

Konfigurieren des pfSense Community Load Balancer für ECE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[pfSense installieren](#)

[Lösungsüberblick](#)

[Vorbereitung](#)

[Installation](#)

[Netzwerk-Setup](#)

[Ersteinrichtung abschließen](#)

[Grundlegende Admin-Einstellungen konfigurieren](#)

[Erforderliche Pakete hinzufügen](#)

[Zertifikate konfigurieren](#)

[Virtuelle IPs hinzufügen](#)

[Firewall konfigurieren](#)

[Konfigurieren von HAProxy](#)

[HAProxy-Konzepte](#)

[Anfängliche HAProxy-Einstellungen](#)

[Konfigurieren des HAProxy-Backends](#)

[Konfigurieren von HAProxy Frontend](#)

Einleitung

Dieses Dokument beschreibt die Schritte zur Einrichtung und Konfiguration von pfSense Community Edition als Load Balancer für Enterprise Chat und Email (ECE).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ECE 12.x
- pfSense Community Edition

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

pfSense installieren

Lösungsüberblick

pfSense Community Edition ist ein Multifunktionsprodukt, das eine Firewall, einen Load Balancer, einen Security Scanner und viele andere Dienste auf einem einzigen Server bietet. pfSense basiert auf Free BSD und hat minimale Hardwareanforderungen. Der Load Balancer ist eine Implementierung von HAProxy, und es wird eine einfach zu verwendende grafische Benutzeroberfläche für die Konfiguration des Produkts bereitgestellt.

Sie können diesen Load Balancer sowohl für die ECE als auch für das Contact Center Management Portal (CCMP) verwenden. In diesem Dokument werden die Schritte zum Konfigurieren von pfSense für ECE beschrieben.

Vorbereitung

Schritt 1: pfSense Software herunterladen

Verwenden Sie die [pfSense-Website](#), um das ISO-Installationsprogramm-Image herunterzuladen.

Schritt 2: Konfigurieren des virtuellen Computers

Konfigurieren Sie eine VM mit den Mindestanforderungen:

- 64-Bit-AMD64-kompatible (x86-64) CPU
- 1 GB oder mehr RAM
- 8 GB oder mehr Festplattenlaufwerk (SSD, HDD usw.)
- Eine oder mehrere kompatible Netzwerkschnittstellenkarten
- Bootfähiges USB-Laufwerk oder optisches Laufwerk mit hoher Kapazität (DVD oder BD) für die Erstinstallation

Für eine Laborinstallation ist nur eine Netzwerkschnittstelle (NIC) erforderlich. Es gibt mehrere Möglichkeiten, die Appliance auszuführen. Am einfachsten ist es jedoch, eine einzelne NIC zu verwenden, die auch als One-Arm-Modus bezeichnet wird. Im One-Arm-Modus gibt es eine

einzelne Schnittstelle, die mit dem Netzwerk kommuniziert. Dies ist zwar eine einfache und für ein Labor geeignete Methode, aber nicht die sicherste.

Eine sicherere Möglichkeit zum Konfigurieren der Appliance besteht darin, mindestens zwei NICs zu haben. Eine Netzwerkkarte ist die WAN-Schnittstelle und kommuniziert direkt mit dem öffentlichen Internet. Die zweite Netzwerkkarte ist die LAN-Schnittstelle und kommuniziert mit dem internen Unternehmensnetzwerk. Sie können auch zusätzliche Schnittstellen hinzufügen, um mit verschiedenen Teilen des Netzwerks zu kommunizieren, die über unterschiedliche Sicherheits- und Firewall-Regeln verfügen. Sie können beispielsweise eine NIC mit dem öffentlichen Internet verbinden, eine NIC mit dem DMZ-Netzwerk, in dem sich alle von außen zugänglichen Webserver befinden, und eine dritte NIC mit dem Unternehmensnetzwerk verbinden. So können interne und externe Benutzer sicher auf die gleichen Webserver zugreifen, die in einer DMZ gespeichert sind. Stellen Sie vor der Implementierung sicher, dass Sie die Sicherheitsauswirkungen jedes Designs verstehen. Wenden Sie sich an einen Sicherheitstechniker, um sicherzustellen, dass für Ihre spezifische Implementierung die Best Practices befolgt werden.

Installation

Schritt 1: Einbinden des ISO in das virtuelle System

Schritt 2: Schalten Sie das virtuelle System ein, und befolgen Sie die Anweisungen zur Installation.

Schrittweise Anleitungen finden Sie in diesem [Dokument](#).

Netzwerk-Setup

Sie müssen der Appliance IP-Adressen zuweisen, um mit der Konfiguration fortzufahren.

 Hinweis: Dieses Dokument zeigt eine Appliance, die im One-Arm-Modus konfiguriert wurde.

Schritt 1: Konfigurieren von VLANs

Wenn Sie VLAN-Unterstützung benötigen, beantworten Sie mit y die erste Frage. Andernfalls nein.

Schritt 2: WAN-Schnittstelle zuweisen

Die WAN-Schnittstelle ist die ungesicherte Seite der Appliance im Zwei-Arm-Modus und die einzige Schnittstelle im Ein-Arm-Modus. Geben Sie bei Aufforderung den Namen der Schnittstelle ein.

Schritt 3: LAN-Schnittstelle zuweisen

Die LAN-Schnittstelle ist die sichere Seite der Appliance im Zweiarmmodus. Geben Sie bei Bedarf den Namen der Schnittstelle ein.

Schritt 4: Andere Schnittstellen zuweisen

Konfigurieren Sie alle anderen Schnittstellen, die Sie für Ihre spezifische Installation benötigen. Diese sind optional und nicht üblich.

Schritt 5: Zuweisen der IP-Adresse zur Verwaltungsschnittstelle

Wenn Ihr Netzwerk DHCP unterstützt, wird die zugewiesene IP-Adresse im Konsolenbildschirm angezeigt.

```
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-Konsole

Wenn keine Adresse zugewiesen ist oder Sie eine bestimmte Adresse zuweisen möchten, führen Sie diese Schritte aus.

1. Wählen Sie Option 2 aus dem Konsolenmenü.
2. Antworten Sie n, um DHCP zu deaktivieren.
3. Geben Sie die IPv4-Adresse für die WAN-Schnittstelle ein.
4. Geben Sie die Netzmaske in Bitzahlen ein. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Geben Sie die Gateway-Adresse für die WAN-Schnittstelle ein.
6. Wenn Sie möchten, dass dieses Gateway das Standardgateway für die Appliance ist, beantworten Sie y mit der Gateway-Eingabeaufforderung, andernfalls antworten Sie n.
7. Konfigurieren Sie ggf. die Netzwerkkarte für IPv6.
8. Deaktivieren Sie den DHCP-Server auf der Schnittstelle.
9. Antworten Sie y, um HTTP im WebConfigurator-Protokoll zu aktivieren. Dies wird in den nächsten Schritten verwendet.


Sie erhalten dann eine Bestätigung, dass die Einstellungen aktualisiert wurden.

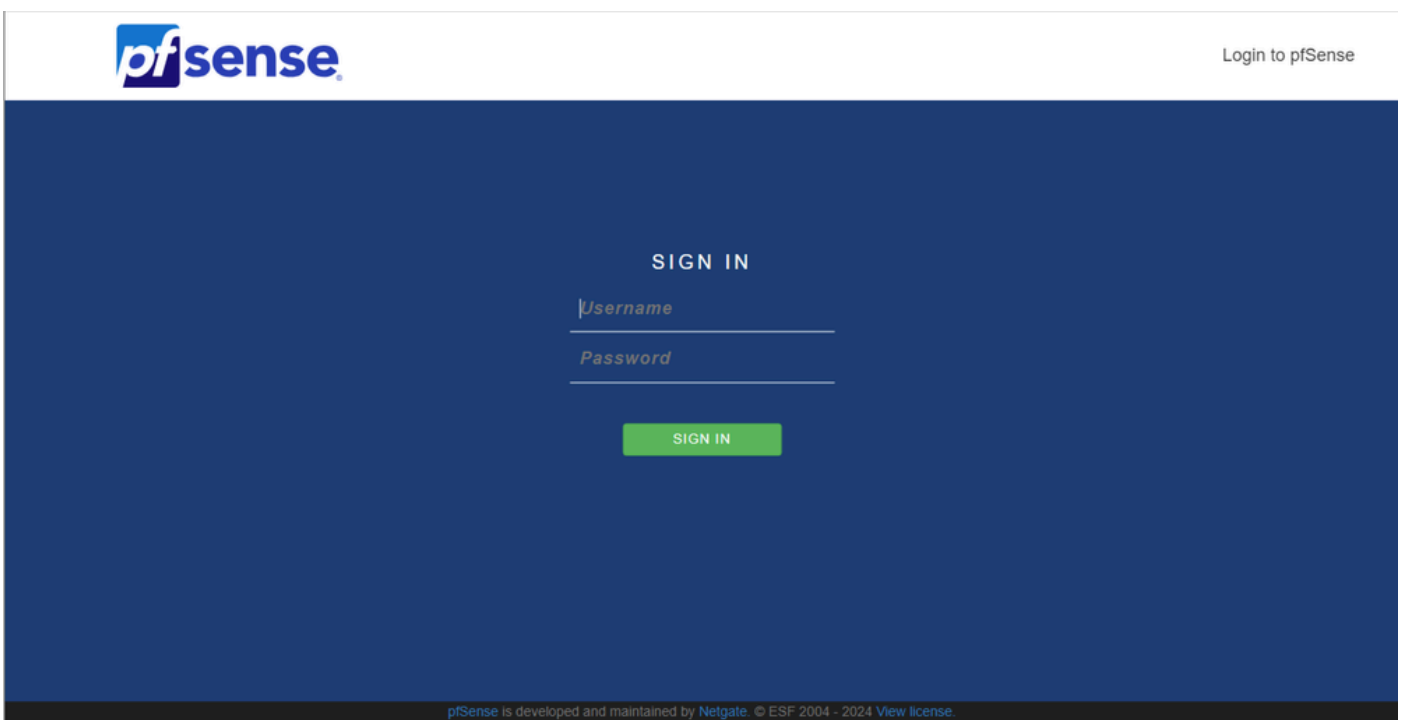
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://14.10.172.250/
Press <ENTER> to continue.
```

pfSense-Bestätigung

Ersteinrichtung abschließen

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zu: http://<ip_address_of_appliance>

 Hinweis: Sie müssen zunächst HTTP und nicht HTTPS verwenden.



