

FIREWALL COM Sense

O Guia Rápido para Iniciantes

SOBRE PEDRO DELFINO

Pedro Delfino é o fundador do PROFISSIONAIS LINUX (<http://profissionaislinux.com.br>) que tem como principal objetivo formar novos profissionais para atuar na área de administração de servidores LINUX assim como soluções opensource, é autor do E-tinet, (<http://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 14 anos, e a mais de 3 anos vem ajudando milhares de pessoas a aprender Linux de forma fácil e rápida, através de artigos em seu Blog.



SUMÁRIO

| | |
|---------------------------------------------------|----|
| Introdução | 4 |
| O que é o pfSense? | 6 |
| Fazendo Download da imagem ISO do pfSense | 11 |
| Montando o ambiente de teste para rodar o pfSense | 15 |
| Configuração da máquina cliente da rede | 22 |
| Iniciando o pfSense | 24 |
| Iniciando a configuração do pfSense | 29 |
| Instalação do pfSense | 36 |
| Finalizando a configuração do pfSense | 41 |
| Configuração essencial de Firewall | 48 |
| Editando regras de Firewall | 52 |
| Trabalhando com o Proxy Squid no pfSense | 61 |

INTRODUÇÃO

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.

O QUE É O
PFSENSE?

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.

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.



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;
- antispymware;
- 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, a pesar de gratuito, pode funcionar com excelência equiparável aos mais diversos produtos do mercado.

```
pfSense (pfSense) 2.3-RELEASE amd64 Fri Apr 08 12:18:28 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***
```

Além dessas vantagens o pfSense é considerado muito leve, exigindo baixíssimos requisitos de hardware, é estável, fácil de utilizar (possui até um dashboard e 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.

OPEN SOURCE SECUR

Secure networks start here.™ With thousands of enterprise-grade software, it is becoming the most trusted open source security solution.

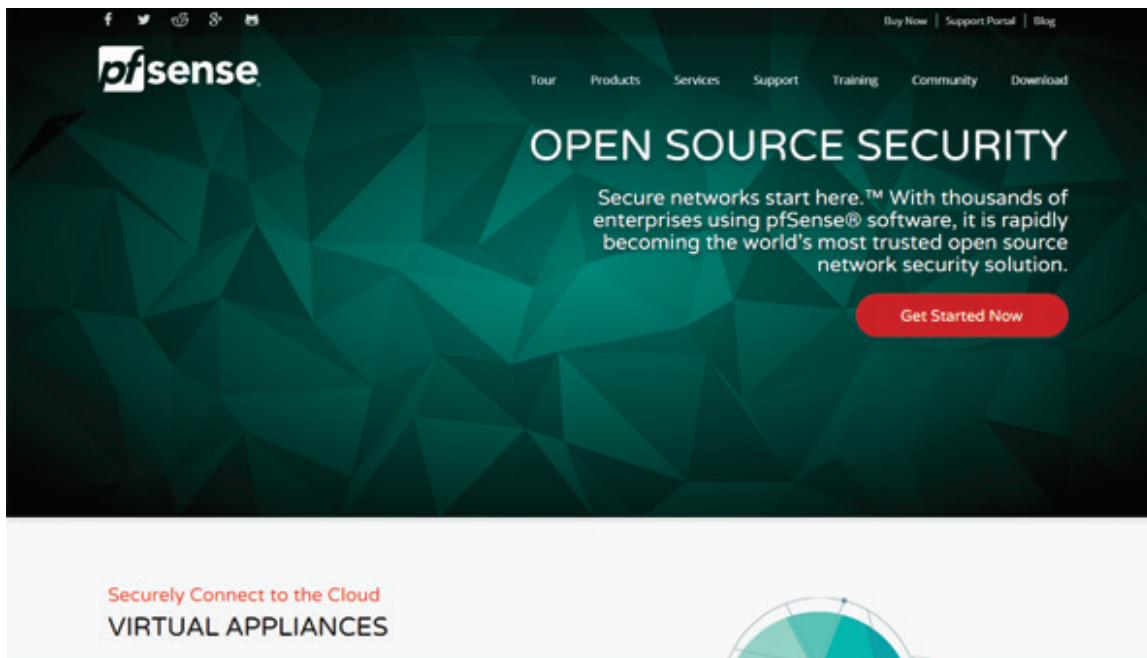
Started M

FAZENDO
DOWNLOAD DA
IMAGEM ISO DO
PFSENSE

Securely Connect to the Cloud
VIRTUAL APPLIANCES

FAZENDO DOWNLOAD DA IMAGEM ISO DO PFSENSE

Então entrando no www.pfsense.org clique em Download.



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

<https://www.pfsense.org/download/mirror.php?section=downloads>

PfSense

Enter your email address to subscribe to our low-volume announcements mailing list:

opens new browser window or tab

Download Full Install

Need to [update an existing installation](#) instead?

Which Image Do I Need?

Computer Architecture:

NOTE: If your system has a 64 bit capable Intel or AMD CPU, use the 64 bit version, 32 bit should only be used with 32 bit CPUs.

Platform:

Or [just show me the mirrors](#) so I can choose which file to download on my own.

Click on a mirror name (second column) to download the appropriate image for the installation information you've selected above.

[MD5 checksum](#) [SHA256 checksum](#)

| Country | Hosting by | Location |
|---------|------------------------------|------------------------|
| | Coltix | Amsterdam, Netherlands |
| | Webcam.Cloud | Ireland |
| | CSR | Austin, TX USA |

Nessa tela você irá escolher então a arquitetura, eu estou usando a AMD64 para computador de 64 bits, você pode usar 32 bits também.

E a plataforma você escolhe a **Live CD**.

Abaixo da terceira seta vermelha, escolha de onde você quer fazer o download da imagem ISO, que tem em média uns 90 MB.



se Backup Tool v1.8 by Koen Zomers

: No arguments provided

SenseBackup.exe -u <username> -p <password> -s <server> [-v <PFS

username of the account to use to log on to
password of the account to use to log on to
P address or DNS name of the pfSense serv
pfSense version. Supported are 1.2, 2.0 ar
Location where to store the backup file (<
ssl: if provided https will be used to co
rd: if provided no RRD statistics data wi
package: if provided no package info data
ent: if provided no output will be shown

ample:

```
pfSenseBackup.exe -u admin -p mypassword -s 192.168.0.1 -u ssl  
pfSenseBackup.exe -u admin -p mypassword -s 192.168.0.1 -o c:\backu  
pfSenseBackup.exe -u admin -p mypassword -s 192.168.0.1 -o c:\backu  
pfSenseBackup.exe -u admin -p mypassword -s 192.168.0.1 -o c:\backu
```

Output:

