

Pedro Delfino

# FIREWALL COM Sense

*O Guia Rápido para Iniciantes*



<b>SOBRE PEDRO DELFINO</b>	<b>4</b>
<b>INTRODUÇÃO</b>	<b>6</b>
<b>O QUE É O PFSENSE</b>	<b>7</b>
<b>PRINCIPAIS VANTAGENS E RECURSOS DO PFSENSE</b>	<b>9</b>
<b>FAZENDO DOWNLOAD DA IMAGEM ISO DO PFSENSE</b>	<b>12</b>
<b>MONTANDO O AMBIENTE DE TESTE PARA RODAR O PFSENSE</b>	<b>14</b>
<b>CHECK LIST PARA MONTAR O AMBIENTE</b>	<b>18</b>
<b>CONFIGURAÇÃO DA MÁQUINA CLIENTE DA REDE</b>	<b>20</b>
<b>INSTALAÇÃO DO PFSENSE</b>	<b>22</b>
<b>INICIANDO O PFSENSE</b>	<b>30</b>
<b>CONFIGURAÇÃO ESSENCIAL DE FIREWALL</b>	<b>34</b>
Configuração de Interfaces	35
Regras de Firewall padrão do pfsense	36
EDITANDO REGRAS DE FIREWALL	40
ADICIONANDO REGRAS DE FIREWALL	42
LIBERANDO A PORTA 80	42
LIBERANDO A PORTA 443	43

<b>ANALISANDO AS REGRAS DE FIREWALL</b>	<b>45</b>
<b>TRABALHANDO COM O PROXY SQUID NO PFSENSE</b>	<b>48</b>
INSTALAÇÃO DO SQUID	50
CONFIGURAÇÃO ESSENCIAL DO SQUID	52

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

## SOBRE PEDRO DELFINO



Pedro Delfino é o fundador do PROFISSIONAIS LINUX (<https://profissionaislinux.com.br>) que tem como principal objetivo formar novos profissionais para atuar na área de administração de servidores LINUX assim como soluções open source, é autor do E-tinet, (<https://e-tinet.com>) um blog sobre soluções LINUX que já ajudou milhares de leitores com seus Ebooks e treinamentos On-line.

Utiliza Linux como ferramenta de trabalho a mais de 18 anos, e a mais de 7 anos vem ajudando milhares de pessoas a aprender Linux de forma fácil e rápida, através de artigos em seu Blog.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

# INTRODUÇÃO

Nesse ebook nós iremos falar de Firewall com pfSense, vamos implementar um firewall com essa solução completa que já está toda embarcada no pfSense .

O pfSense diferente do que algumas pessoas pensam, não é uma distribuição do linux mas sim um freeBSD embarcado em uma imagem ISO ou podendo também embarcar ele em um pendrive.

Então você faz um boot para imagem ISO, pelo pendrive, e você tem uma solução completa com Firewall, Proxy, VPN, FailOver, com todas as soluções necessárias para você controlar a sua rede.

O pfSense irá servir então como gateway para uma rede, irá servir também como firewall para uma DMZ, são várias as soluções que você pode implementar.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

## O QUE É O PFSENSE

Essa deve ser a sua maior dúvida no momento, certo?

A definição que Christopher M. Buechler, um dos idealizadores e criadores do pfSense ao lado de Scott Ullrich, serve muito bem para responder a esta questão:

“pfSense é uma distribuição customizada, livre e open source (código aberto), do projeto FreeBSD criado para ser utilizado como um firewall ou roteador, inteiramente gerido em uma interface web fácil de usar”.

Em outras palavras, o pfSense é uma robusta solução de firewall e/ou roteador amplamente utilizada hoje por empresas e usuários avançados (mais de 1 milhão de downloads foram feitos desde o seu lançamento). Por ser open source, consolidou-se como uma grande concorrente das principais soluções pagas disponíveis no mercado.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Observação: quando pouco se sabe sobre o que é pfSense, é comum deduzir que o sistema precise ser instalado em um desktop, por exemplo. Mas na verdade o sistema deve ser instalado em um appliance, ou servidor dedicado para a função de firewall, por exemplo.

# PRINCIPAIS VANTAGENS E RECURSOS DO PFSENSE



Primeiramente, uma das principais vantagens é a sua licença BSD — licença de código aberto, gratuita, utilizada em sistemas baseados em Unix. Esse tipo de licença permite que o pfSense seja customizado de acordo com as maiores necessidades da empresa.

Um fator que auxilia na customização é a imensa variedade de pacotes de software, muitos deles criados por especialistas da comunidade de desenvolvedores para acrescentar novas funcionalidades.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Na linguagem dos especialistas em Segurança da Informação, a disponibilização dos pacotes para as mais diversas funções credencia o pfSense como um UTM (Unified Threat Management, ou Central Unificada de Gerenciamento de Ameaças, em português), que, em breves palavras, pode ser entendido por um dispositivo com diversas funções, tais como:

- firewall;
- servidor (internet, DHCP, NTP, Proxy...);
- antivírus;
- antispyware;
- antispam;
- filtragem de conteúdo;
- detecção de intrusão, entre outros.

Com tantas funções primordiais de segurança reunidas em uma única solução, um UTM como o pfSense, apesar de gratuito, pode funcionar com

excelência equiparável aos mais diversos produtos do mercado.

Além dessas vantagens o pfSense é considerado muito leve, exigindo baixíssimos requisitos de hardware, é estável, fácil de utilizar (possui até um dashboard é uma interface configurável) e possui excelentes recursos de filtragem.

Entretanto, caso a tarefa de fazer do pfSense a sua solução em firewall/roteador por conta própria seja trabalhosa e não muito condizente com o seu nível de conhecimento técnico, existem várias distribuições de firewall (desenvolvidas diretamente do pfSense) já configuradas que incluem suporte completo e, em alguns casos, um appliance (hardware).

Se, por outro lado, você estiver querendo agir na base do DIY (do it yourself, ou faça você mesmo, em português), confira a seguir algumas dicas de como instalar o pfSense.

# FAZENDO DOWNLOAD DA IMAGEM ISO DO PFSENSE

Então entrando no <https://pfsense.org> clique em Download.

Em seguida você será redirecionado para essa tela como mostra a imagem a seguir.

The screenshot shows the pfSense download page. At the top, there's a navigation bar with links for Get Started, Cloud, Products, Services, Support, Training, Community, and Download. Below the navigation bar, the word "Download" is highlighted. The main content area has a heading "Latest Stable Version (Community Edition)". A note below it says: "This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#)." There are two buttons: "RELEASE NOTES" and "SOURCE CODE". Below these buttons is a section titled "Select Image To Download" with the following fields: "Version": 2.5.2, "Architecture": AMD64 (64-bit), "Installer": DVD Image (ISO) Installer, and "Mirror": New York City, USA. A large blue button labeled "DOWNLOAD" with an upward arrow is present. To the right, there's a sidebar titled "Subscribe To The Netgate Newsletter" with a form for email address and a checkbox for newsletter updates. It also includes a link to the privacy policy.

