

Configurar o Balanceador de Carga da Comunidade pfSense para ECE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instalar o pfSense](#)

[Visão geral da solução](#)

[Preparação](#)

[Instalação](#)

[Instalação de rede](#)

[Concluir configuração inicial](#)

[Definir Configurações Básicas de Administração](#)

[Adicionar Pacotes Necessários](#)

[Configurar certificados](#)

[Adicionar IPs Virtuais](#)

[Configurar firewall](#)

[Configurar HAProxy](#)

[Conceitos do HAProxy](#)

[Configurações iniciais do HAProxy](#)

[Configurar o back-end do HAProxy](#)

[Configurar front-end do HAProxy](#)

Introdução

Este documento descreve as etapas para instalar e configurar o pfSense Community Edition como um Balanceador de Carga para Bate-papo e E-mail Corporativos (ECE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ECE 12.x
- Edição de comunidade do pfSense

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instalar o pfSense

Visão geral da solução

O pfSense Community Edition é um produto multifuncional que fornece um Firewall, Balanceador de Carga, Scanner de Segurança e muitos outros serviços em um único servidor. O pfSense é construído no Free BSD e tem requisitos mínimos de hardware. O Balanceador de carga é uma implementação do HAProxy e uma GUI fácil de usar é fornecida para configurar o produto.

Você pode usar esse balanceador de carga com o ECE e o Contact Center Management Portal (CCMP). Este documento fornece as etapas para configurar o pfSense para ECE.

Preparação

Etapa 1. Download do software pfSense

Use o [site do pfSense](#) para fazer o download da imagem do instalador iso.

Etapa 2. Configurar VM

Configure uma VM com os requisitos mínimos:

- CPU compatível com amd64 (x86-64) de 64 bits
- 1 GB ou mais de RAM
- Unidade de disco de 8 GB ou mais (SSD, HDD, etc.)
- Uma ou mais placas de rede compatíveis
- Unidade USB inicializável ou unidade óptica de alta capacidade (DVD ou BD) para instalação inicial

Para a instalação em laboratório, somente uma interface de rede (NIC) é necessária. Há várias maneiras de executar o dispositivo, mas a mais fácil é com uma única placa de rede, também chamada de modo de um braço. No modo de um braço, há uma única interface que se comunica com a rede. Embora essa seja uma maneira fácil e adequada para um laboratório, não é a maneira mais segura.

Uma maneira mais segura de configurar o dispositivo é ter pelo menos duas NICs. Uma placa de rede é a interface WAN e se comunica diretamente com a Internet pública. A segunda placa de rede é a interface LAN e se comunica com a rede corporativa interna. Você também pode adicionar outras interfaces para se comunicar com várias partes da rede que têm regras de segurança e firewall diferentes. Por exemplo, você pode ter uma placa de rede conectada à Internet pública, uma conectada à rede DMZ, onde estão todos os servidores Web acessíveis externamente, e uma terceira placa de rede conectada à rede corporativa. Isso permite que usuários internos e externos acessem com segurança o mesmo conjunto de servidores Web mantidos em uma DMZ. Assegure-se de que o compreenda as implicações de segurança de qualquer projeto antes da implementação. Consulte um engenheiro de segurança para garantir que as melhores práticas sejam seguidas para sua implementação específica.

Instalação

Etapa 1. Montar o ISO na VM

Etapa 2. Ligue a VM e siga os avisos para instalar.

Consulte este [documento](#) para obter instruções passo a passo.

Instalação de rede

Você deve atribuir endereços IP ao equipamento para continuar a configuração.



Observação: este documento mostra um dispositivo configurado no modo one-arm.

Etapa 1. Configurar VLANs

Se você precisar de suporte para VLAN, responda y à primeira pergunta. Caso contrário, responda n.

Etapa 2. Atribuir interface WAN

A interface WAN é o lado não seguro do dispositivo no modo de dois braços e a única interface no modo de um braço. Digite o nome da interface quando solicitado.

Etapa 3. Atribuir a interface LAN

A interface LAN é o lado seguro do dispositivo no modo de dois braços. Se necessário, insira o nome da interface quando solicitado.

Etapa 4. Atribuir qualquer outra interface

Configure quaisquer outras interfaces necessárias para sua instalação específica. Elas são opcionais e não comuns.

Etapa 5. Atribuir endereço IP à interface de gerenciamento

Se a sua rede suportar DHCP, o endereço IP atribuído será mostrado na tela do 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 não houver endereço atribuído ou se você quiser atribuir um endereço específico, execute estas etapas.

1. Escolha a opção 2 no menu do console.
2. Responda n para desativar o DHCP.
3. Insira o endereço IPv4 da interface WAN.
4. Insira a máscara de rede em contagens de bits. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0.0)
5. Digite o endereço de gateway para a interface WAN.
6. Se quiser que esse gateway seja o gateway padrão do equipamento, responda y ao prompt do gateway, caso contrário, responda n.
7. Configure a placa de rede para IPv6, se desejado.
8. Desative o servidor DHCP na interface.
9. Responda y para ativar o HTTP no protocolo webConfigurator. Isso é usado nas próximas etapas.

Em seguida, você receberá uma confirmação de que as configurações foram atualizadas.


```
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/

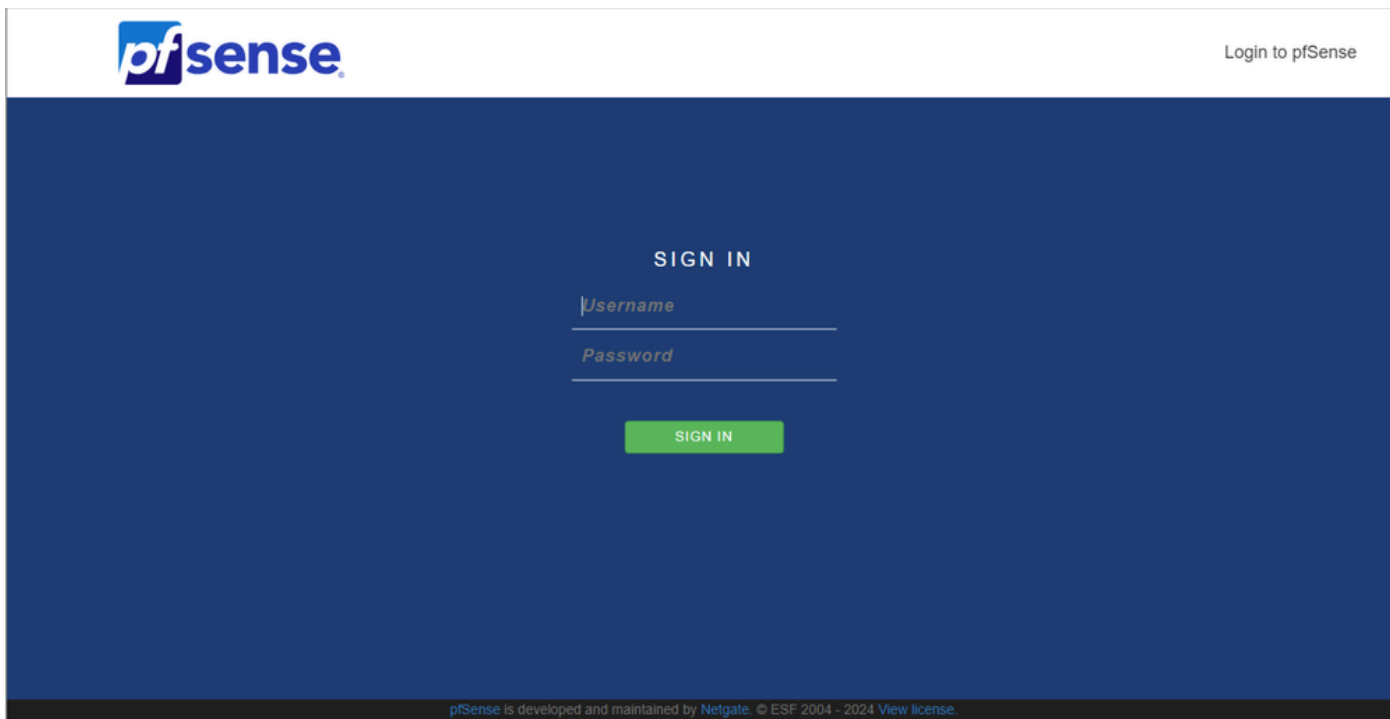
Press <ENTER> to continue. █
```

Confirmação do pfSense

Concluir configuração inicial

Etapa 1. Abra um navegador da Web e navegue até: http://<ip_address_of_appliance>

 Observação: você deve usar HTTP e não HTTPS inicialmente.