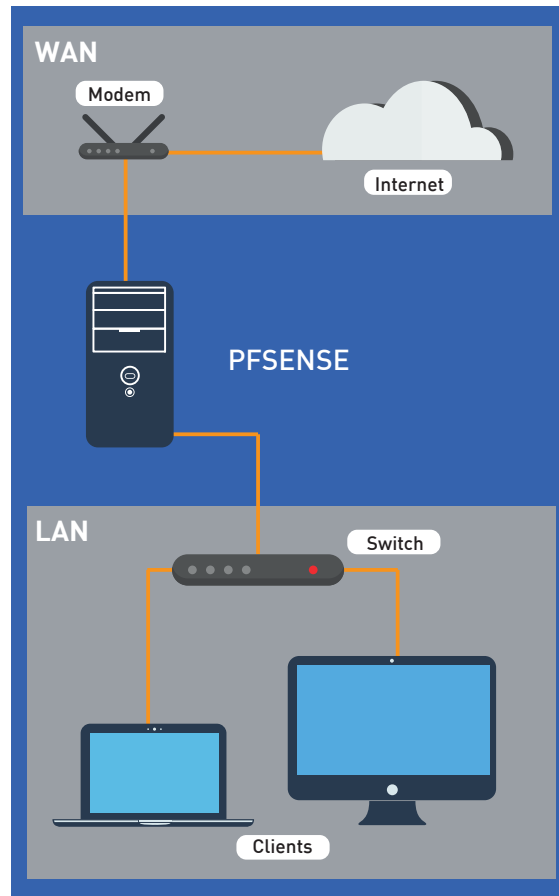
A timestamped file containing the backup will be

C:\>

MONTANDO O
AMBIENTE DE
TESTE PARA
RODAR O PFSENSE

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 fácil montar essa estrutura da imagem a baixo.



Caso você tenha dúvida de como montar uma máquina virtual, pegue uma cópia do ebook Virtualbox: O Guia Passo a Passo (Link: <http://e-tinet.com/lp/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 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.



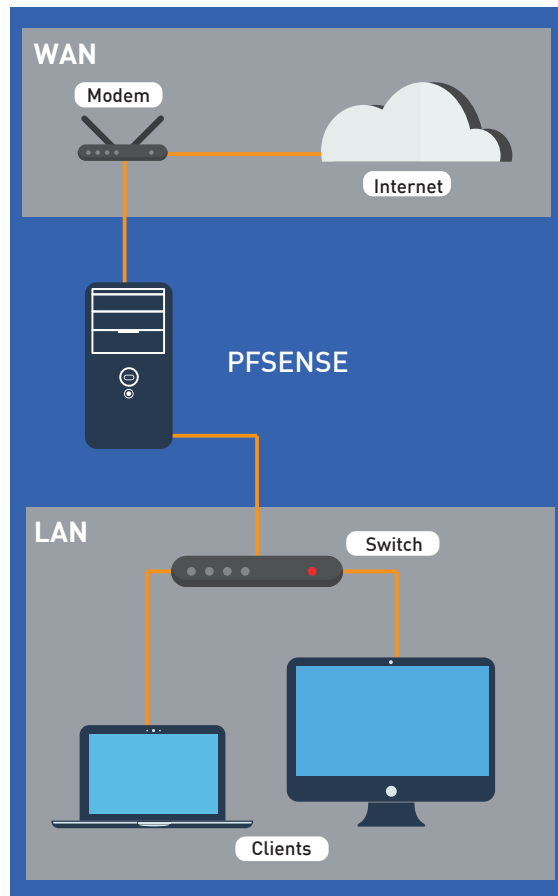
Em minha solução aqui eu irei também montar uma outra máquina para ficar na mesma rede da LAN, ou seja vai ter uma rede interna, onde vou montar um cliente com Ubuntu e este cliente inclusive vou utilizar para acessar as configurações Web do pfSense, e é com ele que vou fazer todas as configurações e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

Então na rede LAN vai estar instalado o Ubuntu, 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 utiliza)
- 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 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

CONFIGURAÇÃO DA MÁQUINA CLIENTE DA REDE

Então aqui está o meu Ubuntu, 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.

```
pedroelfino@pedroelfino-virtual-machine: ~  
pacotes RX:1923 erros:0 descartados:0 excesso:0 quadro:0  
Pacotes TX:1923 erros:0 descartados:0 excesso:0 portadora:0  
colisões:0 txqueuelen:0  
RX bytes:226634 (226.6 KB) TX bytes:226634 (226.6 KB)  
  
pedroelfino@pedroelfino-virtual-machine:~$ ifconfig  
eth0  
Link encap:Ethernet Endereço de HW 00:0c:29:9d:49:7a  
endereço inet6: fe80::20c:29ff:fe9d:497a/64 Escopo:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Métrica:1  
pacotes RX:7572 erros:0 descartados:0 excesso:0 quadro:0  
Pacotes TX:6578 erros:0 descartados:0 excesso:0 portadora:0  
colisões:0 txqueuelen:1000  
RX bytes:4737759 (4.7 MB) TX bytes:1057147 (1.0 MB)  
  
lo  
Link encap:Loopback Local  
inet end.: 127.0.0.1 Masc:255.0.0.0  
endereço inet6: ::1/128 Escopo:Máquina  
UP LOOPBACK RUNNING MTU:65536 Métrica:1  
pacotes RX:1923 erros:0 descartados:0 excesso:0 quadro:0  
Pacotes TX:1923 erros:0 descartados:0 excesso:0 portadora:0  
colisões:0 txqueuelen:0  
RX bytes:226634 (226.6 KB) TX bytes:226634 (226.6 KB)  
  
pedroelfino@pedroelfino-virtual-machine:~$
```

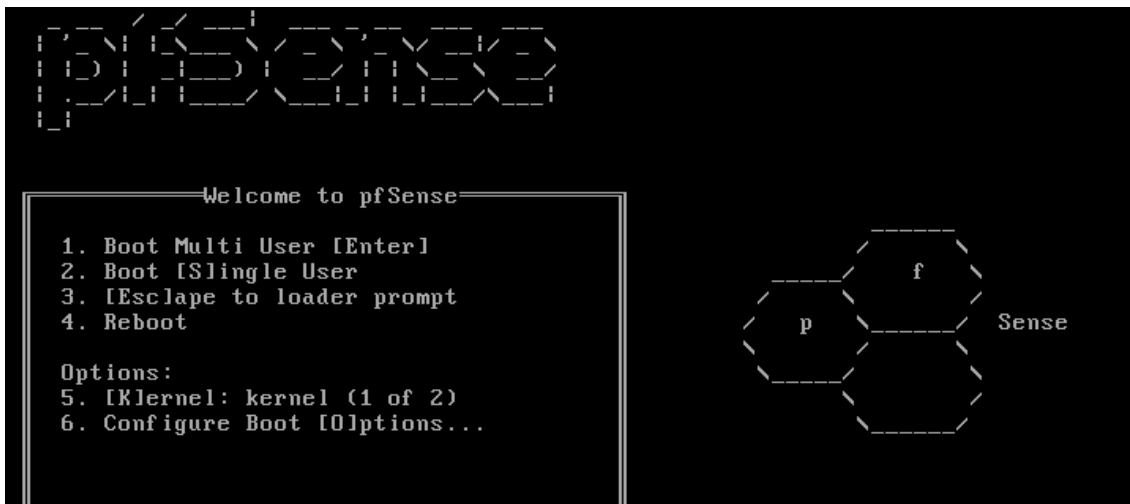
```
=====Welcome to pfSense=====

. Boot Multi User [Enter]
. Boot [S]ingle User
. [E]scape to loader prompt
. Reboot

ptions:
. [K]ernel: kernel (1 of 2)
. Configure Boot [O]ptions...
```

