

PfSense Community-taakverdeling voor ECE configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Installeer PFSense](#)

[Overzicht van oplossing](#)

[Vorbereiding](#)

[Installatie](#)

[Netwerkinstelling](#)

[Eerste configuratie voltooien](#)

[Basisbeheerinstellingen configureren](#)

[Vereiste pakketten toevoegen](#)

[Certificaten configureren](#)

[Virtuele IP's toevoegen](#)

[Firewall configureren](#)

[HAProxy configureren](#)

[HAProxy-concepten](#)

[Eerste HAProxy-instellingen](#)

[HAProxy-backkend configureren](#)

[HAProxy-frontend configureren](#)

Inleiding

Dit document beschrijft de stappen om pfSense Community Edition te configureren en in te stellen als een taakverdeling voor Enterprise Chat en Email (ECE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ECE 12.x
- PFSense Community Edition

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- ECE 12.6(1)
- PFSense Community Edition 2.7.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Installeer PFSense

Overzicht van oplossing

pfSense Community Edition is een multifunctioneel product dat een firewall, taakverdeling, security scanner en veel andere services in één server biedt. pfSense is gebaseerd op gratis BSD en heeft minimale hardwarevereisten. De taakverdeling is een implementatie van HAProxy en er is een eenvoudig te gebruiken GUI om het product te configureren.

U kunt deze taakverdeling gebruiken met zowel ECE als Contact Center Management Portal (CCMP). Dit document bevat de stappen voor het configureren van pfSense voor ECE.

Vorbereiding

Stap 1. Download de PFSense-software

Gebruik de [pfSense website](#) om het installatiebestand van de iso te downloaden.

Stap 2. VM configureren

Een VM configureren met de minimumvereisten:

- 64-bits amd64 (x86-64) compatibele CPU
- 1 GB of meer RAM
- 8 GB of groter schijfstation (SSD, HDD, enz.)
- Een of meer compatibele netwerkinterfacekaarten
- Opstartbaar USB-station of optisch station met hoge capaciteit (DVD of BD) voor eerste installatie

Voor installatie in een lab is slechts één netwerkinterface (NIC) vereist. Er zijn verschillende manieren om het apparaat uit te voeren, maar het eenvoudigst is een enkele NIC, ook wel one-arm mode genoemd. In één-arm modus is er één interface die communiceert met het netwerk. Hoewel dit een makkelijke manier is en geschikt voor een lab, is het niet de meest veilige manier.

Een veiligere manier om het apparaat te configureren is door ten minste twee NIC's te hebben. Eén NIC is de WAN-interface en communiceert rechtstreeks met het openbare internet. De tweede NIC is de LAN-interface en communiceert met het interne bedrijfsnetwerk. U kunt ook extra interfaces toevoegen om te communiceren met verschillende delen van het netwerk die verschillende beveiligings- en firewallregels hebben. U kunt bijvoorbeeld een NIC verbinden met het openbare internet, een verbinding maken met het DMZ-netwerk waar alle extern toegankelijke webserverns zijn, en een derde NIC verbinding maken met het bedrijfsnetwerk. Hierdoor hebt u interne en externe gebruikers veilig toegang tot dezelfde set webserverns die in een DMZ worden bewaard. Zorg ervoor dat u de veiligheidsimplicaties van elk ontwerp begrijpt voordat het wordt geïmplementeerd. Raadpleeg een security engineer om er zeker van te zijn dat de best practices voor uw specifieke implementatie worden gevolgd.

Installatie


Stap 1. De ISO op de VM monteren

Stap 2. Schakel de VM in en volg de aanwijzingen voor installatie.

Raadpleeg dit [document](#) voor stapsgewijze instructies.

Netwerkinstelling

U moet IP-adressen aan het apparaat toewijzen om door te gaan met de configuratie.

 **Opmerking:** in dit document wordt een apparaat weergegeven dat in de modus met één arm is geconfigureerd.

Stap 1. VLAN's configureren

Als u VLAN-ondersteuning nodig hebt, beantwoord dan de eerste vraag. Zo niet, antwoord nr.

Stap 2. WAN-interface toewijzen

De WAN-interface is de niet-beveiligde kant van het apparaat in de modus met twee armen en de enige interface in de modus met één arm. Voer de interfacenaam in wanneer dit wordt gevraagd.

Stap 3. Wijs de LAN interface toe

De LAN-interface is de beveiligde kant van het apparaat in de modus met twee armen. Indien nodig voert u de interfacenaam in wanneer dit wordt gevraagd.

Stap 4. Andere interfaces toewijzen

Configureer eventuele andere interfaces die u nodig hebt voor uw specifieke installatie. Deze zijn optioneel en niet alledaags.

Stap 5. IP-adres aan een beheerinterface toewijzen

Als uw netwerk DHCP ondersteunt, wordt het toegewezen IP-adres weergegeven in het consolescherm.

```
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-console

Als er geen adres is toegewezen of als u een specifiek adres wilt toewijzen, voert u deze stappen uit.

1. Kies optie 2 in het consolemenu.
2. Antwoord op: DHCP uitschakelen.
3. Voer het IPv4-adres voor de WAN-interface in.
4. Geef het netmasker op voor de bittellingen. (24 = 255,255,255,0, 16 = 255,255,0,0, 8 = 255,0,0,0)
5. Voer het gatewayadres voor de WAN-interface in.
6. Als u wilt dat deze gateway de standaardgateway voor het apparaat wordt, antwoordt u op de gatewayprompt, anders antwoordt u op.
7. Configureer de NIC voor IPv6 indien gewenst.
8. DHCP-server op de interface uitschakelen.
9. Antwoord door HTTP in te schakelen op het webConfigurator-protocol. Dit wordt gebruikt in de volgende stappen.

U ontvangt vervolgens een bevestiging dat de instellingen zijn bijgewerkt.