Nessa tela você irá escolher então a arquitetura, eu estou usando a AMD64 para computador de 64 bits.

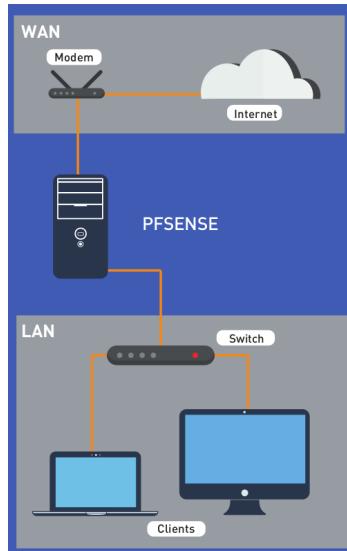
E na plataforma você escolhe o DVD IMAGE.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

# MONTANDO O AMBIENTE DE TESTE PARA RODAR O PFSENSE

Será preciso criar uma máquina virtual, porque para deixar funcionando este nosso firewall com pfSense você irá precisar de duas placas de rede, a não ser que você já tenha uma máquina com duas placas de rede e que seja.



Caso você tenha dúvida de como montar uma máquina virtual, pegue uma cópia do ebook Virtualbox: O Guia Passo a Passo (Link: <https://profissionaislinux.com.br/materiais/como-usar-virtualbox/>)



Agora analisando a imagem anterior, você pode ver o computador ao meio com pfSense, com uma placa de rede chamada de WAN, o pfSense tenta sempre identificar as suas placas de rede automaticamente, você vai perceber esse

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

procedimento quando for fazer a instalação e configuração.

Então aqui a minha primeira placa de rede é a 0, que vai ser minha placa de rede WAN e minha LAN vai ser minha placa de rede 1.

Lembrando que no Linux ( sistemas unix ) as placas de rede começam a ser numeradas de 0 para 1,2,3,4... e assim por diante.

Em minha solução aqui eu irei também montar uma outra máquina para ficar na mesma rede da LAN, ou seja vai ter uma rede interna, onde vou montar um cliente com Ubuntu e este cliente inclusive vou utilizar para acessar as configurações Web do pfSense, e é com ele que vou fazer todas as configurações e todos os testes de Firewall.

Então na rede LAN vai ser instalado uma distribuição do LINUX, que vai estar ligado no Switch, vamos montar a rede interna com os dois

computadores. E na WAN montamos uma outra rede que iremos ligar em nossa rede externa.

Bloqueando qualquer entrada de rede você já tem um firewall que não vai permitir ninguém tentar acessar um dos dois computadores.

Se fizer isso com uma única placa de rede não fará sentido algum, essa é uma regra básica de construção de Firewall não só com pfSense como qualquer outra opção de firewall.

Temos aqui os nossos clientes, eles precisam acessar a internet, e é óbvio que terão de passar por dentro do nosso pfSense.

No pfSense nós iremos colocar as nossas regras, vamos dizer se pode acessar determinada porta, se para acessar terá de usar um Proxy ou não e assim por diante, vai depender muito da sua necessidade, irei te mostrar algumas regras básicas mas as regras irão fazer total sentido se você tiver duas placas de rede.

## CHECK LIST PARA MONTAR O AMBIENTE

- Primeiro passo é iniciar fazendo o download do arquivo ISO do pfSense, conforme mostrei acima.
- Criar uma máquina virtual com duas placas de rede, onde será instalado o pfSense (caso você já tenha uma máquina física com duas placas de redes também poderá ser utilizada)
- Instalar o seu pfSense na máquina e ligar um cabo de rede no seu switch (rede interna), e outro cabo no seu modem de internet
- Colocar o seu computador ligado em no mesmo switch (rede interna), esse computador será utilizado para acessar as configurações do pfSense
- Deixar a configuração desse computador como DHCP Client, ou seja, sem IP algum

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

configurado, pois quando configurar o pfSense, o seu cliente já irá pegar por DHCP.

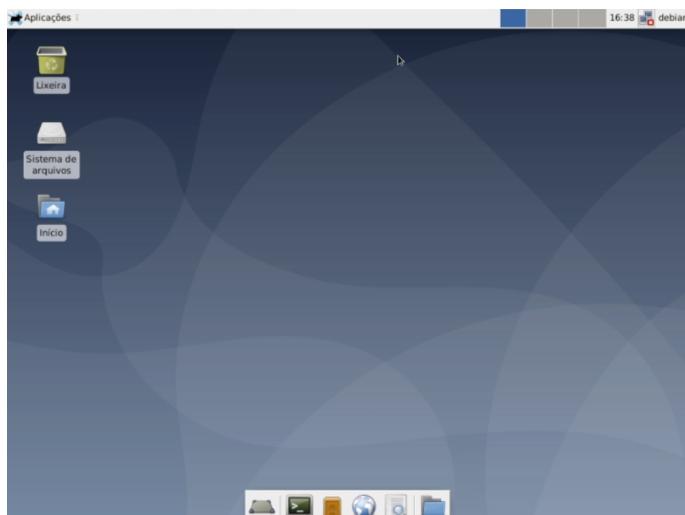
Iremos então instalar o pfSense e você irá entender que ele já vai ser um Firewall, um Gateway, e já vai ter um servidor de DHCP. Conseguimos matar 3 serviços com uma só instalação, praticamente sem fazer nenhuma configuração.

O pfSense trabalha na minha opinião da maneira mais correta, então necessariamente quando você não libera você está bloqueando tudo, e a princípio tudo vai estar bloqueado e vamos abrindo as portas conforme vai surgindo a necessidade.

Resumindo, se não está explícito que está liberado, está bloqueado.

# CONFIGURAÇÃO DA MÁQUINA CLIENTE DA REDE

Então aqui está o meu Debian, nesse momento ele está sem nenhuma rede, por que meu pfSense está desligado ainda.



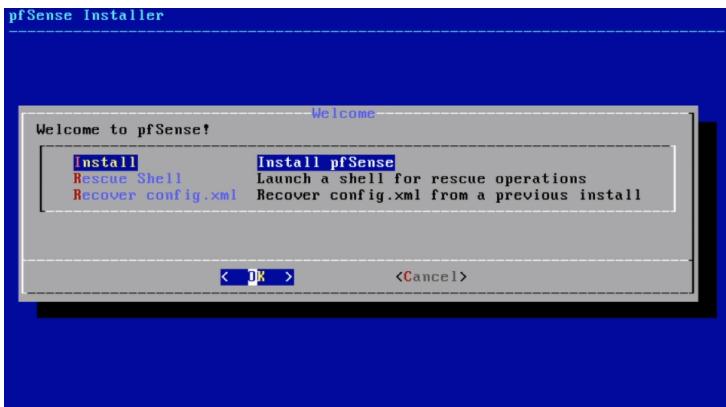
Será com essa máquina que eu irei configurar o pfSense via WEB, você pode usar o seu notebook com Linux, Windows ou MacOS.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

# INSTALAÇÃO DO PFSENSE

Você pode aceitar a opção padrão com a tecla “Enter”.



