier otra interfaz que necesite para su instalación específica. Estos son opcionales y no son comunes.

## Paso 5. Asignar dirección IP a la interfaz de gestión

Si la red admite DHCP, la dirección IP asignada se muestra en la pantalla de la consola.

```
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:
```

Consola pfSense

Si no hay ninguna dirección asignada, o si desea asignar una dirección específica, siga estos pasos.

1. Seleccione la opción 2 en el menú de la consola.
2. Responda n para desactivar DHCP.
3. Introduzca la dirección IPv4 de la interfaz WAN.
4. Introduzca la máscara de red en recuentos de bits. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Introduzca la dirección del gateway para la interfaz WAN.
6. Si desea que esta puerta de enlace sea la puerta de enlace predeterminada para el dispositivo, responda y a la solicitud de la puerta de enlace; de lo contrario, responda n.
7. Configure la NIC para IPv6 si lo desea.
8. Desactive el servidor DHCP en la interfaz.
9. Responda y para activar HTTP en el protocolo webConfigurator. Esto se utiliza en los siguientes pasos.

A continuación, recibirá la confirmación de que los parámetros se han actualizado.


```
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/

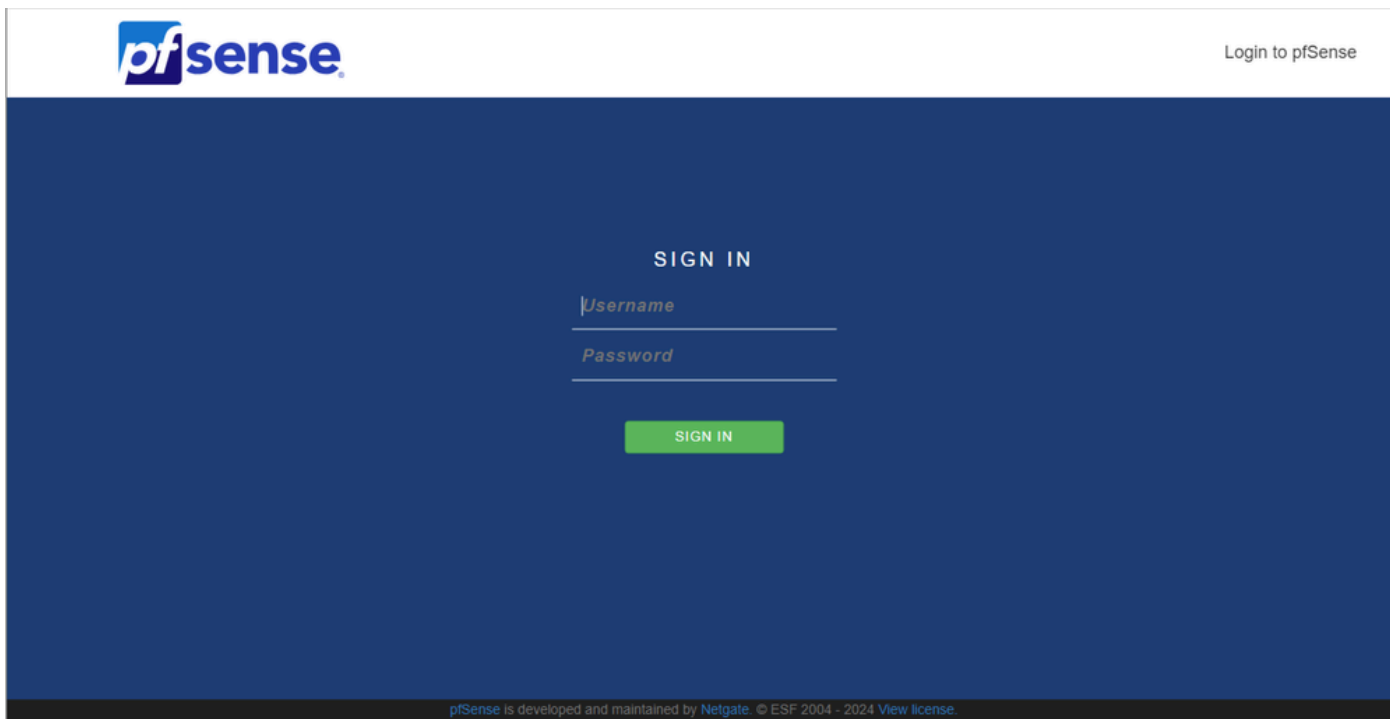
Press <ENTER> to continue. █
```

Confirmación de pfSense

## Completar configuración inicial

Paso 1. Abra un navegador web y navegue hasta: [http://<ip\\_address\\_of\\_appliance>](http://<ip_address_of_appliance>)

 Nota: inicialmente debe utilizar HTTP y no HTTPS.

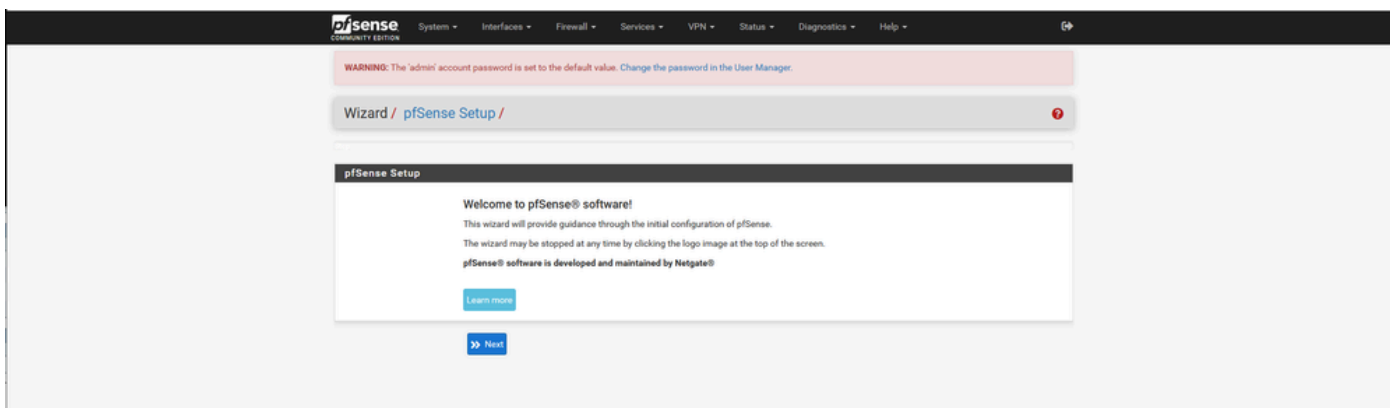


pfSense Admin Login

Paso 2. Inicie sesión con el nombre de usuario predeterminado admin / pfSense

Paso 3. Completar la configuración inicial

Haga clic en Siguiente en las dos primeras pantallas.



Asistente de configuración de pfSense: 1

Proporcione el nombre de host, el nombre de dominio y la información del servidor DNS.

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**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**   
Name of the firewall host, without domain part.  
Examples: pfsense, firewall, edgefw

**Domain**   
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

[» Next](#)

Asistente de configuración de pfSense: 2

Valide la información de la dirección IP. Si inicialmente eligió DHCP, puede cambiarlo ahora.

Proporcione el nombre de host del servidor de hora NTP y seleccione la zona horaria correcta en el menú desplegable.

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**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**   
Enter the hostname (FQDN) of the time server.