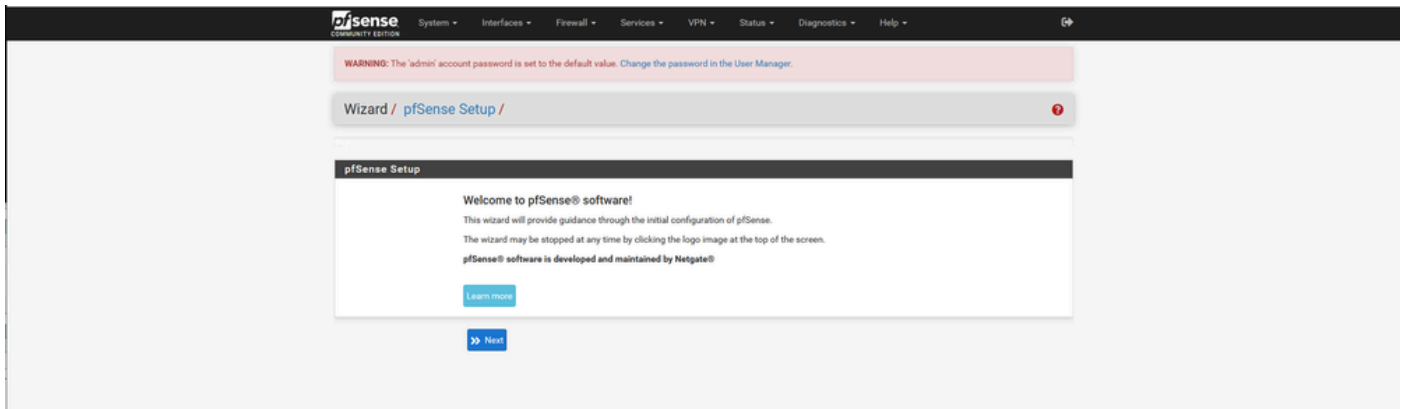
The screenshot shows the pfSense login page. At the top left is the pfSense logo, and at the top right is the text "Login to pfSense". The main content area has a dark blue background with the text "SIGN IN" centered. Below this are two input fields: "Username" and "Password", each with a horizontal line underneath. A green "SIGN IN" button is centered below the password field. At the bottom of the page, there is a small footer that reads "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license."

pfSense-Administratoranmeldung

Schritt 2: Melden Sie sich mit der Standardanmeldung admin / pfSense an.

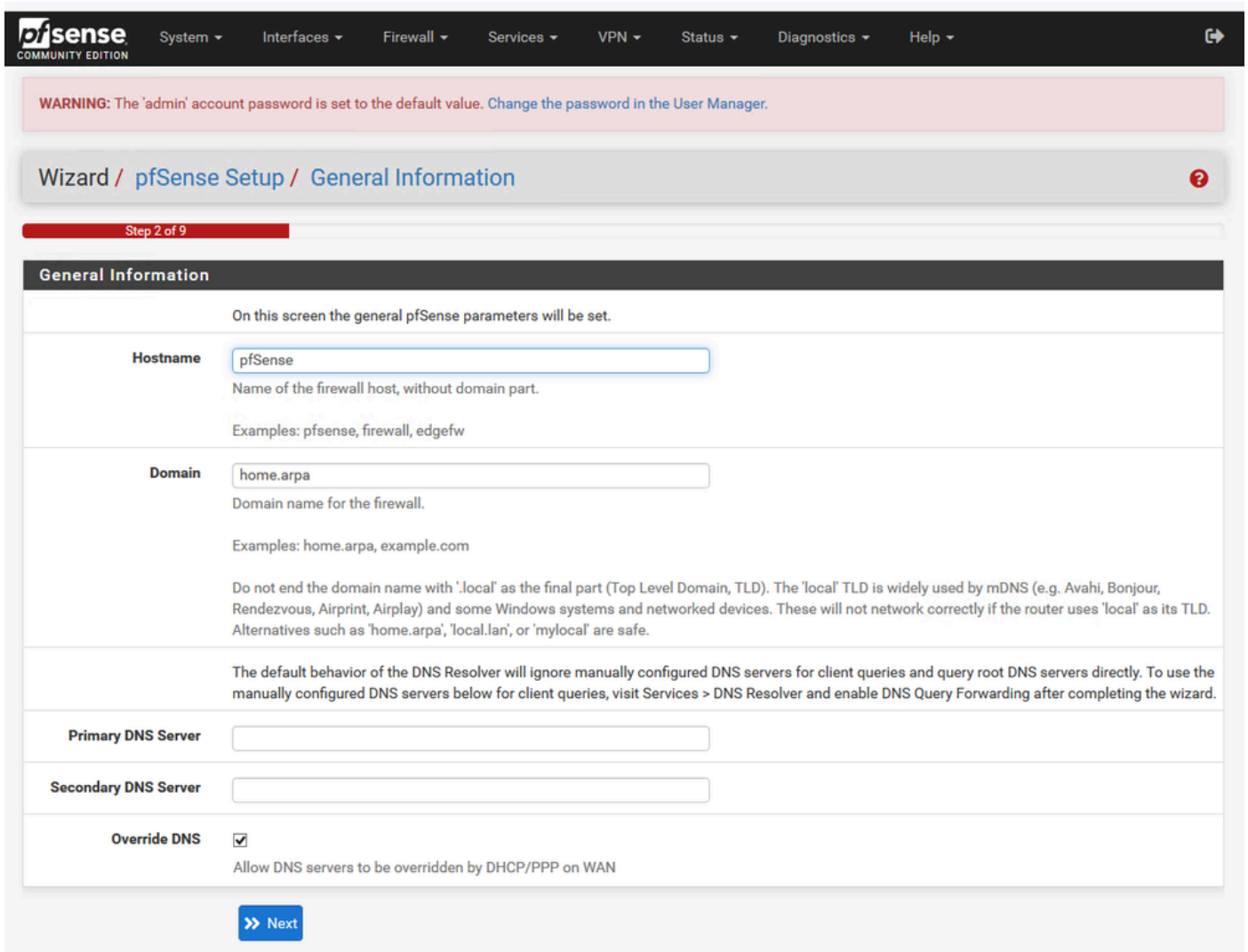
Schritt 3: Abschließen der Ersteinrichtung

Klicken Sie auf Next (Weiter) durch die ersten beiden Bildschirme.



pfSense-Installationsassistent - 1

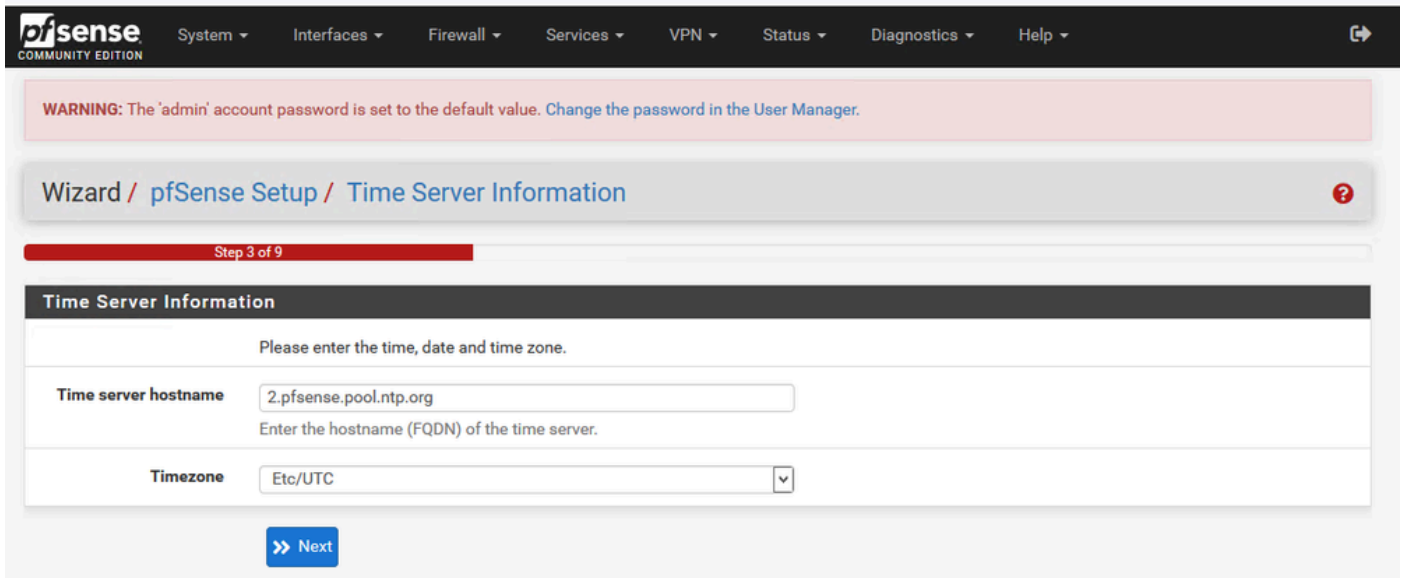
Geben Sie den Hostnamen, den Domännennamen und die DNS-Serverinformationen an.



pfSense-Installationsassistent - 2

Validieren Sie die IP-Adressinformationen. Wenn Sie zunächst DHCP ausgewählt haben, können Sie dies jetzt ändern.

Geben Sie den Hostnamen des NTP-Zeitserver an, und wählen Sie im Dropdown-Menü die richtige Zeitzone aus.



