

Configurazione di pfSense Community Load Balancer per ECE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Installa pfSense](#)

[Panoramica della soluzione](#)

[Preparazione](#)

[Installazione](#)

[Configurazione della rete](#)

[Completa impostazione iniziale](#)

[Configurazione delle impostazioni di amministrazione di base](#)

[Aggiungi pacchetti richiesti](#)

[Configura certificati](#)

[Aggiungi IP virtuali](#)

[Configurare il firewall](#)

[Configura HAProxy](#)

[Nozioni base su HAProxy](#)

[Impostazioni iniziali HAProxy](#)

[Configura back-end HAProxy](#)

[Configura front-end HAProxy](#)

Introduzione

In questo documento viene descritto come configurare pfSense Community Edition come servizio di bilanciamento del carico per Enterprise Chat and Email (ECE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ECE 12.x
- pfSense Community Edition

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Installa pfSense

Panoramica della soluzione

pfSense Community Edition è un prodotto multifunzione che fornisce un firewall, un servizio di bilanciamento del carico, uno scanner di sicurezza e molti altri servizi in un unico server. pfSense è costruito su Free BSD e ha requisiti hardware minimi. Il load balancer è un'implementazione di HAProxy ed è disponibile un'interfaccia grafica di facile utilizzo per configurare il prodotto.

È possibile utilizzare questo servizio di bilanciamento del carico sia con ECE che con il portale di gestione del contact center (CCMP). In questo documento viene descritto come configurare pfSense per ECE.

Preparazione

Passaggio 1. Scarica il software pfSense

Utilizzare il [sito Web pfSense](#) per scaricare l'immagine del programma di installazione ISO.

Passaggio 2. Configura macchina virtuale

Configurare una VM con i requisiti minimi:

- CPU compatibile con amd64 (x86-64) a 64 bit
- 1 GB o più di RAM
- Unità disco da 8 GB o più (SSD, HDD, ecc.)
- Una o più schede di rete compatibili
- Unità USB avviabile o unità ottica ad alta capacità (DVD o BD) per installazione iniziale

Per un'installazione in laboratorio, è necessaria una sola interfaccia di rete (NIC). L'accessorio può essere eseguito in diversi modi, ma il modo più semplice consiste nell'utilizzare una singola scheda NIC, detta anche modalità a braccio singolo. In modalità one-arm, c'è una singola interfaccia che comunica alla rete. Si tratta di un metodo semplice e adeguato per essere utilizzato in laboratorio, ma non è il più sicuro.

Un modo più sicuro di configurare l'accessorio consiste nel disporre di almeno due schede NIC. Una NIC è l'interfaccia WAN e comunica direttamente con l'Internet pubblico. La seconda scheda NIC è l'interfaccia LAN e comunica con la rete aziendale interna. È inoltre possibile aggiungere ulteriori interfacce per comunicare con diverse parti della rete che hanno regole di sicurezza e firewall diverse. Ad esempio, è possibile avere una scheda NIC connessa alla rete pubblica Internet, una connessa alla rete DMZ in cui si trovano tutti i server Web accessibili esternamente e una terza scheda NIC connessa alla rete aziendale. Ciò consente agli utenti interni ed esterni di accedere in modo sicuro allo stesso set di server Web conservati in una DMZ. Prima dell'implementazione, accertarsi di comprendere le implicazioni di sicurezza di qualsiasi progetto. Consultare un tecnico addetto alla sicurezza per garantire che vengano seguite le best practice per l'implementazione specifica.

Installazione

Passaggio 1. Montare l'ISO sulla VM

Passaggio 2. Accendere la VM e seguire le istruzioni per l'installazione.

Fare riferimento a questo [documento](#) per istruzioni dettagliate.

Configurazione della rete

Per continuare la configurazione, è necessario assegnare gli indirizzi IP all'accessorio.



Nota: nel documento viene mostrato un accessorio configurato in modalità monolama.

Passaggio 1. Configurazione delle VLAN

Per il supporto di VLAN, rispondere alla prima domanda con y. In caso contrario, rispondere n.

Passaggio 2. Assegnazione interfaccia WAN

L'interfaccia WAN è il lato non sicuro dell'accessorio in modalità a due bracci e l'unica interfaccia in modalità a un braccio. Quando richiesto, immettere il nome dell'interfaccia.

Passaggio 3. Assegnazione dell'interfaccia LAN

L'interfaccia LAN è il lato sicuro dell'accessorio in modalità a due bracci. Se necessario, immettere il nome dell'interfaccia quando richiesto.

Passaggio 4. Assegnazione di altre interfacce

Configurare tutte le altre interfacce necessarie per l'installazione specifica. Si tratta di opzioni facoltative e non comuni.

Passaggio 5. Assegna indirizzo IP all'interfaccia di gestione

Se la rete supporta DHCP, l'indirizzo IP assegnato verrà visualizzato nella schermata della console.

```
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:
```

Console pfSense

Se non è stato assegnato alcun indirizzo o se si desidera assegnare un indirizzo specifico, effettuare le seguenti operazioni.

1. Scegliere l'opzione 2 dal menu della console.
2. Rispondere n per disabilitare DHCP.
3. Immettere l'indirizzo IPv4 per l'interfaccia WAN.
4. Immettere la netmask nel numero di bit. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0)
5. Immettere l'indirizzo del gateway per l'interfaccia WAN.
6. Se si desidera che il gateway sia quello predefinito per l'accessorio, rispondere y al prompt del gateway, altrimenti rispondere n.
7. Se desiderato, configurare la scheda NIC per IPv6.
8. Disabilitare il server DHCP sull'interfaccia.
9. Rispondere y per abilitare HTTP sul protocollo webConfigurator. Questa opzione verrà utilizzata nei passaggi successivi.

Si riceve quindi la conferma che le impostazioni sono state aggiornate.

```
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/

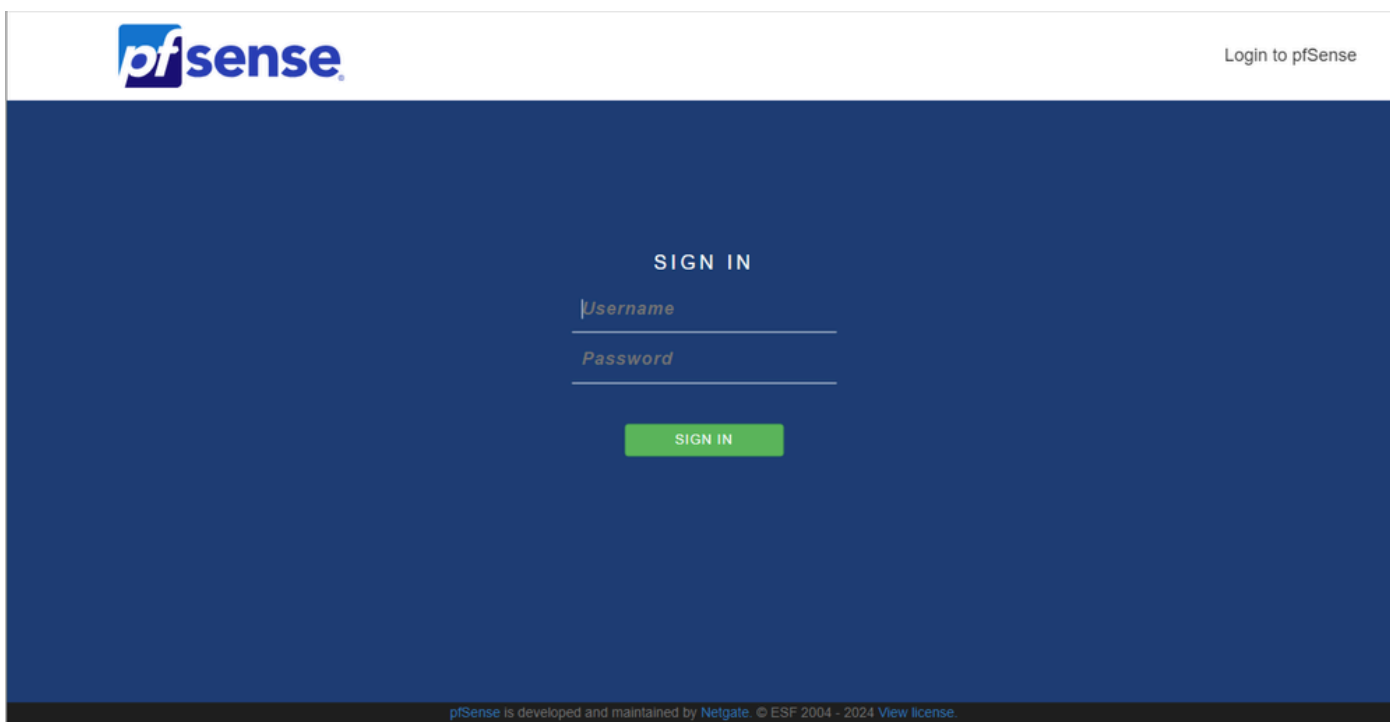
Press <ENTER> to continue. █
```

Conferma pfSense

Completa impostazione iniziale

Passaggio 1. Aprire un browser Web e selezionare: http://<indirizzo_ip_accessorio>

 Nota: inizialmente è necessario utilizzare HTTP e non HTTPS.