```
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/

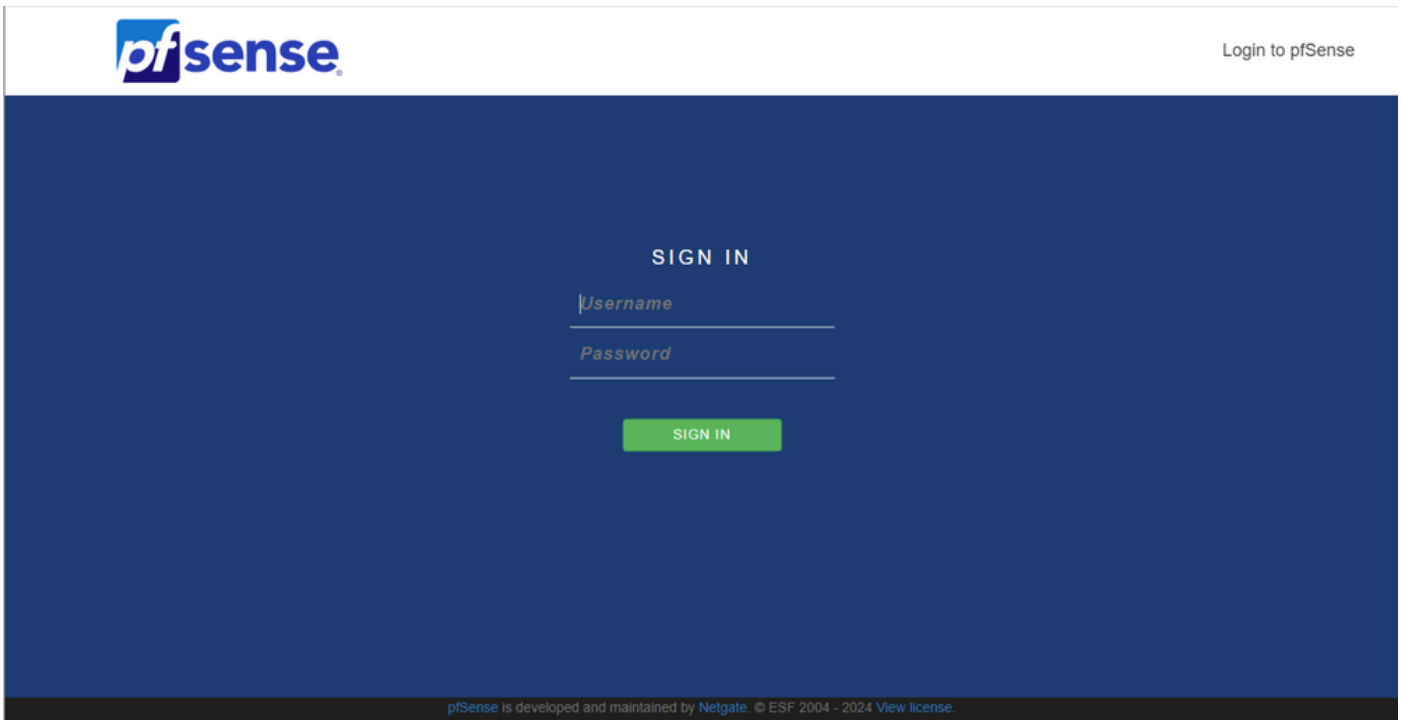
Press <ENTER> to continue. █
```

PFsense-bevestiging

Eerste configuratie voltooien

Stap 1. Open een webbrowser en navigeer naar: http://<ip_address_of_application>

 Opmerking: u moet eerst HTTP en niet HTTPS gebruiken.

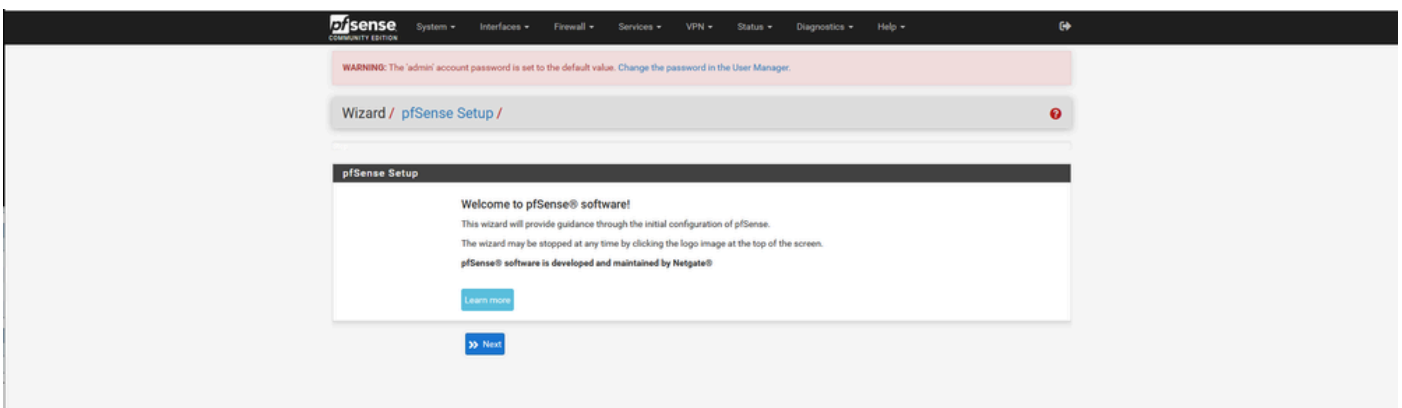


Aanmelden bij PFSense Admin

Stap 2. Login met de standaardlogin van admin / pfSense

Stap 3. De eerste configuratie voltooien

Klik op volgende door de eerste twee schermen.



Wizard PFSense instellen - 1

Geef de hostnaam, domeinnaam en DNS-serverinformatie op.

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

Wizard PFSense instellen - 2

Valideer de IP-adresinformatie. Als u aanvankelijk DHCP koos, kunt u dit nu veranderen.
Geef de NTP-tijdserver hostnaam en selecteer de juiste tijdzone in de vervolgkeuzelijst.

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

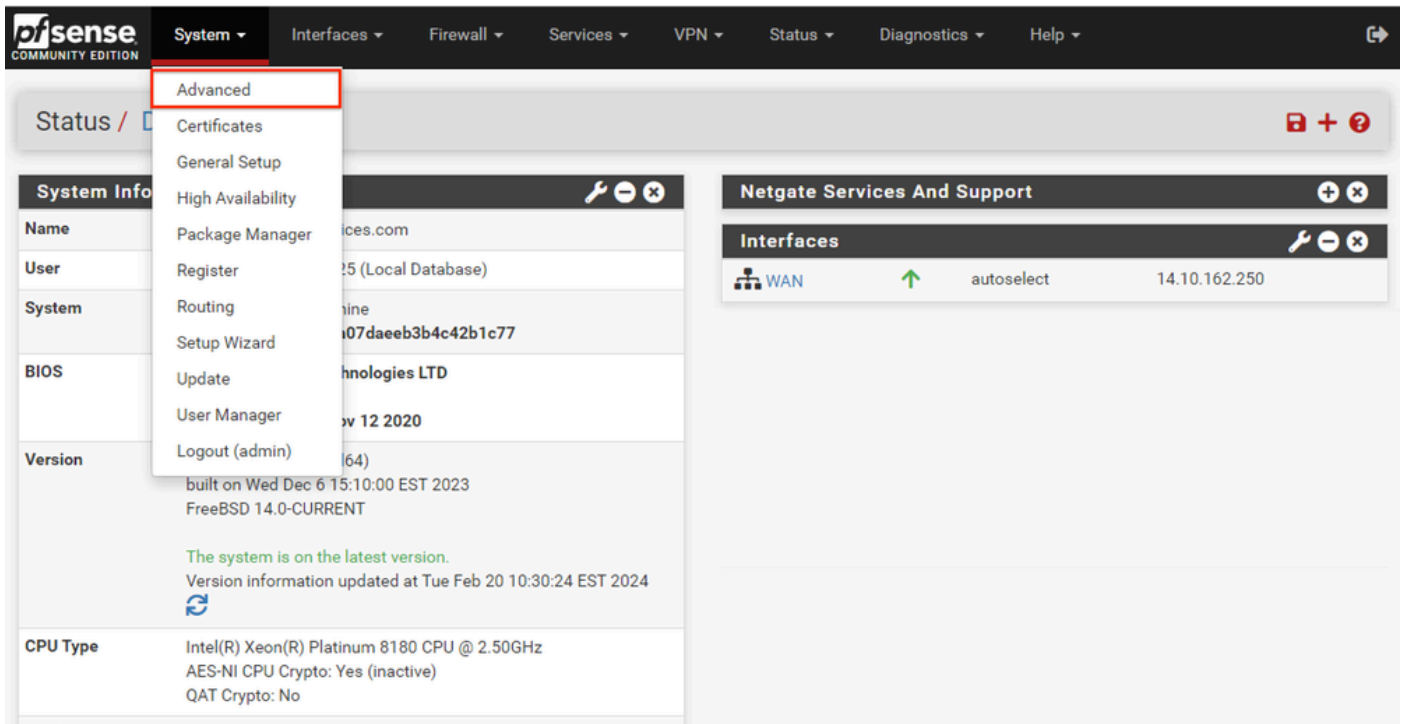
Wizard PFSense instellen - 3

Ga door met de installatiewizard tot het einde. De interface GUI wordt opnieuw opgestart en u wordt doorgestuurd naar de nieuwe URL zodra deze is voltooid.

Basisbeheerinstellingen configureren

Stap 1. Aanmelden bij de beheerinterface

Stap 2. Selecteer Geavanceerd in het vervolgkeuzemenu System




PfSense GUI - Admin Dropdown

Stap 3. WebConfigurator-instellingen bijwerken

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	<input type="text" value="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	<input type="text" value="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	<input type="text" value="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 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.</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 Wikipedia.</p>

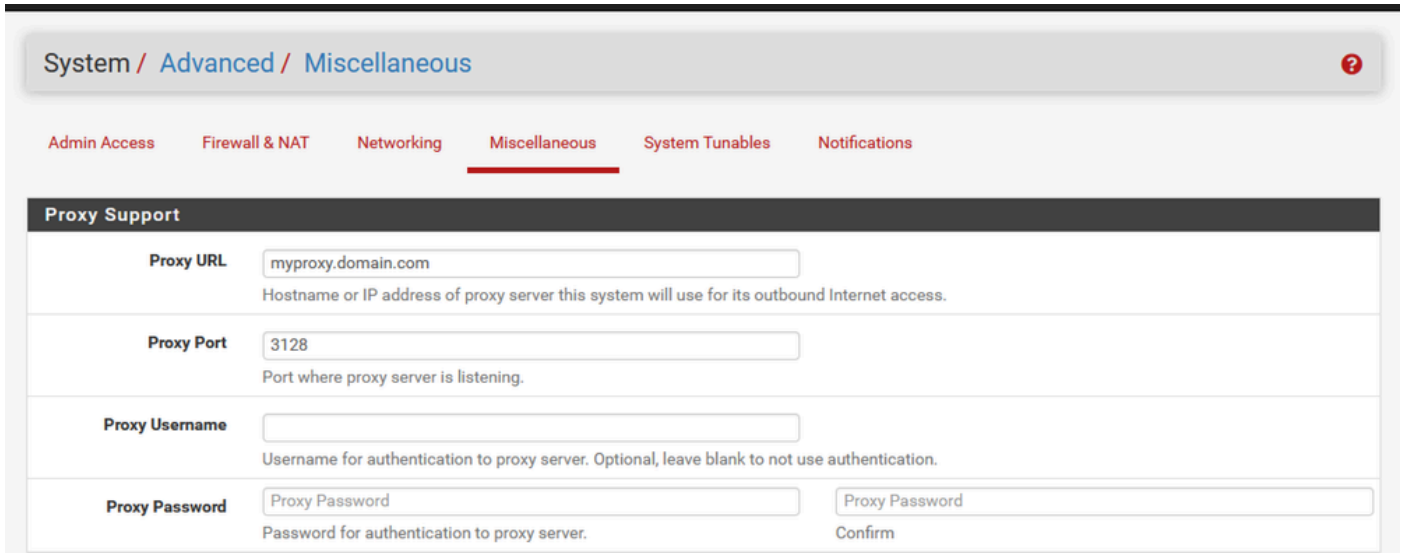
PFSense GUI - Admin-configuratie

1. Selecteer het HTTPS-protocol (SSL/TLS).
2. Laat het SSL/TLS-certificaat op dit moment over aan het zelfondertekende certificaat.
3. Verander de TCP-poort in een andere poort dan 443 om de interface beter te beveiligen en problemen met poortoverlap te voorkomen.
4. Selecteer de optie WebGUI redirect om de beheerinterface op poort 80 uit te schakelen.
5. Selecteer de Browser HTTP_REFERER handhavingsoptie.
6. Schakel Secure Shell in door de optie Secure Shell inschakelen te selecteren.

 **Opmerking:** Zorg ervoor dat u de knop Opslaan selecteert voordat u doorgaat. Je wordt dan doorgestuurd naar de nieuwe https link.

Stap 4. Proxyserver configureren, indien nodig

Indien nodig kunt u de proxy-informatie op het tabblad Diversen configureren. Om de installatie en configuratie te voltooien, moet het apparaat toegang tot internet hebben.



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

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

Proxy Support

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


PFsense GUI - Proxy-configuratie

 **Opmerking:** Zorg ervoor dat u de knop Opslaan selecteert nadat u de wijzigingen hebt aangebracht.

Vereiste pakketten toevoegen

Stap 1. Selecteer Systeem > Packet Manager

Stap 2. Beschikbare pakketten selecteren

 **Opmerking:** het kan een paar minuten duren om alle beschikbare pakketten te laden. Als dit keer uit, verifieer dat de DNS servers correct worden gevormd. Vaak verhelpt een herstart van het apparaat de internetverbinding.

System / Package Manager / Available Packages ?

Installed Packages Available Packages

Search

Search term Both