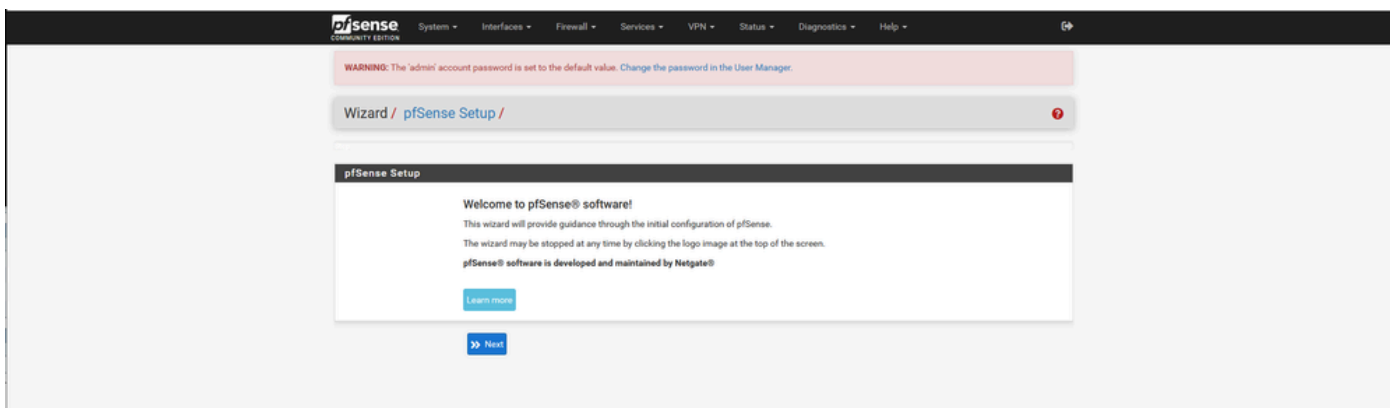


Logon do administrador do pfSense

Etapa 2. Faça login com o login padrão admin / pfSense

Etapa 3. Concluir a configuração inicial

Clique em Next (Avançar) nas duas primeiras telas.



Assistente para configuração do pfSense - 1

Forneça o nome do host, o nome do domínio e as informações do servidor DNS.

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

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

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

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

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

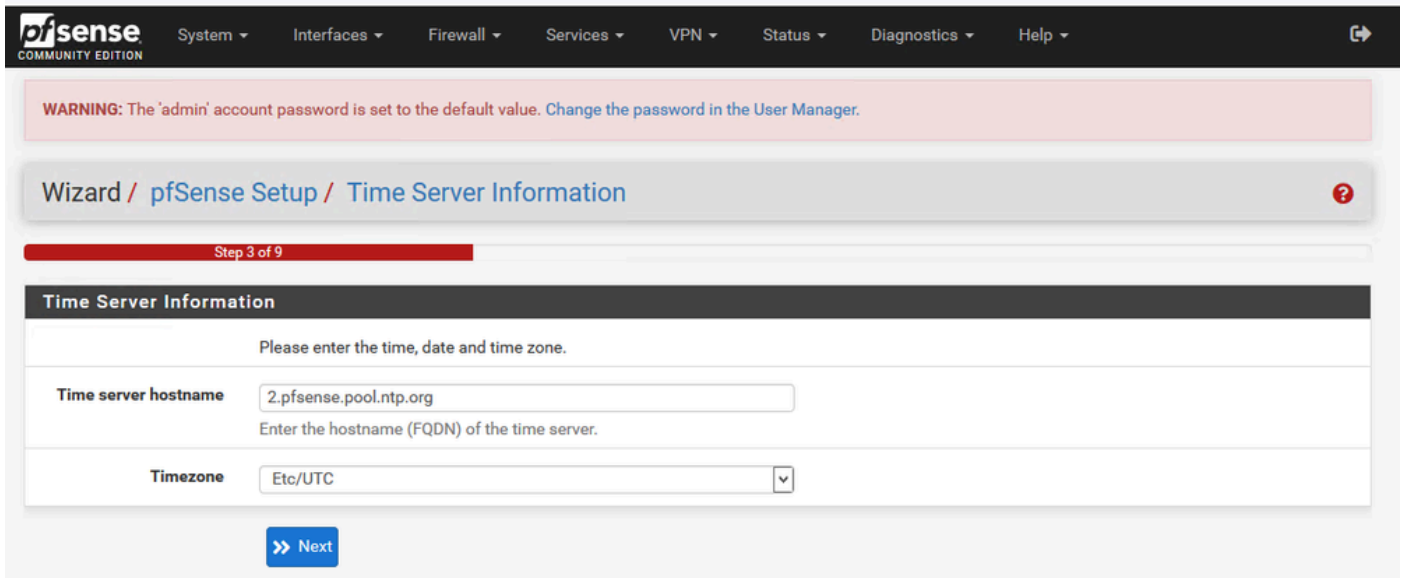
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

Assistente para configuração do pfSense - 2

Valide as informações de endereço IP. Se você escolheu DHCP inicialmente, poderá alterá-lo agora.

Forneça o nome de host do servidor de horário NTP e selecione o fuso horário correto na lista suspensa.



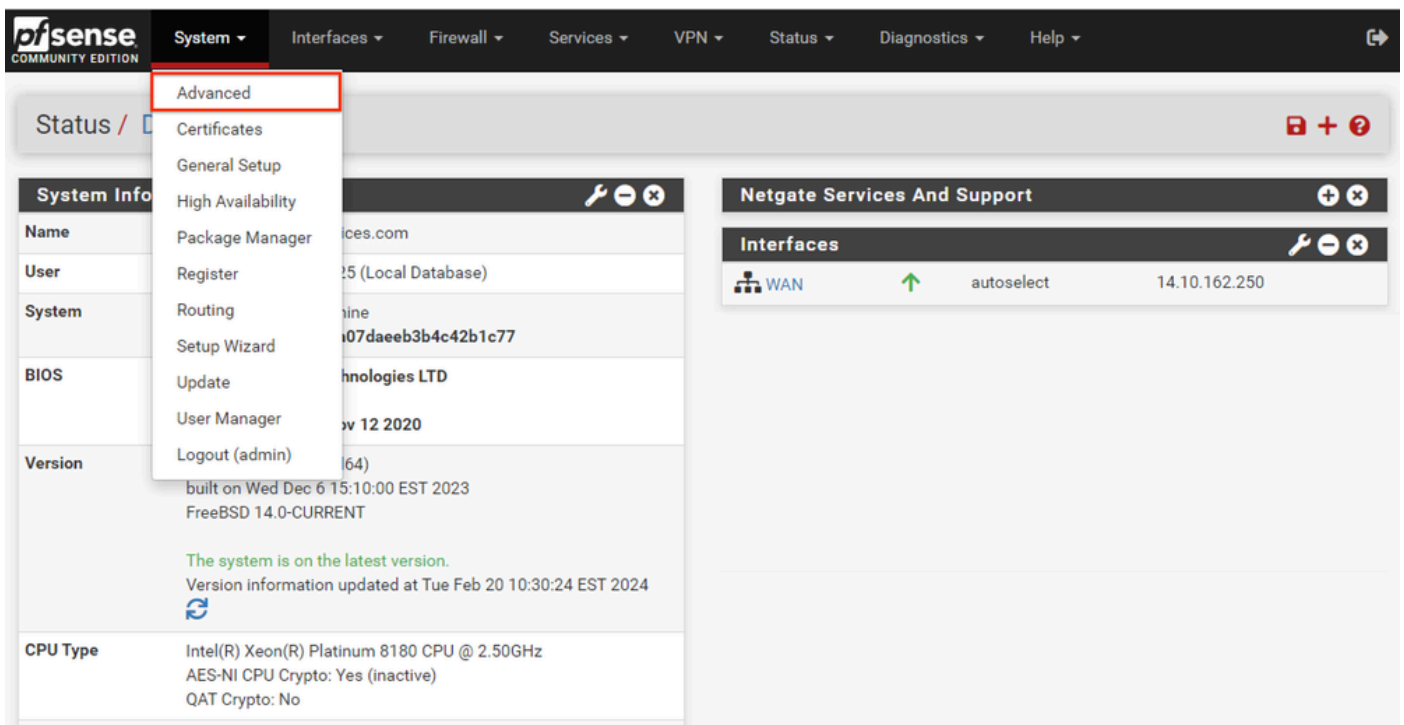
Assistente para configuração do pfSense - 3

Continue no assistente de configuração até o final. A interface GUI é reiniciada e você é redirecionado para a nova URL depois de concluído.