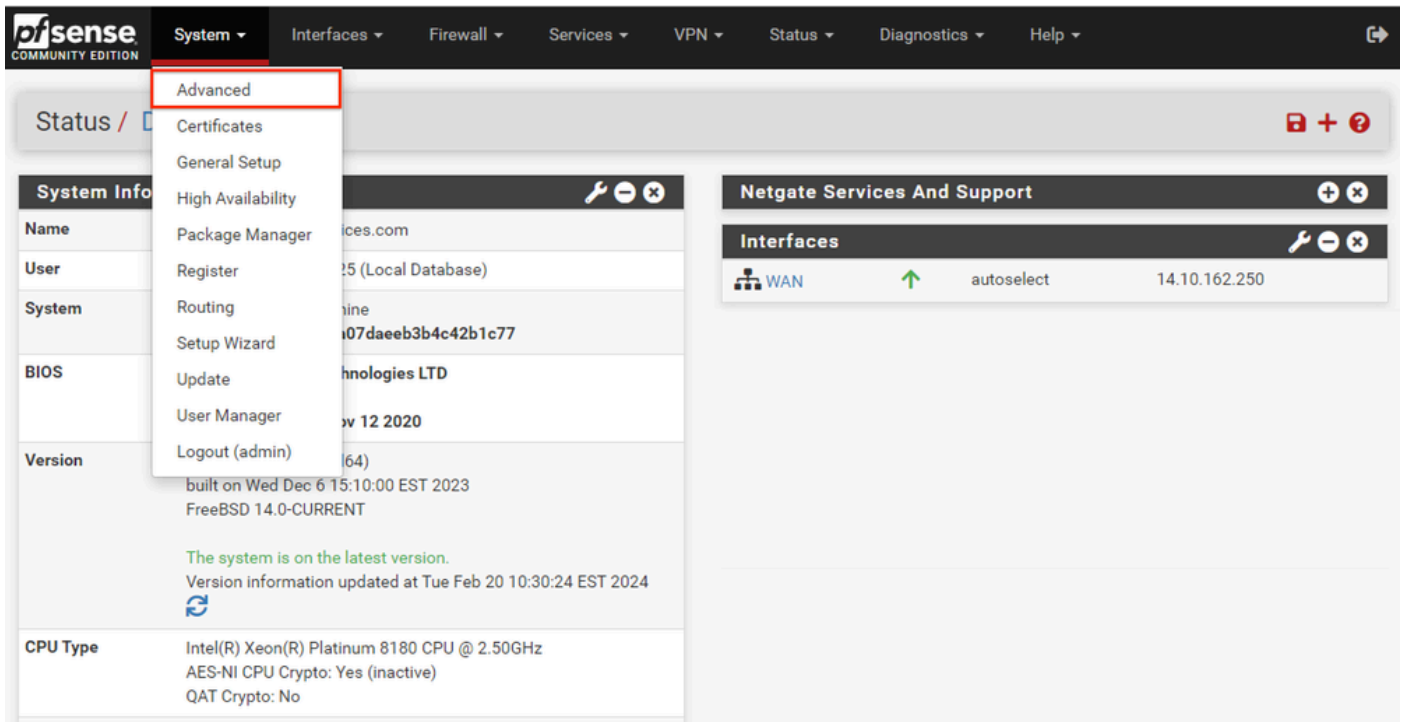
pfSense-Installationsassistent - 3

Fahren Sie mit dem Setup-Assistenten bis zum Ende fort. Die Benutzeroberfläche wird neu gestartet, und Sie werden nach Abschluss des Vorgangs zur neuen URL weitergeleitet.

Grundlegende Admin-Einstellungen konfigurieren

Schritt 1: Anmeldung bei der Admin-Schnittstelle

Schritt 2: Wählen Sie im Dropdown-Menü System die Option Erweitert aus.



pfSense-GUI - Administrator-Dropdown


Schritt 3: WebConfigurator-Einstellungen aktualisieren

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-Konfiguration

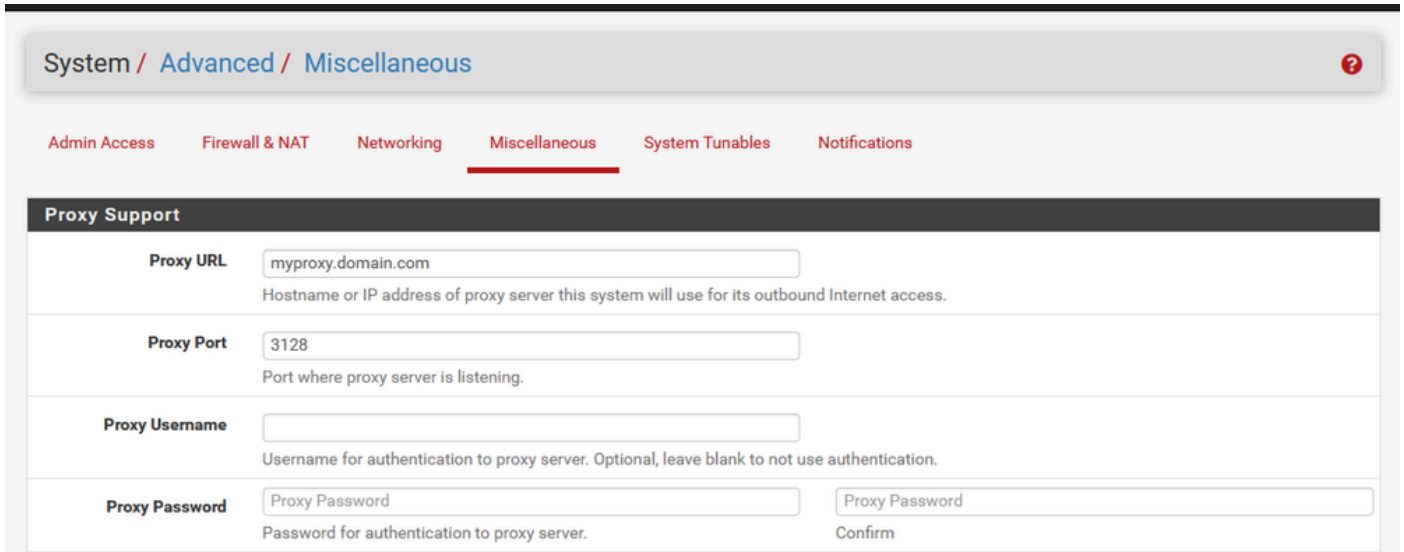
1. Wählen Sie das HTTPS-Protokoll (SSL/TLS) aus.
2. Lassen Sie das SSL/TLS-Zertifikat jetzt dem selbst signierten Zertifikat überlassen.
3. Ändern Sie den TCP-Port auf einen anderen als den 443-Port, um die Schnittstelle besser zu sichern und Probleme mit Portüberschneidungen zu vermeiden.
4. Wählen Sie die WebGUI-Umleitungsoption aus, um die Admin-Schnittstelle an Port 80 zu deaktivieren.
5. Wählen Sie die Erzwingungsoption HTTP_REFERER im Browser aus.

6. Aktivieren Sie Secure Shell, indem Sie die Option Secure Shell aktivieren auswählen.

 Hinweis: Wählen Sie vor dem Fortfahren die Schaltfläche Speichern. Sie werden dann zum neuen https-Link weitergeleitet.

Schritt 4: Proxyserver bei Bedarf konfigurieren


Konfigurieren Sie ggf. die Proxyinformationen auf der Registerkarte Verschiedenes. Um Setup und Konfiguration abzuschließen, muss die Appliance über einen Internetzugang verfügen.



The screenshot shows the pfSense GUI configuration page for Proxy Support. The breadcrumb trail is System / Advanced / Miscellaneous. The 'Miscellaneous' tab is selected. The 'Proxy Support' section contains the following fields:

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="password" value="Proxy Password"/>	Proxy Password
		Confirm


pfSense GUI - Proxy-Konfiguration

 Hinweis: Stellen Sie sicher, dass Sie nach dem Ändern die Schaltfläche Speichern auswählen.

Erforderliche Pakete hinzufügen

Schritt 1: Wählen Sie System > Package Manager

Schritt 2: Verfügbare Pakete auswählen

 Hinweis: Es kann einige Minuten dauern, bis alle verfügbaren Pakete geladen sind. Wenn diese Zeitüberschreitung auftritt, überprüfen Sie, ob die DNS-Server richtig konfiguriert sind. Häufig wird die Internetverbindung durch einen Neustart der Appliance repariert.

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.

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

pfSense GUI - Paketliste

Schritt 3: Suchen und Installieren erforderlicher Pakete

1. Havproxy
2. Open-VM-Tools



Hinweis: Wählen Sie das haproxy-devel-Paket nicht aus.