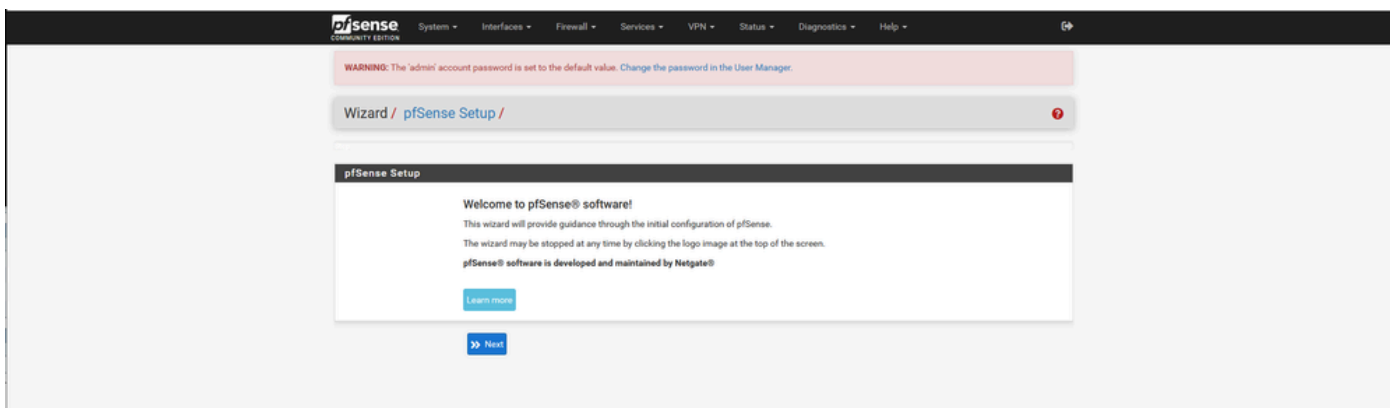


Accesso amministratore pfSense

Passaggio 2. Accedere con il login predefinito di admin / pfSense

Passaggio 3. Completare la configurazione iniziale

Fare clic su Avanti nelle prime due schermate.



Installazione guidata di pfSense - 1

Specificare il nome dell'host, il nome di dominio e le informazioni sul server DNS.

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

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / **pfSense Setup** / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

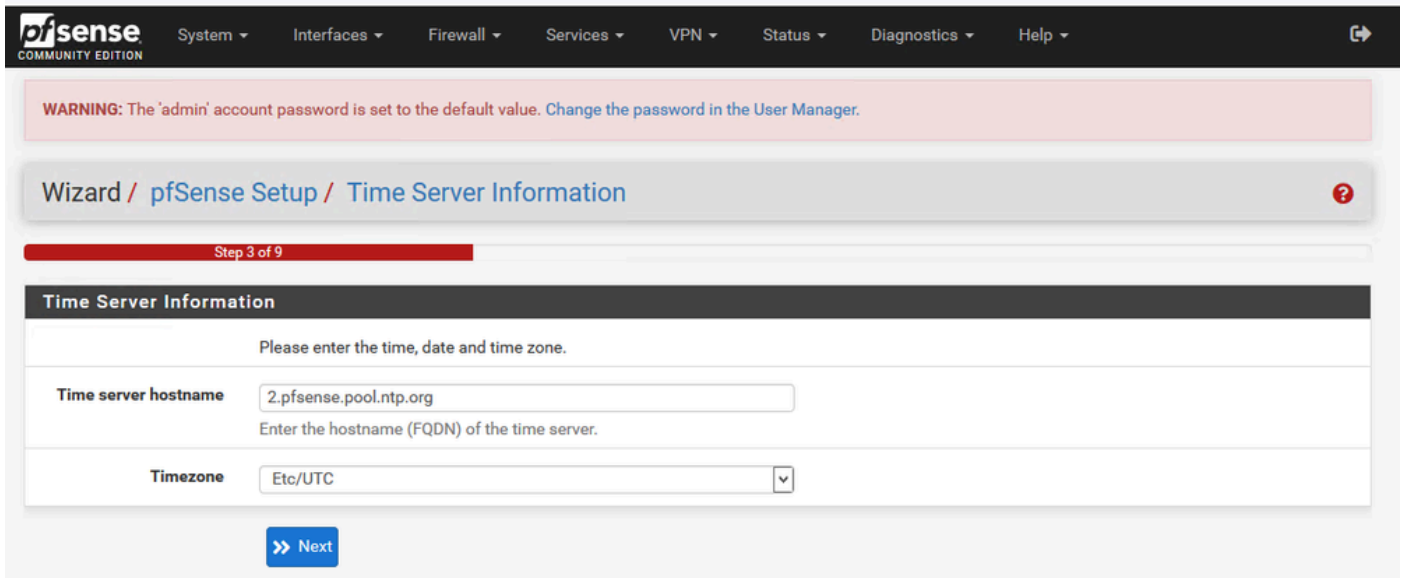
Hostname	<input type="text" value="pfSense"/>
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
Domain	<input type="text" value="home.arpa"/>
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

[» Next](#)

Installazione guidata di pfSense - 2

Convalidare le informazioni sull'indirizzo IP. Se all'inizio è stato scelto DHCP, è possibile modificarlo ora.

Fornire il nome host del Time server NTP e selezionare il fuso orario corretto nell'elenco a discesa.



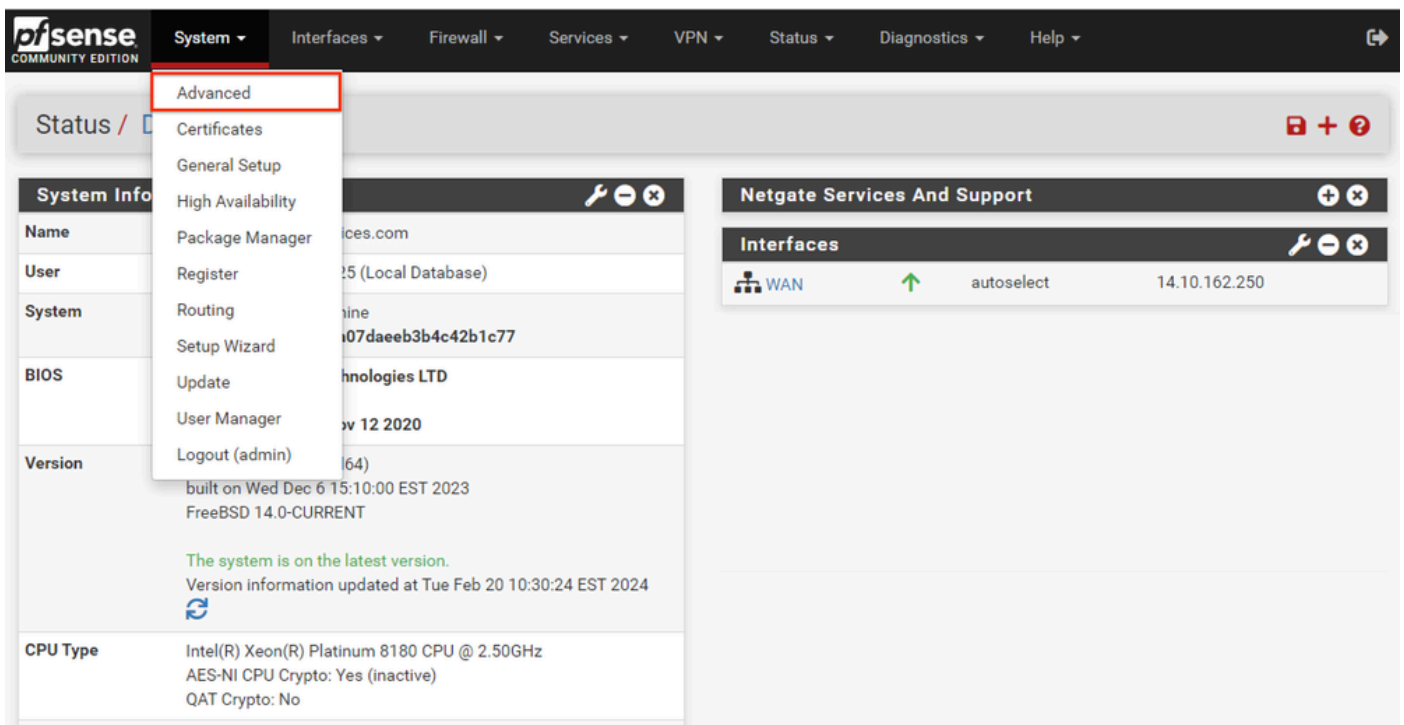
Installazione guidata di pfSense - 3

Continuare l'installazione guidata fino alla fine. La GUI dell'interfaccia si riavvia e l'utente viene reindirizzato al nuovo URL una volta completato.