Definir Configurações Básicas de Administração

Etapa 1. Faça login na interface do administrador

Etapa 2. Selecione Avançado no menu suspenso Sistema




GUI pfSense - menu suspenso Admin

Etapa 3. Atualizar configurações do 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>

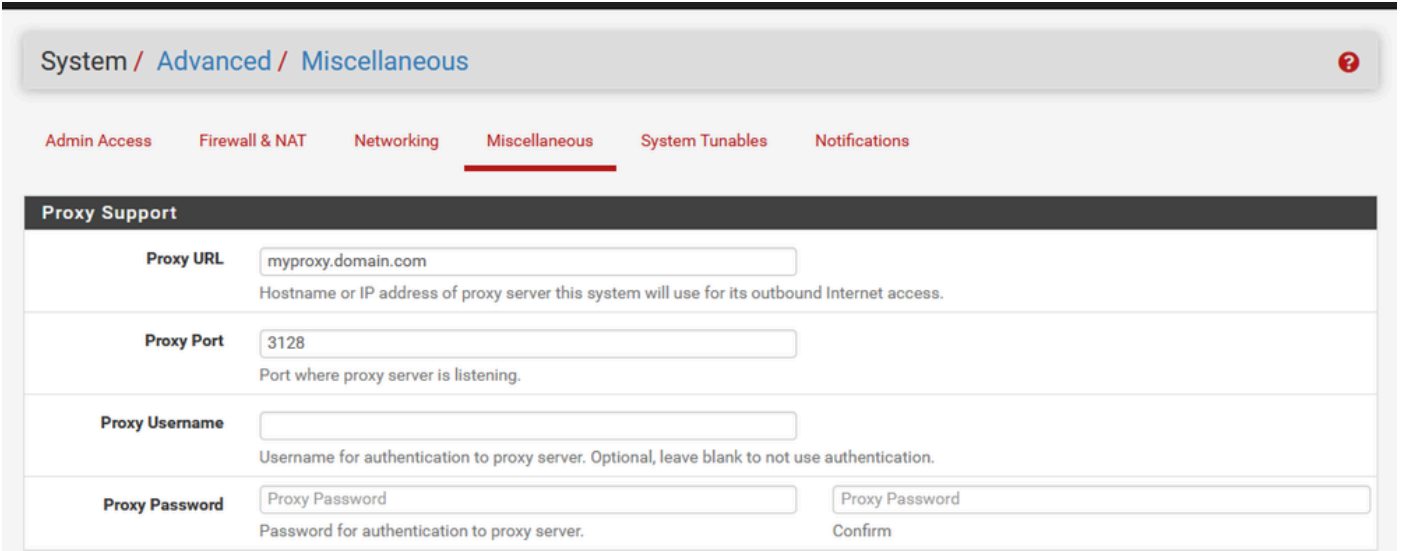
GUI pfSense - Configuração do administrador

1. Selecione o protocolo HTTPS (SSL/TLS).
2. Deixe o certificado SSL/TLS para o certificado autoassinado neste momento.
3. Altere a porta TCP para uma porta diferente de 443 para proteger melhor a interface e evitar problemas com sobreposição de porta.
4. Selecione a opção WebGUI redirect para desativar a interface admin na porta 80.
5. Selecione a opção de imposição Navegador HTTP_REFERER.
6. Habilite o Secure Shell selecionando a opção Habilitar Secure Shell.

 Observação: certifique-se de selecionar o botão Salvar antes de continuar. Em seguida, você é redirecionado para o novo link https.

Etapa 4. Configurar o servidor proxy, se necessário

Se necessário, configure as informações de proxy na guia Diversos. Para concluir a instalação e a configuração, o equipamento deve ter acesso à 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


GUI pfSense - Configuração de proxy

 Observação: certifique-se de selecionar o botão Salvar depois de fazer as alterações.

Adicionar Pacotes Necessários

Etapa 1. Selecione System > Package Manager

Etapa 2. Selecionar pacotes disponíveis

 Observação: pode levar alguns minutos para carregar todos os pacotes disponíveis. Se o tempo limite for excedido, verifique se os servidores DNS estão configurados corretamente. Frequentemente, uma reinicialização do dispositivo corrige a conectividade com a Internet.

System / Package Manager / Available Packages ?

Available Packages

Search

Search term Both

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

Packages

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

GUI pfSense - Lista de pacotes

Etapa 3. Localizar e instalar os pacotes necessários

1. haproxy
2. Ferramentas Open-VM

 Observação: não selecione o pacote haproxy-devel.

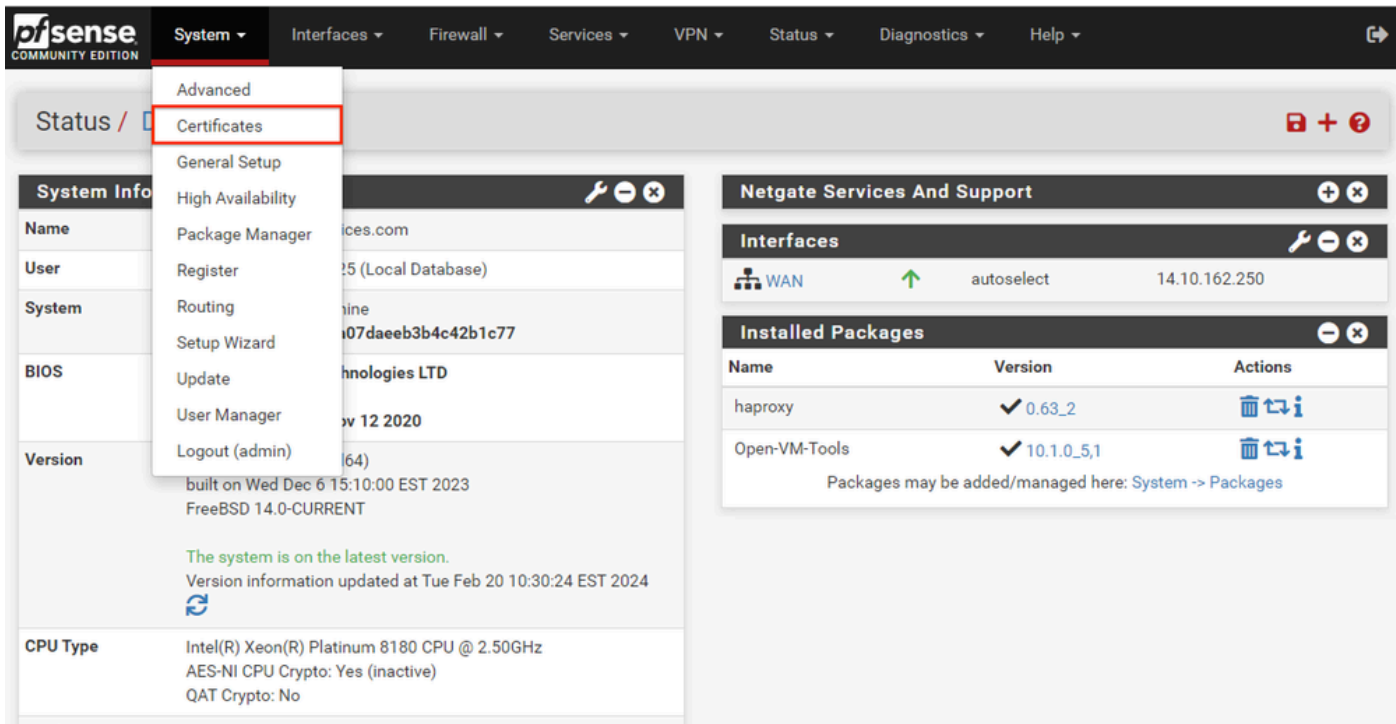
Configurar certificados

O pfSense pode criar um certificado autoassinado ou pode integrar-se com uma CA pública, uma CA interna ou pode atuar como uma CA e emitir certificados assinados por uma CA. Este guia mostra as etapas para integração com uma CA interna.

Antes de iniciar esta seção, verifique se você tem esses itens disponíveis.

