

CONSTRUINDO UM FIREWALL NO LINUX DEBIAN 6.0

Gerson Ribeiro Gonçalves
www.websolutti.com.br

Sumário

1 INSTALANDO DEBIAN.....	3
2 COMANDOS BÁSICO DO EDITOR VIM.....	11
3 CONFIGURANDO IP ESTÁTICO PARA REDE LOCAL.....	12
4 CONFIGURANDO DHCP.....	13
5 INICIANDO BIND.....	14
6 CONFIGURANDO SQUID.....	14
7 CONFIGURANDO SCRIPT FW.SH.....	16
8 CONFIGURANDO SINCRONIZAÇÃO DO RELÓGIO.....	17
9 INSTALANDO E CONFIGURANDO SARG (RELATÓRIO DO SQUID).....	18
10 CONFIGURANDO SARG.....	19
11 INSTALANDO WEBMIN (GERENCIADOR DE CONFIGURAÇÕES WEB).....	21
12 INICIALIZANDO SERVIÇOS NA INICIALIZAÇÃO.....	21
13 REINICIANDO SISTEMA.....	22
14 ADICIONANDO BLOQUEIOS DE SITES.....	22

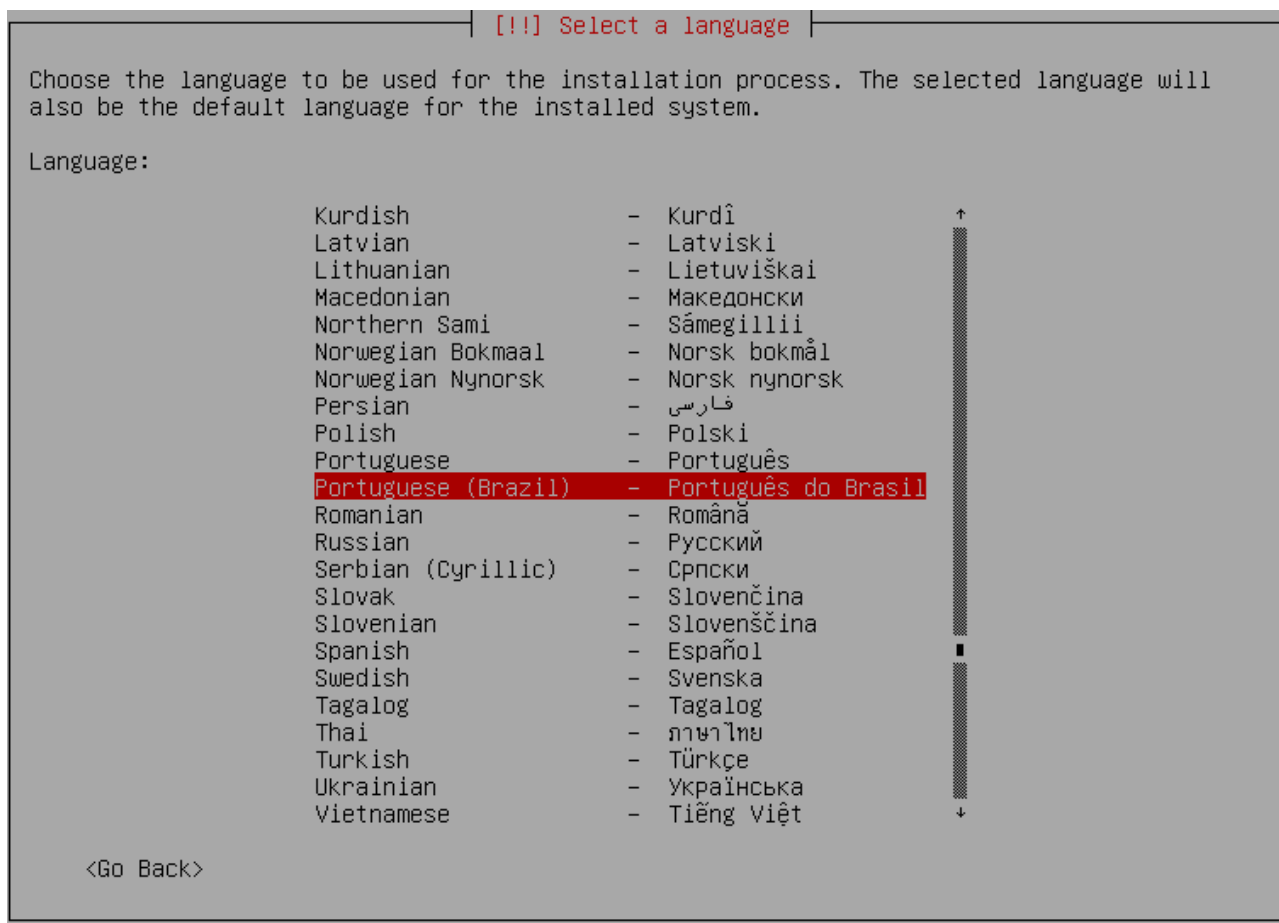
MANUAL DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL – DEBIAN