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.	<input type="button" value="+ Install"/>
Package Dependencies: pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11			
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	<input type="button" value="+ Install"/>
Package Dependencies: apcupsd-3.14.14_4			
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers.	<input type="button" value="+ Install"/>
Package Dependencies: arping-2.21_1			
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.	<input type="button" value="+ Install"/>

PFSense GUI - pakketlijst

Stap 3. Vereiste pakketten zoeken en installeren

1. proxy
2. Open-VM-tools

 **Opmerking:** selecteer het haproxy-devel pakket niet.

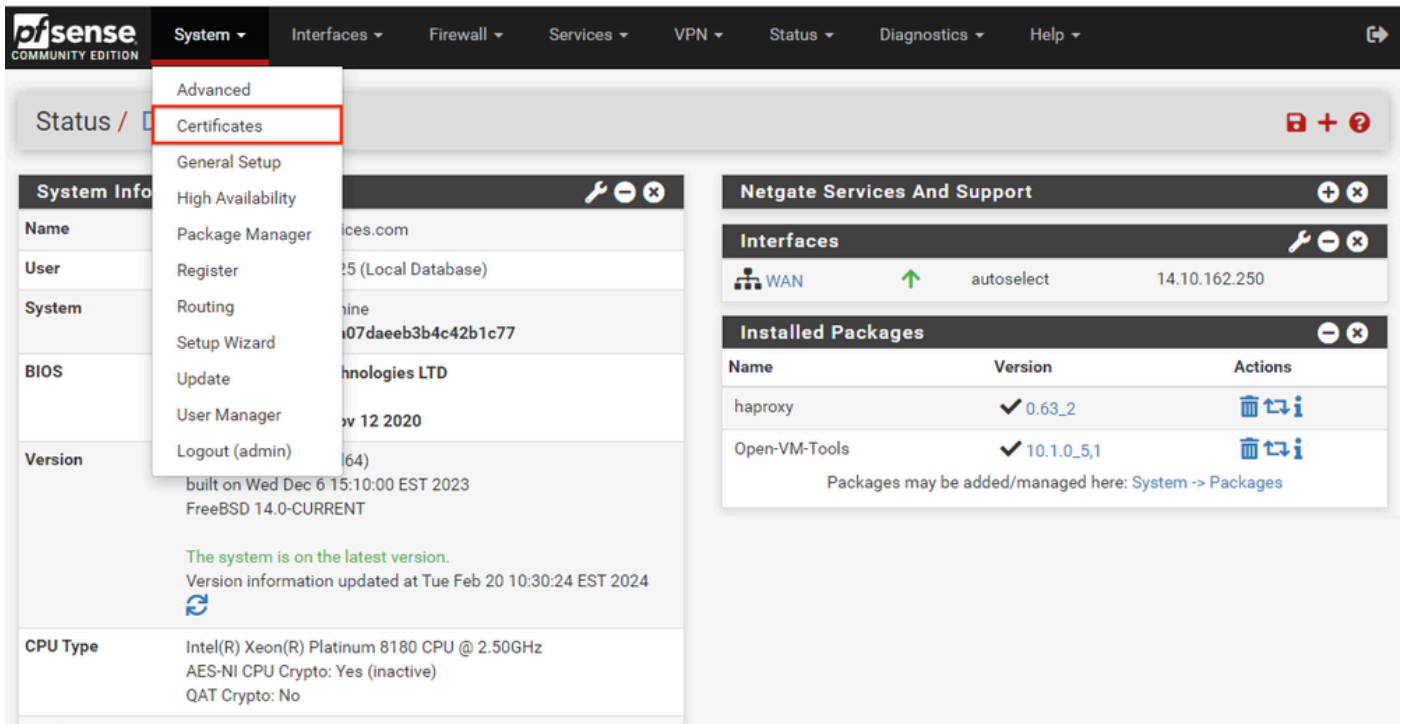
Certificaten configureren

pfSense kan zelfondertekend certificaat maken of het kan integreren met een openbare CA, een interne CA, of kan optreden als een CA en CA-ondertekende certificaten uitgeven. Deze handleiding bevat de stappen die u kunt integreren met een interne CA.

Zorg ervoor dat deze items beschikbaar zijn voordat u met deze sectie begint.

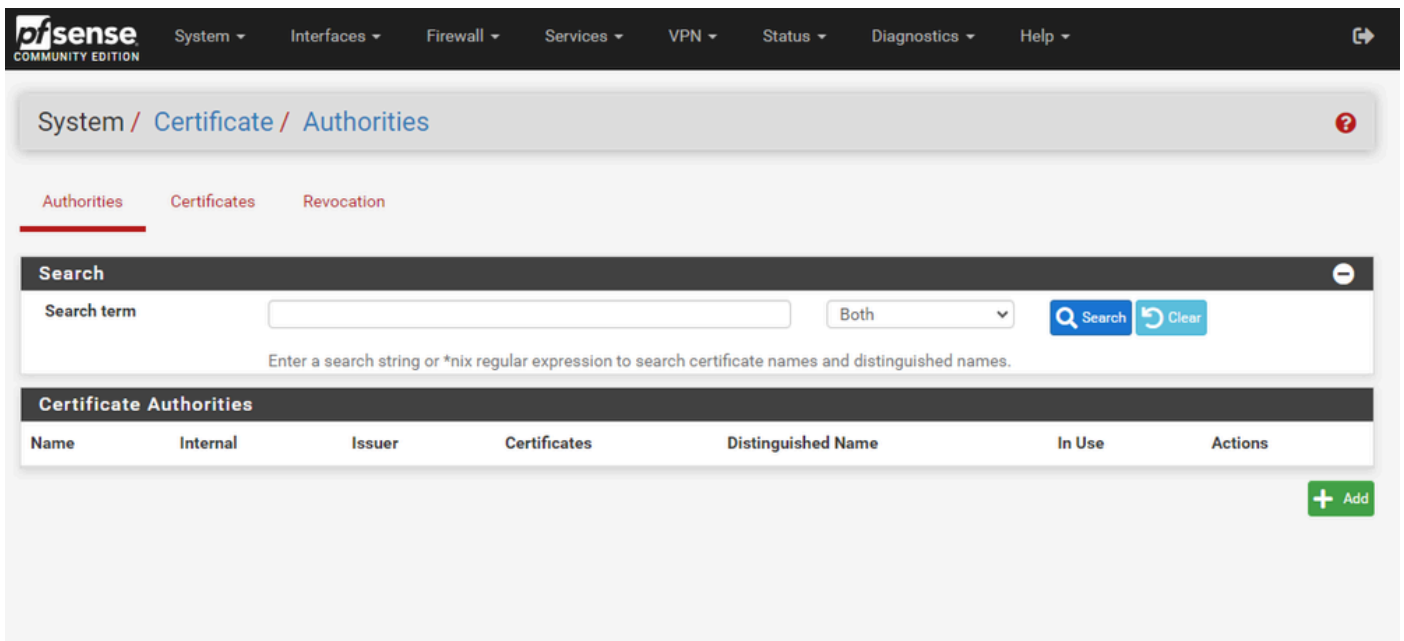
1. basiscertificaat voor CA opgeslagen als PEM- of Base-64-gecodeerd formaat.
2. Alle intermediaire (soms afgeven) certificaten voor CA die zijn opgeslagen als een PEM- of Base-64-gecodeerd formaat

Stap 1. Selecteer Certificaten in het vervolgkeuzemenu System



PfSense GUI - vervolgkeuzelijst Certificaten

Stap 2. Het CA Root Certificate importeren



SfSense GUI - CA-certificaatlijst

Selecteer de knop Toevoegen.

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.

Pfsense GUI - CA-import

Zoals in het beeld:

1. Verstrek een unieke, beschrijvende naam
2. Selecteer Importeren van een bestaande certificeringsinstantie in de vervolgkeuzelijst Methode.
3. Controleer of de selectievakjes Trust Store en Randomize Serial zijn geselecteerd.
4. Plakt het gehele certificaat in het tekstvak Certificaatgegevens. Zorg ervoor dat u van de -----BEGIN CERTIFICAAT----- en -----END CERTIFICAAT----- lijnen omvat.
5. Selecteer Opslaan.
6. Controleer dat het certificaat wordt geïmporteerd zoals in de afbeelding.

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 i Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500		✎ ⚙️ 🗑️

➕ Add

RFSense GUI - CA-lijst

Stap 3. Het CA-tussencertificaat importeren

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.

SFSense GUI - CA tussenproducten importeren

Herhaal de stappen om het basis CA certificaat te importeren om het tussenliggende CA certificaat te importeren.

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="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>
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="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>

RFSense GUI - CA-links

Controleer de certificeringsinstanties om te controleren of het tussenproduct correct is gekoppeld aan het basiscertificaat zoals wordt aangegeven in de afbeelding.

Stap 4. Maak en exporteer een CSR voor de website met taakverdeling

Dit beschrijft de stappen om een MVO te creëren, MVO uit te voeren, dan het ondertekende certificaat in te voeren. Als u al een bestaand certificaat in een PFX-indeling hebt, kunt u dit certificaat importeren. Raadpleeg de documentatie bij pfSense voor deze stappen.

1. Selecteer het menu Certificaten en selecteer vervolgens de knop Toevoegen/ondertekenen.