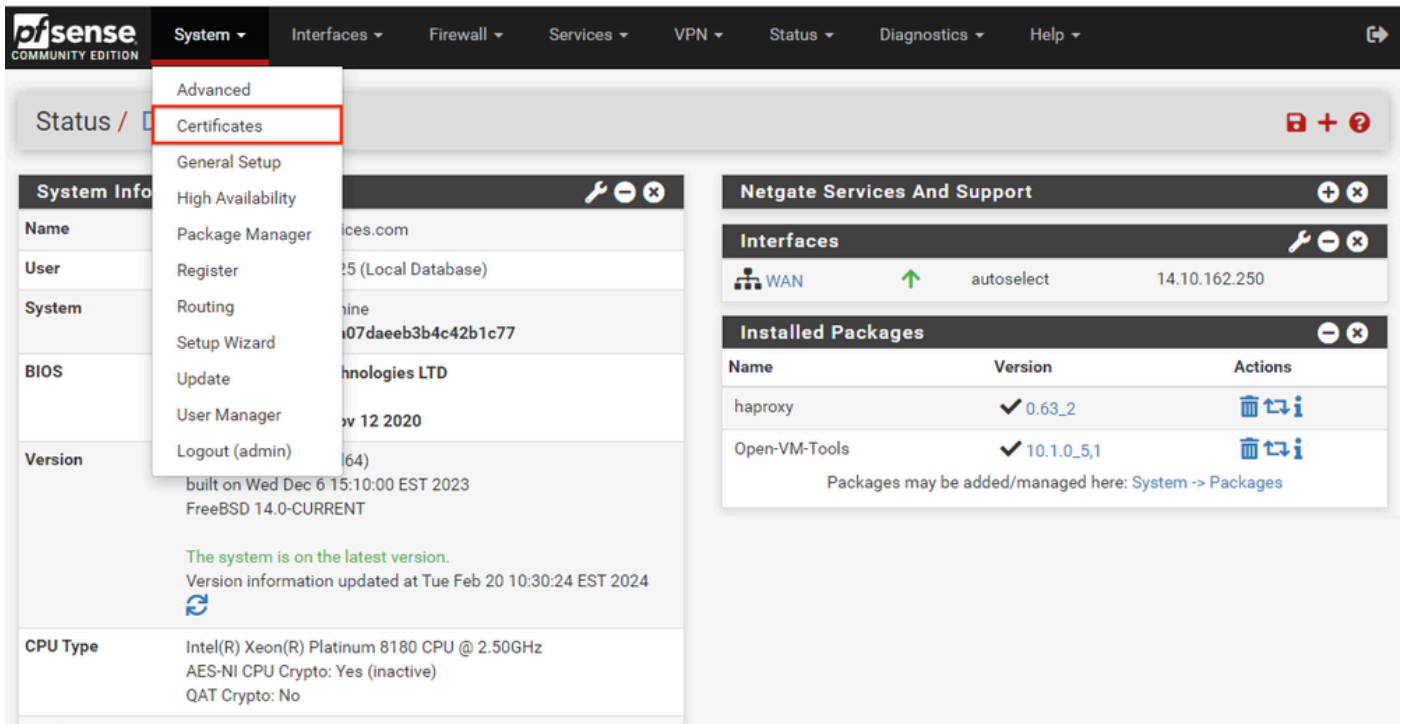
Zertifikate konfigurieren

pfSense kann selbstsigniertes Zertifikat erstellen oder es kann in eine öffentliche Zertifizierungsstelle, eine interne Zertifizierungsstelle integriert werden, oder es kann als Zertifizierungsstelle fungieren und von der Zertifizierungsstelle signierte Zertifikate ausgeben. Dieser Leitfaden zeigt die Schritte zur Integration in eine interne Zertifizierungsstelle.

Bevor Sie mit diesem Abschnitt beginnen, stellen Sie sicher, dass diese Optionen verfügbar sind.

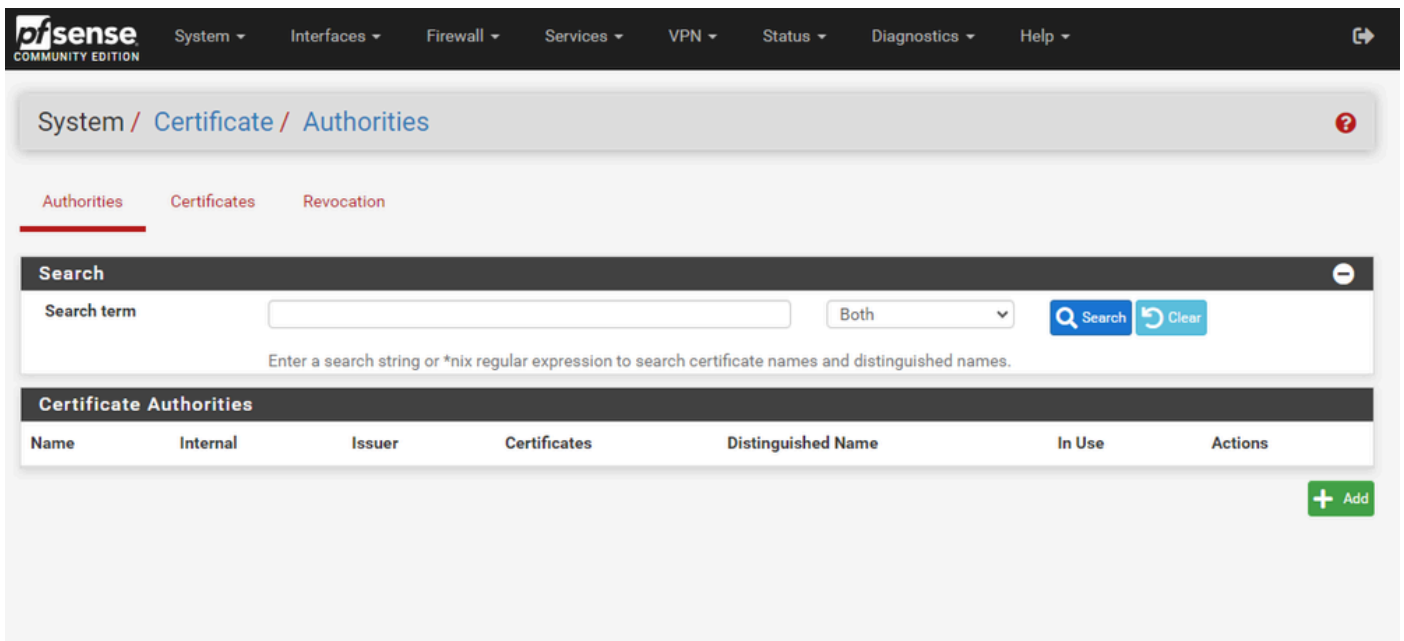
1. Das Stammzertifikat für die Zertifizierungsstelle wird entweder als PEM- oder Base-64-kodiertes Format gespeichert.
2. Alle Zwischenzertifikate (manchmal auch als Ausstellung bezeichnet) für eine Zertifizierungsstelle werden entweder als PEM- oder Base-64-kodiertes Format gespeichert.

Schritt 1: Wählen Sie Zertifikate aus dem Dropdown-Menü System aus.



pfSense GUI - Zertifikatauswahl

Schritt 2: CA-Stammzertifikat importieren



pfSense GUI - Zertifizierungsstellen-Zertifikatliste

Wählen Sie die Schaltfläche Hinzufügen aus.

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

Wie in der Abbildung dargestellt:

1. Geben Sie einen eindeutigen beschreibenden Namen ein.
2. Wählen Sie im Dropdown-Menü "Methode" die Option "Vorhandene Zertifizierungsstelle importieren".
3. Stellen Sie sicher, dass die Kontrollkästchen "Seriell übernehmen" und "Seriell zuordnen" aktiviert sind.
4. Fügen Sie das gesamte Zertifikat in das Textfeld Zertifikatdaten ein. Vergewissern Sie sich, dass Sie den Posten -----BEGIN CERTIFICATE----- und -----END CERTIFICATE----- hinzufügen.
5. Wählen Sie Speichern.
6. Überprüfen Sie, ob das Zertifikat wie im Bild dargestellt importiert wurde.

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

pfSense-GUI - Zertifizierungsstellenliste

Schritt 3: Zwischenzertifikat der Zertifizierungsstelle importieren

[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 Intermediate Import

Wiederholen Sie die Schritte zum Importieren des Stammzertifikats der Zertifizierungsstelle, um das Zwischenzertifikat der Zertifizierungsstelle zu importieren.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

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="Refresh"/> <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="Refresh"/> <input type="button" value="Delete"/>

pfSense-GUI - CA-Links

Überprüfen Sie die Zertifizierungsstellen, um sicherzustellen, dass der Intermediate ordnungsgemäß mit dem Stammzertifikat verknüpft ist, wie im Bild gezeigt.

Schritt 4: Erstellen und Exportieren einer CSR-Anfrage für die Website mit Lastenausgleich

In diesem Abschnitt werden die Schritte zum Erstellen eines CSR, Exportieren des CSR und Importieren des signierten Zertifikats beschrieben. Wenn Sie bereits über ein Zertifikat im PFX-Format verfügen, können Sie dieses Zertifikat importieren. Weitere Informationen zu diesen Schritten finden Sie in der Dokumentation von pfSense.

1. Wählen Sie das Menü Zertifikate und anschließend die Schaltfläche Hinzufügen/Signieren.

[System](#) / [Certificates](#) / [Certificates](#)

[Authorities](#) [Certificates](#) [Certificate Revocation](#)

Search

Search term: Both [Search](#) [Clear](#)

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

Certificates

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

[+ Add/Sign](#)

pfSense GUI - Zertifikatsliste

2. Füllen Sie das Formular für die Zertifikatsignierungsanforderung aus.

pfSense
COMMUNITY EDITION

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

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create a Certificate Signing Request ▾

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

External Signing Request

Key type RSA ▾

2048 ▾
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

prime256v1 [HTTPS] [IPsec] [OpenVPN] ▾

Digest Algorithm sha256 ▾
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Common Name myece.mydomain.com

The following certificate subject components are optional and may be left blank.

Country Code US ▾

State or Province North Carolina

City Research Triangle Park

Organization Cisco Systems Inc

Organizational Unit Cisco TAC

pfSense-GUI - CSR-Erstellung

- Methode: Wählen Sie im Dropdown-Menü Create a Certificate Signing Request aus.
- Beschreibender Name: Geben Sie einen Namen für das Zertifikat ein.
- Schlüsseltyp und Digest-Algorithmus: Überprüfen Sie, ob diese Ihren Anforderungen entsprechen.
- Common Name (Allgemeiner Name): Vollqualifizierter Domänenname auf der Website angeben
- Geben Sie die verbleibenden Zertifikatsinformationen an, die für Ihre Umgebung erforderlich sind.

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 Advanced

- Zertifikatstyp: Wählen Sie im Dropdown-Menü die Option Serverzertifikat aus.
- Alternative Namen: Geben Sie alle für Ihre Implementierung erforderlichen alternativen Namen (SAN) für den Betreff an.

 Hinweis: Der allgemeine Name wird dem Feld SAN automatisch hinzugefügt. Sie müssen lediglich weitere Namen hinzufügen.

Wählen Sie Speichern, sobald alle Felder korrekt sind.

3. Exportieren Sie den CSR in eine Datei.

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	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		

Wählen Sie die Schaltfläche "Exportieren", um den CSR zu speichern, und signieren Sie ihn mit Ihrer Zertifizierungsstelle. Speichern Sie das signierte Zertifikat als PEM- oder Base-64-Datei, um den Vorgang abzuschließen.

4. Importieren Sie das signierte Zertifikat.

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, the breadcrumb path is System / Certificates / Certificates. A green notification bar at the top indicates "Created certificate signing request ece-web-2024". The main content area has three tabs: Authorities, Certificates (selected), and Certificate Revocation. Below the tabs is a search bar with a search term input field, a dropdown menu set to "Both", and buttons for "Search" and "Clear". Below the search bar is a table of certificates with columns for Name, Issuer, Distinguished Name, In Use, and Actions. The table contains two entries: "GUI default (65cced5b25159) Server Certificate" and "ece-web-2024". The "Actions" column for "ece-web-2024" contains a pencil icon (highlighted with a red box), a plus icon, and a trash icon. At the bottom right of the table is a green "+ Add/Sign" button.