1 INSTALANDO DEBIAN

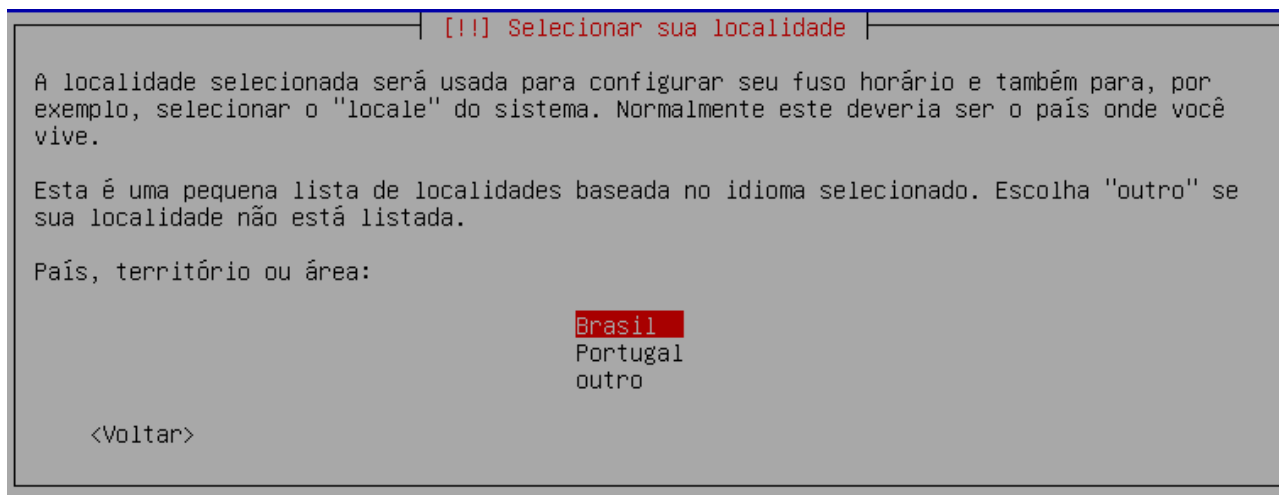
Toda instalação será feita utilizando a distribuição Debian 6.0 em modo texto, também pode ser instalado na versão gráfica (normalmente não utilizada), é necessário que o firewall tenha duas placas de redes, uma irá receber o ip da operadora ou prestadora de serviço e a outras placa será utilizada para comunicação na rede local e acesso dos clientes em direção a internet.

Abaixo segue os passos para instalação do Debian 6.0.