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 (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 type="button" value="i"/> webConfigurator	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="key"/> <input type="button" value="refresh"/>

2. Vul het aanvraagformulier voor de ondertekening van het certificaat in.

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

- Methode: Selecteer Aanvraag voor certificaatondertekening maken in de vervolgkeuzelijst
- Beschrijvende naam: geef een naam voor het certificaat
- Key type en Digest Algoritme: Controleer of ze overeenkomen met uw vereisten
- Veelvoorkomende naam: Geef de volledig gekwalificeerde domeinnaam website
- Geef de resterende certificaatinformatie zoals vereist voor uw omgeving

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


PFSense GUI - CSR geavanceerde security

- Certificaatype: Selecteer Servercertificaat in de vervolgkeuzelijst.
- Alternatieve namen: Geef elk onderwerp alternatieve namen (SAN) die nodig zijn voor uw implementatie.









 **Opmerking:** de algemene naam wordt automatisch toegevoegd aan het SAN-veld. U hoeft alleen extra namen toe te voegen.

Selecteer Opslaan als alle velden juist zijn.

3. Exporteer de MVO naar een bestand.



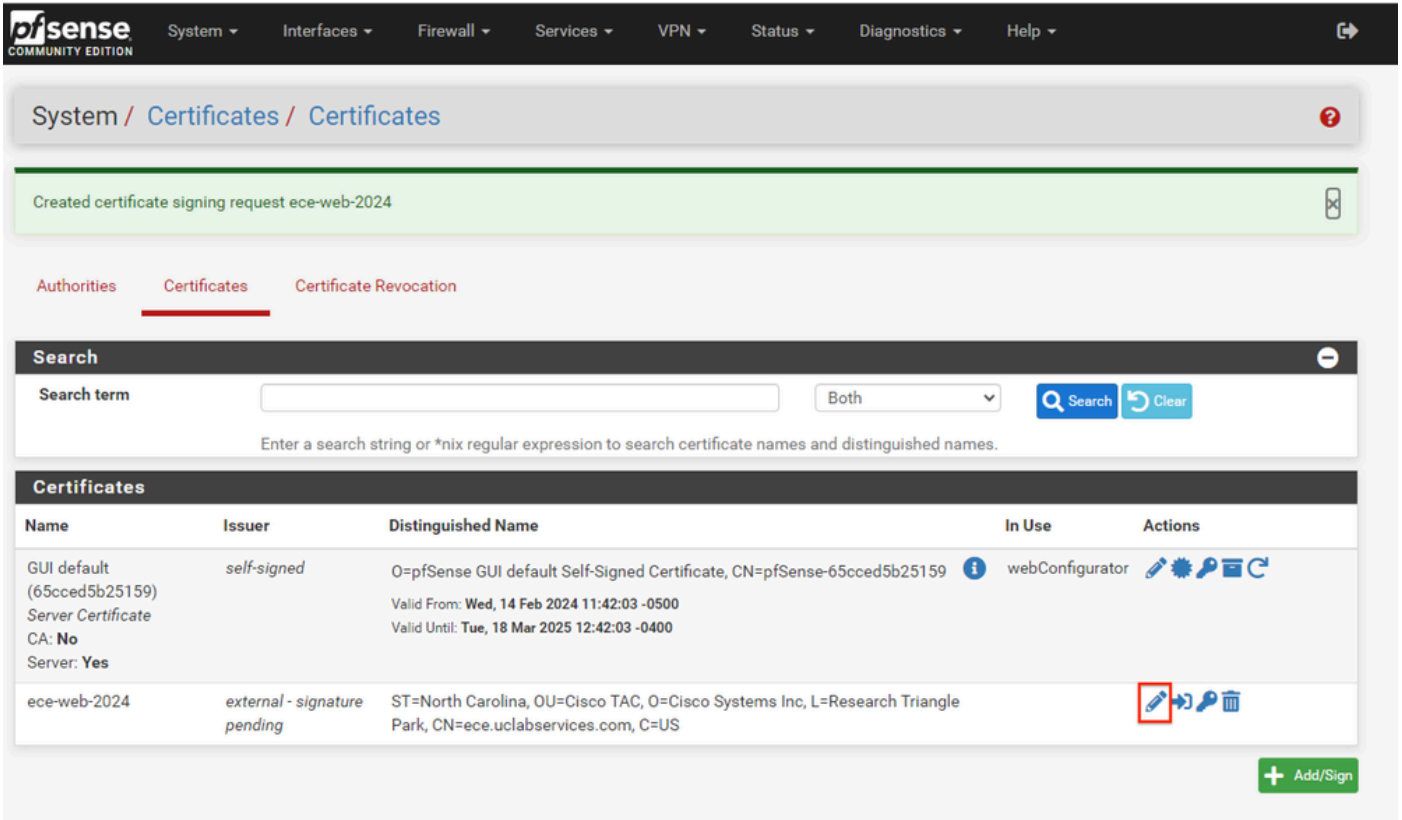
The screenshot shows the pfSense GUI interface for managing certificates. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area shows the breadcrumb 'System / Certificates / Certificates' and a notification 'Created certificate signing request ece-web-2024'. Below this, there are tabs for Authorities, Certificates (which is selected), and Certificate Revocation. A search bar is present with a search term field, a dropdown menu set to 'Both', and buttons for 'Search' and 'Clear'. The main section displays a table of 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		   









At the bottom right of the table, there is a green button labeled '+ Add/Sign'.

Selecteer de knop Exporteren om de CSR op te slaan en onderteken dit vervolgens met uw CA. Zodra u het ondertekende certificaat hebt, slaat u dit op als een PEM- of Base-64-bestand om het proces te voltooien.

4. Voer het ondertekende certificaat in.



The screenshot shows the pfSense GUI interface for managing certificates. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation, a breadcrumb trail reads 'System / Certificates / Certificates'. A green notification bar at the top states 'Created certificate signing request ece-web-2024'. The main content area has three tabs: 'Authorities', 'Certificates' (which is selected), and 'Certificate Revocation'. Below the tabs is a search bar with a 'Search term' input field, a dropdown menu set to 'Both', and 'Search' and 'Clear' buttons. A note below the search bar says 'Enter a search string or *nix regular expression to search certificate names and distinguished names.' The main section is titled 'Certificates' and contains a table with the following data:

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		   

At the bottom right of the table, there is a green '+ Add/Sign' button.

Selecteer het pictogram Potlood om het ondertekende certificaat te importeren.

5. Plakt de certificaatgegevens in het formulier.

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-----
MIIDvDCCAqCAQAwgZcxHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
MAkGA1UEBHMCMVVMxZzAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMRowGAYDVQQKEwFDaXNjbyBTeXN0ZW1zIEIu
YzESMBAGA1UECzMjQ2LzY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

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

Final certificate data