Lembrando que o pfSense é um freeBSD, então a instalação é bem diferente de uma distro LINUX.

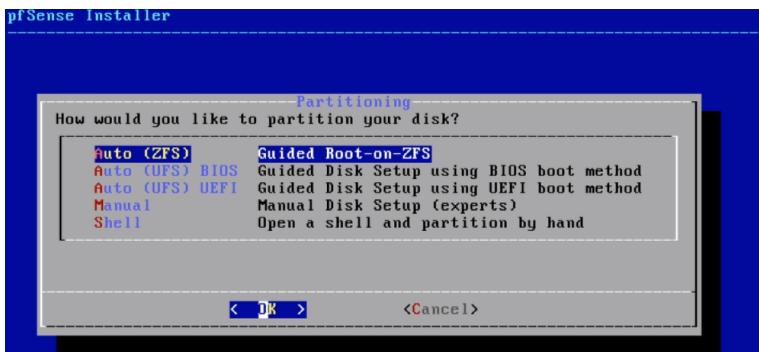
Aguardando o início da configuração, o instalador irá tentar fazer tudo automático.



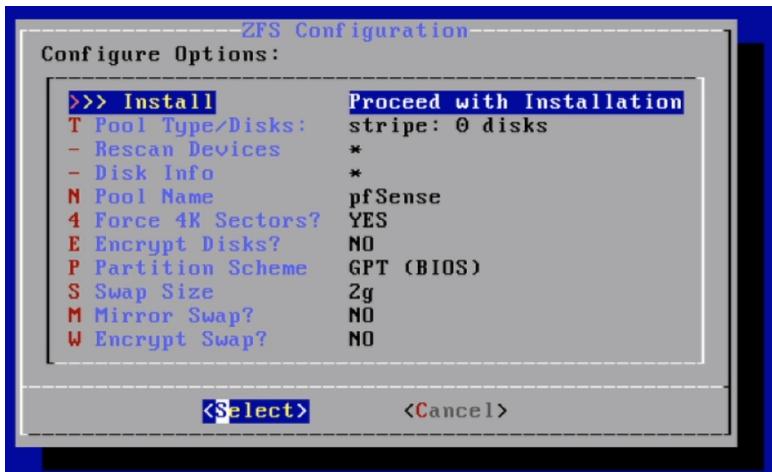
Na tela acima, você precisa selecionar o layout do seu teclado. Na imagem acima está a configuração do meu teclado (que contém “ç”).



Depois de escolher o layout do seu teclado, escolha a opção: “Continue with br.kbd keymap”, no meu caso o br.kbd é o nome do layout que eu escolhi.



Na tela acima você deve escolher a opção Auto (ZFS), para que o instalado do pfsense cuide do particionamento do disco, lembrando que instalado sempre irá utilizar o disco completo, e apagará qualquer informação que você tenha.

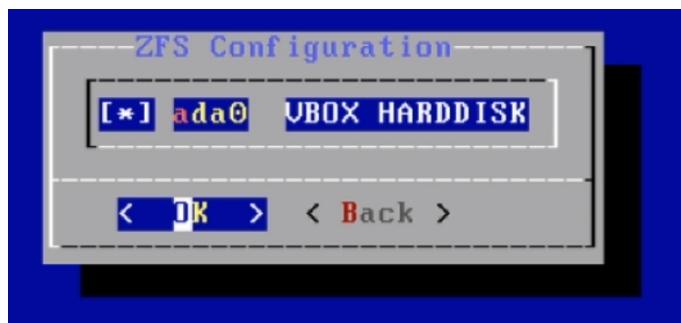


Na tela acima, uma pequena revisão de tudo que será feito em seu disco, você deve escolher a opção “>>> Install : Proceed with Installation”.



Na tela acima, vamos escolher a opção “stripe: Stripe - No Redundancy”.

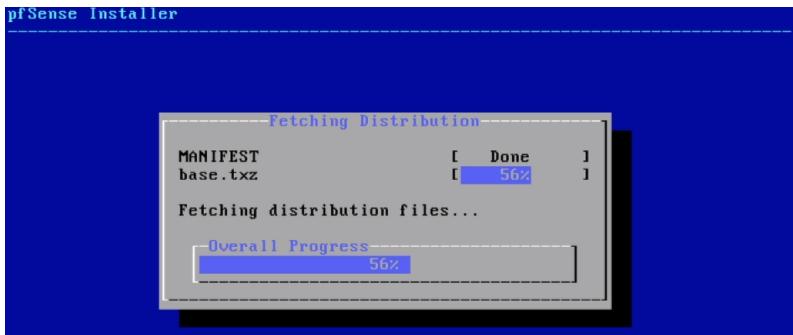
O instalador do pfsense suporta a configuração de vários níveis de raid, para trabalhar com redundância de disco via software. Nesta instalação não iremos configurar raid.



Na tela acima, apenas confirme o disco onde será feito a configuração, no meu caso eu tenho apenas um disco.

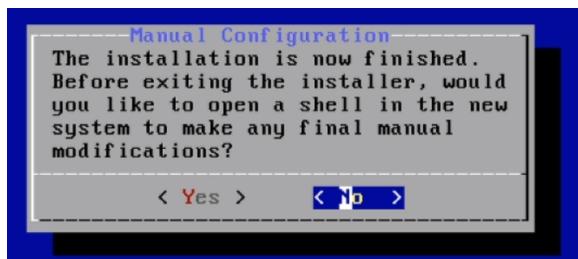


Confirme, que você realmente deseja continuar com a formatação do disco, conforme a tela acima.

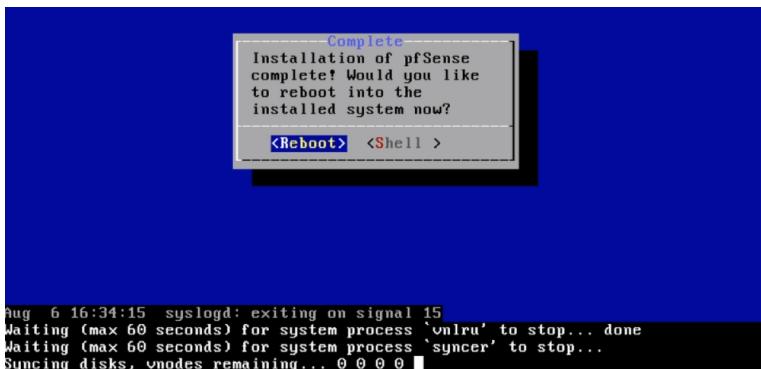


Conforme a tela acima, o processo de instalação do pfsense será iniciado.

É um processo bem rápido, dependendo da configuração de hardware do seu servidor.



Na tela acima, escolha “No” para configurar que você não irá fazer configurações manuais na instalação que acabou de finalizar.



Na tela acima escolha “Reboot”, para reiniciar o sistema do pfSense.