Configurazione delle impostazioni di amministrazione di base

Passaggio 1. Accedere all'interfaccia di amministrazione

Passaggio 2. Selezionare Avanzate dal menu a discesa Sistema.



pfSense GUI - Menu a discesa Amministratore


Passaggio 3. Aggiorna impostazioni WebConfigurator

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>

GUI pfSense - Configurazione amministratore

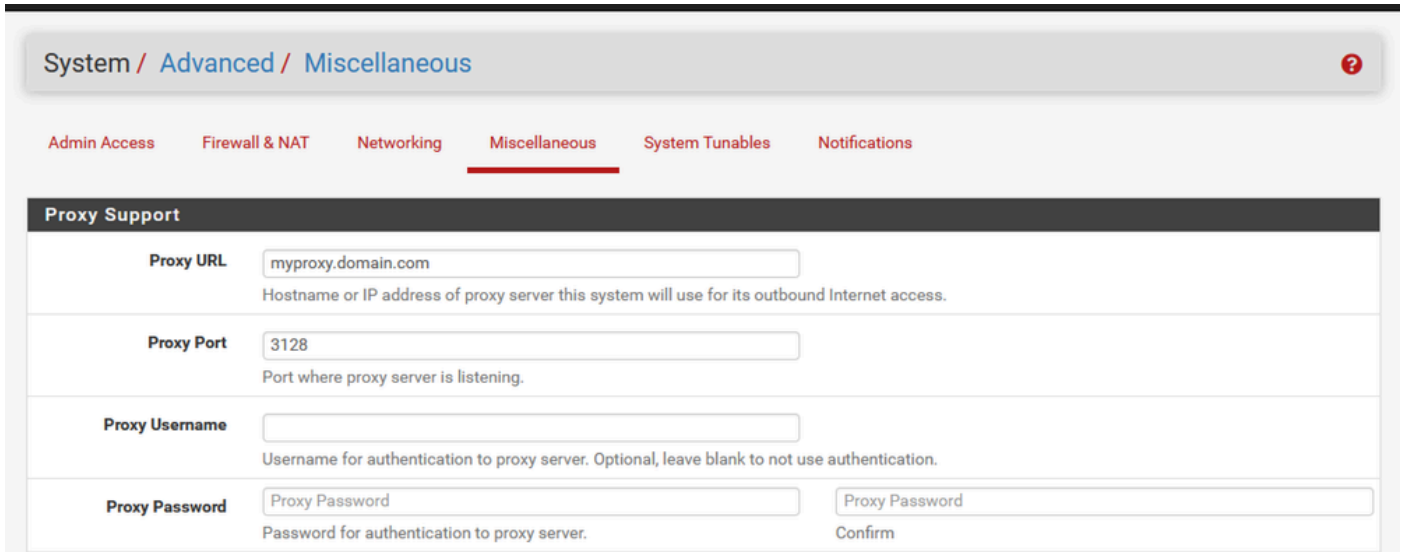
1. Selezionare il protocollo HTTPS (SSL/TLS).
2. In questo momento, lasciare il certificato SSL/TLS sul certificato autofirmato.
3. Modificare la porta TCP su una porta diversa dalla porta 443 per proteggere meglio l'interfaccia e prevenire problemi di sovrapposizione delle porte.
4. Selezionare l'opzione di reindirizzamento WebGUI per disabilitare l'interfaccia di amministrazione sulla porta 80.
5. Selezionare l'opzione di imposizione Browser HTTP_REFERER.

6. Abilitare Secure Shell selezionando l'opzione Abilita Secure Shell.

 Nota: selezionare il pulsante Salva prima di procedere. L'utente viene quindi reindirizzato al nuovo collegamento https.

Passaggio 4. Configurare il server proxy, se necessario

Se necessario, configurare le informazioni sul proxy nella scheda Varie. Per completare l'installazione e la configurazione, l'accessorio deve disporre di accesso a Internet.



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 - Configurazione proxy

 Nota: assicurarsi di selezionare il pulsante Salva dopo aver apportato le modifiche.

Aggiungi pacchetti richiesti

Passaggio 1. Selezionare Sistema > Gestione pacchetti

Passaggio 2. Seleziona pacchetti disponibili

 Nota: il caricamento di tutti i pacchetti disponibili può richiedere alcuni minuti. Se si verifica il timeout, verificare che i server DNS siano configurati correttamente. Spesso il riavvio dell'accessorio risolve il problema della connettività Internet.

System / Package Manager / Available Packages ?

Installed Packages Available Packages

Search -

Search term Both Search Clear

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

Name	Version	Description	
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: 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 - Elenco pacchetti

Passaggio 3. Trova e installa i pacchetti richiesti

1. haproxy
2. Open-VM-Tools

 Nota: non selezionare il pacchetto haproxy-devel.

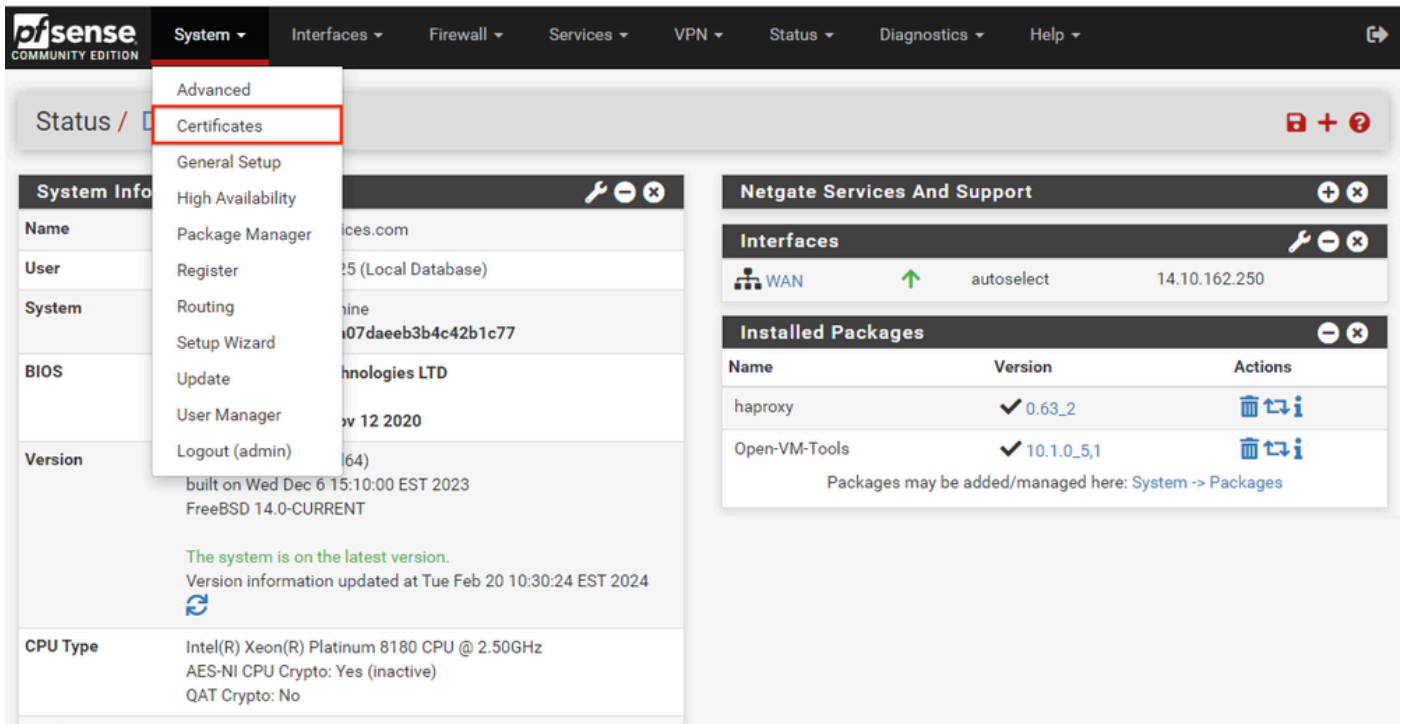
Configura certificati

pfSense può creare un certificato autofirmato o integrarsi con una CA pubblica, una CA interna, oppure può fungere da CA e rilasciare certificati firmati dalla CA. In questa guida vengono illustrati i passaggi da integrare con una CA interna.

Prima di iniziare questa sezione, assicurarsi di avere a disposizione questi elementi.