```
GBSAPwQkwas305JkKISY/pYEI2EW/7EZcDmHRURnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yiZ3IT4TJwDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5Mnuqx1PN97EPQngO/1IgxO4xDz6Dg+Iwt9pyrRZdxpmy
-----END CERTIFICATE-----
```

 Paste the certificate received from the certificate authority here.

SFSense GUI - Certificaat importeren

Selecteer Bijwerken om het certificaat op te slaan.

6. Bekijk de certificaatgegevens om te controleren of deze correct zijn.

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 (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		

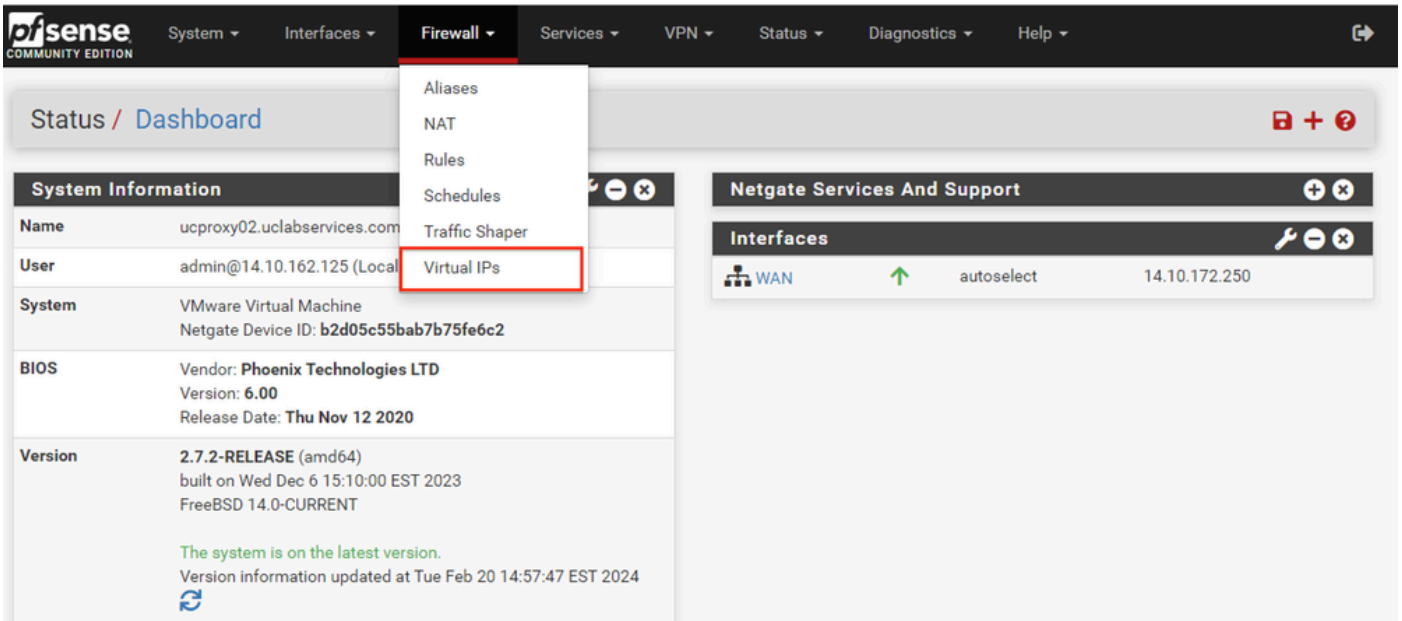
PfSense GUI - certificaatlijst

7. Herhaal dit proces als u meerdere sites op deze pcSense wilt hosten.

Virtuele IP's toevoegen

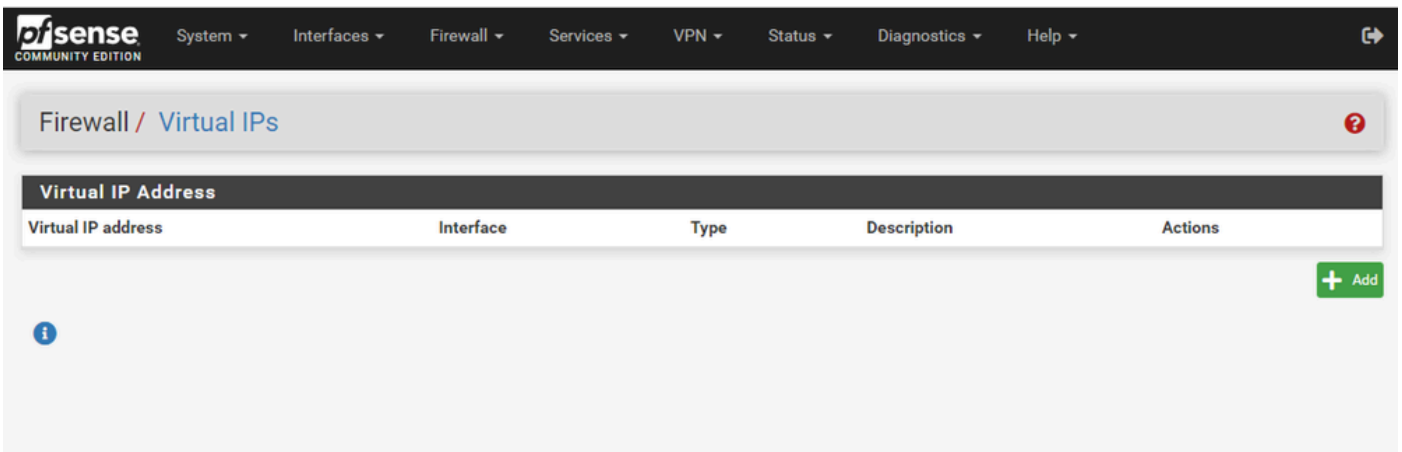
Minstens één IP is vereist om websites op de pfSense te hosten. In pfSense gebeurt dit met virtuele IP's (VIP's).

Stap 1. Selecteer virtuele IP's in de vervolgkeuzelijst Firewall



PfSense GUI - VIP-drop-down

Stap 2. Selecteer de knop Toevoegen



PfSense GUI - VIP-landingspagina

Stap 3. Adresinformatie opgeven

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

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).

i

PFSense GUI - VIP-configuratie

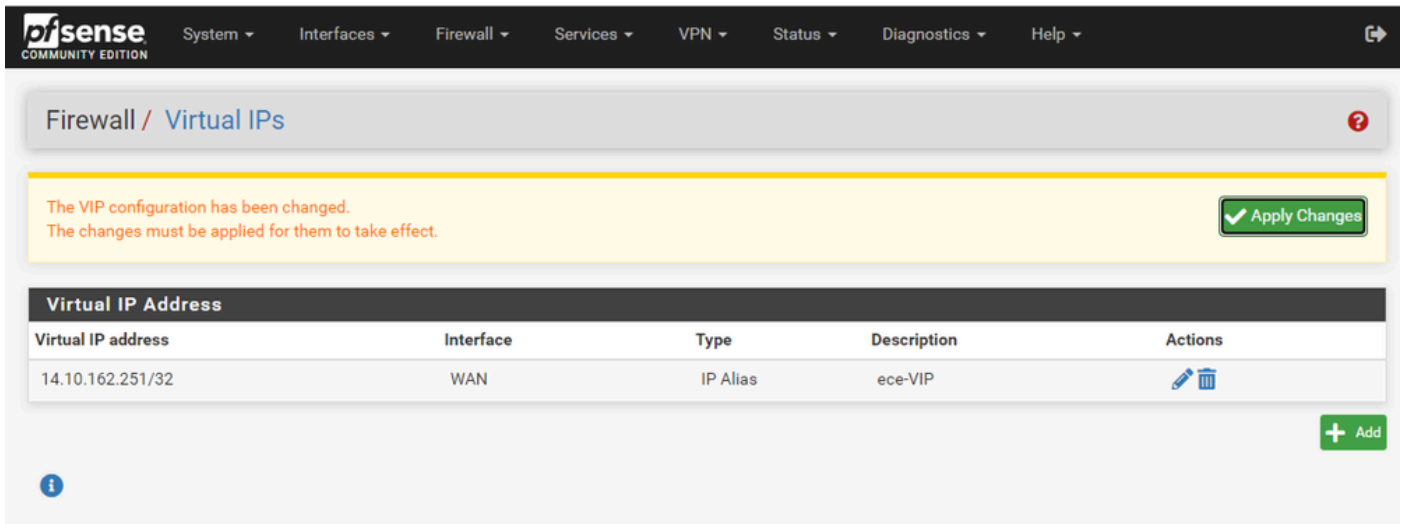
Gebruik de informatie om een VIP toe te voegen.

- Type: IP-alias selecteren
- Interface: Selecteer de interface voor dit IP-adres dat moet worden uitgezonden
- Adres(sen): IP-adres invoeren
- Adresmasker: voor IP-adressen die worden gebruikt voor taakverdeling, moet het masker een /32 zijn
- Beschrijving: Geef een korte tekst om de configuratie later beter te begrijpen

Selecteer Opslaan om de wijziging toe te voegen.

Herhaal dit voor elk IP-adres dat vereist is voor de configuratie.

Stap 4. Configuratie toepassen



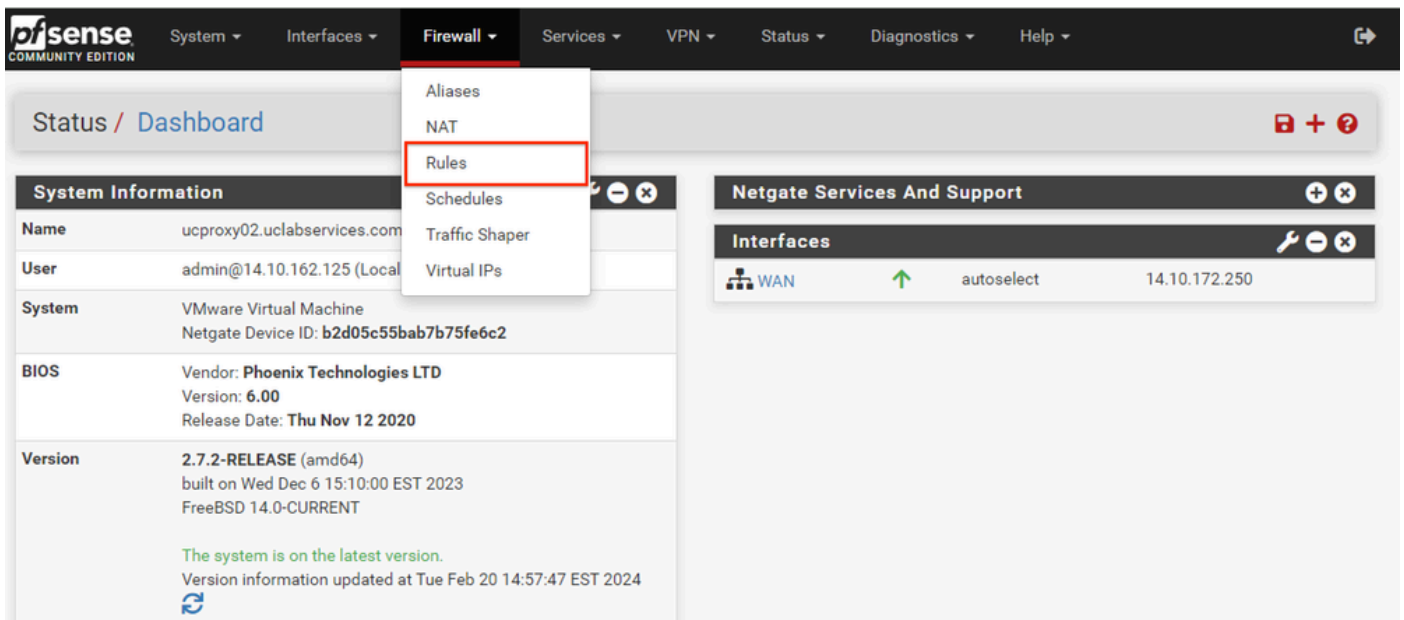
PfSense GUI - VIP-lijst

Selecteer de knop Wijzigingen toepassen nadat alle VIP's zijn toegevoegd.

Firewall configureren

pfSense heeft een ingebouwde firewall. De standaardregel-set is zeer beperkt. Zorg ervoor dat u een uitgebreid firewallbeleid opstelt voordat het apparaat in productie wordt genomen.

Stap 1. Selecteer Regels in de vervolgkeuzelijst Firewall



PfSense GUI - vervolgkeuzelijst met firewallregels

Stap 2. Selecteer een van de knoppen Toevoegen

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

Firewall / Rules / WAN 📊 📄 ?

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"/>	0/13.35 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"/>	0/3.63 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.

⬆️ Add
⬆️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
➕ Separator

ℹ️

RFSense GUI - lijst met firewallregels

Merk op dat de ene knop de nieuwe regel boven de geselecteerde regel toevoegt, terwijl de andere knop de regel onder de geselecteerde regel toevoegt. Beide knoppen kunnen voor de eerste regel worden gebruikt.

Stap 3. Firewallregel maken om verkeer toe te staan naar poort 443 voor het IP-adres

[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

Configuratie van PFSense GUI - Firewall Pass-regel

Gebruik de informatie om de regel te maken.

- Actie: kies Pass
- Interface: Kies de interface waarop de regel van toepassing is
- Adresfamilie en -protocol: kies de gewenste keuze
- Bron: Laat geselecteerd als Any
- Bestemming: Selecteer Adres of Alias uit de vervolgkeuzelijst Bestemming en voer vervolgens het IP-adres in waarop de regel van toepassing is
- Poortbereik bestemming: Selecteer HTTPS (443) in de vervolgkeuzelijst Van en Tot