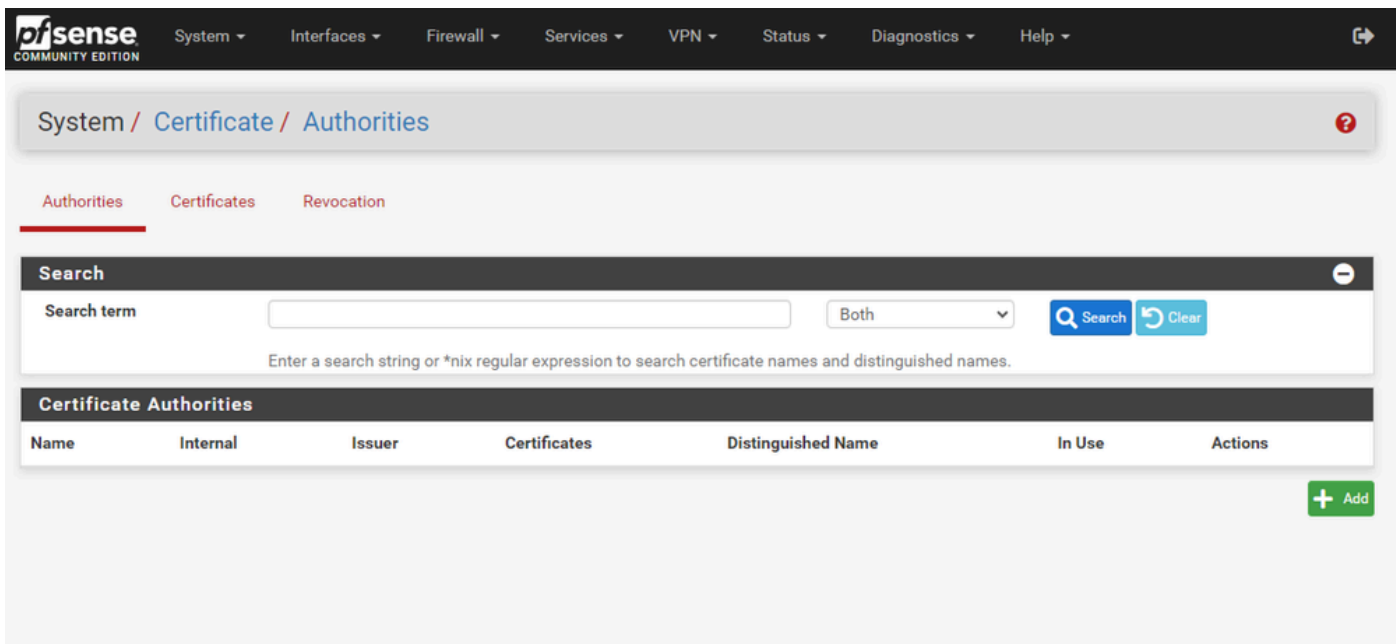
1. Certificado raiz para CA salvo como um formato codificado PEM ou Base-64.
2. Todos os certificados intermediários (às vezes chamados de emissores) para CA salvos como um formato codificado PEM ou Base-64.

Etapa 1. Selecione Certificados no menu suspenso Sistema



GUI pfSense - menu suspenso Certificados

Etapa 2. Importar o certificado raiz da autoridade de certificação



GUI pfSense - Lista de certificados CA

Selecione o botão Add.

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

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

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

Method

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

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

Existing Certificate Authority

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

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

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

GUI pfSense - Importação de CA

Conforme mostrado na imagem:

1. Forneça um nome exclusivo e descritivo
2. Selecione Importar uma Autoridade de Certificação existente na lista suspensa Método.
3. Verifique se as caixas de seleção Trust Store e Randomize Serial estão marcadas.
4. Cole o certificado inteiro na caixa de texto Dados do certificado. Certifique-se de incluir as linhas -----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----.
5. Selecione Salvar.
6. Verifique se o Certificado é importado conforme mostrado na imagem.

pfSense
COMMUNITY EDITION

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

System / Certificate / Authorities ?

Authorities Certificates Revocation

Search ⊖

Search term Both Q 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	<input checked="" type="checkbox"/>	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

GUI pfSense - Lista de CA

Etapa 3. Importar o Certificado Intermediário da CA

pfSense
COMMUNITY EDITION

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

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

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

Method

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

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

Existing Certificate Authority

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

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

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

GUI pfSense - CA Intermediate Import

Repita as etapas para importar o certificado CA raiz e importar o certificado CA intermediário.

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

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

Certificate Authorities

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

GUI pfSense - Links da CA

Revise as Autoridades de Certificação para garantir que o Intermediário esteja corretamente encadeado ao certificado raiz conforme mostrado na imagem.

Etapa 4. Criar e exportar um CSR para o site com balanceamento de carga

Descreve as etapas para criar um CSR, exportar o CSR e importar o certificado assinado. Se você já tiver um certificado existente em um formato PFX, poderá importar esse certificado. Consulte a documentação do pfSense para obter esses passos.

1. Selecione o menu Certificados e, em seguida, selecione o botão Adicionar/Assinar.

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. Preencha o formulário de Solicitação de Assinatura de Certificado.

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create a Certificate Signing Request

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

External Signing Request

Key type RSA

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

prime256v1 [HTTPS] [IPsec] [OpenVPN]

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

Common Name myece.mydomain.com
 The following certificate subject components are optional and may be left blank.

Country Code US

State or Province North Carolina

City Research Triangle Park

Organization Cisco Systems Inc

Organizational Unit Cisco TAC

- Método: selecione Criar uma solicitação de assinatura de certificado no menu suspenso
- Nome descritivo: forneça um nome para o certificado
- Tipo de chave e algoritmo de resumo: revise para garantir que eles correspondam aos seus requisitos
- Nome comum: forneça o site da Web de nome de domínio totalmente qualificado
- Forneça as informações de certificado restantes conforme necessário para o seu ambiente

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 Avançado

- Tipo de certificado: selecione Certificado do servidor na lista suspensa.
- Nomes alternativos: forneça todos os nomes alternativos do assunto (SAN) necessários para sua implementação.



Observação: o nome comum é automaticamente adicionado ao campo SAN. Você só precisa adicionar outros nomes necessários.

Selecione Salvar quando todos os campos estiverem corretos.

3. Exporte o CSR para um arquivo.

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	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Export"/> <input type="button" value="Import"/>
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"/>	<input type="button" value="Export"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>

Selecione o botão Exportar para salvar o CSR e, em seguida, assine-o com sua CA. Quando tiver o certificado assinado, salve-o como um arquivo PEM ou Base-64 para concluir o processo.

4. Importe o certificado assinado.



The screenshot shows the pfSense GUI interface for managing certificates. At the top, there is a navigation bar with the pfSense logo and various menu items. Below the navigation bar, there is a breadcrumb trail: 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, a dropdown menu set to "Both", and buttons for "Search" and "Clear". Below the search bar is a table of certificates. The table has columns for Name, Issuer, Distinguished Name, In Use, and Actions. The first row is for the "GUI default (65cced5b25159) Server Certificate" with a "self-signed" issuer and is in use by "webConfigurator". The second row is for the "ece-web-2024" certificate with an "external - signature pending" issuer. The "Actions" column for the "ece-web-2024" certificate has a red box around the edit icon (pencil). 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		   

Selecione o ícone do Lápis para importar o certificado assinado.

5. Cole os dados do certificado no form.

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-----
MIIDvDCCAqQCAQAwgZcxHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
MAkGA1UEBHMCMVVMxZjZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMR8wHQYDVQHEXZS
ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMR0wGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
YzESMBAGA1UECzMjQ21zY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

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

Final certificate data

```
GBSAPwQWkas305JkKISY/pYEI2EW/7EZcDmHRUrnEFcWoRR2984LJgDgs1pmlcPL
V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yiZ3IT4TJwDLLEXAGJqB+jy8G5bfsZQf
QNYnxuZ5Mnuqx1PN97EPQngO/1IgxO4xDz6Dg+Iwt9pyrRZdxpmy
-----END CERTIFICATE-----
```

Paste the certificate received from the certificate authority here.

GUI do pfSense - Importação de certificado

Selecione Update para salvar o certificado.

6. Revise os dados do certificado para garantir que estejam corretos.

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 (65ccd5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65ccd5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	webConfigurator	
ece-web-2024 CA: No Server: Yes	MyIntermediateCA	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US Valid From: Tue, 20 Feb 2024 12:31:00 -0500 Valid Until: Thu, 19 Feb 2026 12:31:00 -0500		