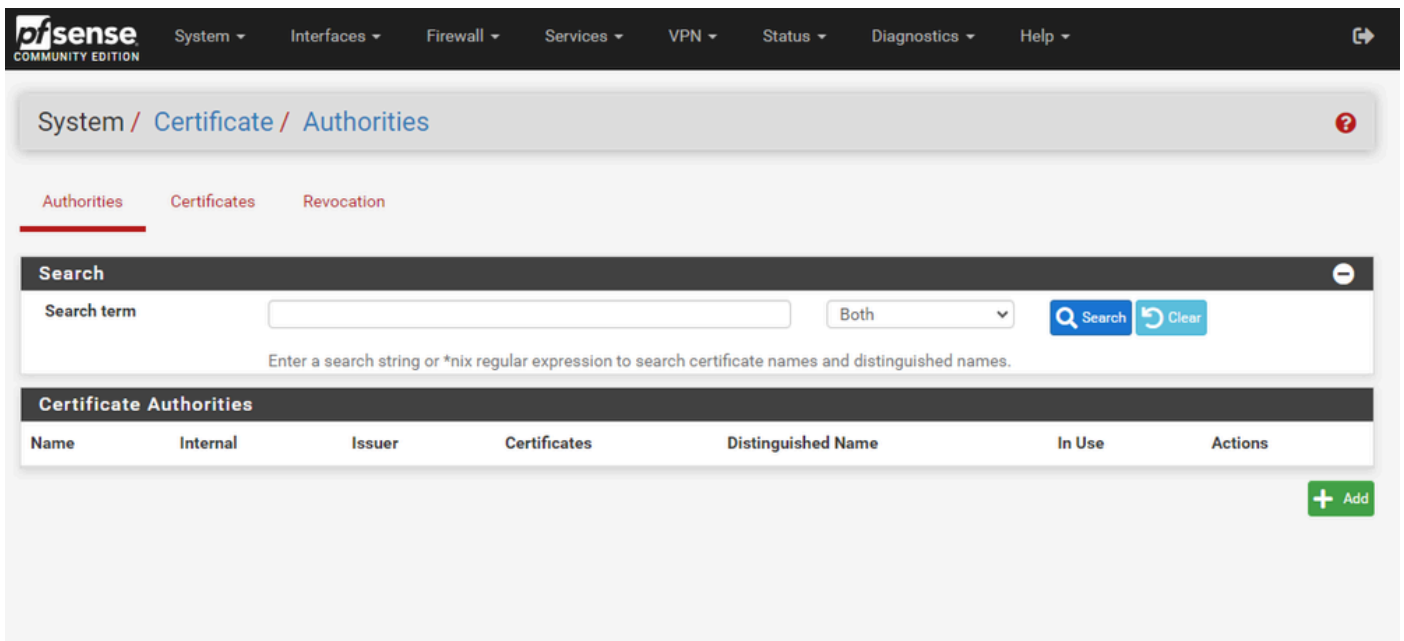
1. Certificato radice per CA salvato in formato PEM o con codifica Base 64.
2. Tutti i certificati intermedi (talvolta denominati emettere) per CA salvati come formato PEM o con codifica Base 64.

Passaggio 1. Selezionare Certificati dal menu a discesa Sistema.



pfSense GUI - Elenco a discesa dei certificati

Passaggio 2. Importa certificato radice CA



pfSense GUI - Elenco certificati CA

Selezionare il pulsante Aggiungi.

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 - Importazione CA

Come mostrato nell'immagine:

1. Fornire un nome univoco e descrittivo
2. Selezionare Importa un'autorità di certificazione esistente dall'elenco a discesa Metodo.
3. Verificare che le caselle di controllo Archivio attendibile e Numero di serie casuale siano selezionate.
4. Incollare l'intero certificato nella casella di testo Dati certificato. Assicurarsi di includere dalle righe —BEGIN CERTIFICATE— e —END CERTIFICATE—.
5. Selezionare Salva.
6. Verificare che il certificato sia stato importato come mostrato nell'immagine.

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 - Elenco CA

Passaggio 3. Importa certificato intermedio CA

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

System / Certificate / Authorities / Edit ?

Authorities Certificates Revocation

Create / Edit CA

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

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

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

Existing Certificate Authority

Certificate data
Paste a certificate in X.509 PEM format here.

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

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

PfSense GUI - Importazione intermedia CA

Ripetere i passaggi per importare il certificato CA radice per importare il certificato CA intermedio.

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

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

Certificate Authorities

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

Interfaccia utente di pfSense - Collegamenti CA

Esaminare le Autorità di certificazione per verificare che il certificato intermedio sia correttamente concatenato al certificato radice, come mostrato nell'immagine.

Passaggio 4. Creare ed esportare un CSR per il sito Web con carico bilanciato

In questa sezione vengono descritti i passaggi necessari per creare un CSR, esportare il CSR e quindi importare il certificato firmato. Se si dispone già di un certificato in formato PFX, è possibile importare questo certificato. Consultare la documentazione di pfSense per questi passaggi.

1. Selezionare il menu Certificati, quindi selezionare il pulsante Aggiungi/Firma.

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term Both

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

Certificates

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

2. Completare il modulo di richiesta di firma del certificato.

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

GUI pfSense - Creazione CSR

- Metodo: selezionare Crea richiesta di firma certificato dall'elenco a discesa.
- Nome descrittivo: fornire un nome per il certificato
- Tipo di chiave e algoritmo digest: rivedere per verificare che soddisfino i requisiti
- Nome comune: fornire il sito Web del nome di dominio completo
- Fornire le restanti informazioni sul certificato necessarie per l'ambiente in uso

Certificate Attributes

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

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

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


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

Alternative Names
 Type Value

Add SAN Row

GUI pfSense - CSR avanzata

- Tipo di certificato: selezionare Certificato server nell'elenco a discesa.
- Nomi alternativi: fornire tutti i nomi alternativi soggetto (SAN) necessari per l'implementazione.

 Nota: il nome comune viene aggiunto automaticamente al campo SAN. È sufficiente aggiungere altri nomi.

Selezionare Salva una volta che tutti i campi sono corretti.

3. Esportare il file CSR in un file.

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

System / Certificates / Certificates









Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

Search

Search term Both










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

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

Selezionare il pulsante Esporta per salvare il CSR, quindi firmarlo con la CA. Una volta ottenuto il certificato firmato, salvarlo come file PEM o Base-64 per completare il processo.

4. Importare il certificato firmato.

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. A search bar is present with a search term input, a dropdown menu set to 'Both', and buttons for Search and Clear. Below the search bar, a table lists certificates. The table has columns for Name, Issuer, Distinguished Name, In Use, and Actions. Two certificates are listed: 'GUI default (65cced5b25159) Server Certificate' and 'ece-web-2024'. The 'ece-web-2024' certificate is highlighted with a red box around its 'Actions' column, which contains a pencil icon (Edit/Import) and other icons. A green '+ Add/Sign' button is located at the bottom right of the table.

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		   

Selezionare l'icona Matita per importare il certificato firmato.

5. Incollare i dati del certificato nel modulo.

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-----
 MIIDvDCCAQCAQAwZcHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
 MAKGA1UEBHMCMVVMxZzAVBgNVBAGTDk5cncRoIENhcm9saW5hMR8wHQYDVQQUHExZS
 ZXNlYXJjaCBUcm1hbmdsZSBQYXJrMR0wGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
 YzESMBAGA1UECzMjQ2LzY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
 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 - Importazione certificati

Selezionare Aggiorna per salvare il certificato.

6. Esaminare i dati del certificato per accertarsi che siano corretti.

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.