**Timezone**  ▾

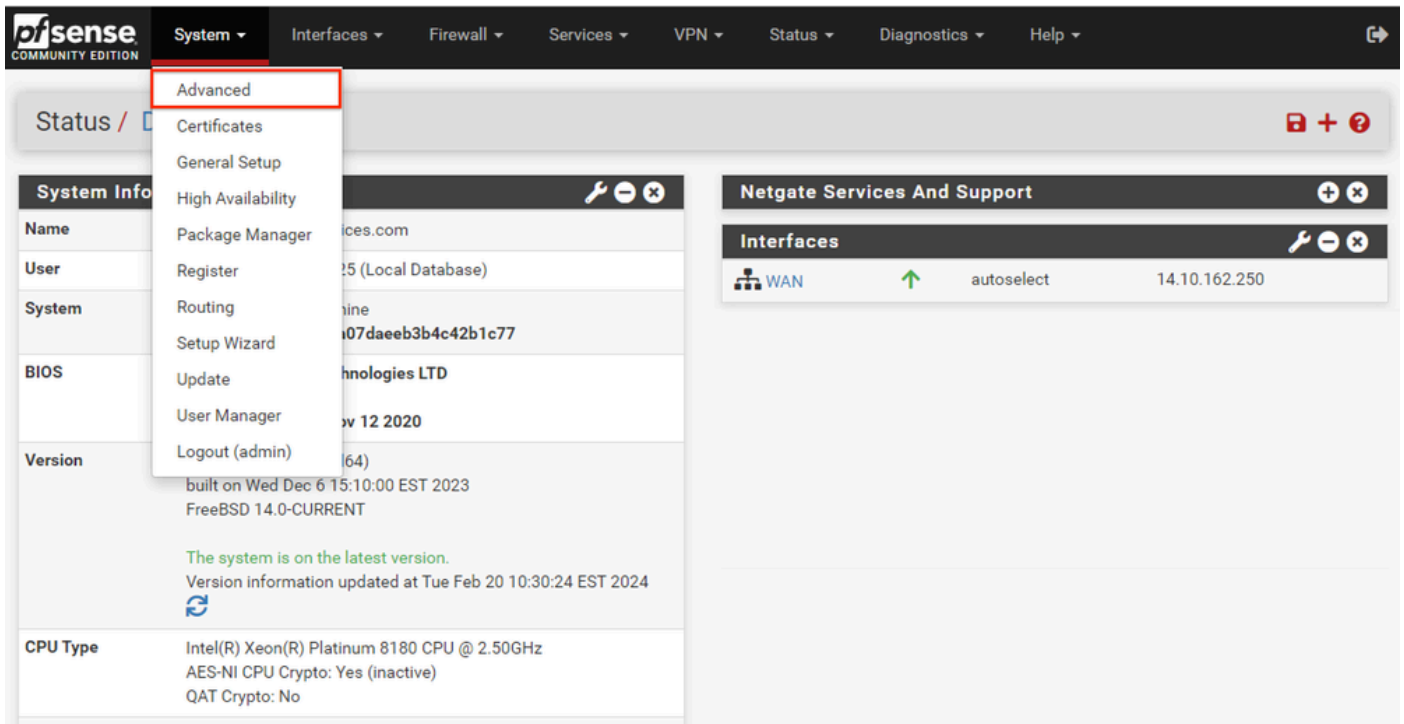
[» Next](#)

Continúe con el asistente de configuración hasta el final. La GUI de la interfaz se reinicia y se le redirige a la nueva URL una vez completada.

## Configuración de los parámetros básicos de administración

Paso 1. Inicie sesión en la interfaz de administración

Paso 2. Seleccione Avanzadas en el menú desplegable Sistema



GUI de pfSense: menú desplegable Admin

Paso 3. Actualizar configuración de webConfigurator

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	GUI default (65cced5b25159) <p>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.</p>
TCP port	8443 <p>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.</p>
Max Processes	2 <p>Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.</p>
WebGUI redirect	<input checked="" type="checkbox"/> Disable webConfigurator redirect rule <p>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.</p>
HSTS	<input type="checkbox"/> Disable HTTP Strict Transport Security <p>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.)</p>
OCSP Must-Staple	<input type="checkbox"/> Force OCSP Stapling in nginx <p>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.</p>
WebGUI Login Autocomplete	<input checked="" type="checkbox"/> Enable webConfigurator login autocomplete <p>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).</p>
GUI login messages	<input type="checkbox"/> Lower syslog level for successful GUI login events <p>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.</p>
Roaming	<input checked="" type="checkbox"/> Allow GUI administrator client IP address to change during a login session <p>When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes.</p>
Anti-lockout	<input type="checkbox"/> Disable webConfigurator anti-lockout rule <p>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!) <i>Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.</i></p>
DNS Rebind Check	<input type="checkbox"/> Disable DNS Rebinding Checks <p>When this is unchecked, the system is protected against <a href="#">DNS Rebinding attacks</a>. 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.</p>
Alternate Hostnames	<input type="text"/> <p>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.</p>
Browser HTTP_REFERER enforcement	<input checked="" type="checkbox"/> Disable HTTP_REFERER enforcement check <p>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 <a href="#">Wikipedia</a>.</p>

pfSense GUI - Configuración de administración

1. Seleccione el protocolo HTTPS (SSL/TLS).
2. Deje el certificado SSL/TLS en el certificado autofirmado en este momento.
3. Cambie el puerto TCP a un puerto distinto de 443 para proteger mejor la interfaz y evitar problemas de superposición de puertos.
4. Seleccione la opción de redirección WebGUI para desactivar la interfaz de administración en el puerto 80.
5. Seleccione la opción de aplicación Navegador HTTP\_REFERER.



6. Active Secure Shell seleccionando la opción Enable Secure Shell (Activar Secure Shell).

 Nota: Asegúrese de que selecciona el botón Guardar antes de continuar. A continuación, se le redirige al nuevo enlace https.

Paso 4. Configurar el servidor proxy si es necesario

Si es necesario, configure la información de proxy en la ficha Miscelánea. Para completar la instalación y la configuración, el dispositivo debe tener acceso a Internet.

System / [Advanced](#) / [Miscellaneous](#) ?

[Admin Access](#) [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

### Proxy Support

<b>Proxy URL</b>	<input type="text" value="myproxy.domain.com"/>
	Hostname or IP address of proxy server this system will use for its outbound Internet access.
<b>Proxy Port</b>	<input type="text" value="3128"/>
	Port where proxy server is listening.
<b>Proxy Username</b>	<input type="text"/>
	Username for authentication to proxy server. Optional, leave blank to not use authentication.
<b>Proxy Password</b>	<input type="password" value="Proxy Password"/> <input type="password" value="Proxy Password"/>
	Password for authentication to proxy server. <span style="float: right;">Confirm</span>


GUI de pfSense: configuración de proxy

 Nota: Asegúrese de que selecciona el botón Guardar después de realizar los cambios.

## Agregar paquetes requeridos

Paso 1. Seleccione Sistema > Administrador de paquetes

Paso 2. Seleccionar paquetes disponibles

 Nota: Puede tardar unos minutos en cargar todos los paquetes que están disponibles. Si se agota el tiempo de espera, compruebe que los servidores DNS están configurados correctamente. A menudo, un reinicio del dispositivo repara la conectividad a Internet.

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.

Name	Version	Description	
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: <a href="#">pecl-ssh2-1.3.1</a> <a href="#">socat-1.7.4.4</a> <a href="#">php82-8.2.11</a> <a href="#">php82-ftp-8.2.11</a>	<a href="#">+ Install</a>
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: <a href="#">apcupsd-3.14.14_4</a>	<a href="#">+ Install</a>
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: <a href="#">arping-2.21_1</a>	<a href="#">+ Install</a>
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.	<a href="#">+ Install</a>

pfSense GUI - Lista de paquetes

### Paso 3. Buscar e instalar los paquetes necesarios

1. haproxy
2. Open-VM-Tools

 Nota: No seleccione el paquete haproxy-devel.

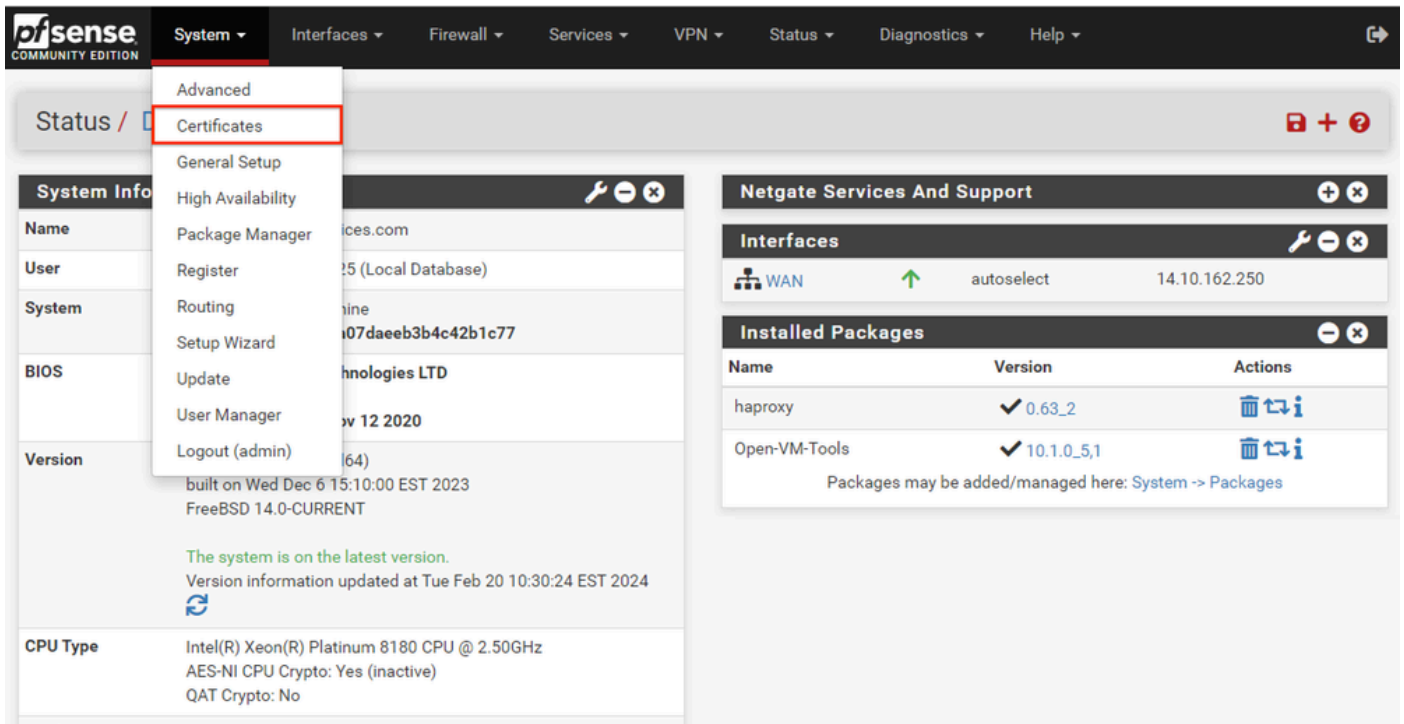
## Configurar certificados

pfSense puede crear un certificado autofirmado o puede integrarse con una CA pública, una CA interna o puede actuar como CA y emitir certificados firmados por CA. Esta guía muestra los pasos para la integración con una CA interna.