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		  

Wählen Sie das Bleistiftsymbol aus, um das signierte Zertifikat zu importieren.

5. Fügen Sie die Zertifikatdaten in das Formular ein.

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
MAKGA1UEBHMCMVVMxZjZAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMRRowGAYDVQQKExFDZXNjbyBTeXN0ZW1zIEIu
YzESMBAGA1UECzMjQ21zY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
-----END CERTIFICATE REQUEST-----
```

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.

pfSense GUI - Zertifikatimport

Wählen Sie Aktualisieren, um das Zertifikat zu speichern.

6. Überprüfen Sie die Zertifikatdaten, um sicherzustellen, dass sie richtig sind.

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		

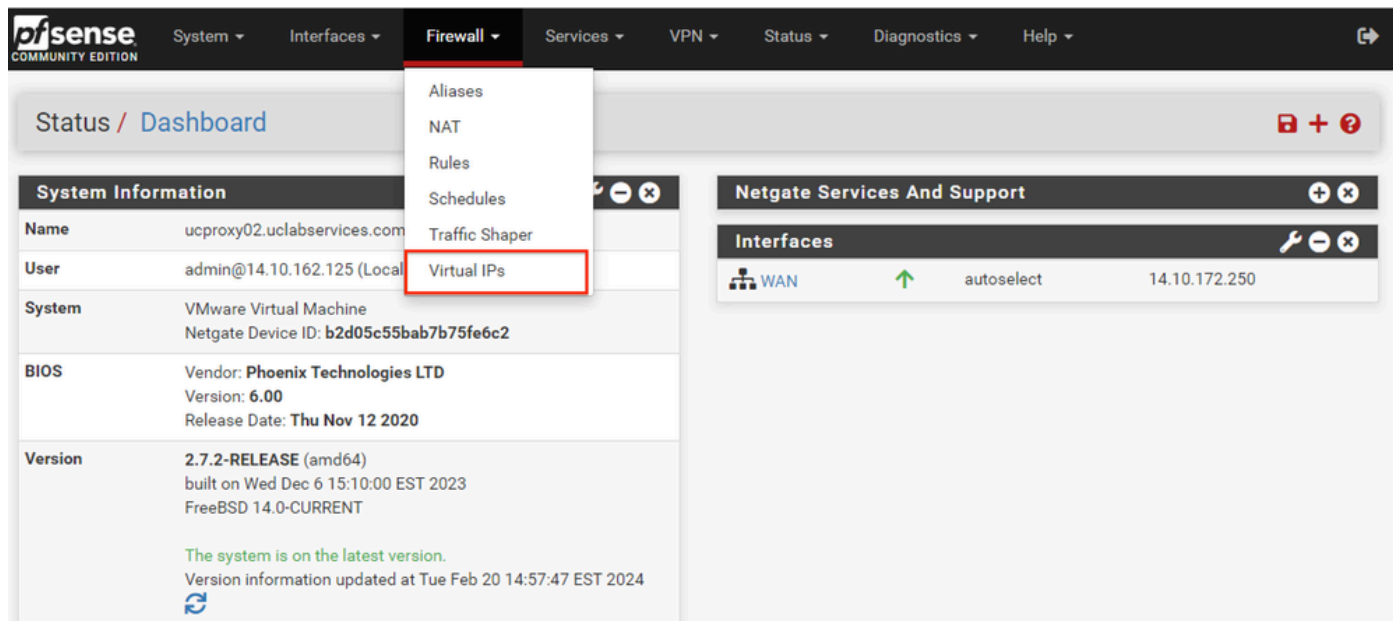
pfSense GUI - Zertifikatsliste

7. Wiederholen Sie diesen Vorgang, wenn Sie mehrere Sites auf dieser pfSense hosten möchten.

Virtuelle IPs hinzufügen

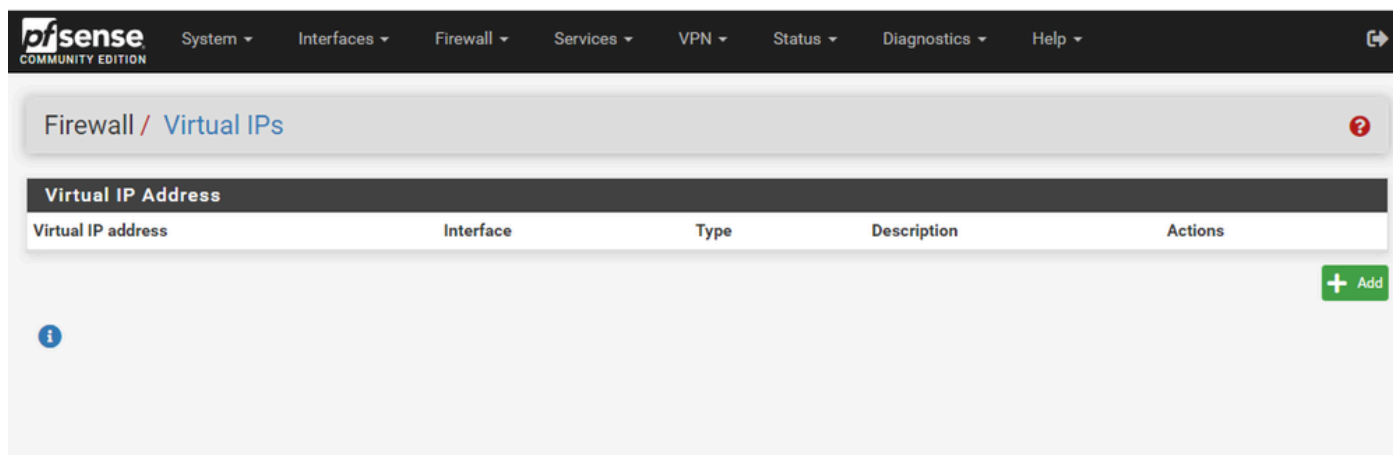
Mindestens eine IP ist erforderlich, um Websites auf der pfSense zu hosten. In pfSense geschieht dies mit Virtual IPs (VIPs).

Schritt 1: Wählen Sie virtuelle IPs aus dem Dropdown-Menü Firewall aus.



pfSense GUI - VIP-Dropdown

Schritt 2: Wählen Sie die Schaltfläche Hinzufügen



pfSense GUI - VIP-Startseite

Schritt 3: Adressinformationen angeben

[System](#) ▾ [Interfaces](#) ▾ [Firewall](#) ▾ [Services](#) ▾ [VPN](#) ▾ [Status](#) ▾ [Diagnostics](#) ▾ [Help](#) ▾

Firewall / [Virtual IPs](#) / [Edit](#)

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface

Address type

Address(es) /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.

Advertising frequency

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

A description may be entered here for administrative reference (not parsed).

pfSense GUI - VIP-Konfiguration

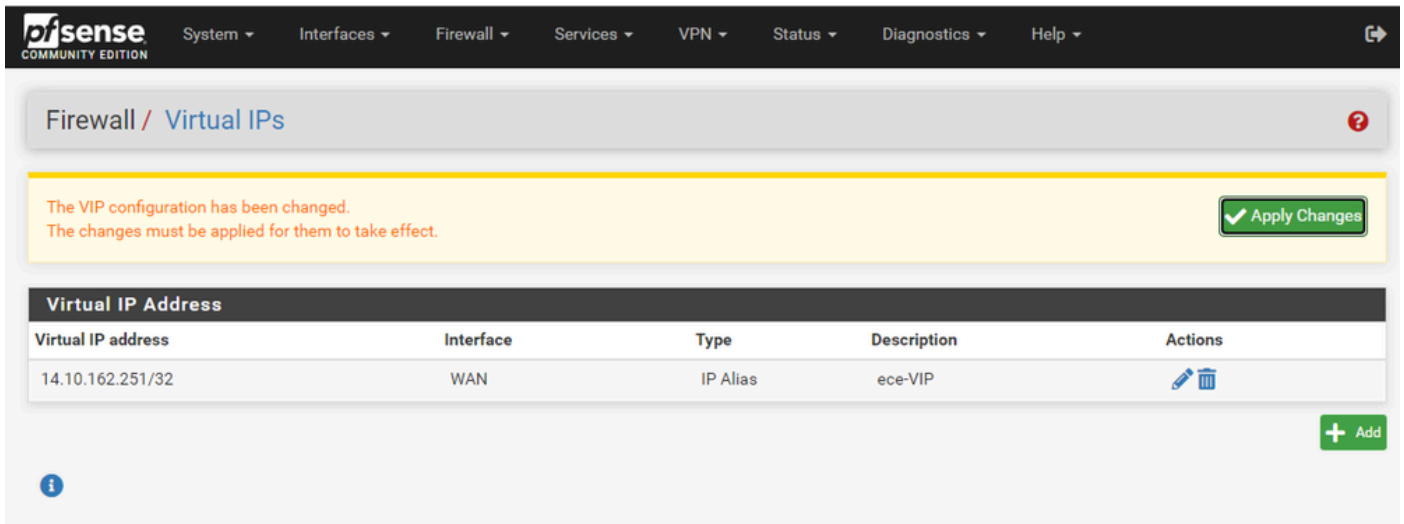
Verwenden Sie die Informationen, um einen VIP hinzuzufügen.

- Typ: IP-Alias auswählen
- Schnittstelle: Wählen Sie die Schnittstelle für diese IP-Adresse aus, die übertragen werden soll.
- Adresse(n): Geben Sie die IP-Adresse ein
- Adressmaske: Für IP-Adressen, die für den Lastenausgleich verwendet werden, muss die Maske /32 sein.
- Beschreibung: Stellen Sie einen kurzen Text bereit, um die Konfiguration später besser zu verstehen.

Wählen Sie Speichern, um die Änderung zu übernehmen.

Wiederholen Sie dies für jede IP-Adresse, die für Ihre Konfiguration erforderlich ist.

Schritt 4: Konfiguration anwenden



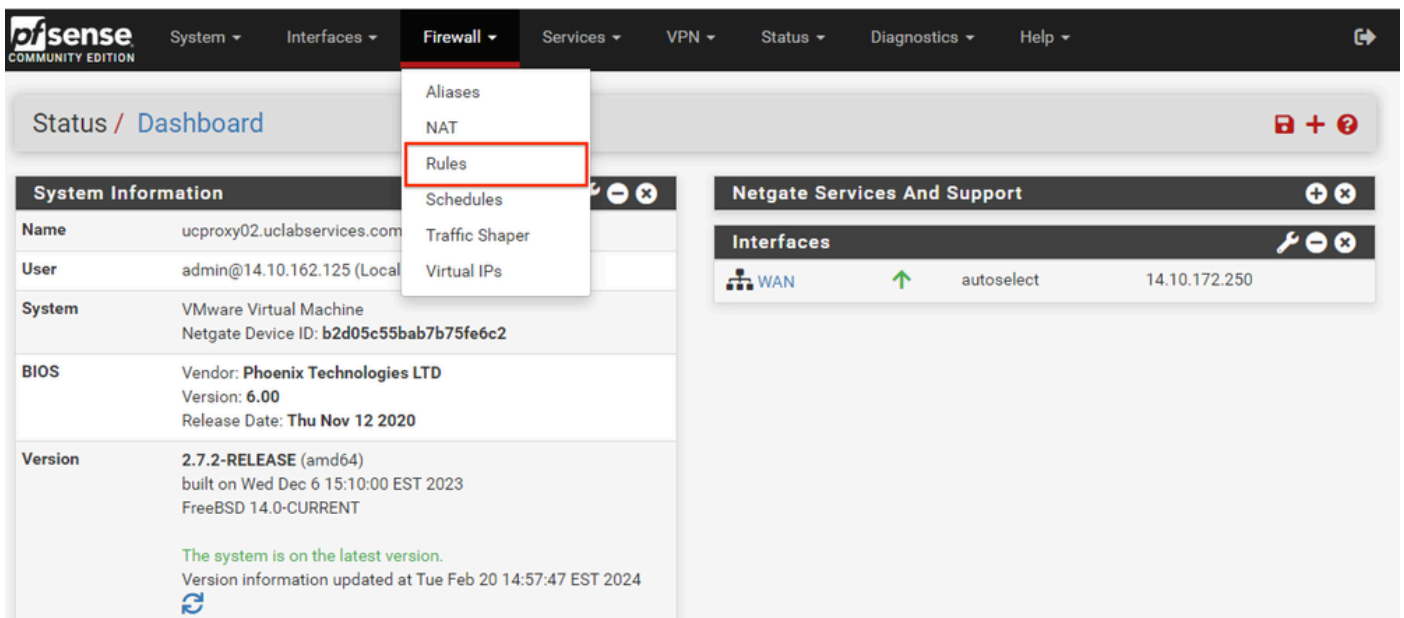
pfSense GUI - VIP-Liste

Klicken Sie auf die Schaltfläche "Änderungen übernehmen", nachdem alle VIPs hinzugefügt wurden.

Firewall konfigurieren

pfSense hat eine eingebaute Firewall. Der Standardregelsatz ist sehr begrenzt. Bevor die Appliance in Betrieb genommen wird, stellen Sie sicher, dass Sie eine umfassende Firewall-Richtlinie erstellen.

Schritt 1: Wählen Sie im Dropdown-Menü Firewall die Option Regeln aus.



pfSense GUI - Firewall Rules Dropdown

Schritt 2: Wählen Sie eine der Schaltflächen zum Hinzufügen aus.

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

pfSense GUI - Liste der Firewall-Regeln

Beachten Sie, dass eine Schaltfläche die neue Regel über der ausgewählten Zeile hinzufügt, während die andere die Regel unter der ausgewählten Regel hinzufügt. Beide Schaltflächen können für die erste Regel verwendet werden.

Schritt 3: Erstellen einer Firewall-Regel, um Datenverkehr an Port 443 für die IP-Adresse zuzulassen

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

pfSense-GUI - Konfiguration der Firewall-Passregel

Verwenden Sie die Informationen, um die Regel zu erstellen.

- Aktion: Wählen Sie Bestanden aus.
- Schnittstelle: Wählen Sie die Schnittstelle aus, auf die die Regel angewendet wird.
- Adressfamilie und Protokoll: Je nach Bedarf auswählen
- Quelle: Als Beliebig markiert lassen
- Ziel: Wählen Sie im Dropdown-Menü "Ziel" die Option Adresse oder Alias aus, und geben Sie dann die IP-Adresse ein, für die die Regel gilt.
- Zielportbereich: Wählen Sie in den Dropdown-Menüs "Von" und "Bis" HTTPS (443) aus.
- Protokoll: Aktivieren Sie das Kontrollkästchen, um alle Pakete zu protokollieren, die dieser Regel für die Abrechnung entsprechen.

- Beschreibung: Geben Sie Text für einen späteren Verweis auf die Regel ein.

Wählen Sie Speichern aus.

Schritt 4: Erstellen Sie eine Firewall-Regel, um den gesamten anderen Datenverkehr an pfSense zu verwerfen.

Klicken Sie auf die Schaltfläche Hinzufügen, um die Regel unter der neu erstellten Regel einzufügen.