INICIANDO
O PFSENSE

INICIANDO O PFSense



Você pode aceitar a opção padrão com a tecla “Enter” ou esperar os 9 segundos, a instalação irá começar.

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.

```
[ Press R to enter recovery mode or ]  
[   press I to launch the installer   ]  
  
(R)ecovery mode can assist by rescuing config.xml  
from a broken hard disk installation, etc.  
  
(I)nstaller may be invoked now if you do  
not wish to boot into the liveCD environment at this time.  
  
(C) continues the LiveCD bootup without further pause.  
Timeout before auto boot continues (seconds): 6█
```

Irei pressionar **C** para dizer que quero continuar com o boot .

E você verá que o instalador do pfSense vai fazer tudo automático.

```
Starting CRON... done.
an 7 18:15:04 php-fpm[6487]: /rc.start_packages: Restarting/Starting all packa
es.
fSense (cdrom) 2.2.6-RELEASE amd64 Mon Dec 21 14:58:08 CST 2015
ootup complete

reeBSD/amd64 (pfSense.localdomain) (ttyv0)

** Welcome to pfSense 2.2.6-RELEASE-cdrom (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.168.169/24
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) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade 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

9) Install pfSense to a hard drive, etc.

Enter an option: ^[[J
```

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.

Nessa mesma tela eu já consigo fazer a instalação, fazer algumas configurações inclusive.

Lembrando, o **pfSense** já está configurado como **LIVE**, nós iremos ainda fazer a instalação dele em nosso disco rígido.

INICIANDO A CONFIGURAÇÃO DO PFSENSE

p Sense

Welcome to pfSense 2.0.1-RELEASE

Mounting unionfs directories.

Creating symlinks.....done.

Launching the init system...

Initializing.....

Starting device manager (dev

[Press R to enter recovery

[press I to launch the ins

(R)ecovery mode can assist

from a broken hard disk ins

(I)nstaller may be invoked

not wish to boot into the

(C)ontinues the LiveCD bo

Timeout before auto boot c

INICIANDO A CONFIGURAÇÃO DO PFSense

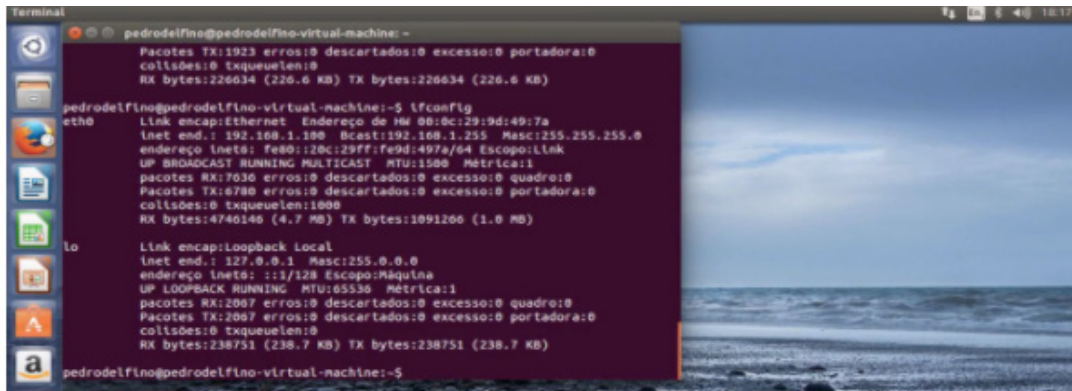
Então este é o modo de configuração do pfSense, iremos voltar nesta tela logo para fazer a instalação definitiva do pfSense em nosso servidor.

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.168.169/24
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) pfSense Developer Shell
4) Reset to factory defaults   13) Upgrade 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

39) Install pfSense to a hard drive, etc.

Enter an option: ^[[J
```

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



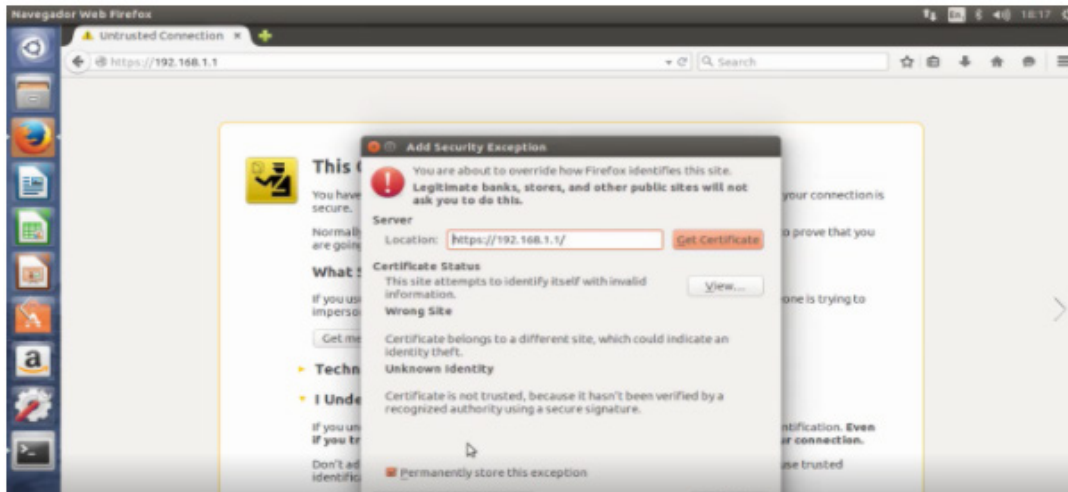
```
Terminal
pedroelfino@pedroelfino-virtual-machine: ~
Pacotes TX:1923 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:226634 (226.6 KB) TX bytes:226634 (226.6 KB)