Antes de empezar esta sección, asegúrese de que dispone de estos elementos.

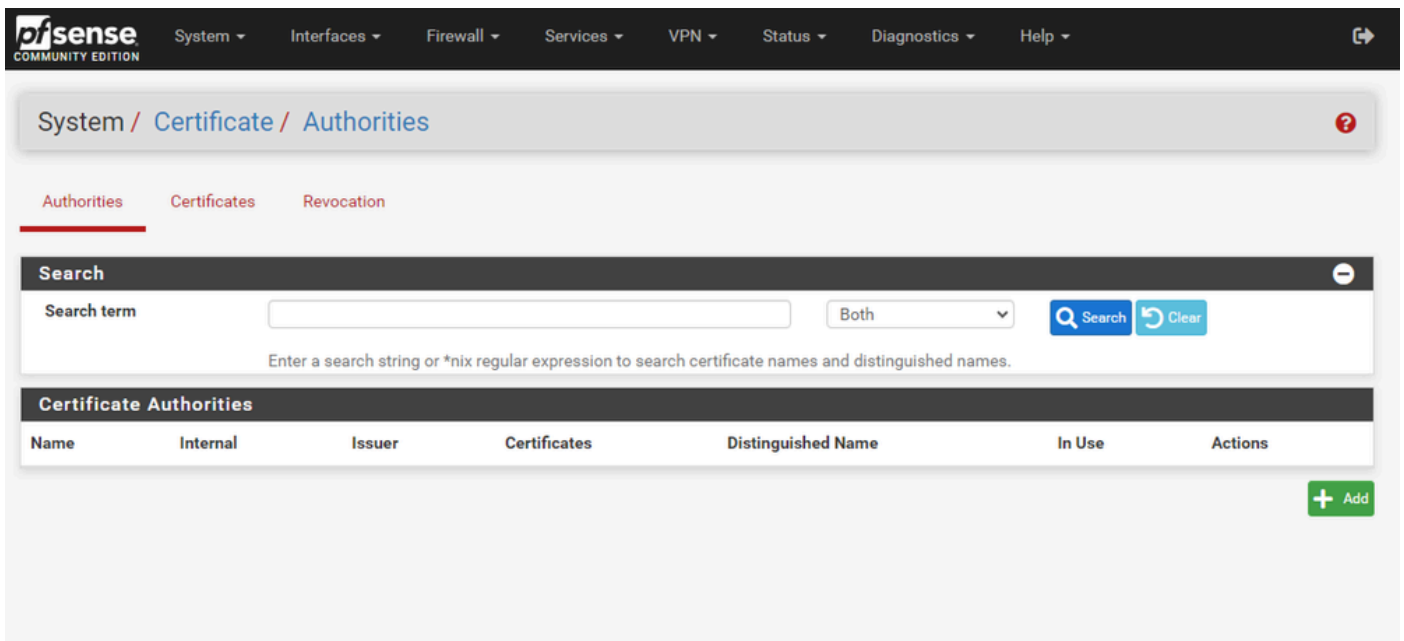
1. Certificado raíz para CA guardado como formato PEM o codificado en Base-64.
2. Todos los certificados intermedios (a veces denominados emisores) para CA se guardan como formato PEM o codificado en Base-64.

### Paso 1. Seleccione Certificados en el menú desplegable Sistema



GUI de pfSense: menú desplegable Certificados

## Paso 2. Importar el certificado raíz de la CA



GUI de pfSense: lista de certificados de CA

Seleccione el botón Agregar.

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

### Create / Edit CA

**Descriptive name**   
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**

**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**   
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.

GUI de pfSense: importación de CA

Como se muestra en la imagen:

1. Proporcione un nombre único y descriptivo
2. Seleccione Importar una autoridad de certificación existente en el menú desplegable Método.
3. Asegúrese de que las casillas de verificación Almacén de confianza y Aleatorizar serie estén activadas.
4. Pegue el certificado completo en el cuadro de texto Datos del certificado. Asegúrese de incluir desde las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.
5. Seleccione Guardar.
6. Compruebe que el certificado se ha importado como se muestra en la imagen.

pfSense COMMUNITY EDITION
System ▾
Interfaces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Help ▾
↗

System / Certificate / Authorities ?

Authorities
Certificates
Revocation

**Search** ⊖  
 Search term  Both ▾ 🔍 Search 🔄 Clear  
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 <span>ℹ</span> Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500		<span>✎</span> <span>⚙</span> <span>🗑</span>

+ Add

GUI de pfSense: lista de CA

Paso 3. Importar el certificado intermedio de la CA

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

### Create / Edit CA

**Descriptive name**   
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**

**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**   
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.

GUI de pfSense: importación intermedia de CA

Repita los pasos para importar el certificado de CA raíz e importar el certificado de CA intermedio.

System / Certificate / Authorities

Authorities Certificates Revocation

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	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	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/>
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	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/>

GUI de pfSense: enlaces de CA

Revise las autoridades de certificados para asegurarse de que el intermedio está correctamente encadenado al certificado raíz como se muestra en la imagen.

Paso 4. Crear y exportar un CSR para el sitio web con equilibrio de carga

Describe los pasos para crear una CSR, exportar la CSR e importar el certificado firmado. Si ya tiene un certificado existente en formato PFX, puede importar este certificado. Consulte la documentación de pfSense para obtener información sobre estos pasos.

1. Seleccione el menú Certificados y, a continuación, el botón Agregar/Firmar.

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

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 (65ccd5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65ccd5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	<input type="checkbox"/> webConfigurator	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>

## 2. Complete el formulario de solicitud de firma de certificado.

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

- Método: seleccione Crear una solicitud de firma de certificado en el menú desplegable
- Nombre descriptivo: proporcione un nombre para el certificado
- Tipo de clave y algoritmo de resumen: revise para asegurarse de que coinciden con sus requisitos
- Nombre común: Proporcione el sitio web del nombre de dominio completo
- Proporcione la información de certificado restante según sea necesario para su entorno



**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**  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 Value

**Add SAN Row**

GUI de pfSense: CSR Advanced

- Tipo de certificado: seleccione Certificado de servidor en el menú desplegable.
- Nombres alternativos: proporcione cualquier nombre alternativo de asunto (SAN) necesario para su implementación.

 Nota: el nombre común se agrega automáticamente al campo SAN. Sólo tiene que agregar los nombres adicionales necesarios.

Seleccione Guardar cuando todos los campos sean correctos.