Certificates

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

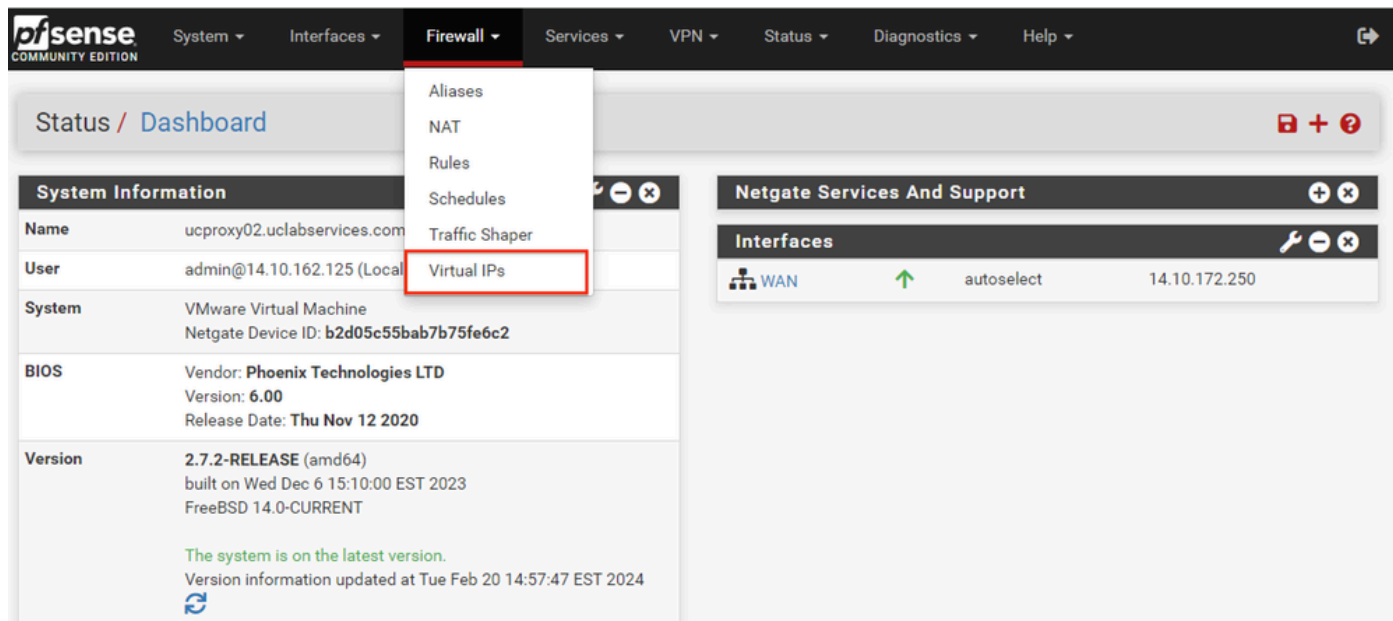
pfSense GUI - Elenco certificati

7. Ripetere questa procedura se si desidera ospitare più siti su questo pfSense.

Aggiungi IP virtuali

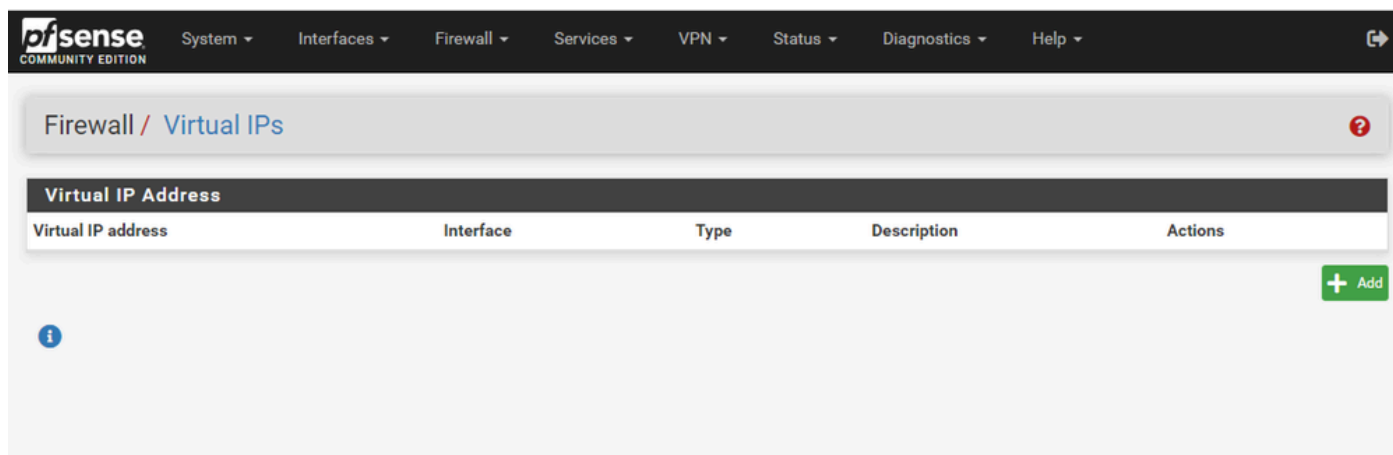
È necessario almeno un indirizzo IP per ospitare i siti Web in pfSense. In pfSense ciò viene fatto con gli IP virtuali (VIP).

Passaggio 1. Selezionare IP virtuali dall'elenco a discesa Firewall



GUI pfSense - Elenco a discesa VIP

Passaggio 2. Selezionare il pulsante Aggiungi



GUI pfSense - Pagina iniziale VIP

Passaggio 3. Fornire informazioni sull'indirizzo

[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).

GUI pfSense - Configurazione VIP

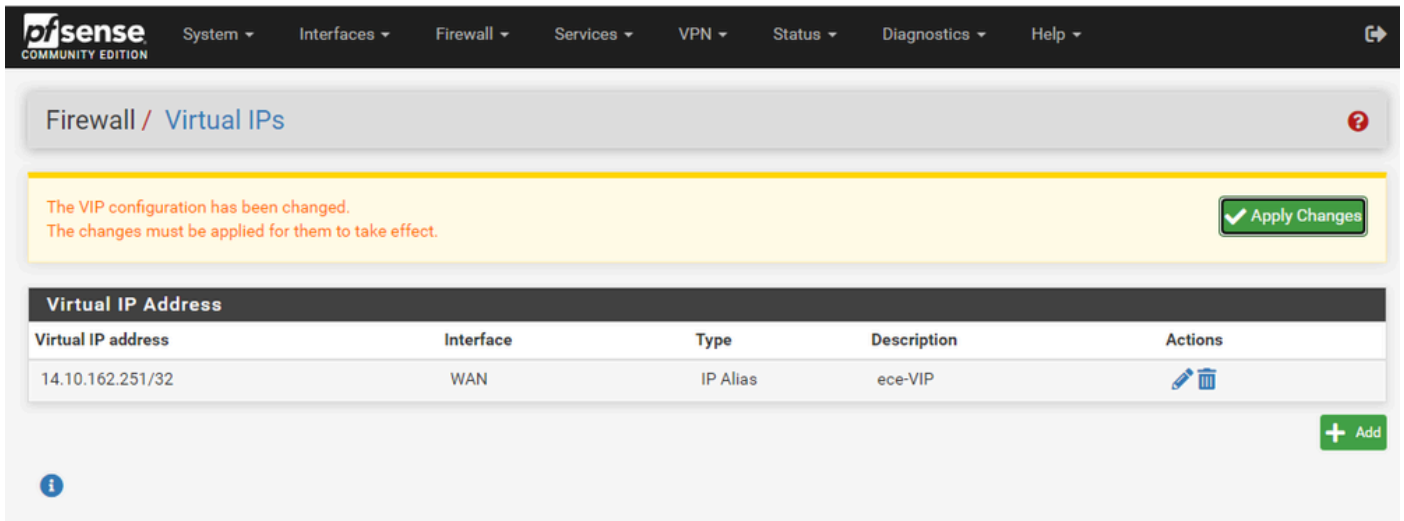
Utilizzare le informazioni per aggiungere un VIP.

- Tipo: Seleziona alias IP
- Interfaccia: selezionare l'interfaccia per l'indirizzo IP da trasmettere
- Indirizzi: immettere l'indirizzo IP
- Maschera indirizzo: per gli indirizzi IP utilizzati per il bilanciamento del carico, la maschera deve essere una /32
- Descrizione: fornire un breve testo per semplificare la comprensione della configurazione in un secondo momento

Selezionare Salva per eseguire il commit della modifica.

Ripetere questa operazione per ciascun indirizzo IP richiesto per la configurazione.

Passaggio 4. Applica configurazione



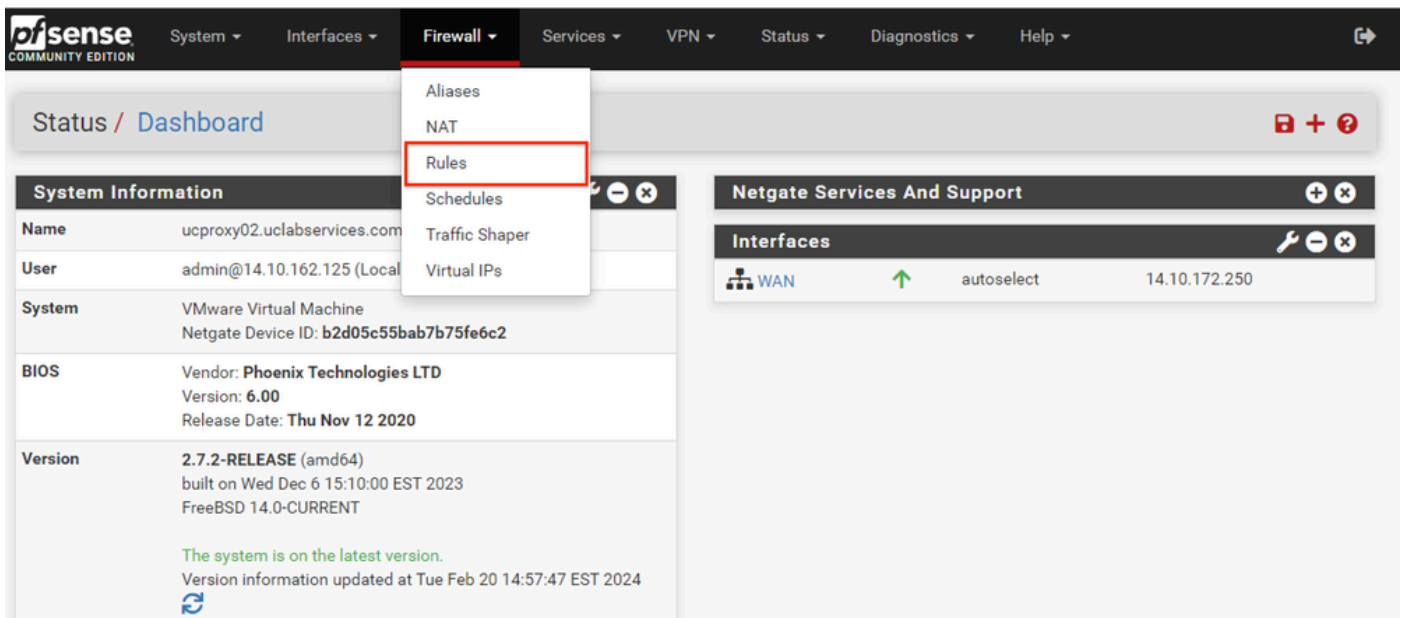
GUI pfSense - Elenco VIP

Selezionare il pulsante Applica modifiche dopo aver aggiunto tutti i VIP.

Configurare il firewall

pfSense dispone di un firewall incorporato. Il set di regole predefinito è molto limitato. Prima che l'accessorio venga messo in produzione, è necessario creare una policy firewall completa.