- Log: Selecteer het aanvinkvakje om alle pakketten te registreren die aan deze regel voor accounting voldoen

- Beschrijving: Geef tekst om later naar de regel te verwijzen

Selecteer Opslaan.

Stap 4. Maak een firewallregel om al het andere verkeer naar de pfSense te laten vallen

Selecteer de knop Toevoegen om de regel onder de nieuwe regel in te voegen.

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 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](#)

SFSense GUI - configuratie van drop-regels voor firewall

- Actie: Blok selecteren

- Interface: Kies de interface waarop de regel van toepassing is
- Adresfamilie en -protocol: kies de gewenste keuze
- Bron: Laat geselecteerd als Any
- Bestemming: als zodanig geselecteerd
- Log: Selecteer het aanvinkvakje om alle pakketten te registreren die aan deze regel voor accounting voldoen
- Beschrijving: Geef tekst om later naar de regel te verwijzen

Selecteer Opslaan.

Stap 5. Herzie de regels en zorg ervoor dat de blokreel onderaan is

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

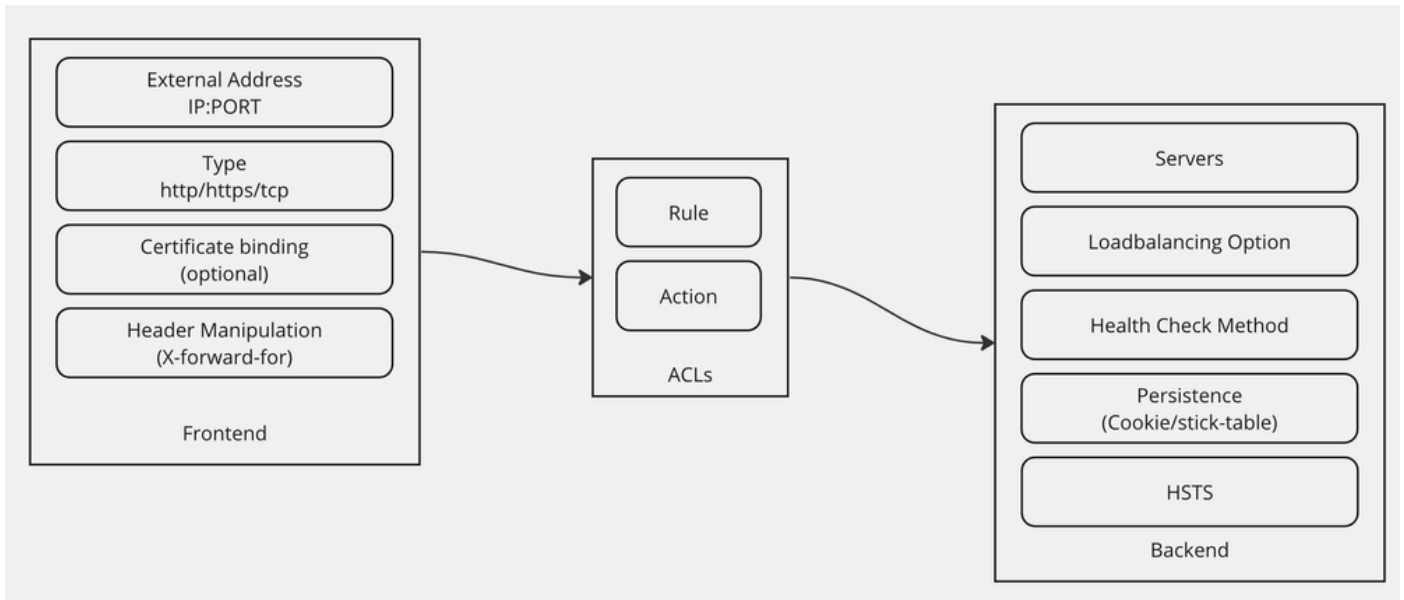
RFSense GUI - lijst met firewallregels

Indien nodig sleept u de regels om ze te sorteren.

Selecteer Wijzigingen toepassen als de firewallregels in de gewenste volgorde zijn geplaatst.

HAProxy configureren

HAProxy-concepten



HAProxy-concepten

HAProxy wordt geïmplementeerd met een Frontend/Backend-model.

Het Frontend definieert de kant van de proxy waarmee klanten communiceren.

Het Frontend bestaat uit een IP en poortcombinatie, certificaatbinding en kan enige headermanipulatie implementeren.

De Backend definieert de kant van de proxy die communiceert met de fysieke webserver.

De Backend definieert de eigenlijke servers en poorten, de loadbalancing methode voor initiële toewijzing, gezondheidscontroles en persistentie.

Een Frontend weet met welke backend te communiceren door of een toegewezen backend of door ACLs te gebruiken.

ACL's kunnen verschillende regels maken, zodat een gegeven frontend kan communiceren met verschillende backends, afhankelijk van verschillende dingen.

Eerste HAProxy-instellingen

Stap 1. Selecteer HAProxy in de vervolgkeuzelijst Services

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

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 14:00:00 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

- 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](#)

PfSense GUI - HAProxy-vervolgkeuzelijst

Stap 2. Basisinstellingen configureren

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.

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.

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.

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

PFsense GUI - HAProxy-hoofdinstellingen

Selecteer het aanvinkvakje Enable HAProxy.

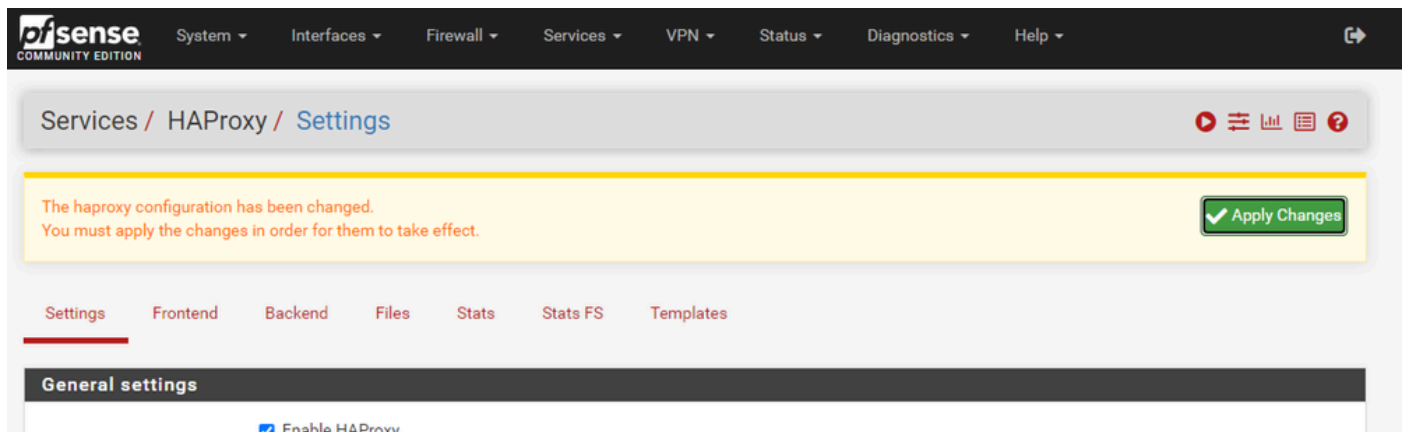
Voer een waarde in voor Maximum aantal verbindingen. Raadpleeg het diagram in deze sectie voor meer informatie over het benodigde geheugen.

Voer een waarde in voor de interne stats poort. Deze poort wordt gebruikt voor de weergave van HAProxy-statistieken van het apparaat, maar wordt niet buiten het apparaat weergegeven.

Voer een waarde in voor de verversingsfrequentie voor de interne status.

Bekijk de resterende configuratie en update zoals vereist voor uw omgeving.

Selecteer Opslaan.



Services / HAProxy / Settings

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

General settings

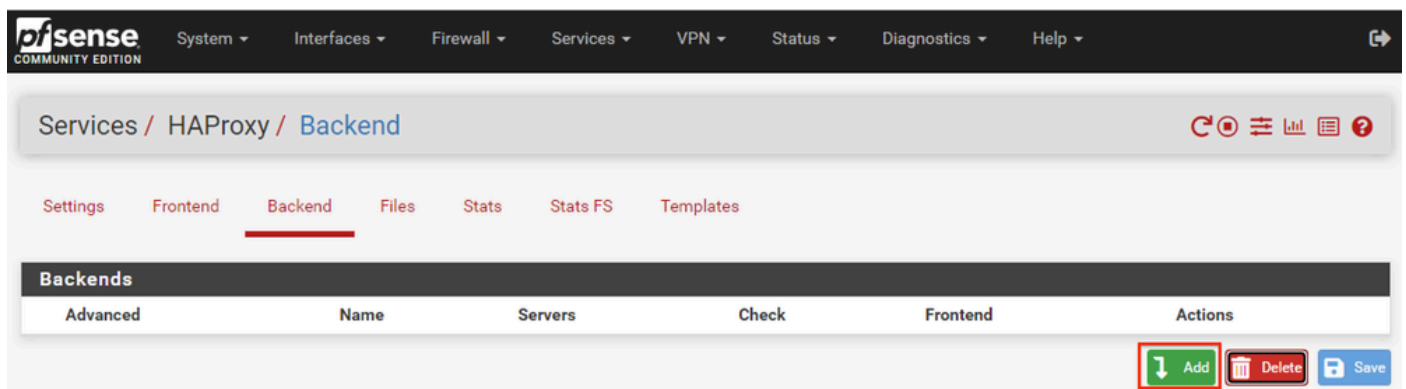
Enable HAProxy

pfSense GUI - HAProxy Wijzigingen toepassen