3. Exporte el CSR a un archivo.

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**

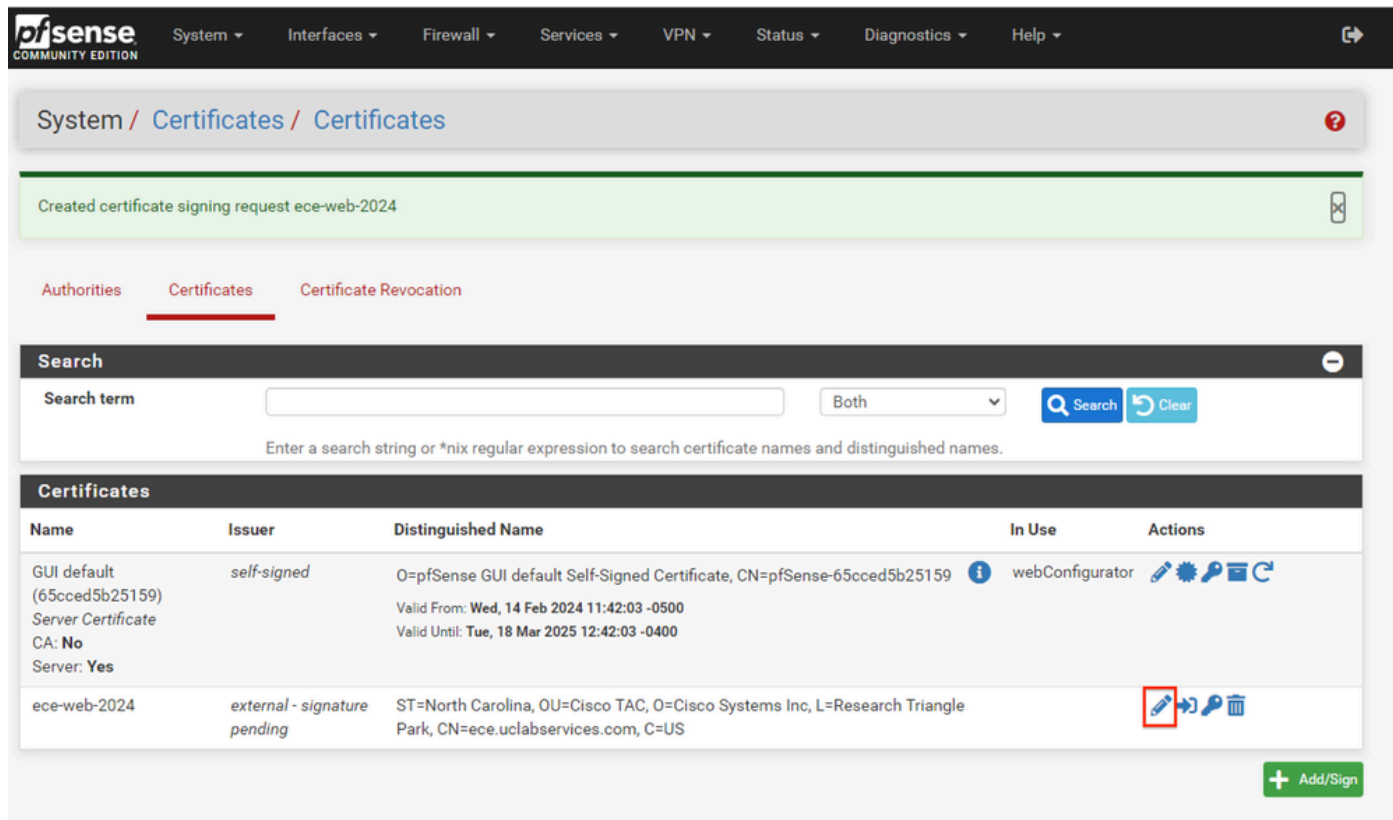
Search term  Both

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

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	<input checked="" type="checkbox"/> 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	<input type="checkbox"/>	   

Seleccione el botón Exportar para guardar el CSR y firme esto con la CA. Una vez que tenga el certificado firmado, guárdelo como un archivo PEM o Base-64 para completar el proceso.

#### 4. Importe el certificado firmado.



GUI de pfSense: importación de certificados

Seleccione el icono Lápiz para importar el certificado firmado.

#### 5. Pegue los datos del certificado en el formulario.

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

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

### Complete Signing Request for ece-web-2024

**Descriptive name**   
 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-----
MIIDvDCCAQQCAQAwZcHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
MAkGA1UEBHMCMVVMxZzAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMR0wGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
YzESMBAGA1UECzMjQ21zY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

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

**Final certificate data**  

```
GBSAPwQWkas305JkKISY/pYEI2EW/7EZcDmHRUrnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yIz3IT4TJwDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5Mnuqx1PN97EPQngO/1IgXo4xDz6Dg+Iwt9pyrRZdxpmy
-----END CERTIFICATE-----
```

 Paste the certificate received from the certificate authority here.

GUI de pfSense: importación de certificados

Seleccione Update para guardar el certificado.

6. Revise los datos del certificado para asegurarse de que son correctos.

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

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

**Search**

Search term  Both ▾

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

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65ccd5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65ccd5b25159 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		

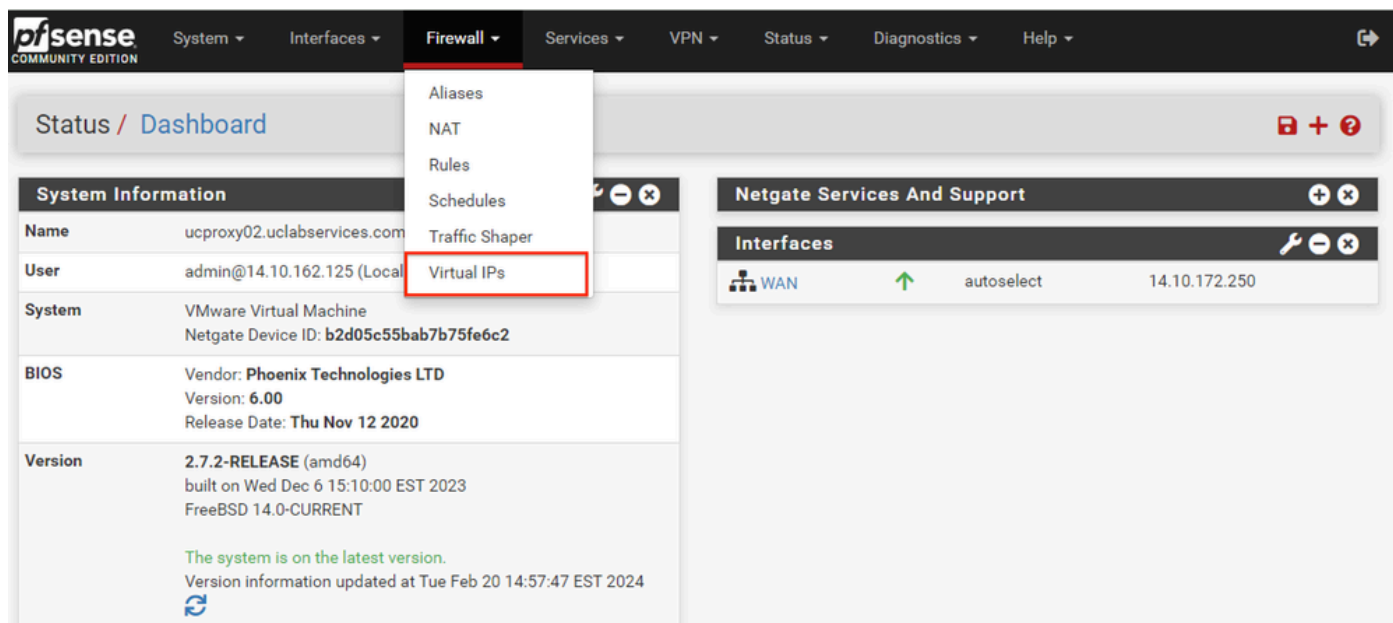
GUI de pfSense: lista de certificados

7. Repita este proceso si desea alojar varios sitios en este pfSense.

## Agregar IP virtuales

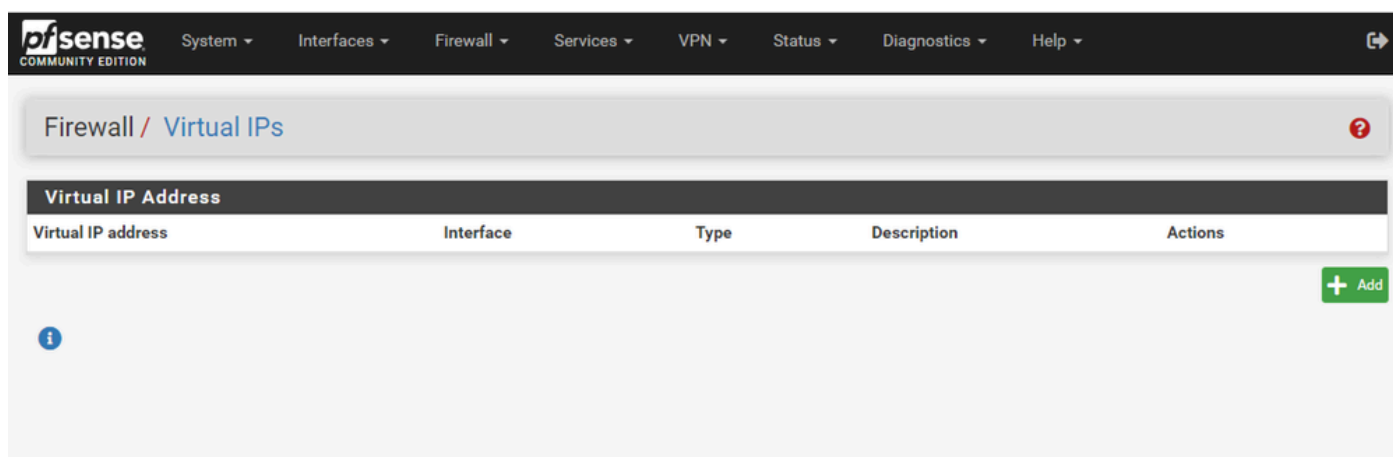
Se necesita al menos una IP para alojar sitios web en pfSense. En pfSense esto se hace con las IP virtuales (VIP).