# INICIANDO O PFSENSE

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: ee186486fcf680ab0609

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 10.0.0.192/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

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: ■
```

Neste momento todas as configurações necessárias já estão prontas.

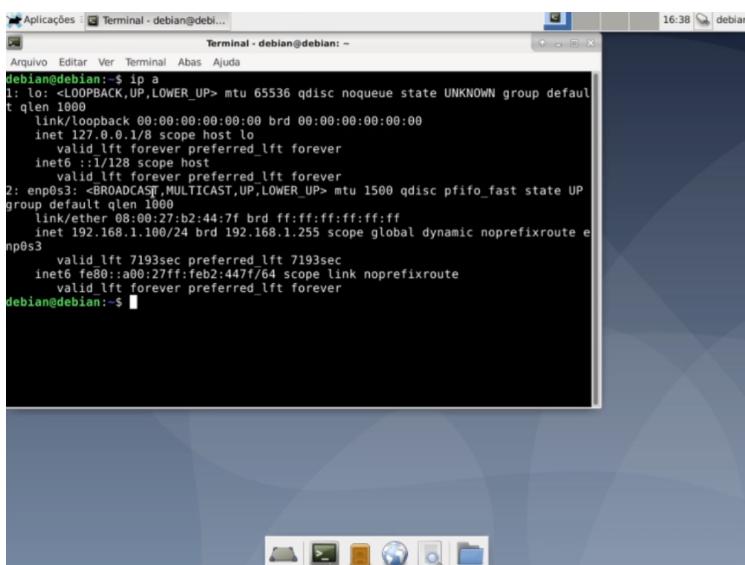
Temos aqui na imagem acima, o IP da WAN que ele pegou por DHCP (o cabo está ligado direto no modem ADSL) e também definiu o IP da LAN.

Então agora o pfSense já está funcionando, se você entrar no seu navegador e digitar o IP da LAN que aparece, iremos entrar na interface web de configuração.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

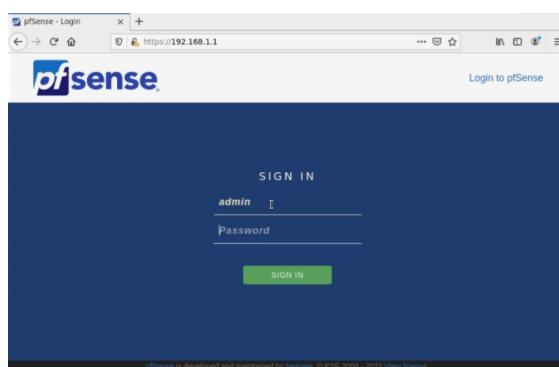
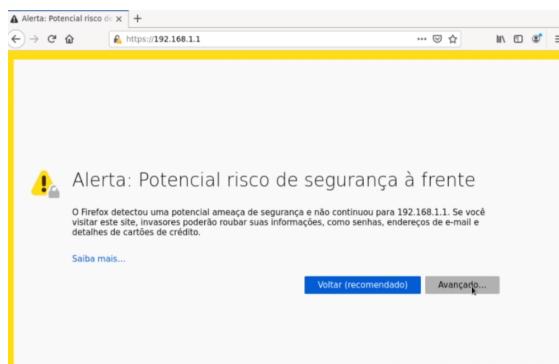
Agora para conhecer um pouco da interface web de configuração do pfSense, podemos entrar no meu Debian (minha máquina cliente da rede, você poderá utilizar qualquer sistema operacional) e mandar ele conectar na rede, iremos ver que o meu Debian já vai pegar um IP, que nesse caso é o IP 192.168.1.100, ou seja já estamos utilizando o DHCP do pfSense.



The screenshot shows a terminal window titled "Terminal - debian@debian:" running on a Debian system. The window displays the output of the "ip a" command, which lists network interfaces and their configurations. The output shows two interfaces: "lo" (loopback) and "enp0s3" (ethernet). The "lo" interface has an IP of 127.0.0.1/8. The "enp0s3" interface has an IP of 192.168.1.100/24. The terminal window is part of a desktop environment with a blue gradient background and various icons in the dock at the bottom.