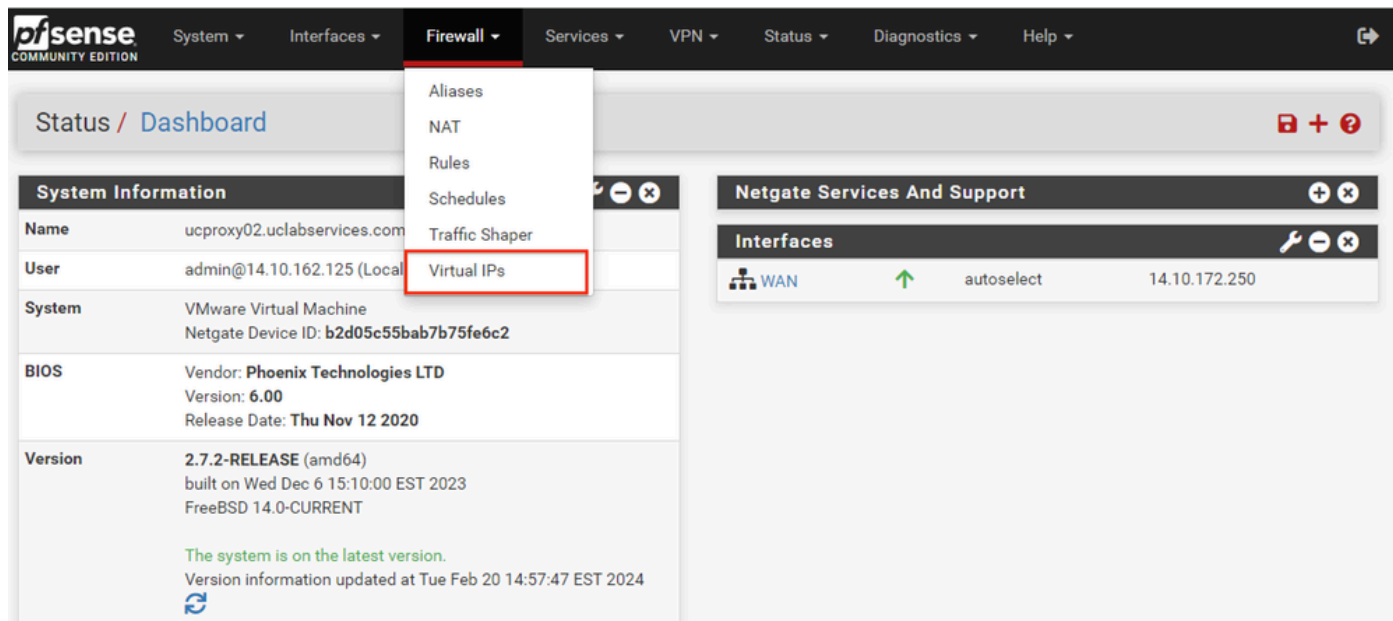
GUI pfSense - Lista de certificados

7. Repita esse processo se desejar hospedar vários sites neste pfSense.

Adicionar IPs Virtuais

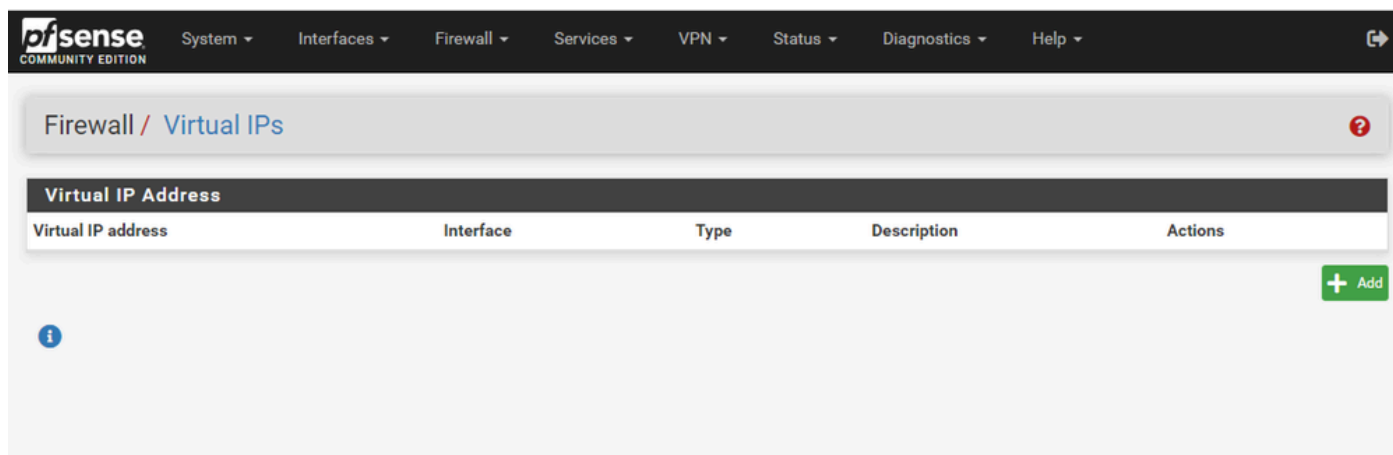
Pelo menos um IP é necessário para hospedar sites no pfSense. No pfSense, isso é feito com VIPs (IPs Virtuais).

Etapa 1. Selecione IPs virtuais no menu suspenso Firewall



GUI pfSense - Menu suspenso VIP

Etapa 2. Selecione o botão Adicionar



GUI pfSense - Página inicial do VIP

Etapa 3. Fornecer informações de endereço

[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 - Configuração VIP

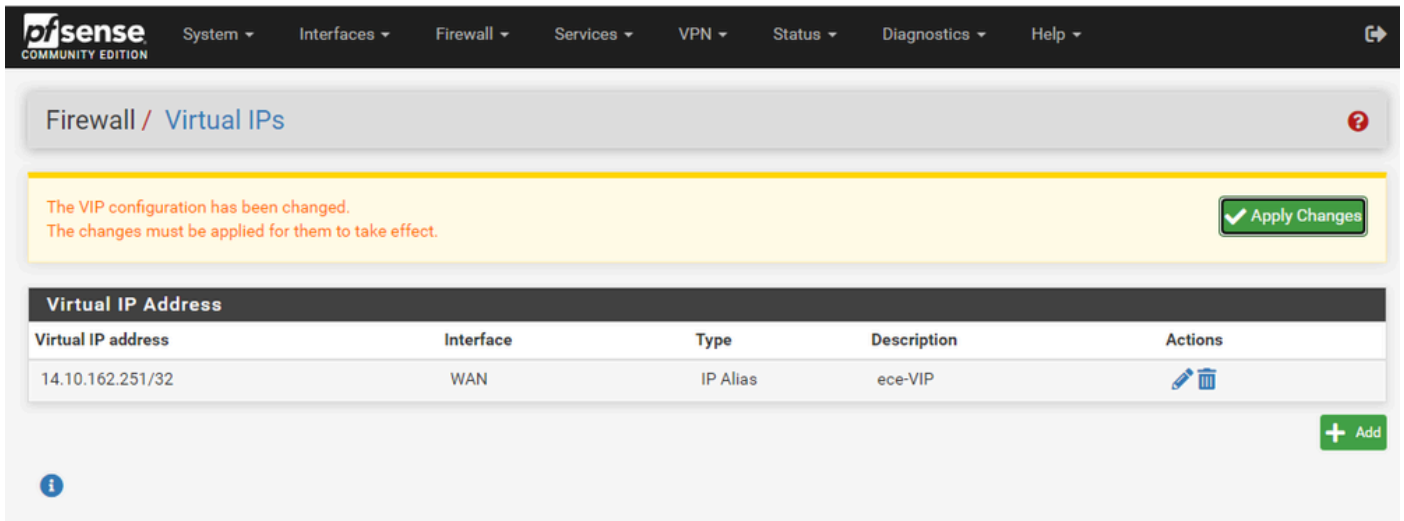
Use as informações para adicionar um VIP.

- Tipo: Selecionar Apelido de IP
- Interface: selecione a interface para este endereço IP ser transmitido
- Endereço(s): insira o endereço IP
- Máscara de endereço: para endereços IP usados para balanceamento de carga, a máscara deve ser /32
- Descrição: forneça um texto curto para facilitar a compreensão da configuração posteriormente

Selecione Save para confirmar a alteração.

Repita esse procedimento para cada endereço IP necessário para a sua configuração.

Etapa 4. Aplicar configuração



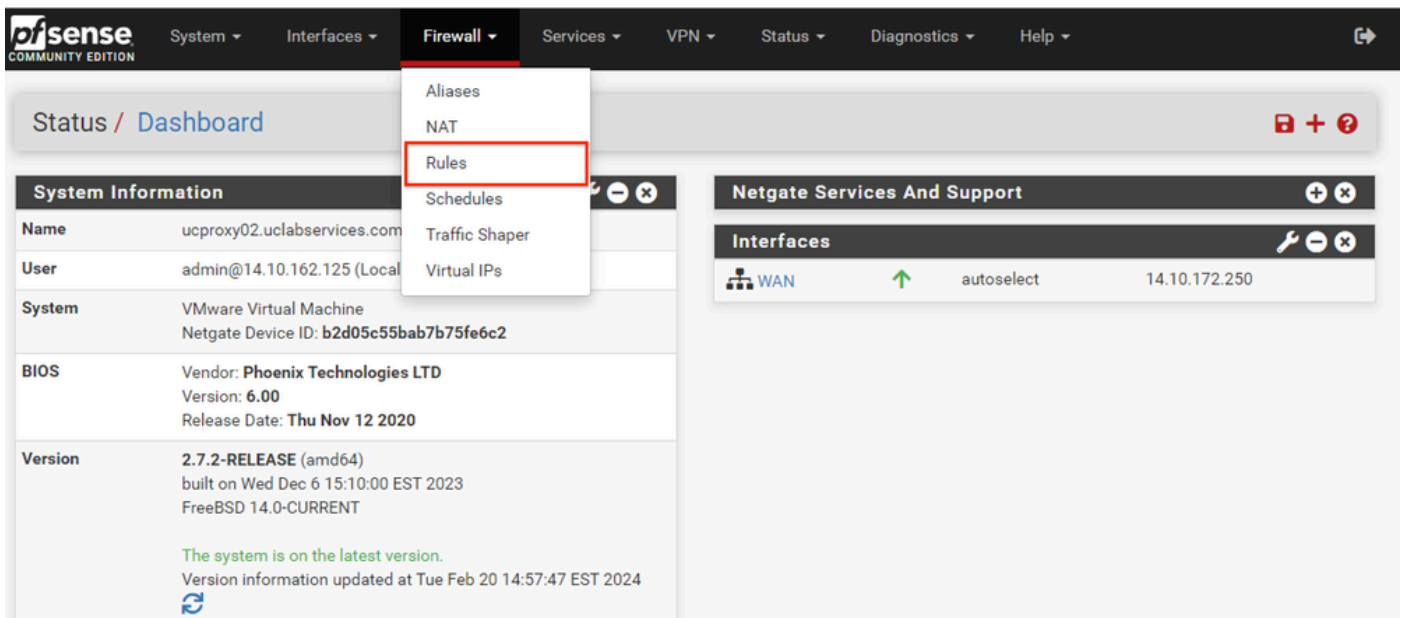
GUI pfSense - Lista VIP

Selecione o botão Apply Changes depois que todos os VIPs tiverem sido adicionados.