Paso 1. Seleccione IP virtuales en el menú desplegable Firewall.



GUI de pfSense: menú desplegable VIP

Paso 2. Seleccione el botón Agregar



GUI de pfSense: página de inicio de VIP

Paso 3. Proporcionar información de dirección

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**

GUI de pfSense: configuración de VIP

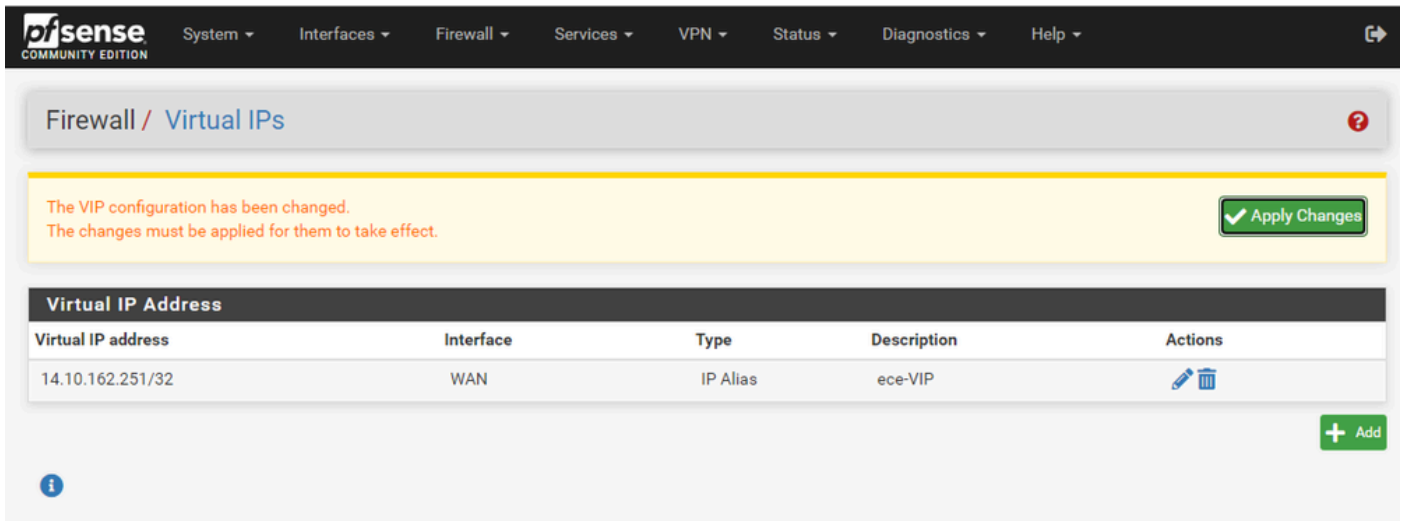
Utilice la información para agregar un VIP.

- Tipo: Seleccionar alias IP
- Interfaz: seleccione la interfaz para esta dirección IP que se va a difundir
- Direcciones: introduzca la dirección IP
- Máscara de dirección: para las direcciones IP utilizadas para el balanceo de carga, la máscara debe ser un /32
- Descripción: proporcione un texto breve para facilitar la comprensión de la configuración más adelante

Seleccione Guardar para aplicar el cambio.

Repita este procedimiento para cada dirección IP necesaria para la configuración.

Paso 4. Aplicar configuración



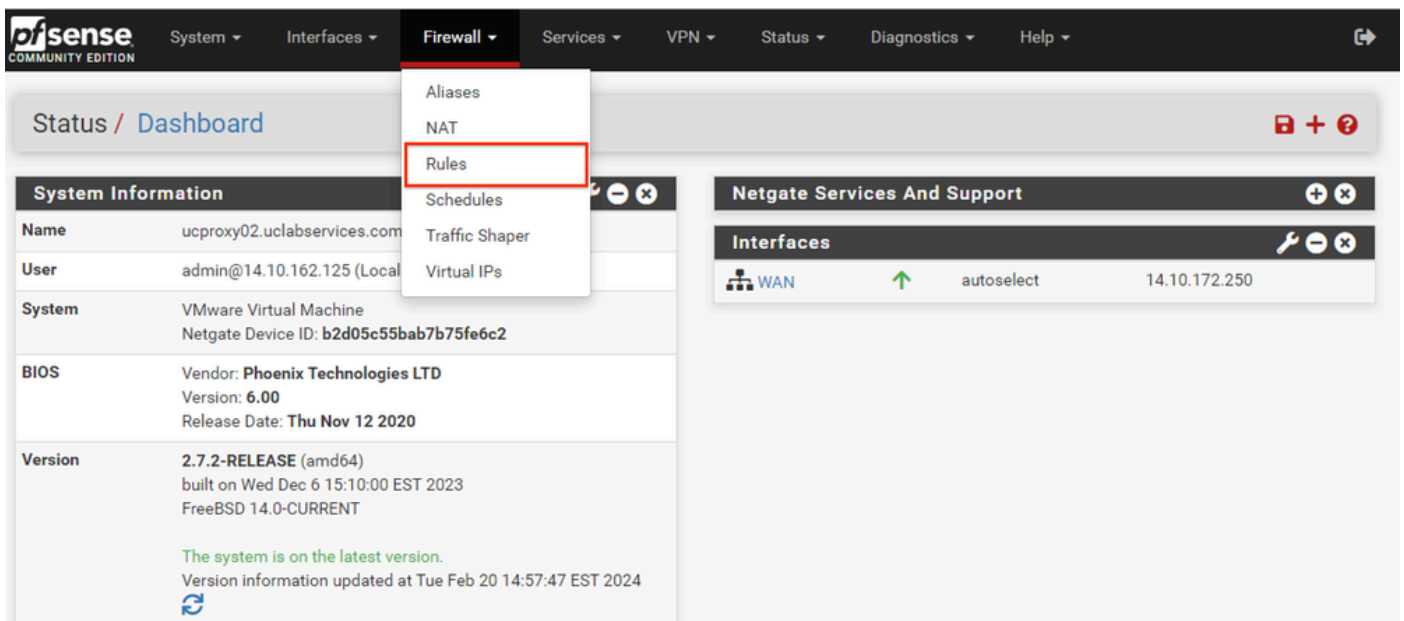
GUI de pfSense: lista VIP

Seleccione el botón Aplicar cambios después de agregar todos los VIP.

## Configurar firewall

pfSense tiene un firewall incorporado. El conjunto de reglas predeterminado es muy limitado. Antes de poner el dispositivo en funcionamiento, asegúrese de crear una política de firewall completa.

Paso 1. Seleccione Reglas en el menú desplegable Firewall



GUI de pfSense: menú desplegable Reglas del firewall

Paso 2. Seleccione uno de los botones Agregar

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The page title is "Firewall / Rules / WAN". There are two tabs: "Floating" and "WAN", with "WAN" selected. Below the tabs is a table titled "Rules (Drag to Change Order)". The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three rules listed:

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	⚙️

Below the table is a yellow warning box: "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." At the bottom right, there is a toolbar with buttons: "Add" (up arrow), "Add" (down arrow), "Delete", "Toggle", "Copy", "Save", and "Separator". The "Add" buttons are highlighted with a red box.

GUI de pfSense: lista de reglas del firewall

Tenga en cuenta que un botón agrega la nueva regla sobre la línea seleccionada mientras que el otro agrega la regla debajo de la regla seleccionada. Se puede utilizar cualquiera de los botones para la primera regla.

Paso 3. Cree una regla de firewall para permitir el tráfico al puerto 443 para la dirección IP

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

Firewall / Rules / Edit ☰ 📄 📄 ?

### Edit Firewall Rule

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

**Address Family**  ▾  
 Select the Internet Protocol version this rule applies to.

**Protocol**  ▾  
 Choose which IP protocol this rule should match.

---

**Source**

**Source**  Invert match  ▾  /  ▾

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  ▾  /  ▾

**Destination Port Range**  ▾   ▾    
 From Custom 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**   
 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**

GUI de pfSense: configuración de reglas de paso de firewall

Utilice la información para crear la regla.

- Acción: Seleccione Pasar
- Interfaz: Seleccione la interfaz a la que se aplica la regla
- Familia de direcciones y protocolo: seleccione lo que corresponda
- Origen: dejar seleccionado como Cualquiera
- Destino: seleccione Dirección o Alias en el menú desplegable Destino e introduzca la dirección IP a la que se aplica la regla
- Intervalo de puertos de destino: seleccione HTTPS (443) en el menú desplegable De y A
- Registro: seleccione la casilla de verificación para registrar cualquier paquete que coincida con esta regla para la contabilización



- Descripción: proporcione texto para hacer referencia a la regla más adelante

Seleccione Guardar.