Passaggio 1. Selezionare Regole dall'elenco a discesa Firewall



pfSense GUI - Elenco a discesa delle regole del firewall

Passaggio 2. Selezionare uno dei pulsanti Aggiungi

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

pfSense GUI - Elenco regole firewall

Si noti che un pulsante consente di aggiungere la nuova regola sopra la riga selezionata, mentre l'altro consente di aggiungere la regola sotto la regola selezionata. Entrambi i pulsanti possono essere utilizzati per la prima regola.

Passaggio 3. Crea regola firewall per consentire il traffico sulla porta 443 per l'indirizzo IP

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

Firewall / Rules / Edit

Edit Firewall Rule

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

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

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

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

Protocol ▾
 Choose which IP protocol this rule should match.

Source

Source Invert match ▾ / ▾

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

Destination

Destination Invert match ▾ / ▾

Destination Port Range ▾ ▾ ▾
 From Custom To Custom

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

Extra Options

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

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

Advanced Options

GUI pfSense - Configurazione regola passaggio firewall

Utilizzare le informazioni per creare la regola.

- Azione: Seleziona superamento
- Interfaccia: scegliere l'interfaccia a cui si applica la regola
- Famiglia di indirizzi e protocollo: selezionare la voce appropriata
- Origine: lasciare selezionata l'opzione Qualsiasi
- Destinazione: selezionare Indirizzo o Alias dall'elenco a discesa Destinazione, quindi immettere l'indirizzo IP a cui si applica la regola.
- Intervallo porte di destinazione: selezionare, HTTPS (443) nell'elenco a discesa Da e A
- Registra: selezionare la casella di controllo per registrare tutti i pacchetti che soddisfano questa regola per l'accounting

- Descrizione: fornire il testo per fare riferimento alla regola in seguito

Selezionare Salva.

Passaggio 4. Crea una regola firewall per indirizzare tutto il resto del traffico a pfSense

Selezionare il pulsante Aggiungi per inserire la regola sotto quella appena creata.

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](#)

GUI pfSense - Configurazione regola di eliminazione firewall

- Azione: Seleziona blocco

- Interfaccia: scegliere l'interfaccia a cui si applica la regola
- Famiglia di indirizzi e protocollo: selezionare la voce appropriata
- Origine: lasciare selezionata l'opzione Qualsiasi
- Destinazione: lascia selezionato come Qualsiasi
- Registra: selezionare la casella di controllo per registrare tutti i pacchetti che soddisfano questa regola per l'accounting
- Descrizione: fornire il testo per fare riferimento alla regola in seguito

Selezionare Salva.

Passaggio 5. Esaminare le regole e verificare che la regola di blocco si trovi nella parte inferiore

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

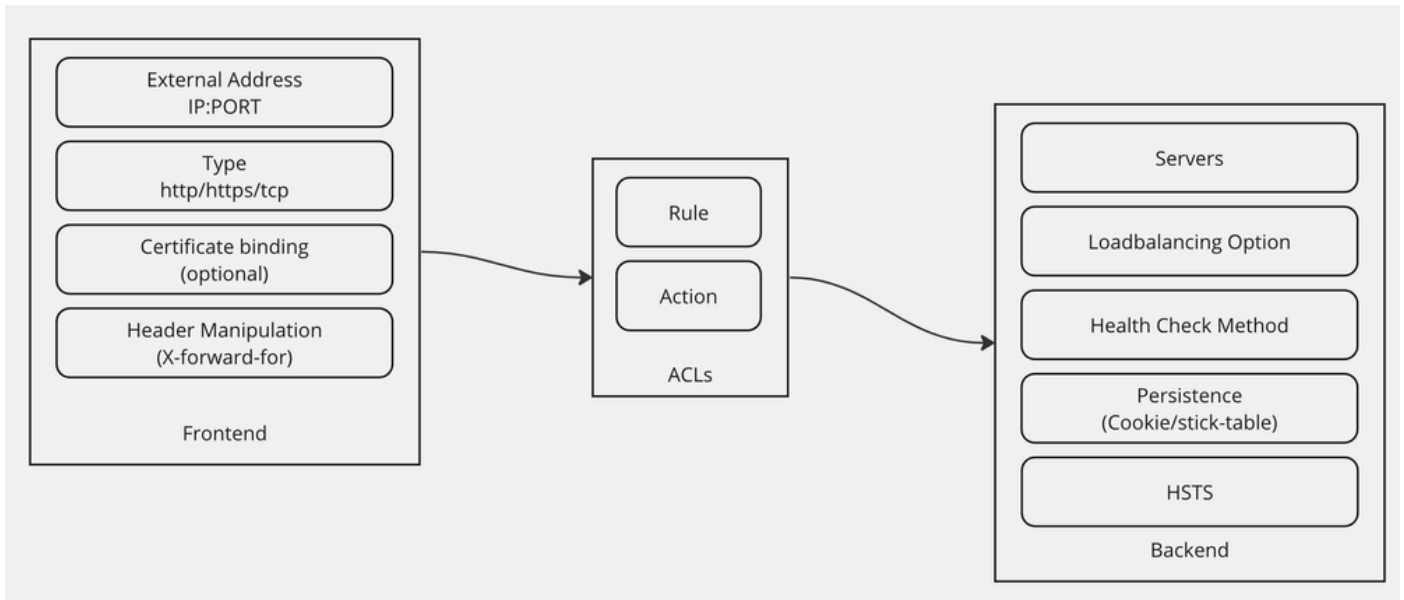
pfSense GUI - Elenco regole firewall

Se necessario, trascinare le regole per ordinarle.

Selezionare Applica modifiche una volta che le regole del firewall sono nell'ordine richiesto per l'ambiente.

Configura HAProxy

Nozioni base su HAProxy



Nozioni base su HAProxy

HAProxy viene implementato con un modello Frontend/Backend.

Il front-end definisce il lato del proxy con cui i clienti comunicano.

Il front-end è costituito da una combinazione di IP e porta, associazione di certificati e può implementare alcune modifiche all'intestazione.

Il back-end definisce il lato del proxy che comunica con i server Web fisici.

Il back-end definisce i server e le porte effettivi, il metodo di bilanciamento del carico per l'assegnazione iniziale, i controlli di integrità e la persistenza.

Un front-end sa con cosa comunicare il back-end tramite un back-end dedicato o utilizzando gli ACL.

Gli ACL possono creare regole diverse in modo che un dato front-end possa comunicare con back-end diversi a seconda delle esigenze.

Impostazioni iniziali HAProxy

Passaggio 1. Selezionare HAProxy dall'elenco a discesa Servizi.

The screenshot shows the pfSense Community Edition interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Services' menu is open, listing various services such as Auto Config Backup, Captive Portal, DHCP Relay, and HAProxy, which is highlighted with a red box. 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 support resources.

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

Netgate Services And Support

Contract type: **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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

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

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

GUI pfSense - Elenco a discesa HAProxy

Passaggio 2. Configurare le impostazioni di base

Services / HAProxy / Settings

Settings Frontend Backend Files Stats Stats FS Templates

General settings

Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections per process.

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

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

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

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

Number of threads to start per process

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

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

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

Reload stop behaviour

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

Carp monitor

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

Stats tab, 'internal' stats port

Internal stats port EXAMPLE: 2200

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

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

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

GUI pfSense - Impostazioni principali HAProxy

Selezionare la casella di controllo Abilita HAProxy.

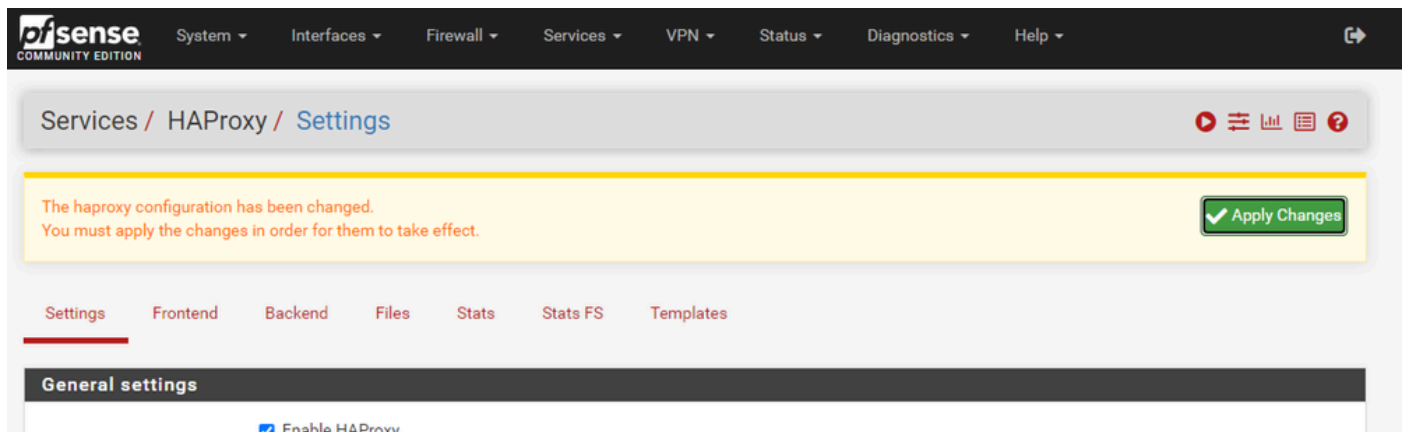
Immettere un valore per Numero massimo di connessioni. Per ulteriori informazioni sulla memoria necessaria, vedere il grafico in questa sezione.