Configurar firewall

o pfSense tem um firewall integrado. O conjunto de regras padrão é muito limitado. Antes de colocar o dispositivo em produção, certifique-se de criar uma política de firewall abrangente.

Etapa 1. Selecione Regras na lista suspensa Firewall



GUI pfSense - Lista suspensa de regras de firewall

Etapa 2. Selecione um dos botões Adicionar

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

GUI pfSense - Lista de regras de firewall

Observe que um botão adiciona a nova regra acima da linha selecionada, enquanto o outro adiciona a regra abaixo da regra selecionada. Qualquer botão pode ser usado para a primeira regra.

Etapa 3. Crie uma regra de firewall para permitir o tráfego para o endereço IP na porta 443

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 - Configuração da regra de passagem de firewall

Use as informações para criar a regra.

- Ação: Selecionar Aprovação
- Interface: Escolha a Interface à qual a regra se aplica
- Família de endereços e protocolo: selecione conforme apropriado
- Origem: Deixar selecionado como Qualquer
- Destino: Selecione Endereço ou Apelido na lista suspensa Destino e, em seguida, informe o endereço IP ao qual a regra se aplica
- Intervalo de portas de destino: Selecione HTTPS (443) nas listas suspensas De e Até
- Log: Marque a caixa de seleção para registrar todos os pacotes que corresponderem a esta regra para contabilização

- Descrição: forneça o texto para fazer referência à regra posteriormente

Selecione Save.

Etapa 4. Crie uma regra de firewall para descartar todo o tráfego restante no pfSense

Selecione o botão Adicionar para inserir a regra abaixo da regra recém-criada.

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

- Action:** Set to 'Block'. A hint explains the difference between block and reject.
- Disabled:** A checkbox to 'Disable this rule' is unchecked.
- Interface:** Set to 'WAN'.
- Address Family:** Set to 'IPv4'.
- Protocol:** Set to 'TCP'.
- Source:** 'Source' is set to 'Any'. A 'Display Advanced' button is present.
- Destination:** 'Destination' is set to 'Any'. 'Destination Port Range' is set to '(other)'. A 'Display Advanced' button is present.
- Extra Options:** 'Log' is checked. 'Description' is 'Drop all other inbound traffic'.

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

GUI pfSense - Configuração de regra de queda de firewall

- Ação: Selecionar Bloco

- Interface: Escolha a Interface à qual a regra se aplica
- Família de endereços e protocolo: selecione conforme apropriado
- Origem: Deixe selecionado como Qualquer
- Destino: deixe selecionado como Qualquer
- Log: Marque a caixa de seleção para registrar todos os pacotes que corresponderem a esta regra para contabilização
- Descrição: forneça o texto para fazer referência à regra posteriormente

Selecione Save.

Etapa 5. Revise as regras e verifique se a regra de bloqueio está na parte inferior

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

Apply Changes

Floating WAN

Rules (Drag to Change Order)

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

↑ Add ↓ Add Delete Toggle Copy Save + Separator

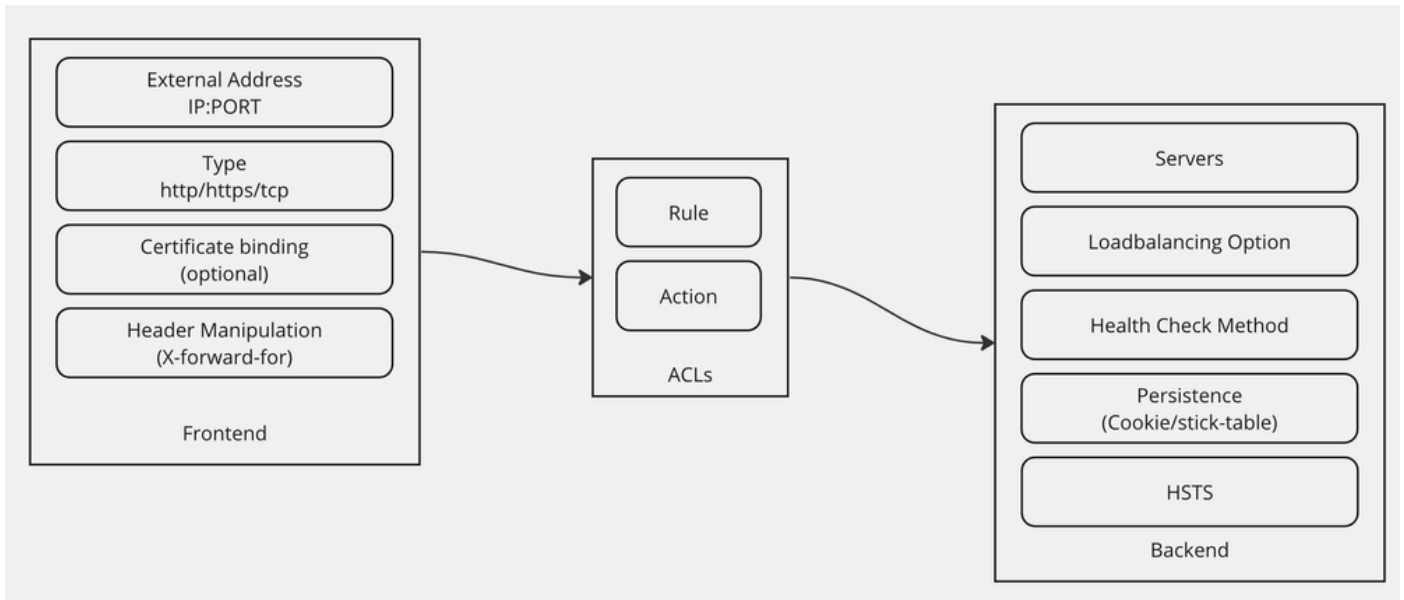
GUI pfSense - Lista de regras de firewall

Se necessário, arraste as regras para classificá-las.

Selecione Aplicar alterações quando as regras de firewall estiverem na ordem necessária para o seu ambiente.

Configurar HAProxy

Conceitos do HAProxy



Conceitos do HAProxy

O HAProxy é implementado com um modelo de front-end/back-end.

O Front-end define o lado do proxy com o qual os clientes se comunicam.

O Front-end consiste em uma combinação de IP e Porta, vinculação de certificado e pode implementar alguma manipulação de cabeçalho.

A infraestrutura define o lado do proxy que se comunica com os servidores Web físicos.

O back-end define os servidores e portas reais, o método de balanceamento de carga para atribuição inicial, verificações de integridade e persistência.

Um front-end sabe com qual back-end se comunicar usando um back-end dedicado ou ACLs.

As ACLs podem criar regras diferentes para que um determinado front-end possa se comunicar com backends diferentes, dependendo de várias coisas.

Configurações iniciais do HAProxy

Etapa 1. Selecione HAProxy no menu suspenso Serviços

pfSense COMMUNITY EDITION

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

Status / Dashboard

System Information	
Name	ucproxy02.uclabservices.com
User	admin@14.10.162.125 (Local Database)
System	VMware Virtual Machine Netgate Device ID: b2d05c55bab7b75fe6c2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 15:10:00 EST 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 14:00:00 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

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

Netgate Services And Support

Contract type **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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

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

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

GUI pfSense - menu suspenso HAProxy

Etapa 2. Definir configurações básicas

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 - Configurações principais do HAProxy

Marque a caixa de seleção Habilitar HAProxy.