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

- Edit Firewall Rule:**
 - Action:** Block (selected). 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 (selected). Choose the interface from which packets must come to match this rule.
 - Address Family:** IPv4 (selected). Select the Internet Protocol version this rule applies to.
 - Protocol:** TCP (selected). Choose which IP protocol this rule should match.
- Source:**
 - Source:** Invert match. Any (selected). Source Address: / (selected).
 - Display Advanced:** A button to show advanced options.
 - Hint:** 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 (selected). Destination Address: / (selected).
 - Destination Port Range:** (other) (selected) From Custom To (other) (selected) 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** button.

A **Save** button is located at the bottom of the page.

- Aktion: Block auswählen
- Schnittstelle: Wählen Sie die Schnittstelle aus, auf die die Regel angewendet wird.
- Adressfamilie und Protokoll: Je nach Bedarf auswählen
- Quelle: Als Beliebig markiert lassen
- Ziel: Als Beliebig markiert lassen
- Protokoll: Aktivieren Sie das Kontrollkästchen, um alle Pakete zu protokollieren, die dieser Regel für die Abrechnung entsprechen.
- Beschreibung: Geben Sie Text für einen späteren Verweis auf die Regel ein.

Wählen Sie Speichern aus.

Schritt 5: Überprüfen Sie die Regeln, und stellen Sie sicher, dass die Blockregel unten steht.

The screenshot shows the pfSense GUI for the Firewall Rules configuration on the WAN interface. A yellow notification bar at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." with an "Apply Changes" button. Below this, the "Rules (Drag to Change Order)" table is displayed. The table has the following columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The rules listed are:

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

At the bottom of the table, there are buttons for "Add" (up and down arrows), "Delete" (trash icon), "Toggle" (power icon), "Copy" (document icon), "Save" (floppy icon), and "Separator" (+ icon).

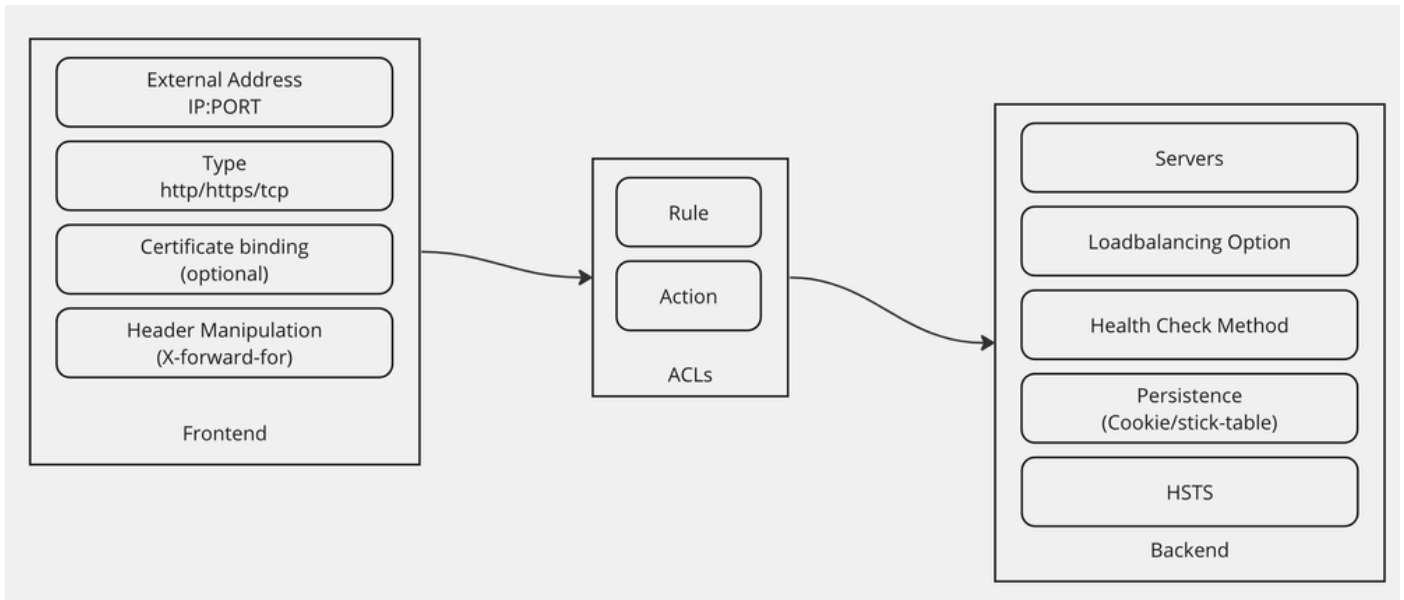
pfSense GUI - Liste der Firewall-Regeln

Ziehen Sie ggf. die Regeln, um sie zu sortieren.

Wählen Sie Apply Changes (Änderungen anwenden) aus, sobald die Firewall-Regeln in der für Ihre Umgebung erforderlichen Reihenfolge vorliegen.

Konfigurieren von HAProxy

HAProxy-Konzepte



HAProxy-Konzepte

HAProxy wird mit einem Frontend/Backend-Modell implementiert.

Das Frontend definiert die Seite des Proxys, mit der die Kunden kommunizieren.

Das Frontend besteht aus einer IP- und Port-Kombination, einer Zertifikatsbindung und kann eine gewisse Header-Manipulation implementieren.

Das Backend definiert die Seite des Proxys, die mit den physischen Webservern kommuniziert.

Das Backend definiert die tatsächlichen Server und Ports, die Lastverteilungsmethode für die Erstzuweisung, Integritätsprüfungen und Persistenz.

Ein Frontend weiß, mit welchem Backend es kommunizieren soll, entweder über ein dediziertes Backend oder über ACLs.

ACLs können unterschiedliche Regeln erstellen, sodass ein bestimmtes Frontend mit verschiedenen Backends kommunizieren kann, je nach den verschiedenen Dingen.

Anfängliche HAProxy-Einstellungen

Schritt 1: Wählen Sie HAProxy aus dem Dropdown-Menü Services aus.

The screenshot shows the pfSense Community Edition interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Services' dropdown menu is open, listing various services such as Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, HAProxy (highlighted with a red box), IGMP Proxy, NTP, PPPoE Server, Router Advertisement, SNMP, and Wake-on-LAN. The main content area is divided into two sections: 'System Information' and 'Netgate Services And Support'. The 'System Information' section displays details like Name (ucproxy02.uclabservices.com), User (admin@14.10.162.125), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), Version (2.7.2-RELEASE), and CPU Type (Intel(R) Xeon(R) Platinum 8180 CPU). The 'Netgate Services And Support' section shows the contract type as 'Community Support' and provides links to 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES'.

pfSense-GUI - HAProxy-Dropdown

Schritt 2: Grundeinstellungen konfigurieren

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-Hauptinstellungen

Aktivieren Sie das Kontrollkästchen HAProxy aktivieren.

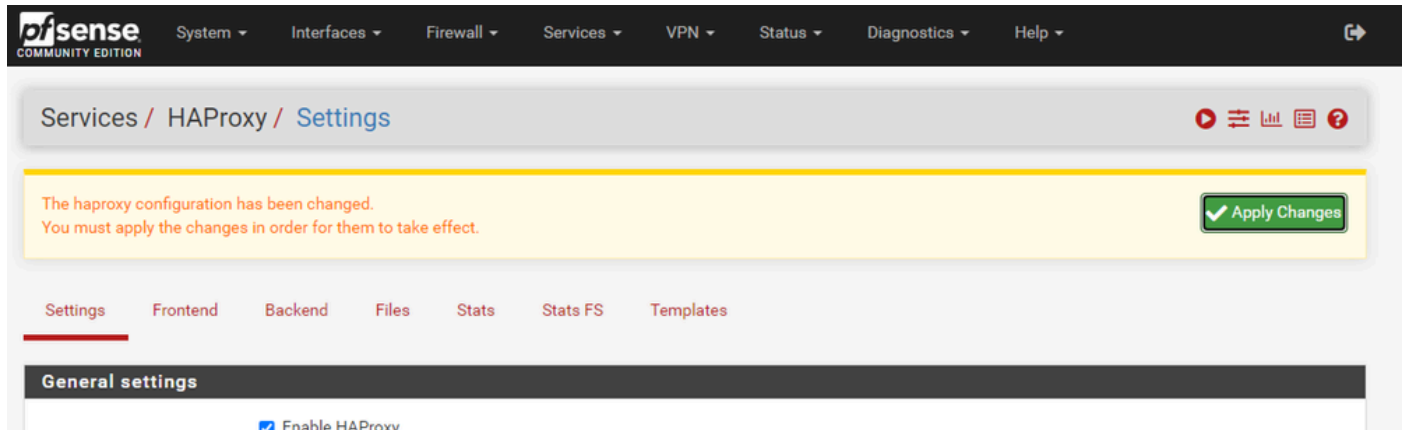