```
Aplicações Terminal - debian@debian... Terminal - debian@debian: ~
Arquivo Editar Ver Terminal Abas Ajuda
debian@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b2:44:7f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7193sec preferred_lft 7193sec
        inet6 fe80::a00:27ff:feb2:447f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
debian@debian:~$
```

Como eu sei que o IP do pfSense é 192.168.1.1 eu já posso entrar no meu navegador e digitar <https://192.168.1.1>, iremos receber uma informação sobre o SSL, confirme para continuar.



Devemos utilizar o usuário **admin** e a senha **pfSense**

Você irá notar que a interface pfSense já está disponível, já temos as interfaces das regras do firewall, a parte de VPN, serviços, tudo na mão.

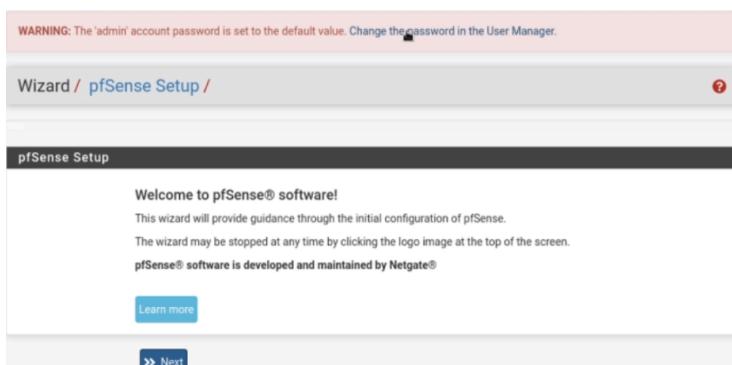
Veja que a rede já está funcional, o pfSense já está atuando como gateway, inclusive eu posso ir no meu computador cliente e dar um ping para qualquer lugar.

Note que ele está liberado, a partir do momento que você configurou o seu cliente já está acessando tudo.

E é realmente um processo totalmente automatizado.

# CONFIGURAÇÃO ESSENCIAL DE FIREWALL

Voltamos agora para a interface Web do pfSense, logando com a senha vista antes.



E agora ele já irá começar configuração, o primeiro passo é configurar uma senha, conforme a imagem acima, escolha a opção “Change the password in the user manager”

Escolha uma nova senha.

The screenshot shows the pfSense dashboard. On the left, there's a sidebar with 'System Information' containing details like Name (pfSense.home.arpa), User (admin@192.168.1.100), System (VirtualBox Virtual Machine), BIOS (Vendor: innoteckGmbH, Version: VirtualBox), Version (2.5.2-RELEASE (amd64)), CPU Type (Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz), and a note about being on the latest version. On the right, there's a 'Netgate Services And Support' section with 'Contract type' set to 'Community Support' and 'Community Support Only'. Below it is a 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' section with a note about purchased support and a link to the 'RESOURCE LIBRARY'. There are also links for 'Upgrade Your Support' and 'Community Support Resources'.

Na tela acima, temos o dashboard do pfSense.

## Configuração de Interfaces

The screenshot shows the pfSense interface configuration screen. The top navigation bar has 'Interfaces' selected. The main content area shows 'Assignments' (selected), 'WAN', and 'LAN'. Below this, there's a 'Status / Dashboard' section with 'System Information' showing Name (pfSense.home.arpa) and User (admin@192.168.1.100 (Local Database)).

A minha WAN já está sendo configurada por DHCP, que está ativo no meu modem ADSL.

Em LAN, podemos escolher um IP diferente para nossa rede.

The screenshot shows the pfSense home interface configuration for the LAN interface. The top bar displays the URL <https://192.168.1.1/interfaces.php?if=lan>. The configuration section for the LAN interface includes:

- IPv4 Address:** 192.168.1.1
- IPv4 Upstream gateway:** None
- Add a new gateway:** A button to add a new gateway.
- Track IPv6 Interface:** WAN
- IPv6 Prefix ID:** 0
- Reserved Networks:**
  - Block private networks and loopback addresses:** An unchecked checkbox with a description about RFC 1918 and RFC 4193 address ranges.
  - Block bogon networks:** An unchecked checkbox with a description about IANA reserved IP addresses.

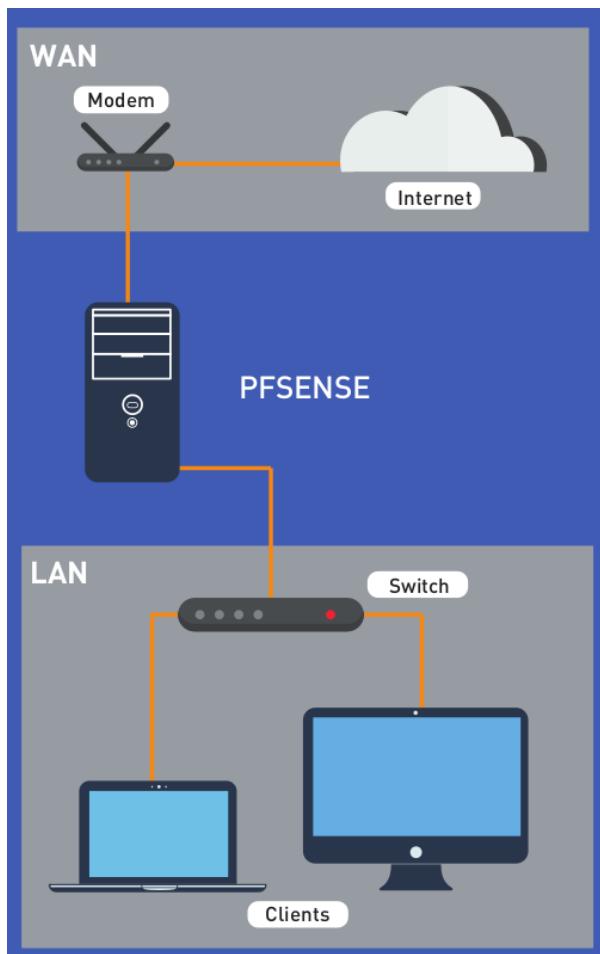
## Regras de Firewall padrão do pfSense

Então como regra geral, o meu cliente, vai conseguir sair para internet, vai conseguir dar

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

PING, enfim, é tudo liberado para os clientes da minha rede.



Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Porém tudo bloqueado para qualquer tipo de entrada para minha rede, pois a interface WAN tem estes bloqueios.

As minhas regras ficam no menu firewall, nesse menu eu encontro as regras de entrada da minha WAN e da LAN.

The screenshot shows the pfSense web interface at https://192.168.1.1/firewall\_rules.php?if=lan. The title bar says "pfSense.home.arpa - Firewall". The navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main menu shows "Firewall / Rules / LAN". Below the menu, there are tabs for Floating, WAN, and LAN, with LAN selected. The main content area is titled "Rules (Drag to Change Order)" and lists the following rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 422 KB	*	*	LAN Address	443 * 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	1 / 97 KB	IPv4 * LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 * LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom are buttons for Add, Add, Delete, Save, and Separator.

Na imagem acima, temos as regras de firewall para a interface LAN

A primeira regra diz o seguinte:

- “Qualquer protocolo, de qualquer origem, com destino para a LAN Address, na porta 443 e 80 será aceito”