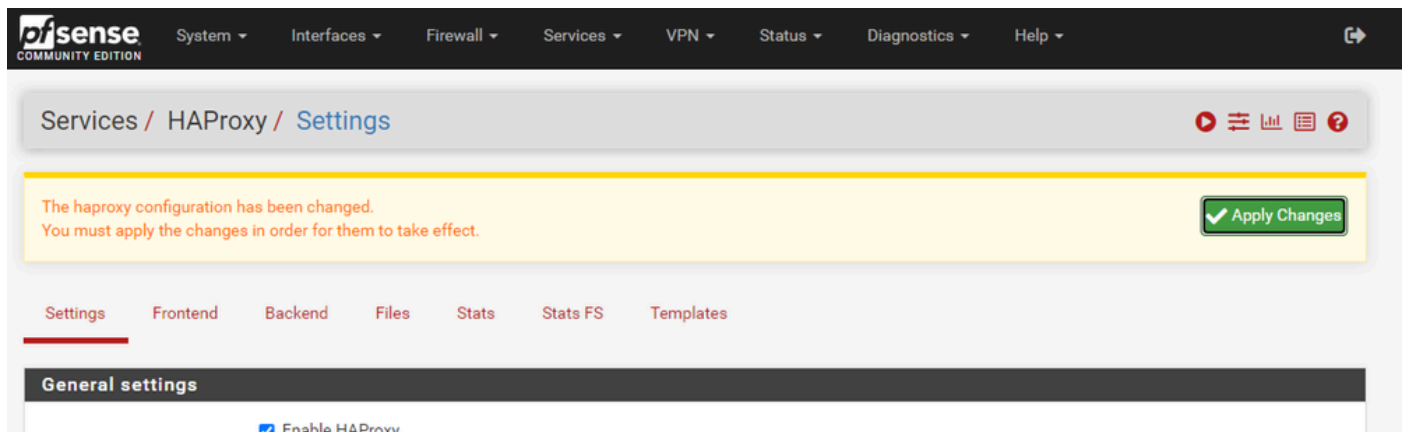
Digite um valor para Máximo de conexões. Consulte o gráfico nesta seção para obter detalhes sobre a memória necessária.

Insira um valor para a porta de estatísticas internas. Essa porta é usada para mostrar estatísticas de HAProxy no equipamento, mas não é exposta fora do equipamento.

Informe um valor para a taxa de atualização de estatísticas Internas.

Revise a configuração restante e atualize-a conforme necessário para o seu ambiente.

Selecione Salvar.



Services / HAProxy / Settings

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


Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

General settings

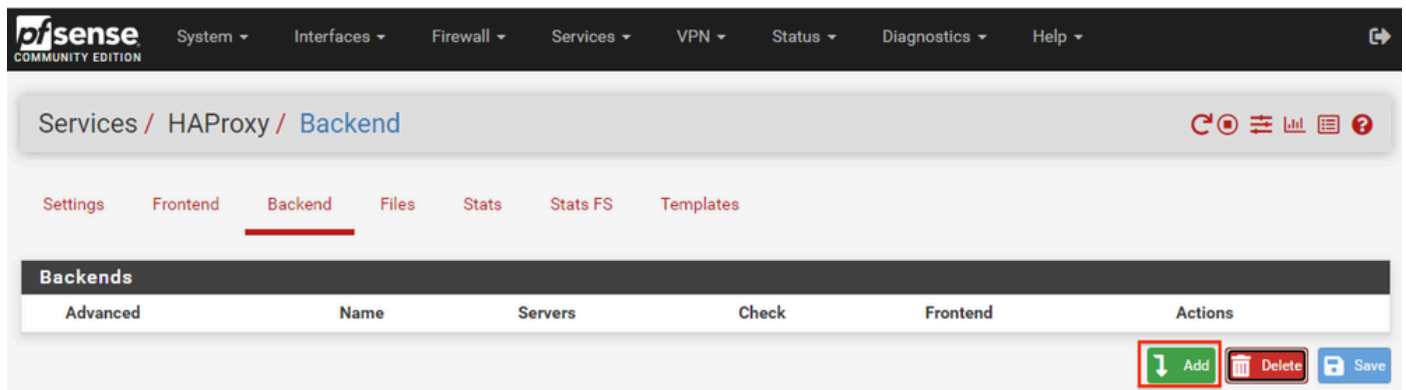
Enable HAProxy

GUI pfSense - HAProxy Aplicar alterações

 Observação: as alterações de configuração não são ativadas até que você selecione o botão Aplicar alterações. Você pode fazer várias alterações de configuração e aplicá-las todas de uma vez. A configuração não precisa ser aplicada para ser usada em outra seção.

Configurar o back-end do HAProxy




Comece com a infraestrutura. A razão para isso é que o front-end deve referenciar um back-end. Verifique se você selecionou o menu Back-end.



Services / HAProxy / Backend

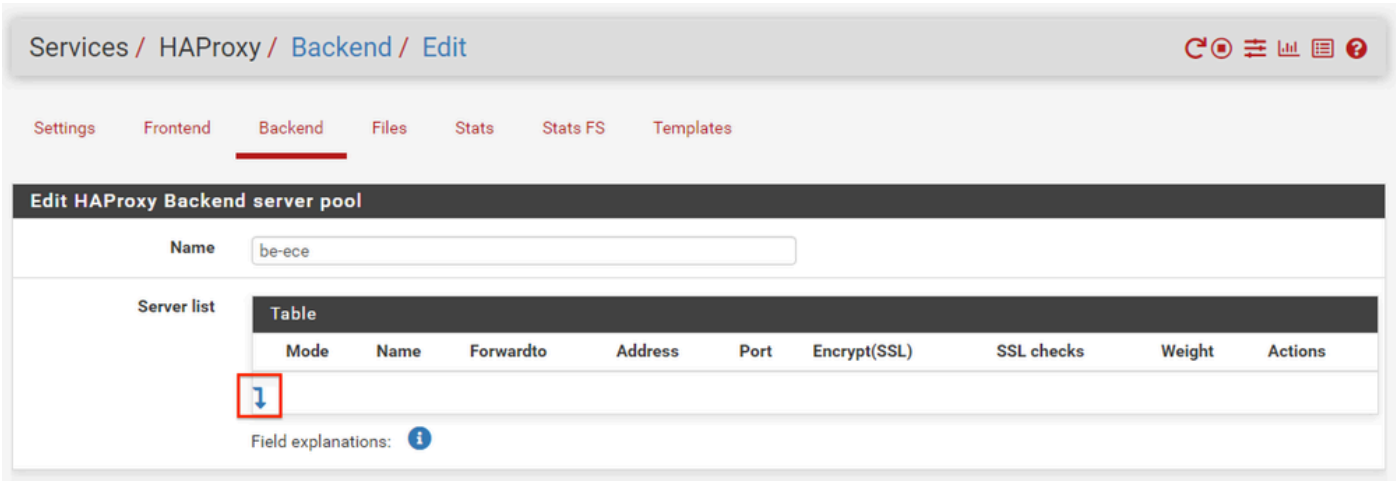
Settings Frontend Backend Files Stats Stats FS Templates

Backends

Advanced	Name	Servers	Check	Frontend	Actions
					  

GUI pfSense - HAProxy Adicionar Back-end

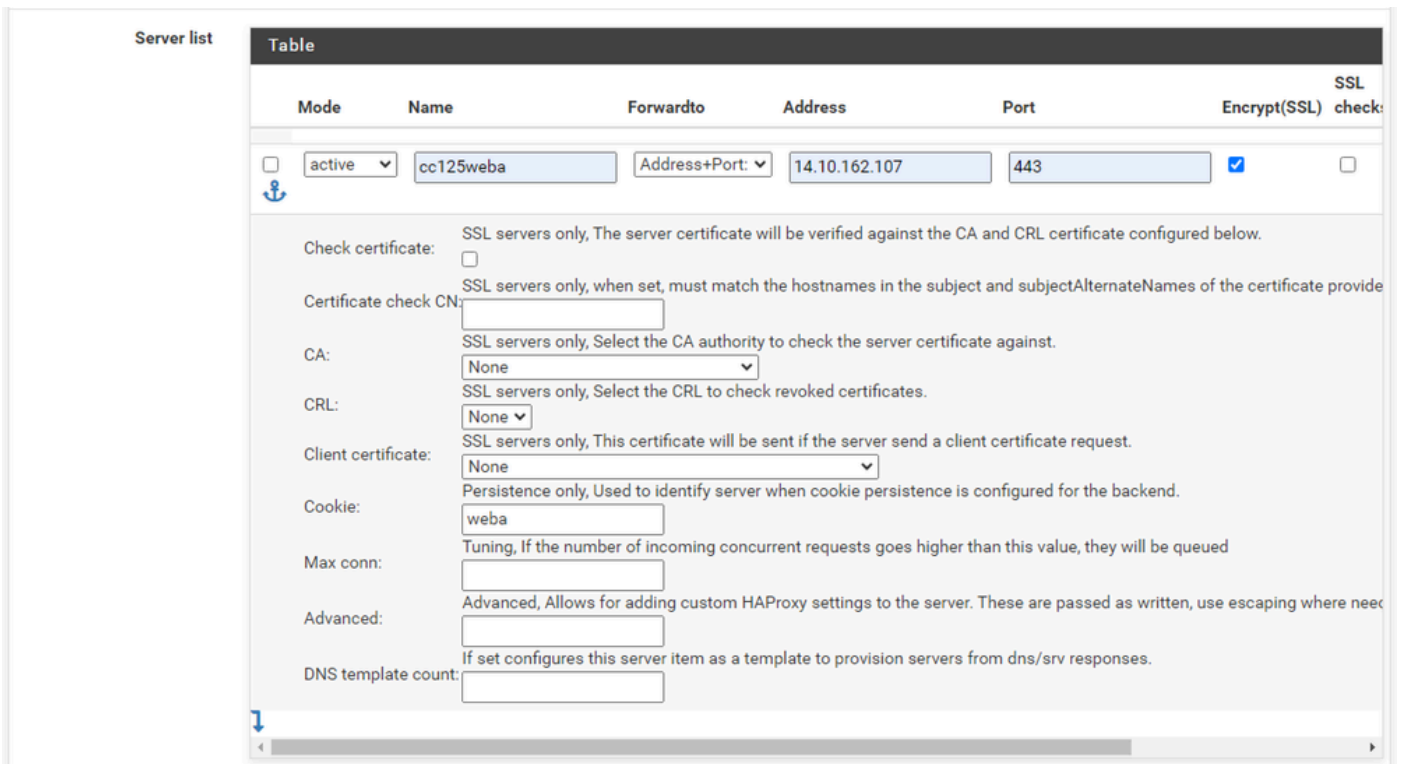
Selecione o botão Add.