Geben Sie einen Wert für Maximum Connections (Maximale Verbindungen) ein. Weitere Informationen zum erforderlichen Arbeitsspeicher finden Sie in der Tabelle in diesem Abschnitt.

Geben Sie einen Wert für den Port für interne Statistiken ein. Dieser Port wird verwendet, um HAProxy-Statistiken auf der Appliance anzuzeigen, ist jedoch außerhalb der Appliance nicht verfügbar.

Geben Sie einen Wert für die Aktualisierungsrate der internen Statistiken ein.


Überprüfen Sie die verbleibende Konfiguration, und aktualisieren Sie sie bei Bedarf für Ihre Umgebung.

Wählen Sie Speichern.



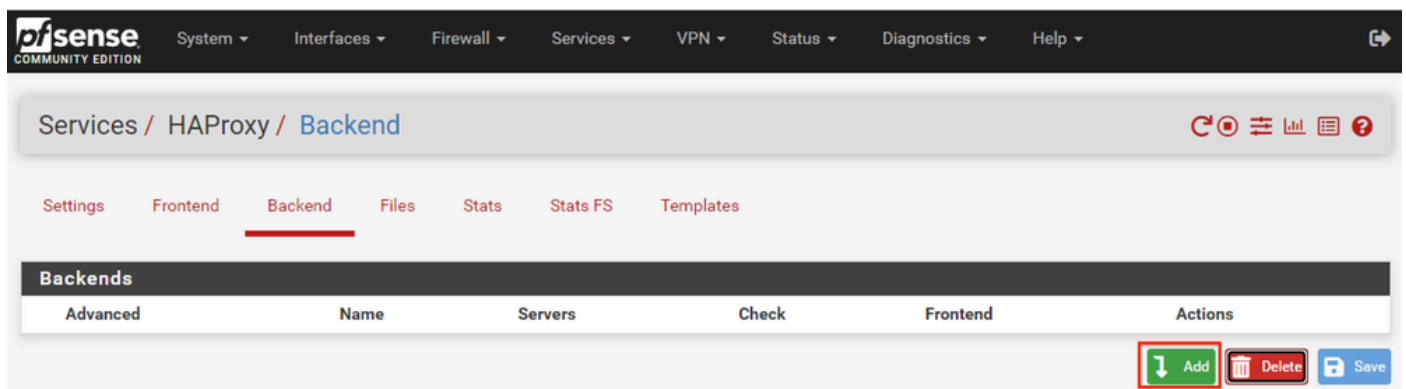
The screenshot shows the pfSense GUI for the HAProxy Settings page. The breadcrumb navigation is 'Services / HAProxy / Settings'. A yellow notification bar at the top states: 'The haproxy configuration has been changed. You must apply the changes in order for them to take effect.' A green 'Apply Changes' button is visible in the notification bar. Below the notification, there are tabs for 'Settings', 'Frontend', 'Backend', 'Files', 'Stats', 'Stats FS', and 'Templates'. The 'Settings' tab is selected. Under the 'General settings' section, the 'Enable HAProxy' checkbox is checked.

pfSense-GUI - HAProxy - Änderungen übernehmen

 Hinweis: Konfigurationsänderungen werden erst aktiviert, wenn Sie die Schaltfläche Apply Changes (Änderungen anwenden) auswählen. Sie können mehrere Konfigurationsänderungen vornehmen und sie alle gleichzeitig anwenden. Die Konfiguration muss nicht angewendet werden, um in einem anderen Abschnitt verwendet zu werden.

Konfigurieren des HAProxy-Backends

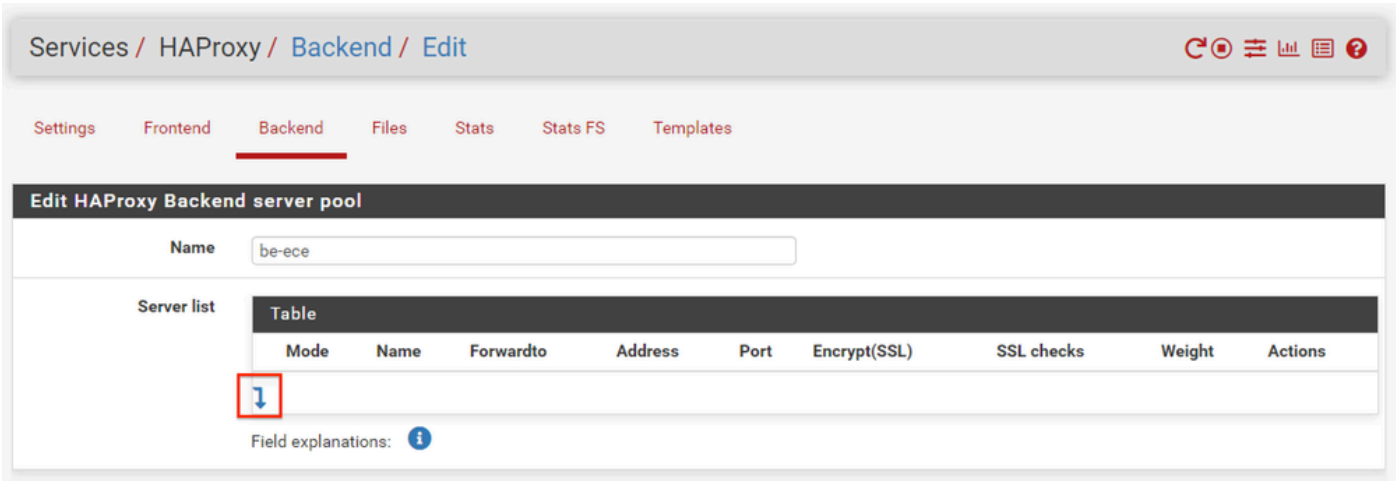
Beginnen Sie mit dem Backend. Der Grund dafür ist, dass das Frontend auf ein Backend verweisen muss. Stellen Sie sicher, dass Sie das Menü Backend ausgewählt haben.



The screenshot shows the pfSense GUI for the HAProxy Backend configuration page. The breadcrumb navigation is 'Services / HAProxy / Backend'. The 'Backend' tab is selected. Below the navigation, there is a table with columns: 'Advanced', 'Name', 'Servers', 'Check', 'Frontend', and 'Actions'. At the bottom right of the table, there are three buttons: 'Add' (highlighted in green), 'Delete', and 'Save'.

pfSense GUI - HAProxy Add Backend

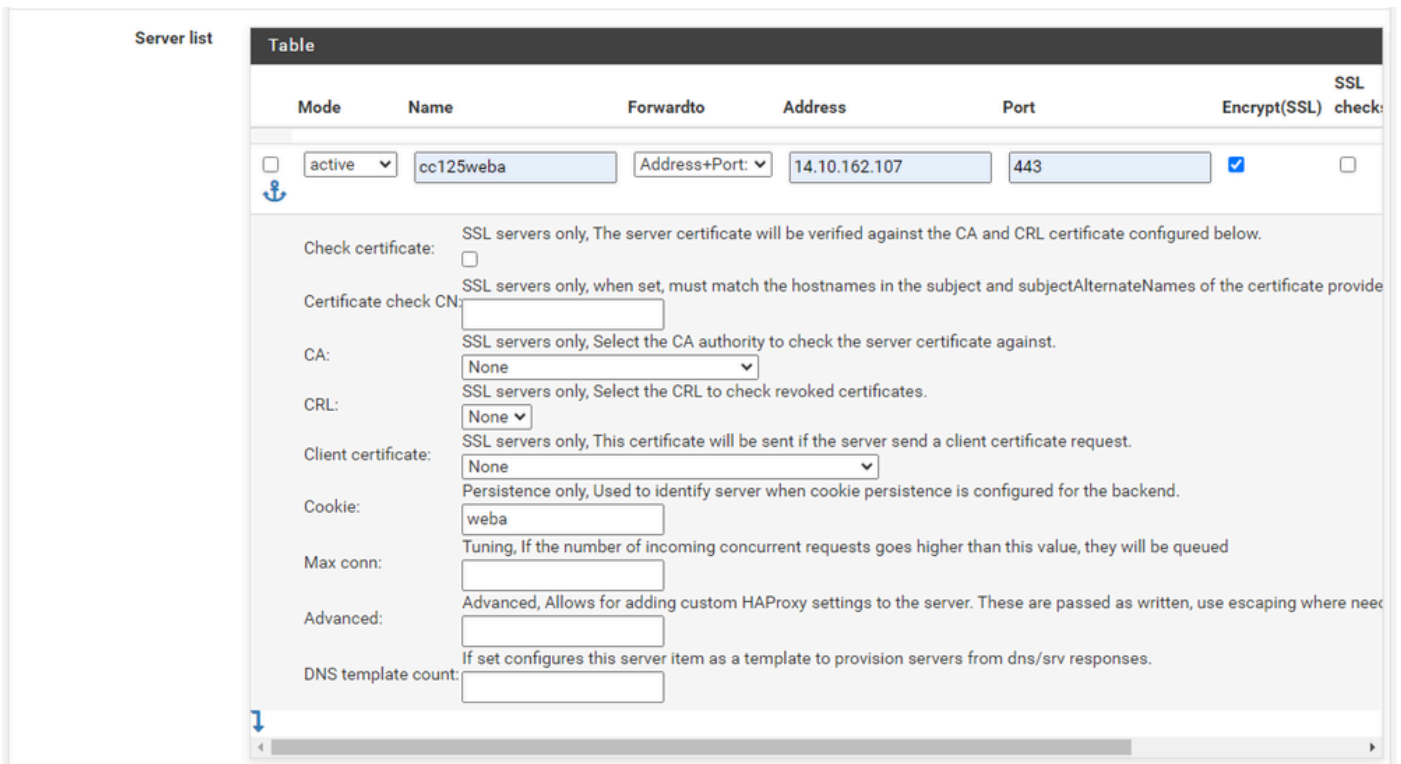
Wählen Sie die Schaltfläche Hinzufügen aus.



pfSense-GUI - HAProxy-Backend-Start

Geben Sie einen Namen für das Backend an.

Wählen Sie den Abwärtspfeil aus, um der Serverliste den ersten Server hinzuzufügen.



Backend - Serverliste

Geben Sie einen Namen für den Server an. Dies muss nicht mit dem tatsächlichen Servernamen übereinstimmen. Dies ist der Name, der auf der Statistikseite angezeigt wird.

Geben Sie die Adresse für den Server an. Diese kann entweder als IP-Adresse für FQDN konfiguriert werden.

Geben Sie den Port an, mit dem die Verbindung hergestellt werden soll. Dies muss Port 443 für ECE sein.

Aktivieren Sie das Kontrollkästchen Verschlüsselung (SSL).

Geben Sie im Feld Cookie einen Wert ein. Dies ist der Inhalt des Session Stickiness-Cookies und muss innerhalb des Backends eindeutig sein.

Wenn der erste Server konfiguriert wurde, klicken Sie auf den Pfeil nach unten, um weitere Webserver in der Umgebung zu konfigurieren.

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 - Lastenausgleich

Konfigurieren Sie die Load Balancing-Optionen.

Für ECE-Server muss dies auf "Least Connections" (Geringste Verbindungen) gesetzt werden.

Access control lists and actions	
Timeout / retry settings	
Connection timeout	<input type="text" value="60000"/> The time (in milliseconds) we give up if the connection does not complete within (default 30000).
Server timeout	<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).
Retries	<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.
Health checking	
Health check method	<input type="text" value="HTTP"/> <div style="border: 1px dashed red; padding: 2px; font-size: small;"> HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers). </div>
Check frequency	<input type="text"/> <small>milliseconds</small> 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	<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>
Url used by http check requests.	<input type="text" value="/system/web/view/platform/common/login/root.jsp?partitionId=1"/> <small>Defaults to / if left blank.</small>
Http check version	<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: HTTP/1.1\r\nHost:\ www Also some hosts might require an accept parameter like this: HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</small>