pedroelfino@pedroelfino-virtual-machine:~$ ifconfig
eth0
Link encap:Ethernet Endereço de HW 08:0c:29:9d:49:7a
Inet addr: 192.168.1.100 Bcast:192.168.1.255 Masc:255.255.0
endereço Inets: fe80::20c:29ff:fe9d:497a/64 Escopo:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Métrica:1
pacotes RX:7036 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:6780 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:1000
RX bytes:4746146 (4.7 MB) TX bytes:1091266 (1.0 MB)

lo
Link encap:Loopback Local
Inet addr: 127.0.0.1 Masc:255.0.0.0
endereço Inets: ::1/128 Escopo:Máquina
UP LOOPBACK RUNNING MTU:65536 Métrica:1
pacotes RX:2067 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:2067 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:238751 (238.7 KB) TX bytes:238751 (238.7 KB)

pedroelfino@pedroelfino-virtual-machine:~$
```

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.



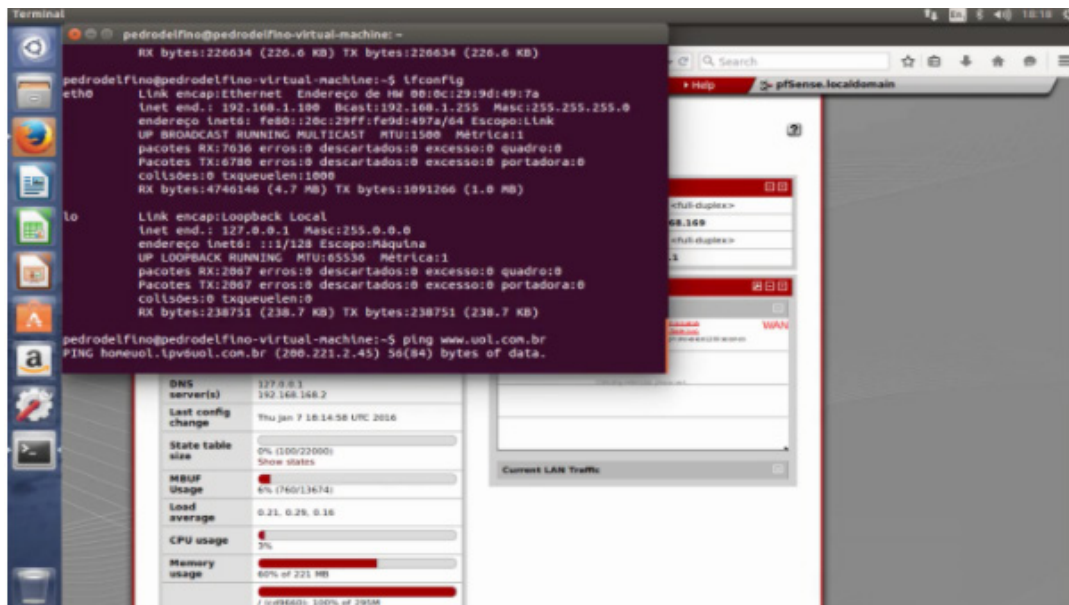
Devemos utilizar o usuário admin e a senha pfSense



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

Mas um detalhe, aqui ele ainda não está instalado no disco rígido, está funcionando como uma live CD. Inclusive eu posso adicionar novas configurações na tela inicial.

Veja que a rede já está funcional, o pfSense já está atuando como gateway, inclusive eu podemos 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.



INSTALAÇÃO DO PFSENSE

INSTALAÇÃO DO PFSense

```
LAN (wan)      -> em0      -> v4/v6: 192.168.168.169/24
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) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system           14) Enable Secure Shell (ssh)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

99) Install pfSense to a hard drive, etc.
Enter an option: ^[[J
```

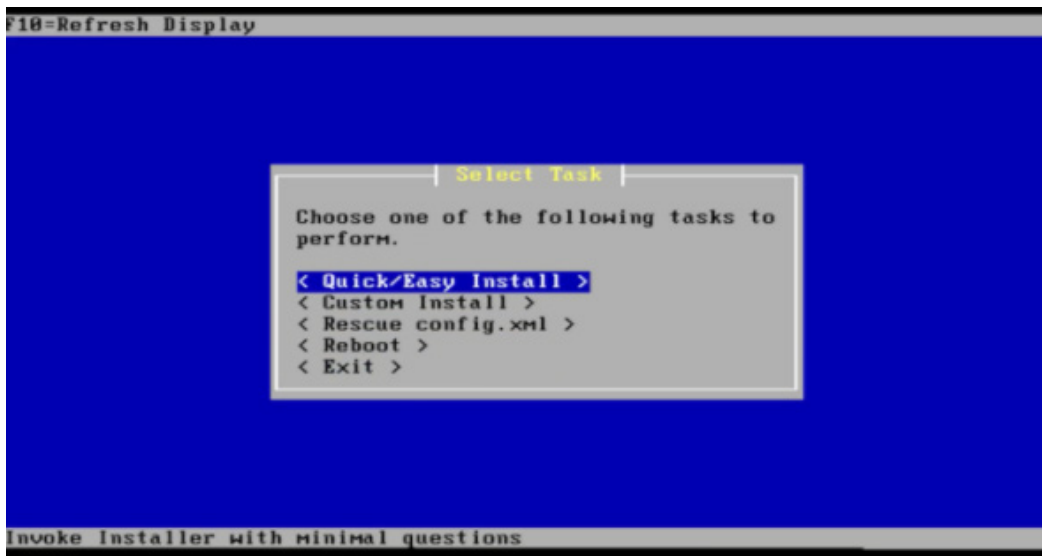
Voltando a tela do pfSense, vamos digitar 99, que é “Install pfSense to a hard drive”.

```
99) Install pfSense to a hard drive, etc.
Enter an option: 99

Launching pfSense Installer...

kern.geom.debugflags: 0 -> 16
VMware detected. The installer will make changes to tune this host..
```

Na próxima tela temos várias configurações, teclado, vídeo, mas eu vou simplesmente aceitar as configurações e escolher **Quick/Easy Install** → OK



Você vai ver que o processo é bem rápido. É só aguardar fazer a instalação.



Escolha a opção **Reboot** e aguarde

Você pode notar então que irá aparecer o usuário e senha.

Username: admin

Password: pfsense

```
*DEFAULT Username*: admin  
*DEFAULT Password*: pfsense  
Rebooting in 5 seconds. CTRL-C to abort.
```

Vamos aguardar o boot agora.

O sistema já está inicializado, é só aguardar o início do processo já fazendo o boot pelo HD, já não estamos mais fazendo o boot via live CD.

Você pode ver que as configurações permanecem, a primeira interface Em0 está com o IP externo da minha rede. Este IP externo está sendo atribuído via DHCP.

Você pode notar que ele realmente está instalado, porque não temos mais a opção 99 para instalar no hard disk.