Paso 4. Cree una regla de firewall para descartar el resto del tráfico a pfSense

Seleccione el botón Agregar para insertar la regla debajo de la regla recién creada.

The screenshot shows the 'Edit Firewall Rule' configuration page in pfSense. The page is divided into several sections:

- Action:** A dropdown menu set to 'Block'. Below it, a hint explains the difference between block and reject.
- Disabled:** A checkbox labeled 'Disable this rule' which is currently unchecked.
- Interface:** A dropdown menu set to 'WAN'.
- Address Family:** A dropdown menu set to 'IPv4'.
- Protocol:** A dropdown menu set to 'TCP'.
- Source:** A section with a checkbox 'Invert match' (unchecked), a dropdown 'Any', and a 'Source Address' field. Below this is a 'Display Advanced' button and a note about source port ranges.
- Destination:** A section with a checkbox 'Invert match' (unchecked), a dropdown 'Any', and a 'Destination Address' field. Below this is a 'Destination Port Range' section with 'From' and 'To' dropdowns (both set to '(other)'), and 'Custom' input fields. A note explains the 'To' field.
- Extra Options:** A section with a checked 'Log' checkbox and a 'Description' text input field containing 'Drop all other inbound traffic'. Below this is another 'Display Advanced' button.

At the bottom of the page, there is a blue 'Save' button.

GUI de pfSense: configuración de reglas de eliminación del firewall

- Acción: Seleccionar bloque

- Interfaz: Seleccione la interfaz a la que se aplica la regla
- Familia de direcciones y protocolo: seleccione lo que corresponda
- Origen: dejar seleccionado como Cualquiera
- Destino: deje seleccionado como Cualquiera
- Registro: seleccione la casilla de verificación para registrar cualquier paquete que coincida con esta regla para la contabilización
- Descripción: proporcione texto para hacer referencia a la regla más adelante

Seleccione Guardar.

Paso 5. Revise las reglas y asegúrese de que la regla de bloqueo se encuentra en la parte inferior

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

Apply Changes

Floating WAN

Rules (Drag to Change Order)

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

↑ Add ↓ Add Delete Toggle Copy Save + Separator

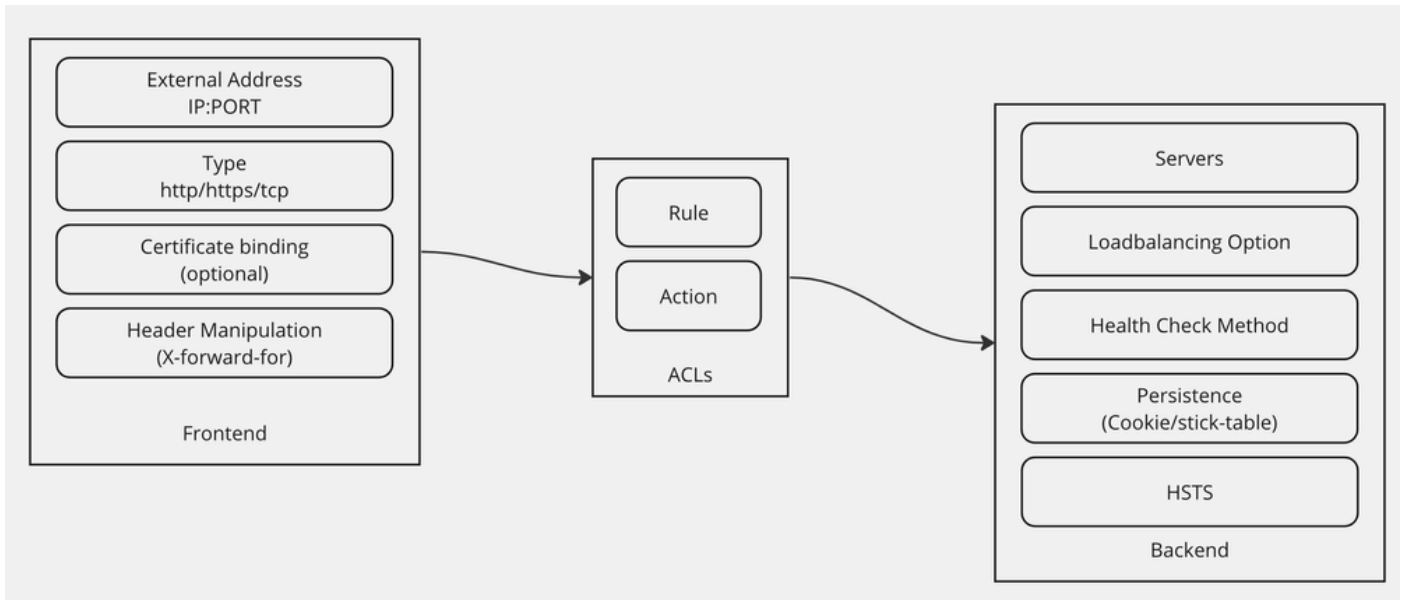
GUI de pfSense: lista de reglas del firewall

Si es necesario, arrastre las reglas para ordenarlas.

Seleccione Aplicar cambios una vez que las reglas del firewall estén en el orden requerido para su entorno.

## Configurar HAProxy

Conceptos de HAProxy



Conceptos de HAProxy

HAProxy se implementa con un modelo de interfaz/servidor.

Frontend define el lado del proxy con el que se comunican los clientes.

El Frontend consiste en una combinación de IP y puerto, vinculación de certificados y puede implementar alguna manipulación de encabezado.

El motor define el lado del proxy que se comunica con los servidores web físicos.

El motor define los servidores y puertos reales, el método de equilibrio de carga para la asignación inicial, las comprobaciones de estado y la persistencia.

Un Frontend sabe con qué backend comunicarse mediante un backend dedicado o mediante el uso de ACL.

Las ACL pueden crear diferentes reglas de modo que un determinado front-end pueda comunicarse con diferentes backends dependiendo de varias cosas.

## Configuración inicial de HAProxy

Paso 1. Seleccione HAProxy en el menú desplegable Servicios

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the following items: System, Interfaces, Firewall, Services (highlighted), VPN, Status, Diagnostics, and Help. Below the navigation bar, the main content area is divided into two columns. The left column contains a 'System Information' table, and the right column contains a 'Netgate Services And Support' section.

**System Information Table:**

<b>Name</b>	ucproxy02.uclabservices.com
<b>User</b>	admin@14.10.162.125 (Local Database)
<b>System</b>	VMware Virtual Machine Netgate Device ID: b2d05c55bab7b75fe6c2
<b>BIOS</b>	Vendor: <b>Phoenix Technologies LTD</b> Version: <b>6.00</b> Release Date: <b>Thu Nov 12 2020</b>
<b>Version</b>	<b>2.7.2-RELEASE</b> (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 14:00:00 EST 2024
<b>CPU Type</b>	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

**Services Menu (highlighted):**

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- HAProxy**
- IGMP Proxy
- NTP
- PPPoE Server
- Router Advertisement
- SNMP
- Wake-on-LAN

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

GUI de pfSense: menú desplegable de HAProxy

## Paso 2. Configurar los parámetros básicos

Services / HAProxy / Settings

Settings Frontend Backend Files Stats Stats FS Templates

### General settings

Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections  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

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

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

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

### Stats tab, 'internal' stats port

Internal stats port  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 resources.

Internal stats refresh rate  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

GUI de pfSense: configuración principal de HAProxy

Active la casilla de verificación Habilitar HAProxy.