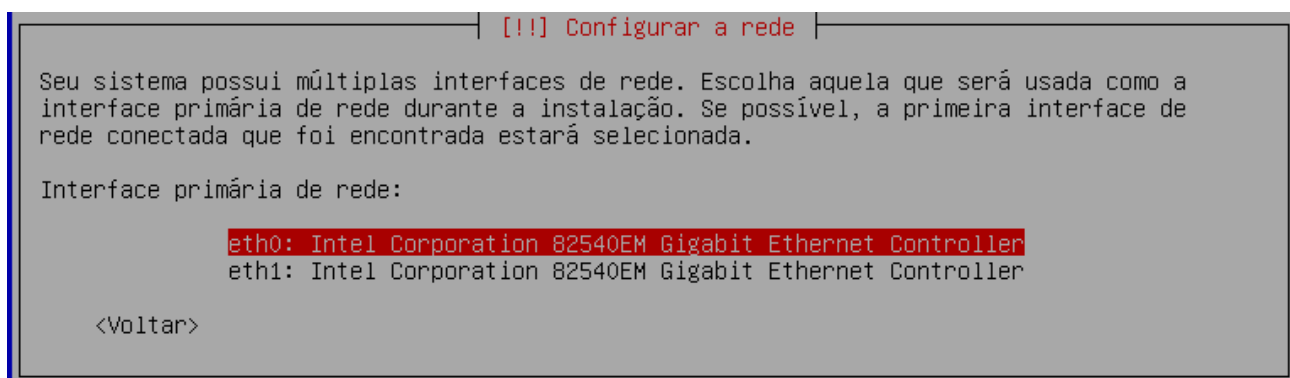
Selecione o idioma para prosseguir com a instalação.



Selecione o país



Selecione o layout do teclado (ABNT2 = teclado com Ç)



Selecione a interface que estará conectada com a internet

[!] Configurar a rede	
Por favor, informe o nome de máquina ("hostname") para este sistema.	
O nome de máquina ("hostname") é uma palavra única que identifica seu sistema na rede. Se você não sabe qual deve ser o nome de sua máquina, consulte o seu administrador de redes. Se você está configurando sua própria rede doméstica, você pode usar qualquer nome aqui.	
Nome de máquina:	
<input type="text" value="firewall"/>	
<Voltar>	<Continuar>

Digite um nome para identificação do firewall

[!] Configurar a rede	
Configuração automática de rede falhou	
Sua rede provavelmente não está usando o protocolo DHCP. Alternativamente, o servidor DHCP pode ser lento ou algum hardware de rede pode não estar funcionando corretamente.	
<Continuar>	

Caso exiba a mensagem acima, o computador não está conectado à internet

[!] Configurar a rede	
O nome do domínio é a parte de seu endereço Internet à direita do nome de sua máquina. Geralmente algo que finaliza com .com.br, .net.br, .edu.br, .org.br, .com, .net, .edu ou .org. Se você está configurando uma rede doméstica, você pode usar qualquer nome, mas certifique-se de usar o mesmo nome de domínio em todos os seus computadores.	
Nome de domínio:	
<input type="text"/>	
<Voltar>	<Continuar>

Caso faça parte de algum domínio

[[!]] Configurar usuários e senhas

Você precisa definir uma senha para o 'root', a conta administrativa do sistema. Um usuário malicioso ou não qualificado com acesso root pode levar a resultados desastrosos, portanto você deve tomar o cuidado de escolher uma senha que não seja fácil de ser adivinhada. Essa senha não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada a você.

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

O usuário root não deverá ter uma senha em branco. Se você deixar este campo vazio, a conta do root será desabilitada e o usuário inicial do sistema receberá o poder de tornar-se root usando o comando "sudo".

Note que você não poderá ver a senha enquanto a digita.

Senha do root:

<Voltar> <Continuar>

Senha do usuário root

[[!]] Configurar usuários e senhas

Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.

Informe novamente a senha para verificação:

<Voltar> <Continuar>

Confirmação da senha do root

[[!]] Configurar usuários e senhas

Uma conta de usuário será criada para você usar no lugar da conta de root para tarefas não-administrativas.

Por favor, informe o nome real deste usuário. Esta informação será usada, por exemplo, como a origem padrão para mensagens enviadas por este usuário bem como por qualquer programa que exiba ou use o nome real do usuário. Seu nome completo é uma escolha razoável.