```
Welcome to pfSense 2.0.1-RELEASE ...  
Mounting unionfs directories...done.  
Creating symlinks.....done.  
Launching the init system... done.  
Initializing.....  
Starting device management...done.
```

```
[ Press R to enter recovery mode ]  
[ press I to install ]
```

```
(R)ecover mode  
from a broken environment etc
```

```
(I)nstaller may  
not wish to boot in this environment
```

```
(C)ontinues the Linux boot process without further
```

```
Timeout before auto boot continues (seconds)
```

FINALIZANDO A
CONFIGURAÇÃO
DO PFSENSE

FINALIZANDO A CONFIGURAÇÃO DO PFSense

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

E agora ele já irá começar o wizard de configuração, porque agora vamos salvar tudo em nosso HD.



Seguimos então escolhendo a opção **next**.

On this screen you will set the general pfSense parameters.

General Information

| | |
|-----------|--------------------------------------------------------------------|
| Hostname: | <input type="text" value="pfsense"/> EXAMPLE: myserver |
| Domain: | <input type="text" value="mydomain.com"/> EXAMPLE: mydomain.com |

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

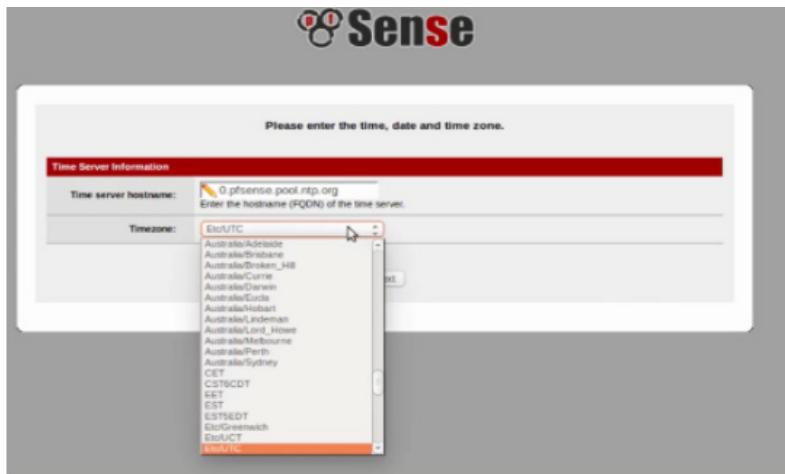
| | |
|-----------------------|-------------------------------------------------------------------------------------------|
| Primary DNS Server: | <input type="text"/> |
| Secondary DNS Server: | <input type="text"/> |
| Override DNS: | <input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN |

Next

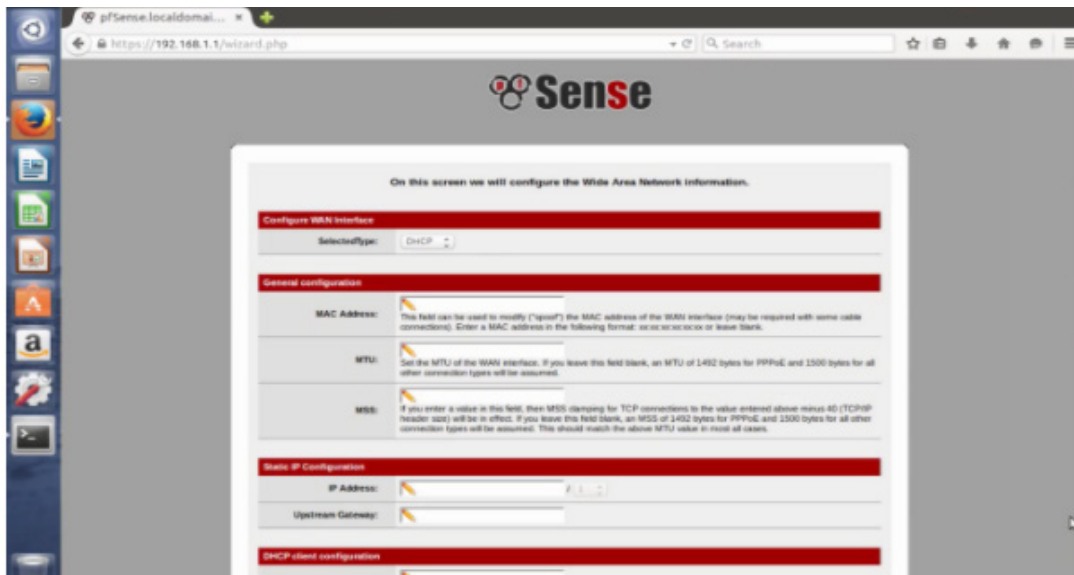
Agora vou escolher um **Hostname, Domínio e DNS (utilizei o do google 8.8.8 e 8.8.8.4)**

Irei deixar marcado a opção “Override DNS” para subscrever e usar o DNS que escolhe e ignorar a configuração do meu modem ADSL.

Na próxima tela eu irei escolher onde vou sincronizar a hora do meu servidor. Para isso basta escolher a região onde você está.



Agora a configuração da WAN



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

Mais abaixo tem a configuração onde vamos simplesmente bloquear todos os pacotes, que podem ser pacotes não identificados. Isso já é mais uma questão de segurança.

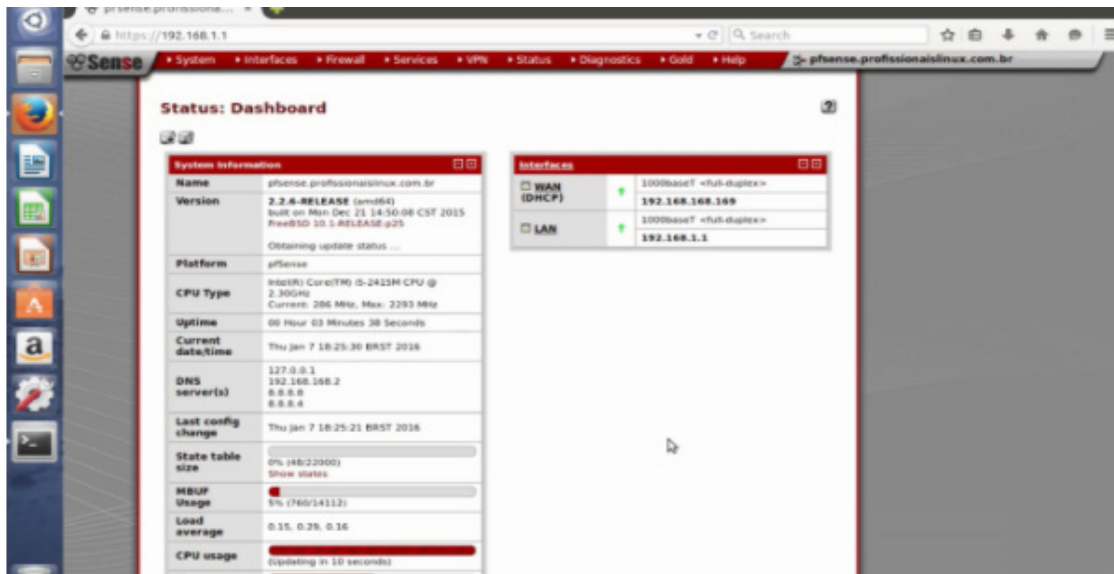
Na próxima tela podemos escolher um IP diferente para sua rede, caso tivesse um outro IP.

Agora o próximo passo é colocar uma outra senha de minha escolha.


Lembrando que o usuário vai ser o admin ainda.



Tudo pronto, escolha a opção “Next” para finalizar a configuração do pfSense.



Com o processo finalizado, clique em continuar e pronto.

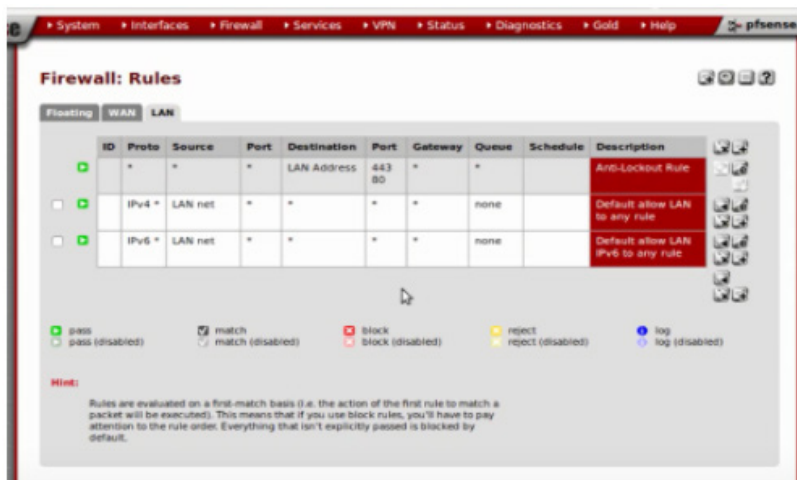
The background of the slide is a blurred image of hands typing on a laptop keyboard, overlaid with a semi-transparent blue filter. A large, solid blue circle is positioned in the center-right of the slide, containing the title text.

CONFIGURAÇÃO ESSENCIAL DE FIREWALL