 **Opmerking:** de wijzigingen in de configuratie worden pas actief gemaakt als u de knop Wijzigingen toepassen selecteert. U kunt meerdere configuratiewijzigingen doorvoeren en ze allemaal tegelijk toepassen. De configuratie hoeft niet te worden toegepast om in een andere sectie te worden gebruikt.

HAProxy-backkend configureren




Begin met het backend. De reden hiervoor is dat de frontend een backend moet noemen. Zorg ervoor dat u het Backend menu hebt geselecteerd.



Services / HAProxy / Backend

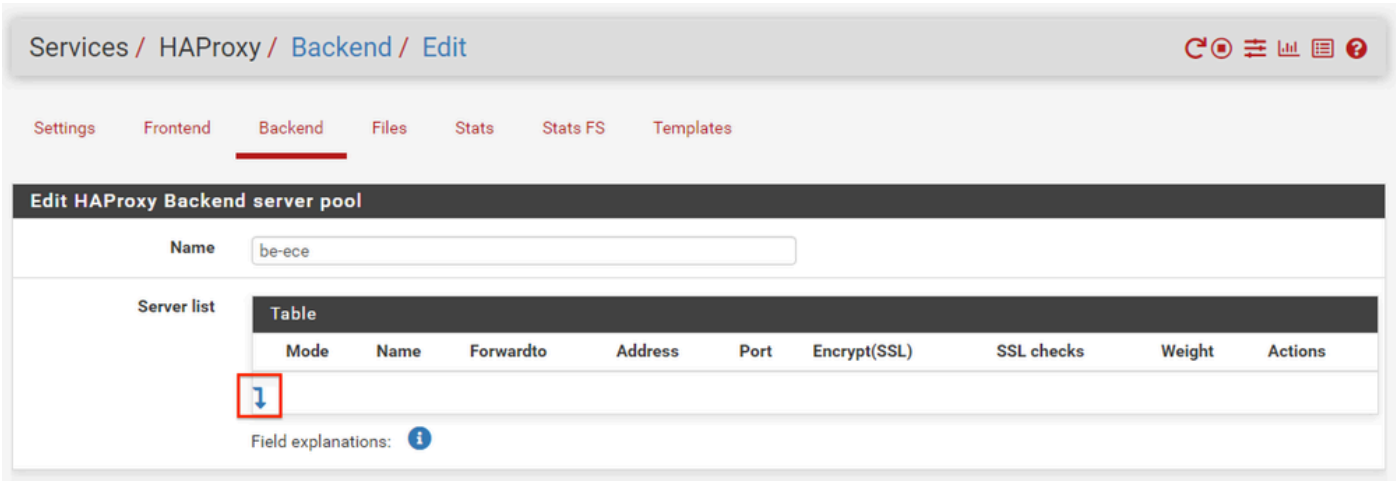
Settings Frontend Backend Files Stats Stats FS Templates

Backends

Advanced	Name	Servers	Check	Frontend	Actions
					  

pfSense GUI - HAProxy Toevoegen Backend

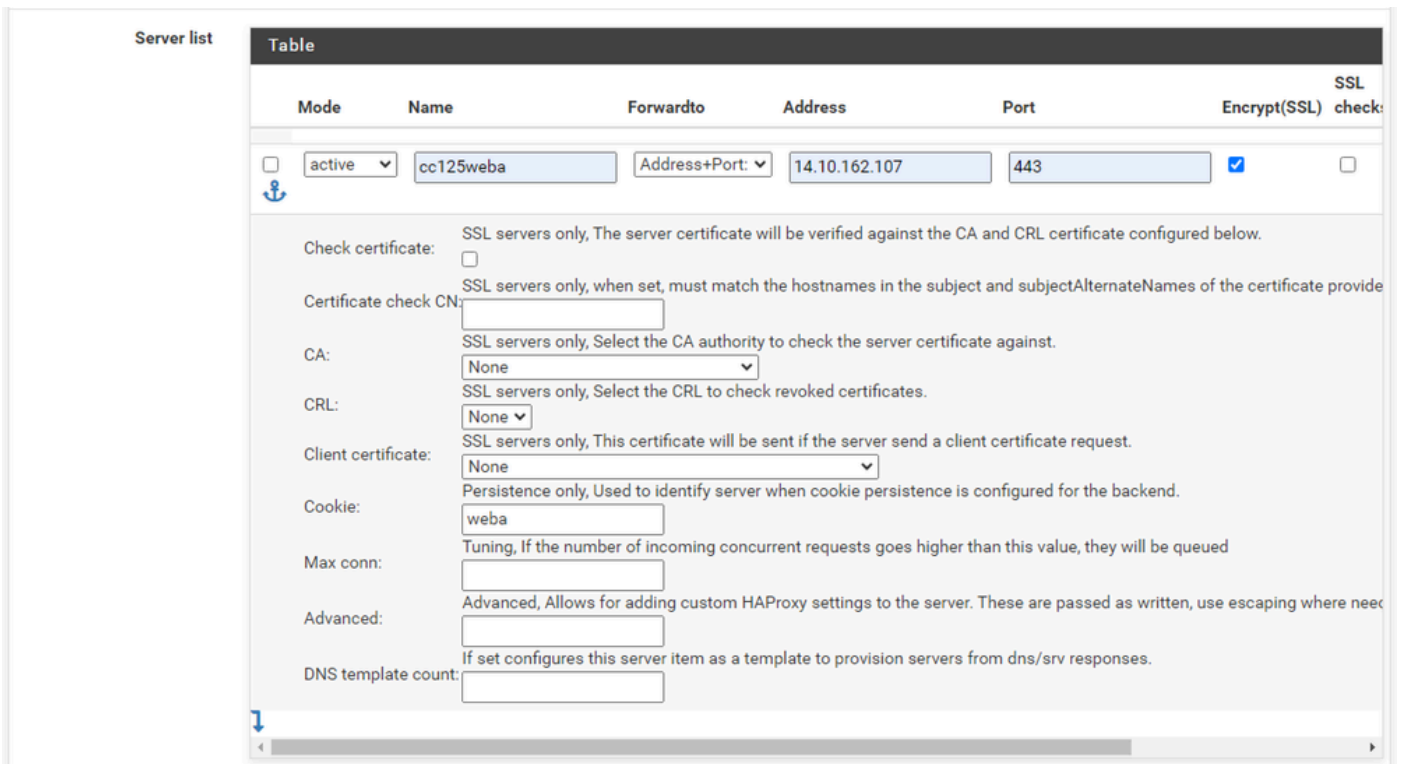
Selecteer de knop Toevoegen.



PfSense GUI - HAProxy backend start

Geef een naam voor het backend.

Selecteer de pijl-omlaag om de eerste server aan de lijst Server toe te voegen



Back-end - serverlijst

Geef een naam op die verwijst naar de server. Dit hoeft niet overeen te komen met de feitelijke servernaam. Dit is de naam die wordt weergegeven op de stats pagina.

Geef het adres van de server op. Dit kan worden geconfigureerd als een IP-adres voor FQDN.

Geef de poort op waarop u verbinding wilt maken. Dit moet haven 443 voor ECE zijn.

Selecteer het selectievakje Encrypt (SSL).

Verstrek een waarde in het veld Cookie. Dit is de inhoud van de sessie stickiness cookie en moet

uniek zijn in het backend.

Nadat de eerste server is geconfigureerd, selecteert u de pijl-omlaag om andere webserver in de omgeving te configureren.

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 Backend - Loadbalancing

Configureer de opties voor taakverdeling.

Voor ECE-servers moet dit worden ingesteld op Minst Connections.

Access control lists and actions	
Timeout / retry settings	
Connection timeout	60000 The time (in milliseconds) we give up if the connection does not complete within (default 30000).
Server timeout	60000 The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).
Retries	2 After a connection failure to a server, it is possible to retry, potentially on another server. This is useful if health-checks are too rare and you don't want the clients to see the failures. The number of attempts to reconnect is set by the "retries" parameter.
Health checking	
Health check method	HTTP <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>
Check frequency	<input type="text"/> milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	<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. 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 <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>
Url used by http check requests.	<input type="text" value="/system/web/view/platform/common/login/root.jsp?partitionId=1"/> Defaults to / if left blank.
Http check version	<input type="text" value="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: <code>HTTP/1.1\r\nHost:\ www</code> Also some hosts might require an accept parameter like this: <code>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</code>

HAProxy Backend - Health check

Toegangscontrolelijsten worden niet gebruikt in deze configuratie.

De instellingen voor time-out/opnieuw proberen kunnen bij hun standaardconfiguratie worden achtergelaten.

Configureer de sectie Gezondheidscontrole.

1. Health check methode: HTTP
2. Controleer frequentie: laat leeg om de standaardinstelling van elke 1 seconde te gebruiken.
3. Logcontroles: Selecteer deze optie om eventuele wijzigingen in de status van de logbestanden te schrijven.
4. HTTP-controlemethode: Selecteer GET in de lijst.