Nome completo para o novo usuário:

<Voltar> <Continuar>

Usuário simples (é necessário para prosseguir a instalação e poderá ser deletado)

[!!] Configurar usuários e senhas	
Informe um nome de usuário para a nova conta. Seu primeiro nome é uma escolha razoável. O nome de usuário deverá ser iniciado com uma letra minúscula, que pode ser seguida de qualquer combinação de números e mais letras minúsculas.	
Nome de usuário para sua conta:	
<input type="text" value="usuario"/>	
<Voltar>	<Continuar>

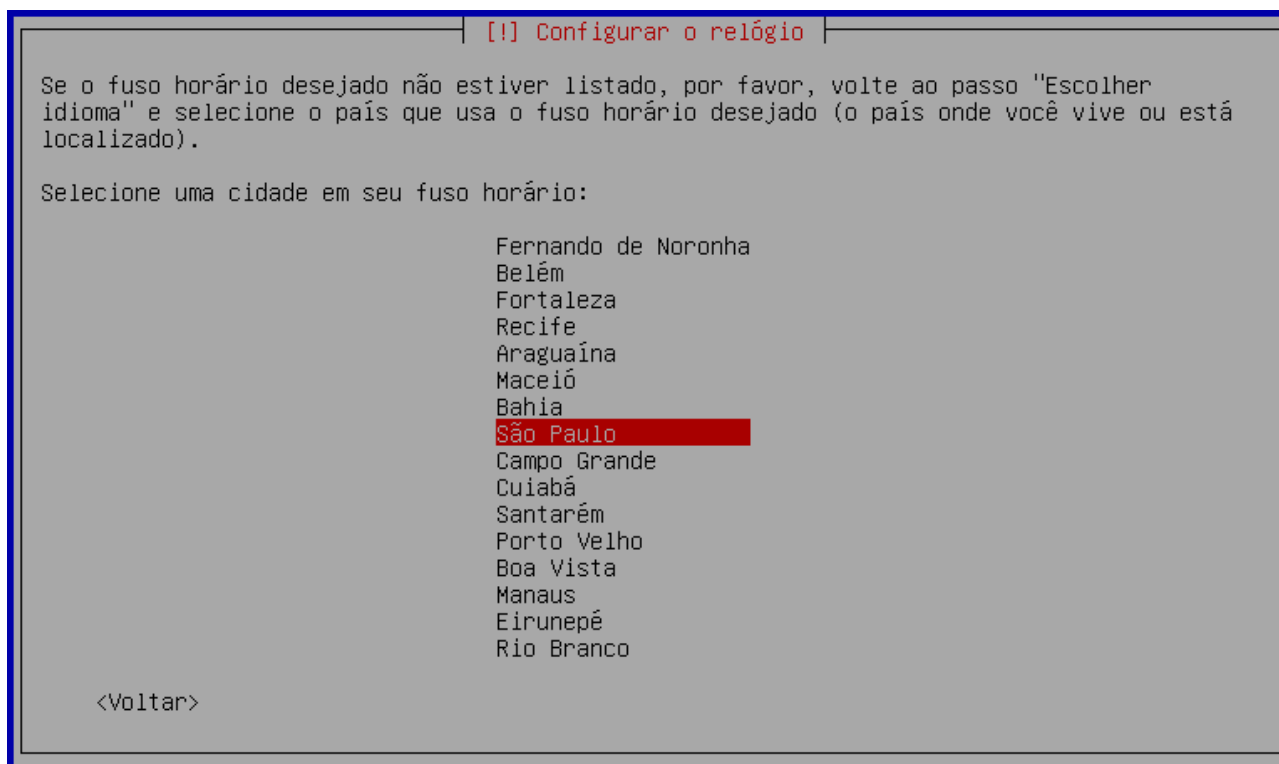
Nome do usuário

[!!] Configurar usuários e senhas	
Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.	
Escolha uma senha para o novo usuário:	
<input type="password" value="*****"/>	
<Voltar>	<Continuar>