HAProxy-Backend - Integritätsprüfung

Zugriffskontrolllisten werden in dieser Konfiguration nicht verwendet.

Timeout-/Wiederholungseinstellungen können bei der Standardkonfiguration belassen werden.

Konfigurieren Sie den Abschnitt Health (Diagnose).

1. Integritätsprüfungsmethode: HTTP
2. Prüffrequenz: Lassen Sie das Feld leer, um die Standardeinstellung für jede Sekunde zu verwenden.
3. Protokollprüfungen: Wählen Sie diese Option aus, um Statusänderungen in die Protokolle zu schreiben.
4. HTTP-Prüfmethode: Wählen Sie GET aus der Liste aus.
5. URL wird von HTTP-Prüfanforderungen verwendet.: Geben Sie für einen ECE-Server `/system/web/view/platform/common/login/root.jsp?partitionId=1` ein.
6. HTTP-Prüfversion: Eingabe, `HTTP/1.1\r\nHost:\ {fqdn_of_server}`

Stellen Sie sicher, dass Sie nach dem letzten umgekehrten Schrägstrich, aber vor dem FQDN des Servers ein Leerzeichen einfügen.

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-Persistenz

Lassen Sie die Agentenüberprüfungen deaktiviert.

Cookie-Persistenz konfigurieren:

1. Cookie Enabled (Cookie aktiviert): Wählen Sie diese Option aus, um die Cookie-basierte Persistenz zu aktivieren.
2. Cookie-Name: Geben Sie einen Namen für das Cookie an.
3. Cookie Mode (Cookie-Modus): Wählen Sie Insert (Einfügen) aus dem Dropdown-Feld aus.
4. Lassen Sie die übrigen Optionen unverändert.

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

Die übrigen Abschnitte des Back-End-Konfigurationsformulars können in den Standardeinstellungen belassen werden.

Wenn Sie HSTS konfigurieren möchten, konfigurieren Sie in diesem Abschnitt einen Timeout-Wert. ECE fügt auch ein HSTS-Cookie ein, sodass diese Konfiguration redundant ist.

Wählen Sie Speichern aus.

Konfigurieren von HAProxy Frontend

Wechseln Sie in das Frontend-Menü.

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 Add Frontend

Wählen Sie die Schaltfläche Hinzufügen

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"/>	
<p>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.</p>						

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

Geben Sie einen Namen für das Front-End an.

Geben Sie eine Beschreibung an, um das Frontend später zu identifizieren.

In der Tabelle Externe Adresse:

1. Listen address: Wählen Sie den VIP aus, den Sie für diese Website erstellt haben.
2. Port: Geben Sie 443 ein.
3. SSL Offloading: Wählen Sie diese Option, damit ein Sitzungscookie eingefügt werden kann.

Lassen Sie das Feld Max. Verbindungen leer.

Stellen Sie sicher, dass Type (Typ) als http / https(offloading) ausgewählt ist.

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 will 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 - Standard-Backend-Auswahl

Die einfachste Konfiguration besteht darin, ein Standard-Backend aus dem Dropdown-Menü auszuwählen. Dies kann ausgewählt werden, wenn der VIP eine Website hostet.

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	C/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 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	
<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-Backend - ACL Advanced

Wie in der Abbildung dargestellt, können ACLs verwendet werden, um ein einzelnes Frontend auf mehrere Backends umzuleiten, je nach den Bedingungen.

Sie sehen, dass die ACL prüft, ob der Host in der Anfrage mit einem Namen und einer Portnummer beginnt. Oder einfach nur mit dem Namen. Auf dieser Grundlage wird ein spezielles Backend verwendet.

Dies ist bei ECE nicht üblich.

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 EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES

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

HAProxy Frontend - Zertifikatbindung

Wählen Sie im Abschnitt "SSL Offloading" (SSL-Auslagerung) das Zertifikat aus, das für die Verwendung mit dieser Site erstellt wurde. Bei diesem Zertifikat muss es sich um ein Serverzertifikat handeln.

Wählen Sie die Option Add ACL (ACL hinzufügen) for certificate Subject Alternative Names aus.

Sie können die übrigen Optionen auf ihren Standardwerten belassen.

Wählen Sie am Ende des Formulars Speichern aus.

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

Add Delete Save

HAProxy - Konfiguration anwenden

Wählen Sie Apply Changes (Änderungen anwenden) aus, um die Frontend- und Backend-Änderungen an der aktuellen Konfiguration zu übernehmen.

Herzlichen Glückwunsch, Sie haben die Einrichtung und Konfiguration von pfSense abgeschlossen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.