5. Url gebruikt door http check request.: Voor een ECE server enter, `/system/web/view/platform/common/login/root.jsp?partitielD=1`
6. HTTP-controleversie: Enter, `HTTP/1.1\r\n\Host:\ {fqdn_of_server}`

Zorg ervoor dat u een ruimte na de laatste backslash, maar vóór de FQDN van de server, opneemt.

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 - Cookie Persistence

Laat de Agent-controles uitgeschakeld.

Cookiepersistentie instellen:

1. Cookie Enabled: Selecteer deze optie om op cookies gebaseerde persistentie in te schakelen.
2. Cookienaam: Geef een naam voor de cookie.
3. Cookiemodus: Selecteer Invoegen in de vervolgkeuzelijst.
4. Laat de resterende opties los.

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](#)

HAProxy Backend - HSTS

De resterende secties van het backend configuratieformulier kunnen bij hun standaardinstellingen worden achtergelaten.

Als u HSTS wilt configureren, configureer dan een tijdelijke waarde in deze sectie. ECE voegt ook een HSTS-cookie in, zodat deze configuratie overbodig is.

Selecteer Opslaan.

HAProxy-frontend configureren

Verandering in het menu 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
									Add Delete Save

pfSense GUI - HAProxy - Frontend toevoegen

Selecteer de knop Toevoegen

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 - frontend header

Geef een naam op voor de voorzijde.

Geef een beschrijving om later de frontend te kunnen identificeren.

In de tabel Extern adres:

1. Luister adres: Selecteer de VIP die je voor deze website hebt gemaakt.
2. Poorten: Typ 443.
3. SSL Offloading: Selecteer deze optie zodat een sessiecookie kan worden ingevoegd.

Laat de Max aansluitingen leeg.

Zorg ervoor dat het type is geselecteerd als http / https (offload).

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

be-ecce

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 - Standaard backend selectie

De eenvoudigste configuratie is om een Default Backend te kiezen uit de vervolgkeuzelijst. Dit kan worden geselecteerd wanneer de VIP een enkele website host.

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 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	
<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".

HAProxy-back-end - geavanceerde ACL

Zoals in het beeld wordt getoond, kunnen ACL's worden gebruikt om één frontend om te leiden naar meerdere backends op basis van voorwaarden.

U kunt zien dat de ACL controleert om te zien of de host in het verzoek begint met een naam en poortnummer. of gewoon de naam. Op basis hiervan wordt een specifiek backend gebruikt.

Dit is niet gebruikelijk bij 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
↓	

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-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, ecde, 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 ecde secp256k1

HAProxy Frontend - Certificaatbinding

Selecteer in het gedeelte SSL Offload het certificaat dat voor gebruik met deze site is gemaakt. Dit certificaat moet een servercertificaat zijn.

Selecteer de optie ACL toevoegen voor alternatieve namen van onderwerpcertificaten.

U kunt de resterende opties bij hun standaardwaarden laten staan.

Selecteer Opslaan aan het einde van dit formulier.

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 - configuratie toepassen

Selecteer, pas Wijzigingen toe om de wijzigingen Frontend en Backend aan de lopende configuratie te verbinden.

Gefeliciteerd, u hebt de setup en configuratie van pfSense voltooid.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.