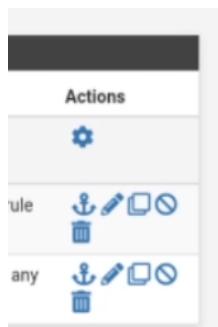
*Essa regra está aqui para aceitar o acesso via porta 443, para que a interface web possa funcionar.*

A segunda regra diz o seguinte:

- “No protocolo IPv4, com origem da LAN net (LAN net é a nossa rede interna), com qualquer protocolo, qualquer destino e qualquer porta, está liberado.

Resumindo, a internet está liberada para todos em nossa rede.

Ao lado direito da tela, você pode mover a regra, editar, excluir ou adicionar uma nova regra.



**No nosso caso vamos editar essa regra,** para criar uma pequena restrição.

## EDITANDO REGRAS DE FIREWALL

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/460 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□ ✓ 4/100 KiB	IPv4	*	LAN net	*	*	*	*	none	Default allow LAN to any rule	
□ ✓ 0/0 B	IPv6	*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Toda regra tem uma ação, a primeira ação é passar, temos também bloquear ou rejeitar.

Com o padrão, essa regra está deixando passar tudo, ou seja está tudo liberado.

Vamos deixar passar apenas alguns protocolos.

Então marque a opção Pass, interface manteremos LAN, em TCP/IP, manteremos o IPv4, e em protocolo vamos escolher UDP.

Temos também como marcar a origem e o destino.

Na origem eu posso dizer que é a LAN Net e o destino posso colocar qualquer um.

Mas o que vou mudar mesmo é a porta de destino (Destination port range), irei escolher apenas DNS(53).

Ou seja, quero liberar no momento apenas o DNS, não esqueça de salvar.

## ADICIONANDO REGRAS DE FIREWALL

Iremos agora adicionar mais uma regra.

Eu liberei a porta 53, então agora para a internet funcionar eu preciso liberar a porta 80.

### ***LIBERANDO A PORTA 80***

Fica assim:

Action -> pass

Interface -> LAN

Protocol -> TCP

Source -> LAN net

Destination : qualquer computador da rede

Destination port range -> HTTP

Veja na imagem abaixo, as duas regras, na segunda linha estamos liberando a porta 53, e estamos liberando a porta 80.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*		none		
<input type="checkbox"/>	<input checked="" type="checkbox"/> 3 /2 KIB	IPv4 UDP	LAN net	*	*	53 (DNS)	*		none		
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /206 KIB	IPv4 TCP	LAN net	*	*	53 (DNS)	*		none	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv6*	LAN net	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator

**Para finalizar eu tenho que aplicar** essas regras, mas antes irei criar mais uma regra.

## LIBERANDO A PORTA 443

Action -> pass

Interface -> LAN

Protocol -> TCP

Source -> LAN net

Destination : qualquer computador da rede

Destination port range -> HTTPS (443)

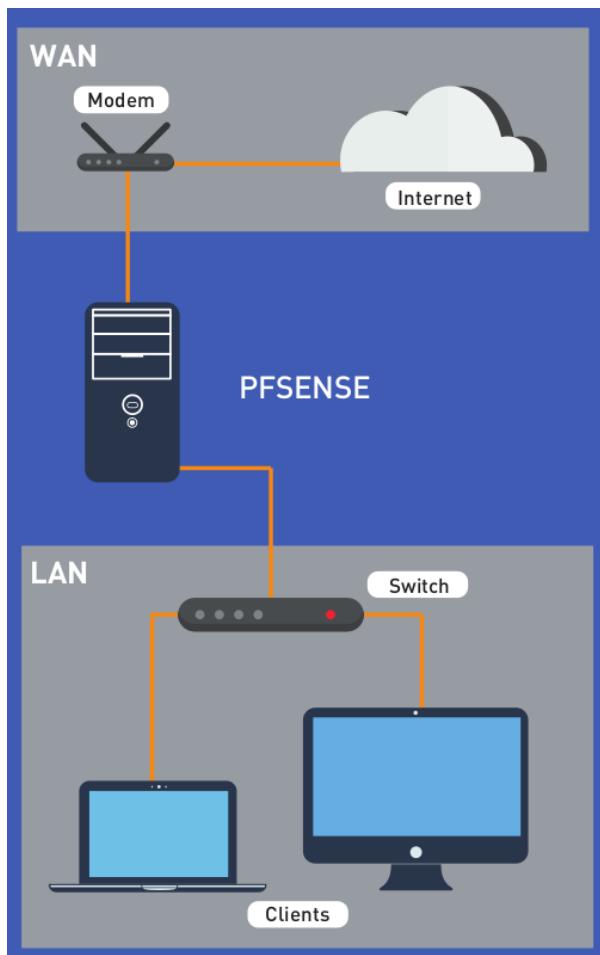
E agora estamos liberando a porta 53, a porta 80 e a porta 443, tudo que preciso para liberar apenas o acesso a internet para a minha rede interna.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	 
<input type="checkbox"/>	✓ 1 /4 KB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			 
<input type="checkbox"/>	✓ 2 /4 KB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			 
<input type="checkbox"/>	✓ 3 /16 KB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none			 
<input type="checkbox"/>	✓ 0 /206 KB	IPv4 TCP	LAN net	*	*	53 (DNS)	*	none		Default allow LAN to any rule	 
<input type="checkbox"/>	✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	 

## Preciso aplicar as novas regras ao meu firewall.

É o básico, para você liberar o acesso a internet de uma rede, passando por um firewall com o pfSense.

# ANALISANDO AS REGRAS DE FIREWALL



Quando acesso a um site já consigo navegar tranquilamente na internet.

Mas se precisar passar um email por exemplo, não vai ser possível, porque só estou liberando para a LAN a porta 53, 80 e 443.

São 3 regras bem básicas, mas que fazem total sentido quando você pensa em fazer uma segurança básica de uma solução conforme o diagrama.

Com essas 3 regras você já tem uma segurança maior para esses computadores, porque está fazendo com que eles passem todas as solicitações por dentro do pfSense.

E você não terá problemas com relação a controles de acesso, por que tudo vai estar controlado pelo pfSense.

Detalhe, o protocolo DNS roda na porta UDP, e os demais na porta TCP.

Lembrando que toda regra tem uma ação, que você libera ou bloqueia, se você não liberar qualquer outra porta, quer dizer que está tudo bloqueado.

Com tudo o que fizemos temos um firewall bem funcional, o mais importante é ficar de olho sempre na Action (ação) que colocou, e qual o protocolo e porta escolher.

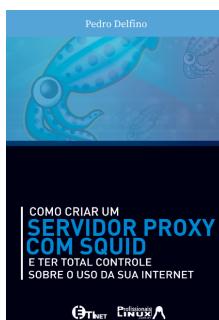
Outra coisa importante é sempre saber de onde vem o protocolo.

# TRABALHANDO COM O PROXY SQUID NO PFSENSE

Iremos fazer uma implementação nova em nosso firewall com pfSense, que é colocar um cache com o famoso Squid.

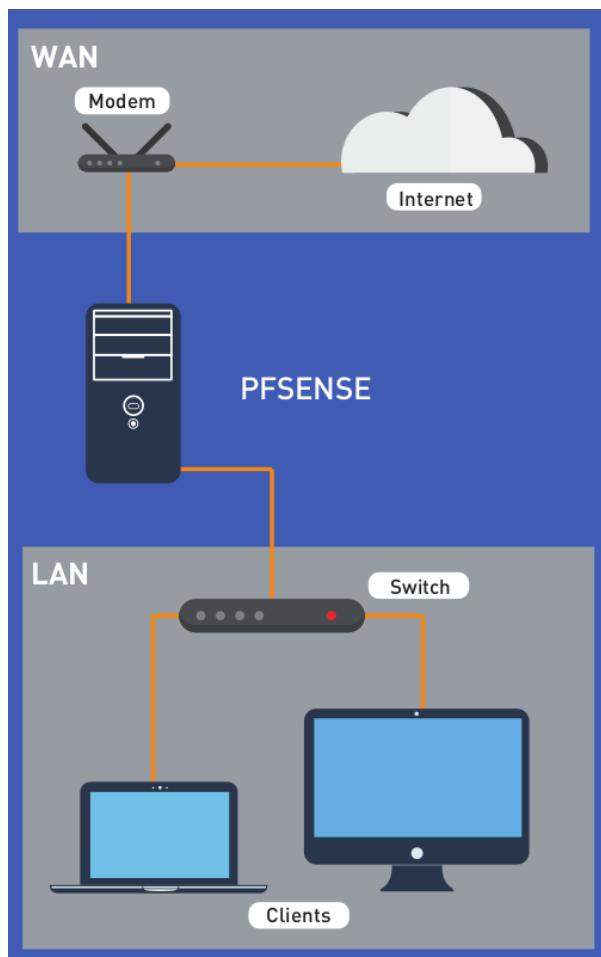
Lembrando que você poderá também fazer download do nosso ebook Como Criar Um Servidor Proxy Com Squid clicando aqui:

(<https://profissionaislinux.com.br/materiais/ebook-proxy-squid/>)



Por: [Pedro Delfino](#)  
[Acesse também o novo método para você dominar o Linux](#)

Então vamos voltar em nosso diagrama para ter uma noção.

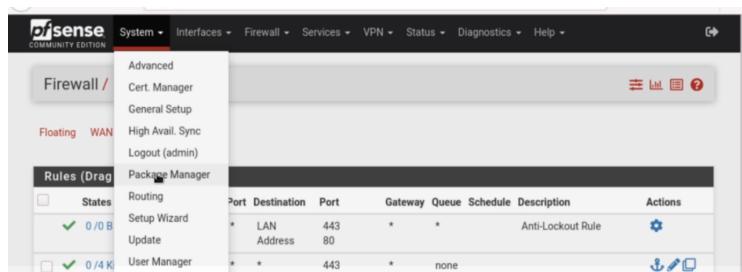


No pfSense podemos instalar facilmente o Squid, temos um gerenciador de pacote dentro dele, que irá baixar alguns adicionais.

Vamos então configurar um Cache, para os computadores da nossa rede, podemos também trabalhar com autenticação, restrição de páginas ou também de tamanho de download, tudo aquilo que tem dentro do proxy com squid pode ser implementado aqui no pfSense.

## INSTALAÇÃO DO SQUID

Para adicionar um novo pacote, vá no menu System -> Packages



Aqui temos os pacotes instalados, e os pacotes disponíveis, para você fazer a instalação.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Você verá que tem vários pacotes, isso tudo é feito de forma online, então você pode adicionar o Apache, o Asterisk... entre outros serviços que já estamos acostumados a utilizar no Linux.

Entre todos estes serviços temos o Squid.

The screenshot shows the pfSense web interface under the 'System / Package Manager / Available Packages' section. A search bar at the top has 'squid' typed into it. Below the search bar, there's a table with two rows. The first row is for 'Lightsquid' version 3.0.6.8, which is described as a high-performance web proxy reporting tool. It lists dependencies on 'lighttpd-1.4.59' and 'lightsquid-1.8\_5'. The second row is for 'squid' version 0.4.45.4, described as a high-performance web proxy cache. It also lists dependencies on 'lighttpd-1.4.59' and 'lightsquid-1.8\_5'. Both rows have a green '+ Install' button to their right.

Name	Version	Description	
Lightsquid	3.0.6.8	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
squid	0.4.45.4	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C!CAP.	+ Install

O processo é simples, só clicar em mais (+ install), e clicar em (confirm).

Ele vai se conectar no site do pfSense e vai baixar o pacote aqui, e disponibilizar toda a configuração desse Squid, nessa mesma interface web, não precisa configurar nenhum arquivo, tudo será feito pela interface web do pfSense.

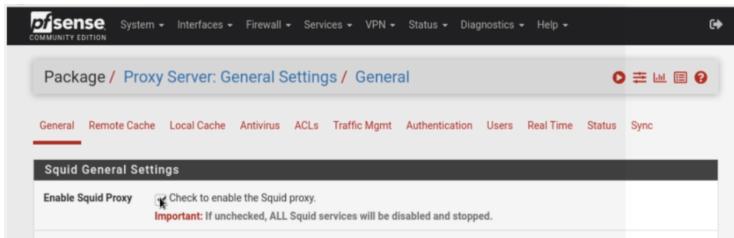
Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

The screenshot shows the pfSense Package Manager interface. At the top, there's a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below that is a breadcrumb trail: System / Package Manager / Package Installer. A message box says "Please wait while the installation of pfSense-pkg-squid completes. This may take several minutes. Do not leave or refresh the page!". Below the message are three tabs: Installed Packages, Available Packages, and Package Installer, with Package Installer being the active one. A progress bar at the bottom indicates "Please wait while the update system initializes".

## CONFIGURAÇÃO ESSENCIAL DO SQUID

The screenshot shows the pfSense Services configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services (which is highlighted), VPN, and Status. The main content area shows the "Status / Dashboard" and "System Information" sections. The "System Information" table provides details about the pfSense setup, including its name, user, system, BIOS, version, and a note that it is on the latest version. To the right of the main content is a vertical sidebar titled "Services" which lists various services: Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, NTP, PPPoE Server, SNMP, and Squid Proxy Server.



Na imagem acima, você deverá habilitar o Squid Proxy.

Temos as principais configurações:

- Proxy interface : LAN
- Allow users on
- Interface: irei liberar

Configuração padrão Squid:

- Porta
- Diretório de Logs
- Hostname

Podemos modificar a linguagem, será utilizado nas mensagens do squid, posso colocar até um DNS alternativo.

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Na opção: Upstream Proxy, eu posso ter vários outros proxy dentro dessa mesma rede e sincronizar a rede dele, é algo bem mais avançado, é interessante para grandes redes.

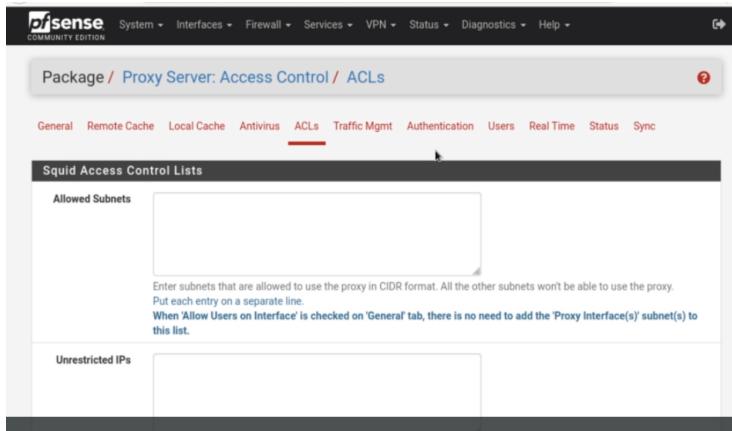
Em Cache Mgmt, eu posso dizer o tamanho do meu Cachê, vou deixar em 100 pois não tenho muito espaço em disco, mas isso depende da sua necessidade.

The screenshot shows a browser window with the URL [https://192.168.1.1/pkg\\_edit.php?xml=squid\\_cache.xml&id=0](https://192.168.1.1/pkg_edit.php?xml=squid_cache.xml&id=0). The page title is "Squid Hard Disk Cache Settings". The configuration fields include:

- Hard Disk Cache Size:** 100 (Amount of disk space in megabytes to use for cached objects)
- Hard Disk Cache System:** ufs (This specifies the kind of storage system to use)
- Clear Disk Cache NOW:** A button to clear the cache immediately.
- Level 1 Directories:** 16 (Specifies the number of Level 1 directories for the hard disk cache)