CONFIGURAÇÃO ESSENCIAL DE FIREWALL

Então como regra geral, o meu cliente, vai conseguir sair para internet, vai conseguir dar PING, enfim, é tudo liberado.

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



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

A primeira regra diz o seguinte:

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

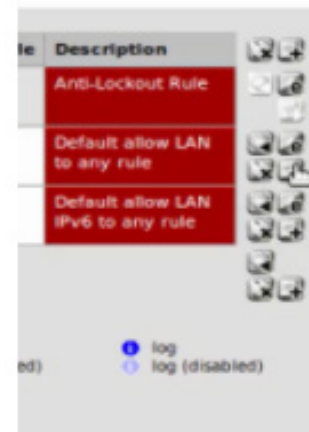
Essa regra está aqui para aceitar o acesso via porta 443, para que a interface web possa funcionar.

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 para qualquer gateway: Resumindo internet 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.



A blue-tinted background image showing a person in profile, looking at a computer screen. The person's hand is resting on their chin. The computer screen displays a complex interface with various windows and data, including a table with columns and rows of text.

EDITANDO REGRAS DE FIREWALL

EDITANDO REGRAS DE FIREWALL



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 passando 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 destino.

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



LIBERANDO A PORTA 53

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 na quarta linha estamos liberando a porta 80.



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 temos 3 regras, 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.

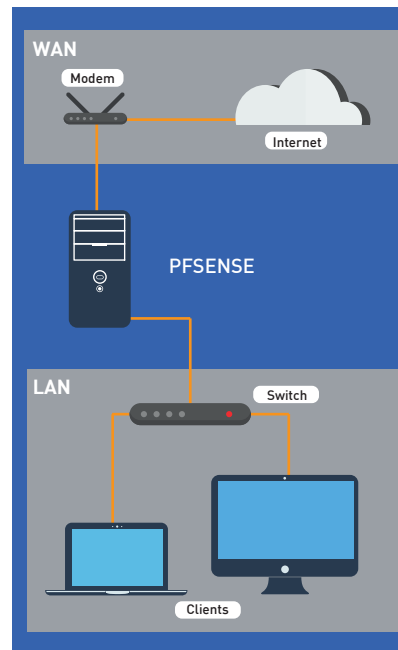
Preciso aplicar nas novas regras ao meu firewall.

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, por que só estou liberando para a LAN a porta 53, 80 e 443.

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



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 liberou 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



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.

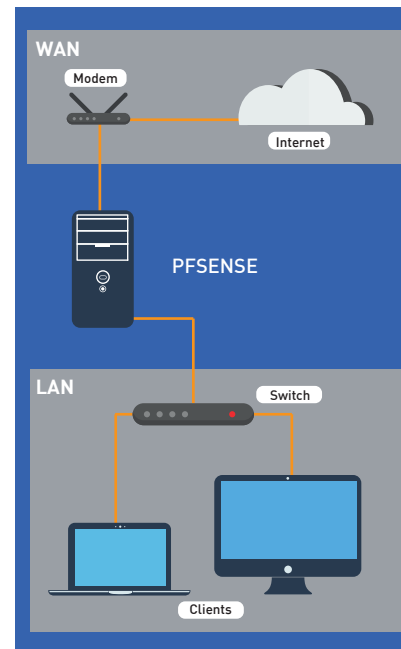
Lembrando que você poderá também fazer download do nosso ebook Como Criar Um **Servidor Proxy Com Squid** clicando aqui:
(<http://e-tinet.com/materiais/ebook-proxy-squid/>)



Então vamos voltar em nosso diagrama para ter uma noção

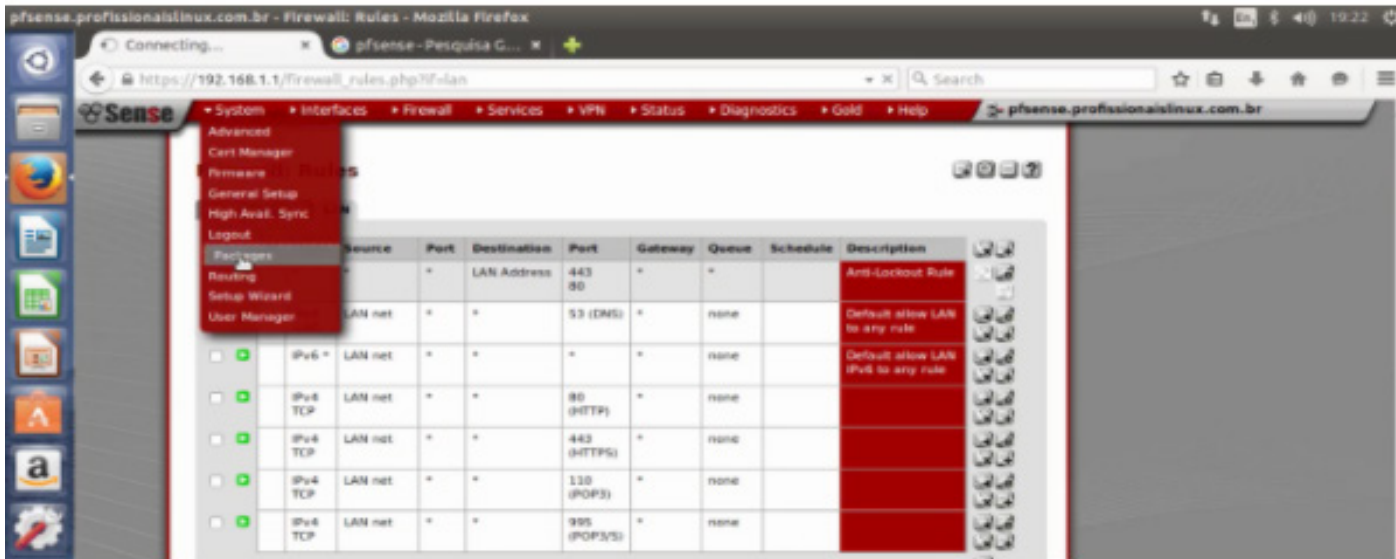
No **pfSense** podemos instalar facilmente o **Squid**, temos um gerenciador de pacote dentro dele, que irá baixar alguns adicionais.

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**



pfSense System Package Manager - Mozilla Firefox

https://192.168.1.1/pkg_mgr.php

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

| Package Name | Category | Version | Platform | Description |
|------------------|--------------------|----------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arping | Network Management | RELEASE 1.2.1 | platform: 2.2 | Broadcasts a who-has ARP packet on the network and prints answers. |