GUI pfSense - Início do back-end do HAProxy

Forneça um nome para o back-end.

Selecione a seta para baixo para adicionar o primeiro servidor à lista de servidores



Infraestrutura - Lista de servidores

Forneça um nome para referenciar o servidor. Isso não precisa corresponder ao nome real do servidor. Este é o nome que é mostrado na página de estatísticas.

Forneça o endereço do servidor. Isso pode ser configurado como um Endereço IP para FQDN.

Forneça a porta à qual se conectar. Esta deve ser a porta 443 para ECE.

Marque a caixa de seleção Criptografar(SSL).

Forneça um valor no campo Cookie. Este é o conteúdo do cookie de fidelidade da sessão e deve

ser exclusivo dentro do back-end.

Depois que o primeiro servidor tiver sido configurado, selecione a seta para baixo para configurar quaisquer outros servidores Web no 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.

Infraestrutura HAProxy - Balanceamento de carga

Configure as opções de Balanceamento de carga.

Para servidores ECE, deve ser definido como Conexões Mínimas.

Access control lists and actions	
Timeout / retry settings	
Connection timeout	60000 The time (in milliseconds) we give up if the connection does not complete within (default 30000).
Server timeout	60000 The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).
Retries	2 After a connection failure to a server, it is possible to retry, potentially on another server. This is useful if health-checks are too rare and you don't want the clients to see the failures. The number of attempts to reconnect is set by the "retries" parameter.
Health checking	
Health check method	HTTP <small>HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).</small>
Check frequency	 milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	<input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged. By default, failed health check are logged if server is UP and successful health checks are logged if server is DOWN, so the amount of additional information is limited.
Http check method	GET <small>OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the webserver and is less easy to filter out of its logs.</small>
Url used by http check requests.	/system/web/view/platform/common/login/root.jsp?partitionId=1 Defaults to / if left blank.
Http check version	HTTP/1.1\r\nHost:\ ece125.uclabservices.com Defaults to "HTTP/1.0" if left blank. Note that the Host field is mandatory in HTTP/1.1, and as a trick, it is possible to pass it after "\r\n" following the version string like this: <code>HTTP/1.1\r\nHost:\ www</code> Also some hosts might require an accept parameter like this: <code>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</code>

Infraestrutura HAProxy - Verificação de integridade

As listas de controle de acesso não são usadas nesta configuração.

As configurações de tempo limite/repetição podem ser deixadas com a configuração padrão.

Configurar a seção Verificação de integridade.

1. Método de verificação de integridade: HTTP
2. Verificar frequência: deixe em branco para usar o padrão a cada 1 segundo.
3. Verificações de log: Selecione esta opção para gravar quaisquer alterações de integridade nos logs.
4. Método de verificação HTTP: selecione GET na lista.
5. Url usada pelas solicitações de verificação http.: Para um servidor ECE, digite /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Versão de verificação HTTP: Enter, HTTP/1.1\r\nHost:\ {fqdn_of_server}

Certifique-se de incluir um espaço após a barra invertida final, mas antes do FQDN do servidor.

Agent checks

Agent checks Use agent checks
Use a TCP connection to read an ASCII string of the form 100%,75%,drain,down (more about this in the [haproxy manual](#))

Cookie persistence

Cookie Enabled Enables cookie based persistence. (only used on "http" frontends)

Server Cookies **Make sure to configure a different cookie on every server in this backend.**

Cookie Name
The string name to track in Set-Cookie and Cookie HTTP headers.
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASPNET_SessionId

Cookie Mode
Determines how HAProxy inserts/prefixes/replaces or examines cookie and set-cookie headers.
EXAMPLE: with an existing PHPSESSIONID you can for example use "Session-prefix" or to create a new cookie use "Insert-silent".

cookie is analyzed on incoming request to choose server and set-cookie value is overwritten if present and set to an unknown value or inserted in response if not present.

cookie <cookie name> insert

Cookie Cachable Allows shared caches to cache the server response.

Cookie Options Only insert cookie on post requests. Prevent usage of cookie with non-HTTP components. Prevent usage of cookie over non-secure channels.

Cookie Options
Max idle time It only works with insert-mode cookies. Max life time It only works with insert-mode cookies.

Cookie domains
Domains to set the cookie for, separate multiple domains with a space.

Cookie dynamic key
Set the dynamic cookie secret key for a backend. This is will be used to generate a dynamic cookie with.

Stick-table persistence

These options are used to make sure separate requests from a single client go to the same backend. This can be required for servers that keep track of for example a shopping cart.

Stick tables
Sticktables that are kept in memory, and when matched make sure the same server will be used.

No stick-table will be used

Email notifications

Mail level
Define the maximum loglevel to send emails for.

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

Infraestrutura HAProxy - Persistência de Cookies

Deixe as verificações do Agente desmarcadas.

Configurar a persistência do cookie:

1. Cookie ativado: selecione para ativar a persistência baseada em cookie.
2. Nome do cookie: forneça um nome para o cookie.
3. Modo Cookie: Selecione Inserir na caixa suspensa.
4. Deixe as opções restantes desmarcadas.

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](#)

Infraestrutura HAProxy - HSTS

As seções restantes do formulário de configuração da infraestrutura podem ser deixadas com as suas configurações padrão.

Se desejar configurar o HSTS, configure um valor de tempo limite nesta seção. O ECE também insere um cookie HSTS para que essa configuração seja redundante.

Selecione Salvar.

Configurar front-end do HAProxy

Mude para o menu de Interface.

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

GUI pfSense - HAProxy Adicionar front-end

Selecione o botão Adicionar,

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 - Cabeçalho de front-end

Forneça um nome para o Front-end.

Forneça uma descrição para ajudar a identificar o front-end posteriormente.

Na tabela Endereço externo:

1. Endereço de escuta: Selecione o VIP que você criou para este site.
2. Porta: Digite 443.
3. Descarregamento de SSL: Selecione esta opção para que um cookie de sessão possa ser inserido.

Deixe o Máximo de conexões em branco.

Verifique se o Tipo está selecionado como http / https(offloading).

Default backend, access control lists and actions

Access Control lists

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

Table

Name	Expression	CS	Not	Value	Actions

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld 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
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.

For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

NOTE Important change in behaviour, since package version 0.32

-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.

-acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions

Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table

Action	Parameters	Condition acl names	Actions

Example:

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

Default Backend

be-ecce

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

Infraestrutura HAProxy - Seleção padrão da infraestrutura

A configuração mais fácil é escolher um back-end padrão no menu suspenso. Isso pode ser selecionado quando o VIP hospeda um único site.

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".

Infraestrutura HAProxy - ACL Avançada

Como mostrado na imagem, as ACLs podem ser usadas para redirecionar um único front-end para vários back-ends com base nas condições.

Você pode ver que a ACL verifica se o host na solicitação começa com um nome e um número de porta ou simplesmente o nome. Com base nisso, uma infraestrutura específica é usada.

Isso não é comum com ECE.

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss."

SNI Filter
Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate
Choose the cert to use on this frontend.
 Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 Add ACL for certificate Subject Alternative Names.

OCSP Load certificate ocsp responses for easy certificate validation by the client.
A cron job wil update the ocsp response every hour.

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

Table	
Certificates	Actions

Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 Add ACL for certificate Subject Alternative Names.

Advanced ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: force-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, ecche, 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 ecche secp256k1

Interface HAProxy - Associação de certificado

Na seção Descarregamento de SSL, selecione o certificado criado para uso com este site. Este certificado deve ser um certificado de servidor.

Selecione a opção Add ACL para o certificado Subject Alternative Names.

Você pode deixar as opções restantes com seus valores padrão.

Selecione Salvar no final deste formulário.

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 - Aplicar configuração

Selecione Apply Changes para confirmar as alterações de front-end e back-end na configuração atual.

Parabéns, você concluiu a instalação e a configuração do pfSense.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.