Immettere un valore per la porta Internal Stats. Questa porta viene utilizzata per visualizzare le statistiche HAProxy sull'accessorio, ma non viene esposta all'esterno dell'accessorio.


Immettere un valore per la frequenza di aggiornamento dello stato Interno.

Esaminare la configurazione rimanente e aggiornarla in base alle esigenze dell'ambiente.

Selezionare Salva.

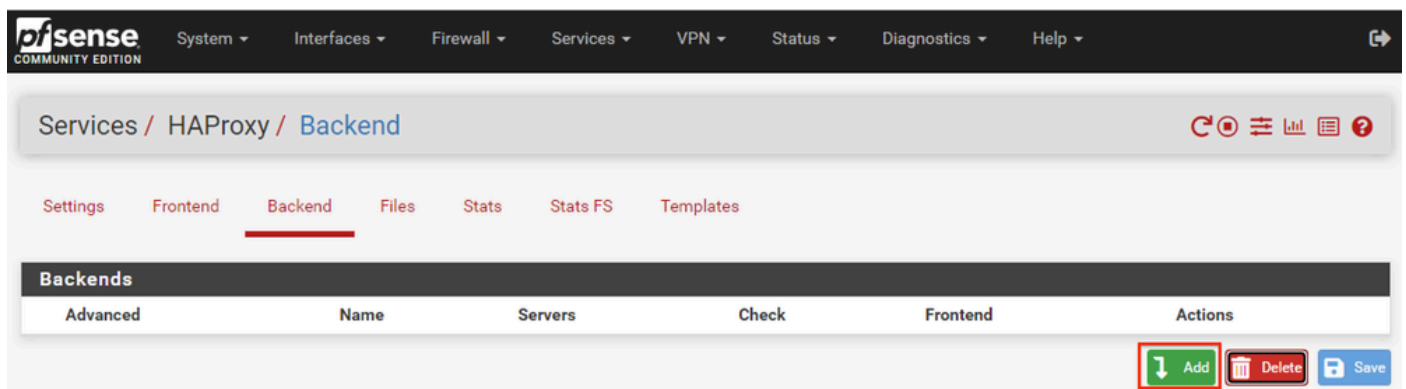


GUI pfSense - Modifiche applicazione HAProxy

 Nota: le modifiche alla configurazione non vengono rese attive fino a quando non si seleziona il pulsante Applica modifiche. È possibile apportare più modifiche alla configurazione e applicarle tutte contemporaneamente. Non è necessario applicare la configurazione per utilizzarla in un'altra sezione.

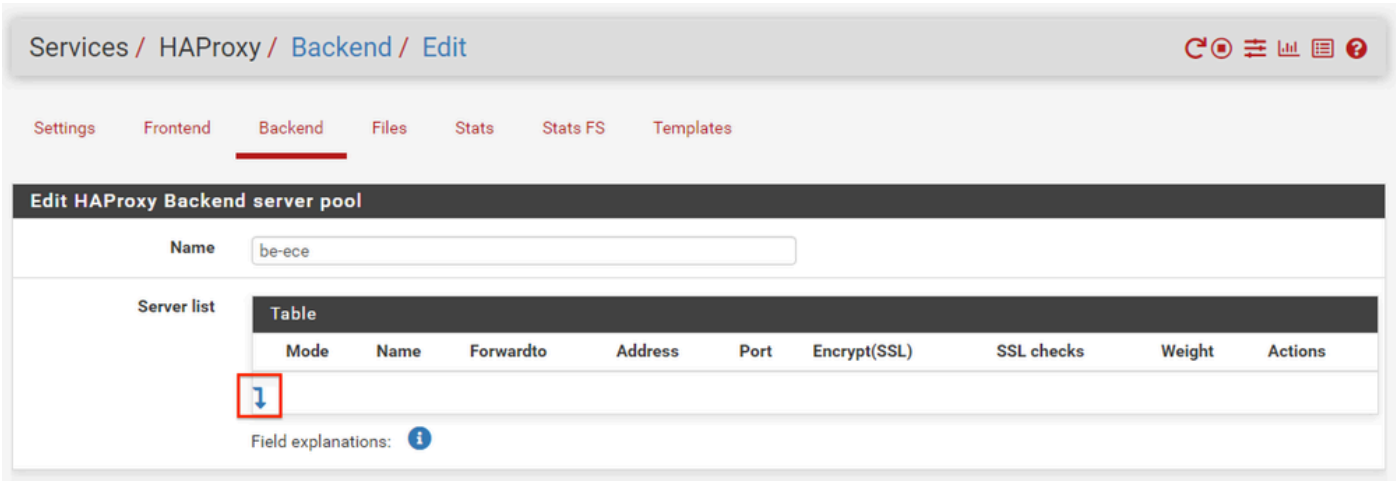
Configura back-end HAProxy

Iniziare con il back-end. Il motivo è che il front-end deve fare riferimento a un back-end. Assicurarsi di aver selezionato il menu Back-end.



pfSense GUI - HAProxy Add Backend

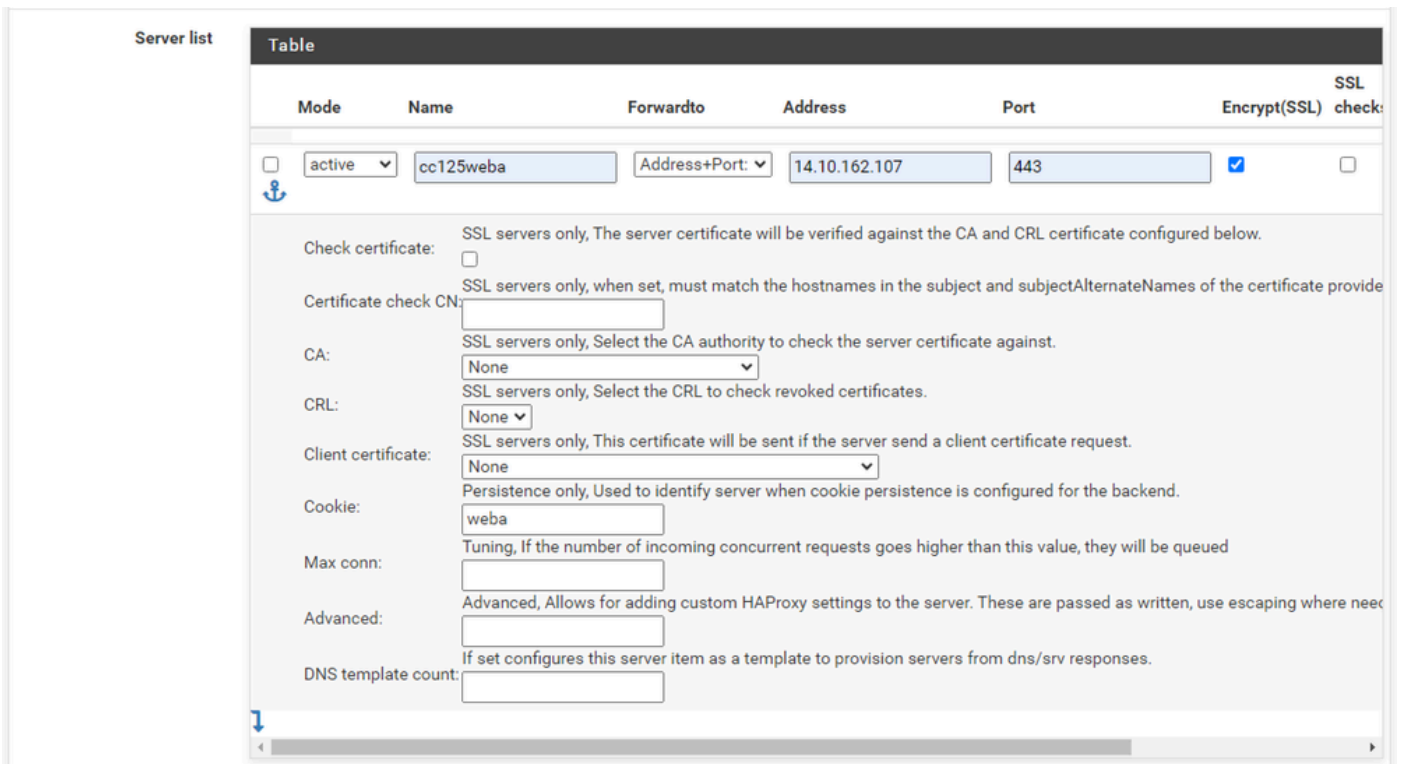
Selezionare il pulsante Aggiungi.



GUI pfSense - Avvio back-end HAProxy

Specificare un nome per il back-end.

Selezionare la freccia rivolta verso il basso per aggiungere il primo server all'elenco Server



Back-end - Elenco server

Specificare un nome per fare riferimento al server. Non è necessario che corrisponda al nome effettivo del server. Questo è il nome visualizzato nella pagina Statistiche.

Specificare l'indirizzo del server. Può essere configurato come indirizzo IP per il nome di dominio completo.

Specificare la porta a cui connettersi. Deve essere la porta 443 per ECE.

Selezionare la casella di controllo Encrypt(SSL).