| arpswitch | Network Management | ALPHA 1.1.5 | platform: 2.2 | Arpswitch monitors Ethernet to IP address pairings. It logs certain changes to syslog. |
| Asterisk | Services | BETA 0.3.4 | platform: 2.2 | Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server. |
| AutoConfigBackup | Services | RELEASE 1.34 | platform: 2.2 | Automatically backs up your pfSense configuration. All contents are encrypted before being sent to the server. Requires Gold Subscription from . |
| Avahi | Network Management | BETA 1.10.4 | platform: 2.2 | Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. This enables you to plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. In addition it supports some nifty things that have never been seen elsewhere like correct mDNS reflection across LAN segments. Compatible technology is found in Apple MacOS X (branded Bonjour and sometimes Zeroconf). |
| Backup | System | BETA 0.2.1 | platform: 2.2 | Tool to Backup and Restore files and directories. |
| bacula-client | Services | RELEASE 1.8.12 | platform: 2.2 | Bacula is a set of Open Source computer programs that permit managings backups, recovery, and verification of computer data across a network of computers of different kinds. |
| bandwhichd | Network Management | BETA 0.6.3 | platform: 2.2 | Bandwhichd tracks usage of TCP/IP network subnets and builds snm files with graphs to display utilization. Charts are built by individual IP's, and by default display utilization over 3 day, 6 day, 10 day, and 30 day periods. |

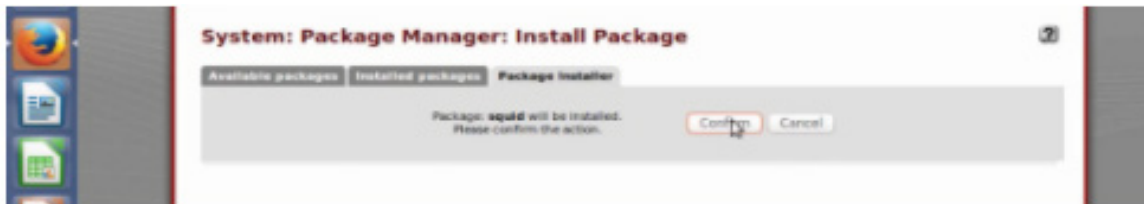
Aqui temos os pacotes instalados, e os pacotes disponíveis, para você fazer a instalação.

Você irá ver 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**. Tem duas versões disponíveis, a dois e três, vamos utilizar a versão dois.

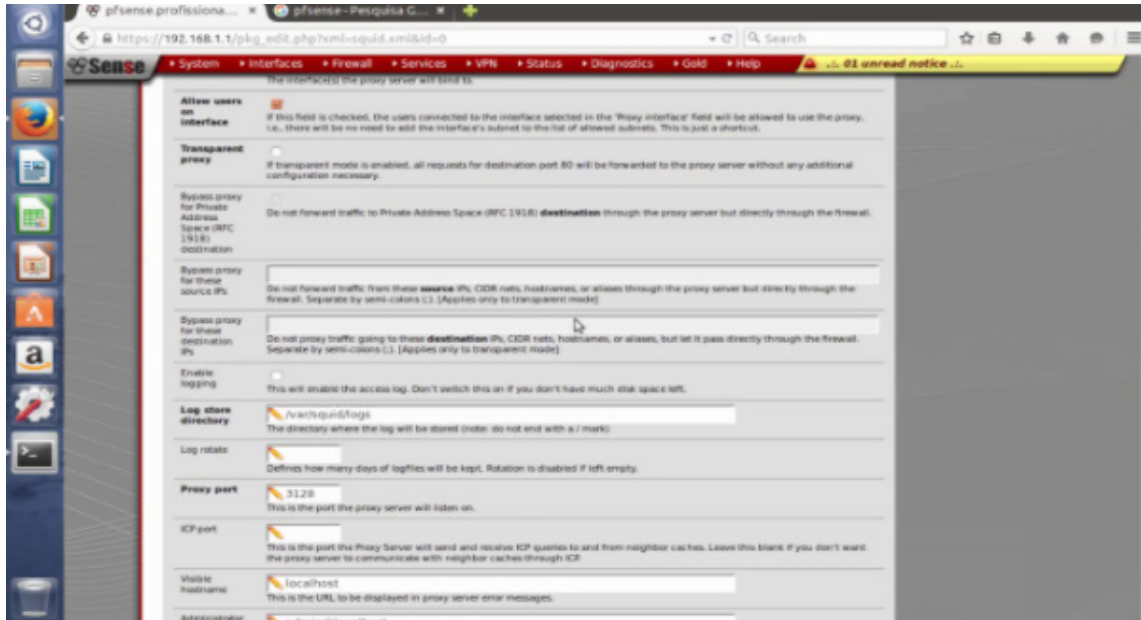


O processo é simples, só clicar em mais (+), e clicar em **confirm**.



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

OPÇÕES DA CONFIGURAÇÃO DO SQUID



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.

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 Cache, vou deixar em 100 pois não tenho muito espaço em disco, mas isso depende da sua necessidade.

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

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

CONFIGURAÇÃO ESSENCIAL DO SQUID

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, **www.google.com** e como **Blacklist** **www.facebook.com** e **www.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**.

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 ir 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.



The screenshot shows the pfSense Firewall Rule configuration page for the LAN interface. The rule is configured to allow TCP traffic from any source to any destination on port 3128. The 'Log' checkbox is checked, and the 'Description' field is empty.

Interface: LAN