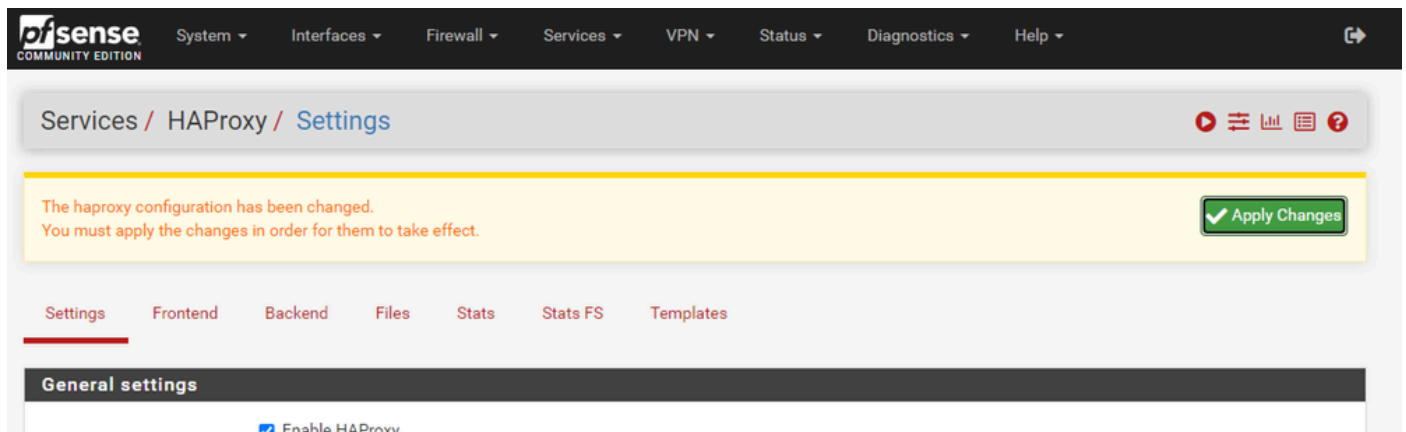
Introduzca un valor para Número máximo de conexiones. Consulte el gráfico de esta sección para obtener más información sobre la memoria necesaria.

Introduzca un valor para el puerto de estado interno. Este puerto se utiliza para mostrar estadísticas de HAProxy en el dispositivo, pero no se expone fuera del dispositivo.


Introduzca un valor para la frecuencia de actualización de estadísticas internas.

Revise la configuración restante y actualícela según sea necesario para su entorno.

Seleccione Guardar.

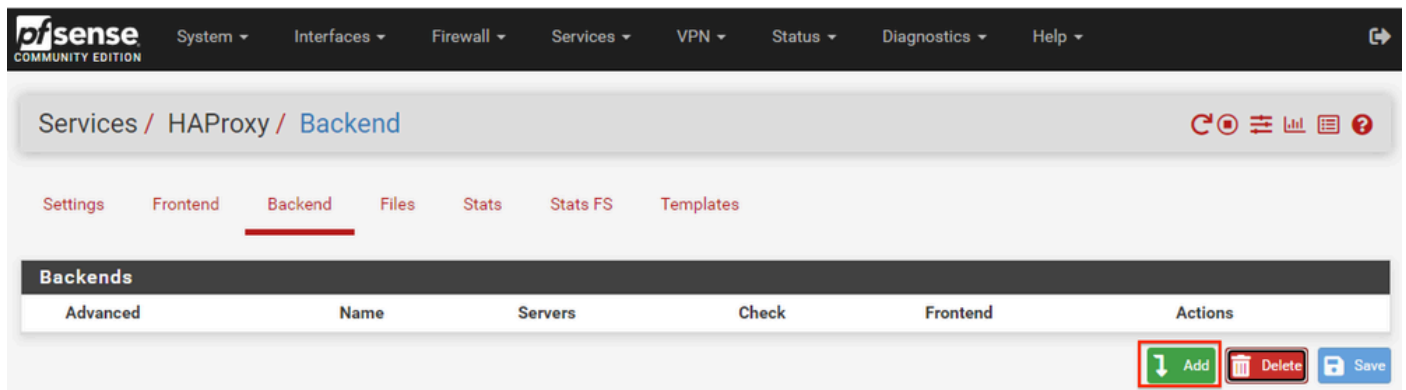


GUI de pfSense: cambios en la aplicación de HAProxy

 Nota: Los cambios de configuración no se activan hasta que se selecciona el botón Aplicar cambios. Puede realizar varios cambios de configuración y aplicarlos todos a la vez. No es necesario aplicar la configuración para utilizarla en otra sección.

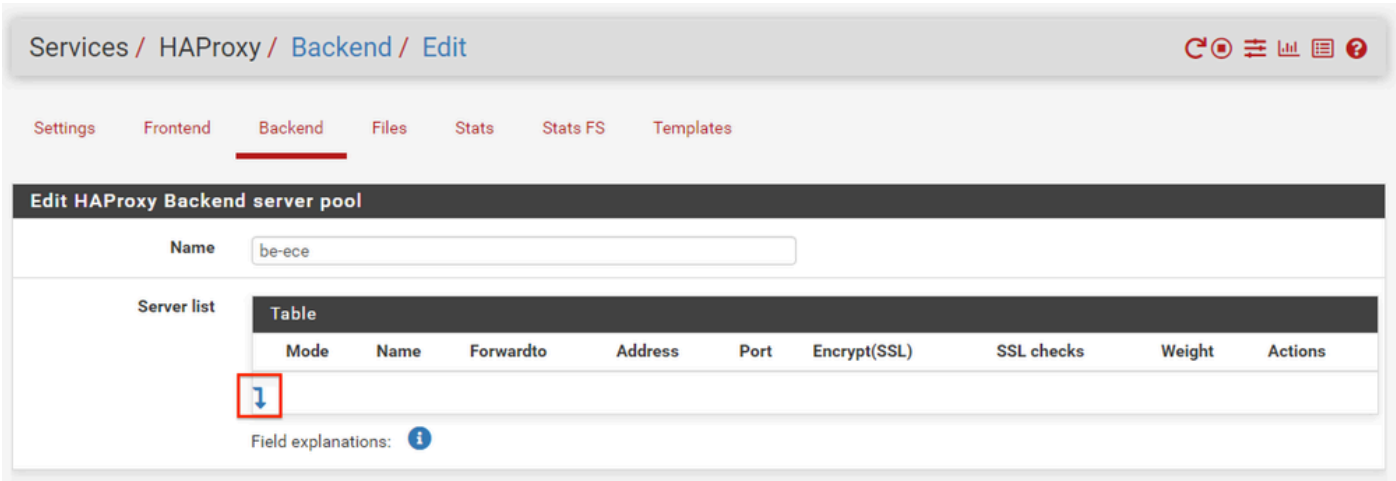
## Configuración del servidor HAProxy

Comience con el motor. Esto se debe a que el front-end debe hacer referencia a un back-end. Asegúrese de que ha seleccionado el menú Motor.



GUI de pfSense: HAProxy Add Backend

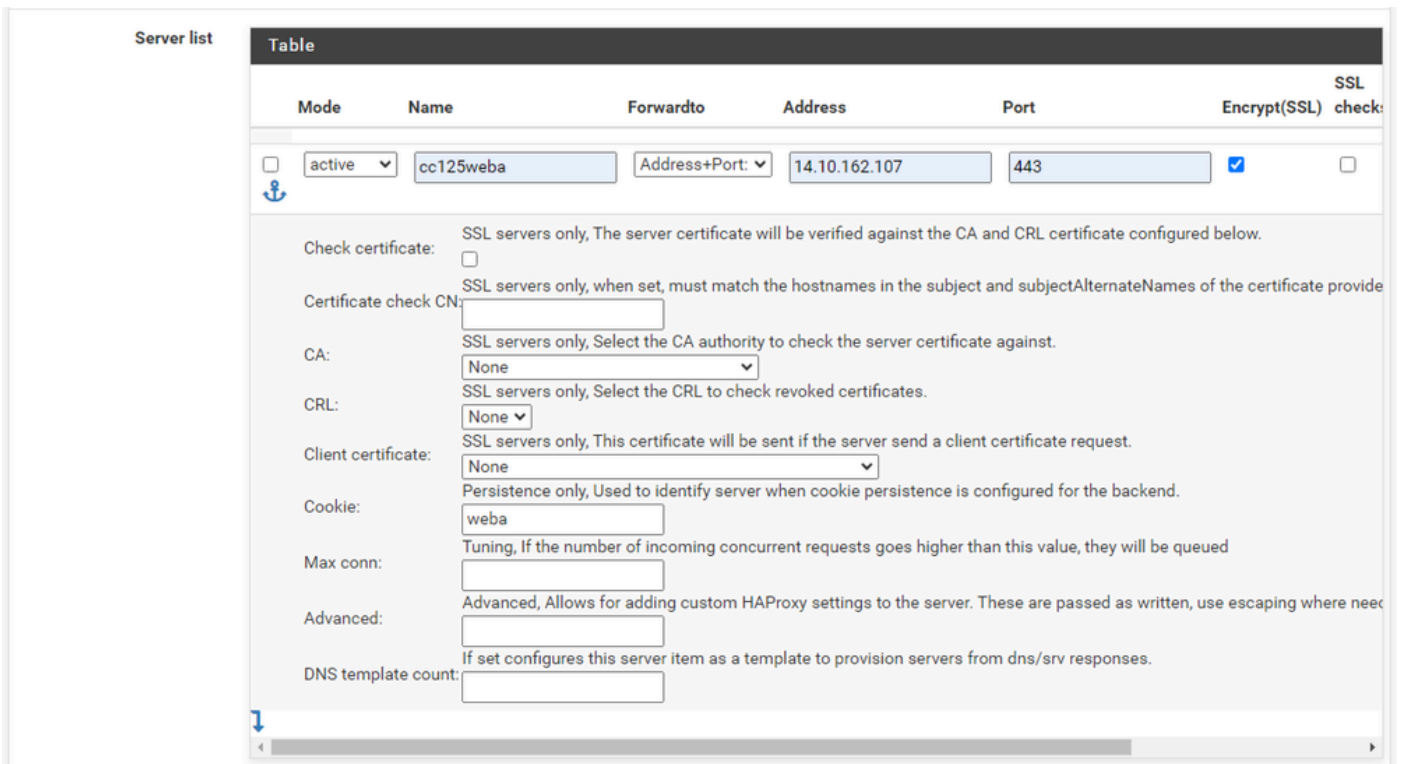
Seleccione el botón Add.