- Hard Disk Cache Location:** /var/squid/cache (This is the directory where the cache will be stored. Default: /var/squid/cache)
- Minimum Object Size:** 0 (Objects smaller than the size specified in kilobytes will not be saved on disk. Default: 0 (meaning there is no limit))
- Maximum Object Size:** 4 (Objects larger than the size specified can be saved in the cache but not served directly. Default: 4 (4MB))

O tipo de sistema de cache, o mais utilizado é ufs.

Enfim, são algumas configurações que dependem da sua necessidade e o que quer para seu Proxy.



No menu Access Control, na primeira lacuna preencha com a rede que vamos liberar, 192.168.1.0/24 que é minha rede interna.

Mais abaixo temos a Whitelist e Blacklist.

Posso colocar como Whitelist por exemplo, google.com e como Blacklist facebook.com e youtube.com. E assim por diante.

Na próxima aba, Traffic Mgmt, define o tamanho de download que você irá liberar. Você pode ir aumentando isso em kilobytes por exemplo.

Pode dizer também quanto de upload você irá liberar ou não.

São regras para restrição mesmo, bem padrão tudo está disponível no Squid.

Em Auth Settings (forma de autenticação), você pode escolher os métodos de autenticação, você pode inclusive deixar como Local.

The screenshot shows the pfSense web interface with the following details:

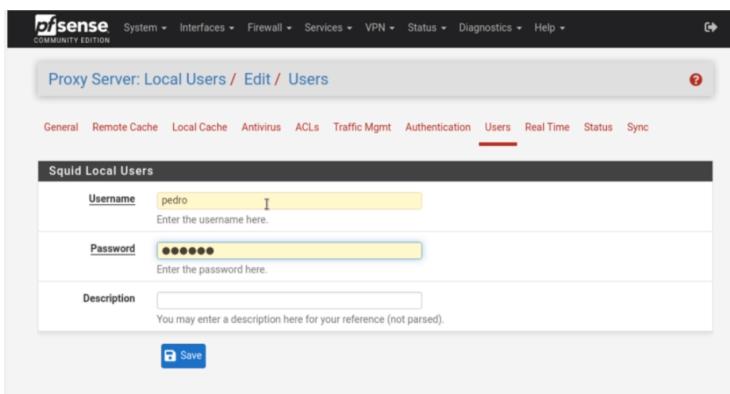
- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Breadcrumbs:** Package / Proxy Server: Authentication / Authentication
- Submenu:** General, Remote Cache, Local Cache, Antivirus, ACLs, Traffic Mgmt, **Authentication**, Users, Real Time, Status, Sync.
- Section:** Squid Authentication General Settings
- Fields:**
  - Authentication Method:** Local (selected)
  - Authentication Server:** [Input field]
  - Authentication server port:** [Input field] (Leave this field blank to use the authentication method's default port.)
  - Authentication Prompt:** [Input field] (Please enter your credentials to access the proxy)
  - Authentication timeout:** [Input field] (Leave this field blank to use the authentication method's default timeout.)

Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

E em Local Users, você pode adicionar novos usuários.

Lembrando que para cada processo, é preciso que salve no final da página. Então com isso, meu proxy inclusive tem autenticação



O serviço do proxy já está configurado, você pode inclusive utilizar este proxy.

Seu proxy será o IP do seu pfSense. Para saber o seu IP é só clicar na própria logo do pfSense, e verificar o IP da LAN.

A porta do seu serviço do proxy, você irá encontrar na parte geral que fica no menu Service->Proxy Server.

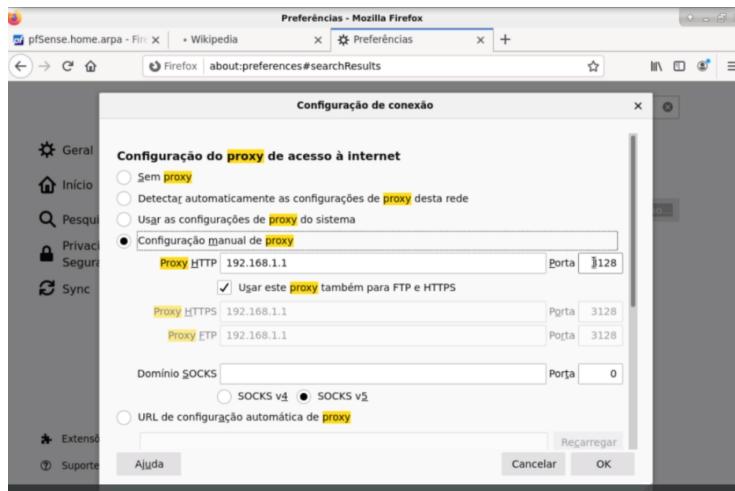
Uma coisa que você também não pode deixar de fazer, é ir em

**Firewall -> Rules -> LAN e liberar a famosa porta 3128, que é a porta padrão do squid.**

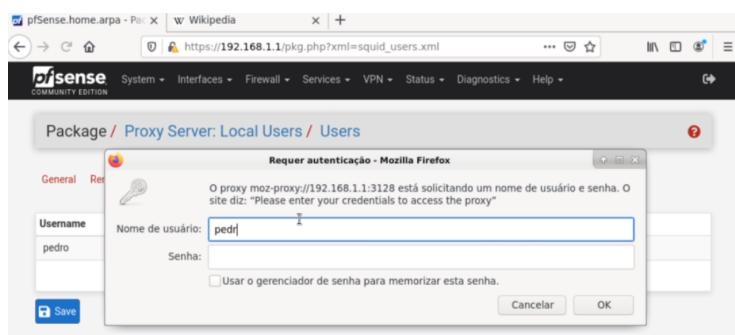
Com isso agora, podemos navegar com o Proxy tranquilamente.

Agora você pode ir no seu navegador, ir em preferências, no caso do firefox.

E configurar o seu proxy:



Basta colocar o IP, e inclusive eu utilizei uma configuração para que não seja utilizado o proxy para determinados endereços.



Por: [Pedro Delfino](#)

[Acesse também o novo método para você dominar o Linux](#)

Quando tento acessar um site irá aparecer uma caixa que solicita login e senha.

Isso porque na configuração do Squid eu disse que o google.com estava em uma “withlist”.

Colocando o Username e senha eu consigo entrar no site normalmente utilizando o proxy.

Com os endereços que coloquei na minha blacklist, tenho um bloqueio imediato, e aparece essa imagem de erro.

Então é uma opção muito rápida para se usar , e eficiente.

Acabamos então de configurar um proxy com Squid.

Podemos ver que a facilidade do pfSense é muito grande, a velocidade também.

É uma configuração muito básica, mas que você pode implementar ela de diversas formas.

Você pode fazer muitas configurações adicionais com essa configuração básica que trabalhamos aqui.

**Uma observação** antes de terminar, caso você deseje que apenas o Squid proxy seja o responsável pelo acesso a internet, **não esqueça de desativar as regras de firewall que estão liberando a porta 80 e 443.**

E-TINET é um projeto pessoal de Pedro Delfino, profissional com mais de 18 anos de experiência em sistemas Linux.

A E-TINET tem como objetivo treinar e capacitar os profissionais de tecnologia a trabalharem com o Linux profissionalmente.

**Instagram:** <https://instagram.com/pedrodelfinoneto/>

**Facebook:** <https://facebook.com/pedrodelfinoneto>

**Youtube:** <https://www.youtube.com/c/Pedrodelfino>

**Blog:** <https://e-tinet.com/blog/>

**Formação Profissionais Linux:**

<https://profissionaislinux.com.br/inscricao/>

**Veja em <https://profissionaislinux.com.br/acesso-nivel-1/> como começar** uma formação Linux profissional **e domine, de uma vez por todas**, esse sistema tão importante para a sua carreira.