Choose which interface packets must be sourced on to match this rule.

TCP/IP Version: IPv4 Select the Internet Protocol version this rule applies to

Protocol: TCP
Choose which IP protocol this rule should match.
Hint: In most cases, you should specify TCP here.

Source: ☐ not
Use this option to invert the sense of the match.
Type: any
Address: [127.0.0.1]
Advanced Show source port range

Destination: ☐ not
Use this option to invert the sense of the match.
Type: any
Address: [127.0.0.1]

Destination port range: From: (other) 3128 To: (other) 3128
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port

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 you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics > System logs > Settings page).

Description: You may enter a description here for your reference.

Save Cancel

Com isso agora, podemos navegar com o Proxy tranquilamente.

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

The screenshot shows the PfSense Firewall Rule configuration page. The rule is named 'LAN'. The interface is set to 'LAN'. The TCP/IP version is 'IPv4'. The protocol is 'TCP'. The source is 'any' and the destination is 'any'. The destination port range is '3128'. The log checkbox is checked.

Interface: LAN
Choose which interface packets must be sourced on to match this rule.

TCP/IP Version: IPv4
Select the Internet Protocol version this rule applies to

Protocol: TCP
Choose which IP protocol this rule should match.
Hint: In most cases, you should specify TCP here.

Source: ☐ not
Use this option to invert the sense of the match.
Type: any
Address: 1.1.1.1
Advanced - Show source port range

Destination: ☐ not
Use this option to invert the sense of the match.
Type: any
Address: 1.1.1.1

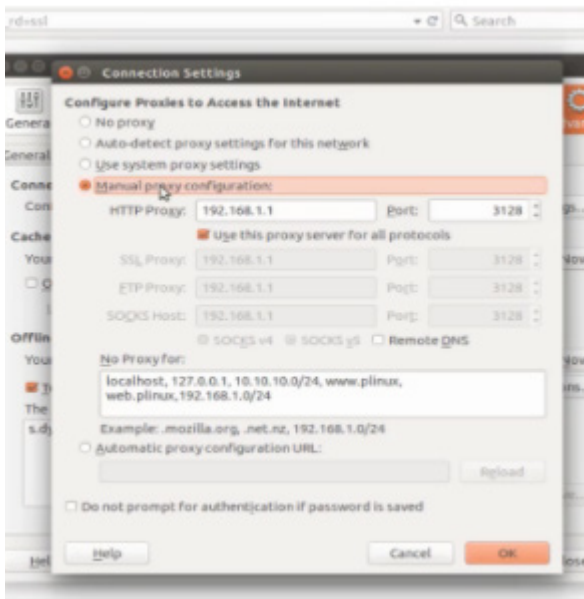
Destination port range: from: (other) 3128 to: (other) 3128
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port

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 you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Description: You may enter a description here for your reference.

Save Cancel

E configurar o seu proxy

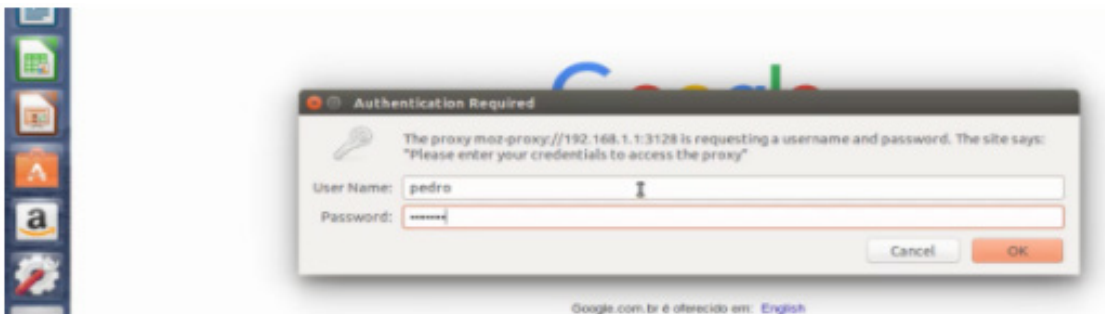


E configurar o seu proxy

Basta colocar o IP, e inclusive eu utilizei uma configuração para que não seja utilizado o proxy para determinado endereços, você pode conferir isso na imagem acima.

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

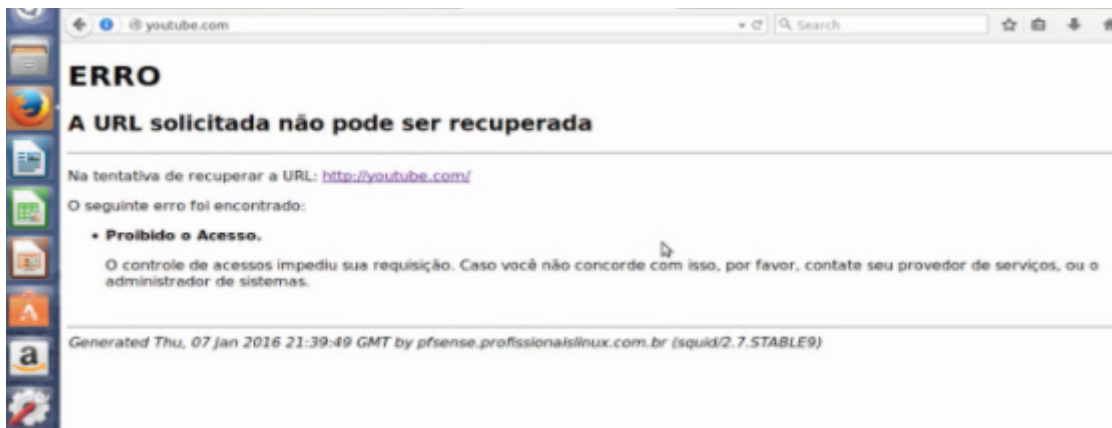
Isso porque na configuração do Squid eu disse que o google.com estava em uma whitelist.



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.



E-TINET é um projeto pessoal de Pedro Delfino, profissional com mais de 14 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.

[Veja aqui](#) como começar uma formação Linux profissional e domine, de uma vez por todas, esse sistema tão importante para a sua carreira.