GUI de pfSense: inicio de servidor proxy de HAP

Proporcione un nombre para el servidor.

Seleccione la flecha hacia abajo para agregar el primer servidor a la lista Servidor



Motor - Lista de servidores

Proporcione un nombre para hacer referencia al servidor. No es necesario que coincida con el nombre real del servidor. Este es el nombre que se muestra en la página de estadísticas.

Proporcione la dirección del servidor. Puede configurarse como una dirección IP para FQDN.

Proporcione el puerto al que conectarse. Debe ser el puerto 443 para ECE.

Active la casilla Cifrar (SSL).

Proporcione un valor en el campo Cookie. Este es el contenido de la cookie de permanencia de

sesión y debe ser único dentro del backend.

Una vez configurado el primer servidor, seleccione la flecha hacia abajo para configurar cualquier otro servidor web del entorno.

**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.

Motor HAProxy - Equilibrio de carga

Configure las opciones de equilibrio de carga.

Para los servidores ECE, se debe establecer en el valor de Menores conexiones.



Access control lists and actions	
<b>Timeout / retry settings</b>	
<b>Connection timeout</b>	<input type="text" value="60000"/> The time (in milliseconds) we give up if the connection does not complete within (default 30000).
<b>Server timeout</b>	<input type="text" value="60000"/> The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).
<b>Retries</b>	<input type="text" value="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.
<b>Health checking</b>	
<b>Health check method</b>	<input type="text" value="HTTP"/> <small>HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).</small>
<b>Check frequency</b>	<input type="text"/> <small>milliseconds</small> <small>For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.</small>
<b>Log checks</b>	<input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged. <small>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.</small>
<b>Http check method</b>	<input type="text" value="GET"/> <small>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 webserver and is less easy to filter out of its logs.</small>
<b>Url used by http check requests.</b>	<input type="text" value="/system/web/view/platform/common/login/root.jsp?partitionId=1"/> <small>Defaults to / if left blank.</small>
<b>Http check version</b>	<input type="text" value="HTTP/1.1\r\nHost:\ ece125.uclabservices.com"/> <small>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:  <small>HTTP/1.1\r\nHost:\ www</small>  <small>Also some hosts might require an accept parameter like this:  <small>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</small> </small> </small>

Motor HAProxy: comprobación de estado

Las listas de control de acceso no se utilizan en esta configuración.

Los valores de tiempo de espera/reintento se pueden dejar en la configuración predeterminada.

Configure la sección Comprobación de estado.

1. Método de comprobación de estado: HTTP
2. Comprobar frecuencia: deje este campo en blanco si desea utilizar el valor predeterminado cada 1 segundo.
3. Comprobaciones de registro: seleccione esta opción para escribir los cambios de estado en los registros.
4. Método de comprobación HTTP: seleccione GET en la lista.
5. Url utilizada por solicitudes de comprobación http.: Para un servidor ECE, introduzca /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Versión de comprobación de HTTP: introduzca, HTTP/1.1\r\nHost:\ {fqdn\_of\_server}

Asegúrese de incluir un espacio después de la barra diagonal inversa final pero antes del FQDN del servidor.

**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**   
The string name to track in Set-Cookie and Cookie HTTP headers.  
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASPNET\_SessionId

**Cookie Mode**   
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-secure channels.

**Cookie Options**    
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, separate 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 separate 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**   
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**   
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 Backend - Persistencia de cookies

Deje las comprobaciones de agente sin seleccionar.

Configurar persistencia de cookies:

1. Cookie Enabled (Cookie habilitada): seleccione esta opción para habilitar la persistencia basada en cookies.
2. Nombre de cookie: introduzca un nombre para la cookie.
3. Modo de cookies: seleccione Insertar en el cuadro desplegable.
4. Deje las opciones restantes sin definir.

**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" attribute 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**

Save

Motor HAProxy - HSTS

El resto de las secciones del formulario de configuración backend se pueden dejar en sus valores predeterminados.

Si desea configurar HSTS, configure un valor de tiempo de espera en esta sección. ECE también inserta una cookie HSTS para que esta configuración sea redundante.

Seleccione, Guardar.

## Configuración de HAProxy Frontend

Cambie al menú Frontend.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / HAProxy / Frontend

Settings **Frontend** Backend Files Stats Stats FS Templates

**Frontends**

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
									<div style="display: flex; gap: 5px;"> <span style="border: 1px solid red; padding: 2px;">Add</span> <span style="border: 1px solid red; padding: 2px;">Delete</span> <span style="border: 1px solid red; padding: 2px;">Save</span> </div>

GUI de pfSense - HAProxy Add Frontend

Seleccione el botón Agregar.

Settings **Frontend** Backend Files Stats Stats FS Templates

### Edit HAProxy Frontend

**Name**

**Description**

**Status**

**External address** Define what ip:port combinations to listen on for incoming connections.

Table						
	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/>	14.10.162.252 (ece-VIP)	<input type="text"/>	443	<input checked="" type="checkbox"/>	<input type="text"/>	

**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**

This defines the processing type of HAProxy, and will determine the available 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 - Encabezado de Frontend

Proporcione un nombre para el front end.

Proporcione una descripción para ayudar a identificar el front-end más adelante.

En la tabla Dirección externa:

1. Dirección de recepción: seleccione el VIP que ha creado para este sitio web.
2. Puerto: Introduzca 443.
3. SSL Offloading (Descarga de SSL): seleccione esta opción para que se pueda insertar una cookie de sesión.

Deje vacío el número máximo de conexiones.

Asegúrese de que el Tipo está seleccionado como http / https(offloading).

**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	CS	Not	Value	Actions
Backend1acl	Host matches			www.yourdomain.tld	
addHeaderAc	SSL Client certificate valid				

acl's with the same name will be 'combined' using OR criteria.  
 For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

**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	addHeaderAc

**Default Backend**

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 backend: selección predeterminada de backend

La configuración más sencilla consiste en elegir un motor predeterminado del menú desplegable. Esto se puede seleccionar cuando el VIP aloja un solo sitio web.

### 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	
<input type="checkbox"/>		ccmpWS	Host starts with:	no	no	ccmp.uclabservices.com:8085	
<input type="checkbox"/>		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	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

 acl's with the same name will be 'combined' using OR criteria.  
 For more information about ACLs 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	
<input type="checkbox"/>		Use Backend	See below	ccmpSSL	
		backend: be-uclab-ccmp120-ssl			
<input type="checkbox"/>		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	addHeaderAc

**Default Backend**

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

Motor HAProxy: ACL avanzada

Como se muestra en la imagen, las ACL se pueden utilizar para redirigir un único frontend a varios backends en función de las condiciones.

Puede ver que la ACL verifica si el host en la solicitud comienza con un nombre y un número de puerto. o simplemente el nombre. En función de esto, se utiliza un motor específico.

Esto no es común con la ECE.

**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 encryption 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**   
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 haproxy's 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
<input type="checkbox"/> Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)	
<input type="checkbox"/> 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-ssl3, force-tls10 force-tls11 force-tls12 no-ssl3 no-tls10 no-tls11 no-tls12 no-tls-tickets  
Example: no-ssl3 ciphers ECDH+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, ecldhe, curves, ciphers, ssl-min-ver and ssl-max-ver  
Example: alpn h2,http/1.1 ciphers ECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecldhe secp256k1

HAProxy Frontend - Enlace de certificado

En la sección Descarga de SSL, seleccione el certificado creado para su uso con este sitio. Este certificado debe ser un certificado de servidor.

Seleccione la opción Add ACL for certificate Subject Alternative Names.

Puede dejar las opciones restantes en sus valores predeterminados.

Seleccione Guardar al final de este formulario.

Services / HAProxy / Frontend

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

Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

Frontends									
Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	fe-ece	Frontend for ECE	14.10.162.252:443	https	be-ece (default)	

Add Delete Save

HAProxy - Aplicar configuración

Seleccione, Aplicar cambios para aplicar los cambios de Frontend y Backend a la configuración en ejecución.

Enhorabuena, ha completado la instalación y la configuración de pfSense.



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).