Specificare un valore nel campo Cookie. Questo è il contenuto del cookie di persistenza della sessione e deve essere univoco all'interno del back-end.

Dopo aver configurato il primo server, selezionare la freccia rivolta verso il basso per configurare altri server Web nell'ambiente.

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.

Back-end HAProxy - Bilanciamento del carico

Configurare le opzioni di bilanciamento del carico.

Per i server ECE, deve essere impostato su Connessioni minime (Least Connections).

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>

Back-end HAProxy - Verifica dello stato

Gli elenchi di controllo di accesso non vengono utilizzati in questa configurazione.

È possibile lasciare le impostazioni di timeout/ripetizione dei tentativi nella configurazione predefinita.

Configurare la sezione di controllo dello stato.

1. Metodo di verifica dello stato: HTTP
2. Frequenza di controllo: lasciare vuoto per utilizzare il valore predefinito ogni 1 secondo.
3. Controlli registro: selezionare questa opzione per scrivere nei registri eventuali modifiche relative allo stato.
4. Metodo di controllo HTTP: selezionare GET dall'elenco.
5. Url utilizzato dalle richieste di controllo HTTP.: Per un server ECE immettere
 /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Versione controllo HTTP: Invio, HTTP/1.1\r\nHost:\ {fqdn_of_server}

Assicurarsi di includere uno spazio dopo la barra rovesciata finale ma prima del nome di dominio completo del server.

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.

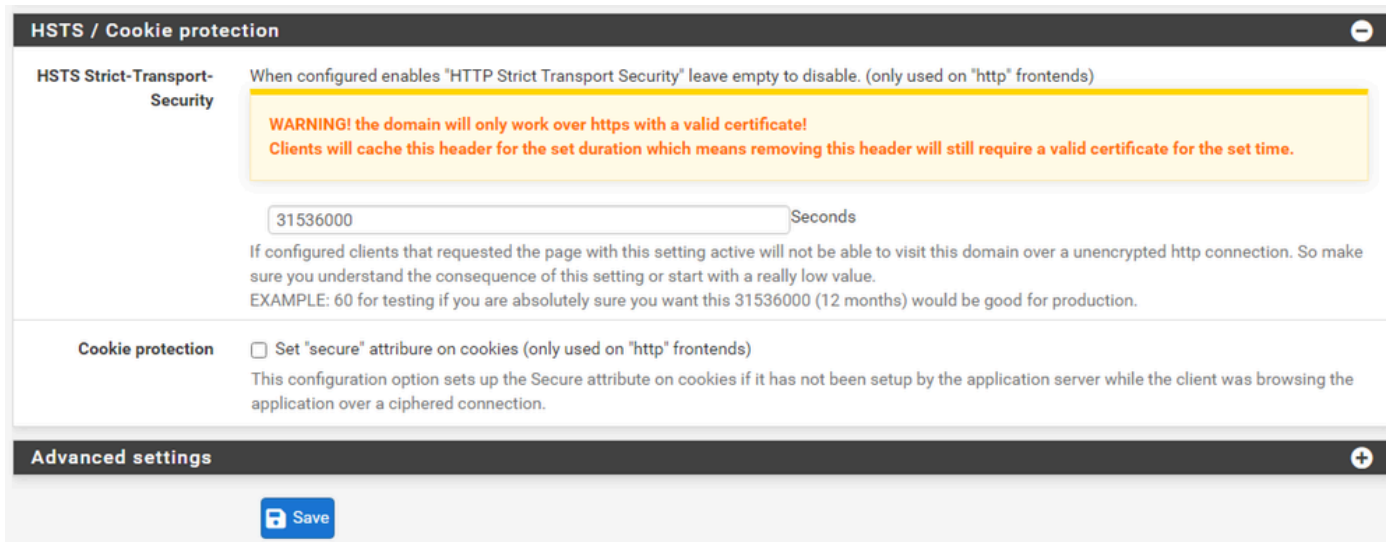
Mail to
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

Backend HAProxy - Persistenza cookie

Non selezionare i controlli dell'agente.

Configura persistenza cookie:

1. Cookie abilitato: selezionare questa opzione per abilitare la persistenza basata su cookie.
2. Nome cookie: specificare un nome per il cookie.
3. Modalità cookie: selezionare Inserisci dall'elenco a discesa.
4. Lasciate deselezionate le altre opzioni.



Backend HAProxy - HSTS

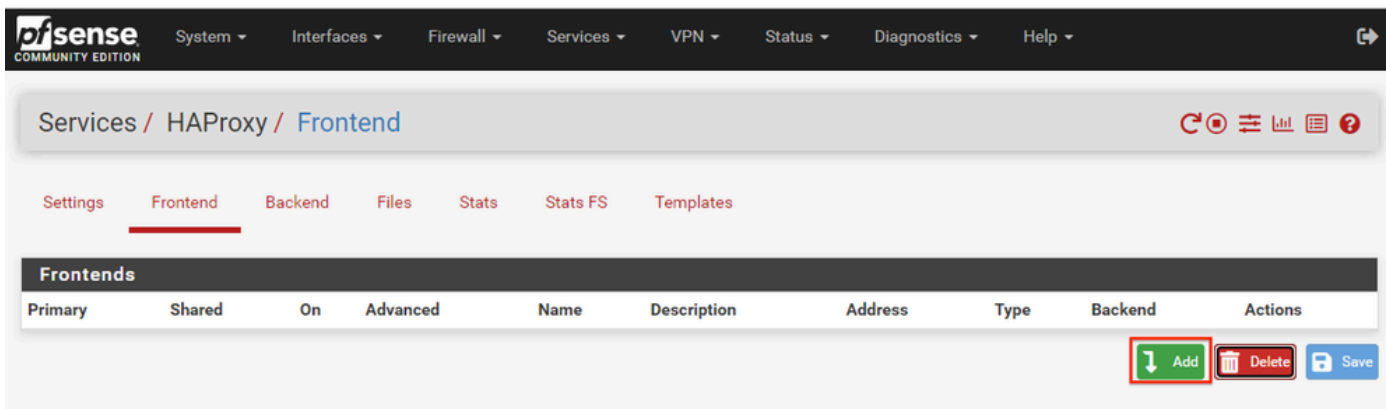
Le sezioni rimanenti del modulo di configurazione back-end possono essere lasciate nelle impostazioni predefinite.

Se si desidera configurare l'host, configurare un valore di timeout in questa sezione. Il modulo ECE inserisce anche un cookie HSTS in modo che questa configurazione sia ridondante.

Selezionare, Salva.

Configura front-end HAProxy

Passate al menu Frontend.



pfSense GUI - HAProxy Add Frontend

Selezionare il pulsante Aggiungi

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 - installazione front-end

Specificare un nome per il front-end.

Fornire una descrizione per identificare il front-end in un secondo momento.

Nella tabella Indirizzi esterni:

1. Indirizzo di ascolto: selezionare l'indirizzo VIP creato per il sito Web.
2. Port: immettere 443.
3. Offload SSL: selezionare questa opzione per consentire l'inserimento di un cookie di sessione.

Lasciare vuote le connessioni Max.

Assicurarsi che il Tipo sia selezionato come 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

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

Backend HAProxy - Selezione back-end predefinita

La configurazione più semplice consiste nel scegliere un back-end di default dall'elenco a discesa. Questa opzione può essere selezionata quando l'indirizzo VIP ospita un singolo sito Web.

Default backend, access control lists and actions

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

Table							
	Name	Expression	CS	Not	Value	Actions	
<input type="checkbox"/>		ccmpWS	Host starts with:	no	no	ccmp.uclabservices.com:8085	
<input type="checkbox"/>		ccmpSSL	Host starts with:	no	no	ccmp.uclabservices.com	

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

Name	Expression	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 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".

Backend HAProxy - ACL - Avanzate

Come mostrato nell'immagine, gli ACL possono essere usati per reindirizzare un singolo front-end a più back-end in base alle condizioni.

È possibile notare che l'ACL verifica se l'host nella richiesta inizia con un nome e un numero di porta o semplicemente con il nome. In base a questo viene utilizzato un back-end specifico.

Ciò non è comune con l'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 ocp responses for easy certificate validation by the client.
A cron job wil update the ocp response every hour.

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

Table	
Certificates	Actions
<input type="checkbox"/> Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)	
<input type="checkbox"/> Add ACL for certificate Subject Alternative Names.	

Advanced ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: force-ssl3, force-tls10 force-tls11 force-tls12 no-ssl3 no-tls10 no-tls11 no-tls12 no-tls-tickets
Example: no-ssl3 ciphers 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

Frontend HAProxy - Associazione certificato

Nella sezione Offload SSL selezionare il certificato creato per l'utilizzo con il sito. Il certificato deve essere un certificato server.

Selezionare l'opzione Add ACL for certificate Subject Alternative Names (Aggiungi ACL per nomi alternativi soggetto certificato).

È possibile lasciare le opzioni rimanenti ai valori predefiniti.

Selezionare, Salva alla fine del modulo.

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 - Applica configurazione

Selezionare Applica modifiche per eseguire il commit delle modifiche di front-end e back-end nella configurazione in esecuzione.

Congratulazioni, hai completato l'installazione e la configurazione di pfSense.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).