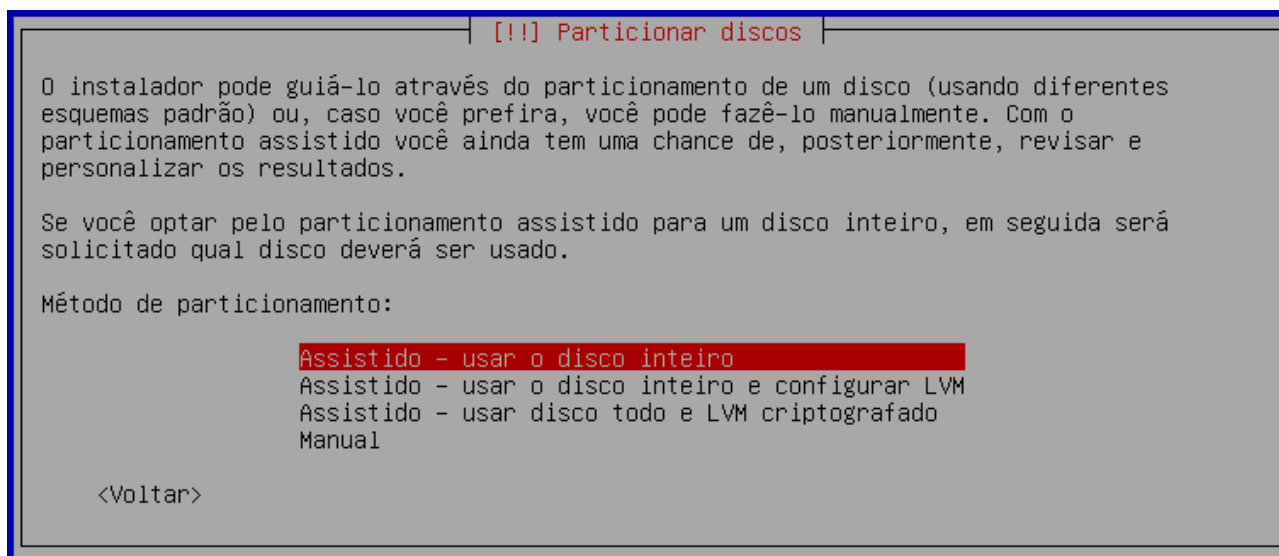
Senha do usuário

[!!] Configurar usuários e senhas	
Por favor, informe novamente a mesma senha de usuário para verificar se você digitou-a corretamente.	
Informe novamente a senha para verificação:	
<input type="password" value="*****"/>	
<Voltar>	<Continuar>

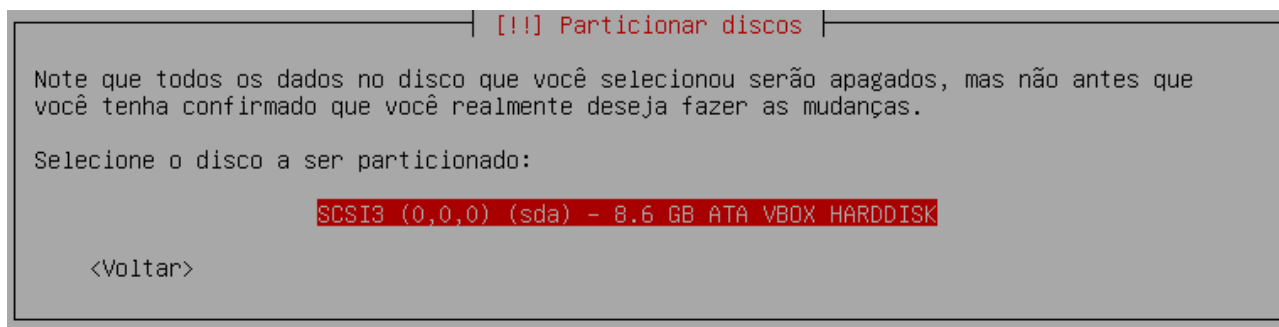
Confirmação da senha do usuário



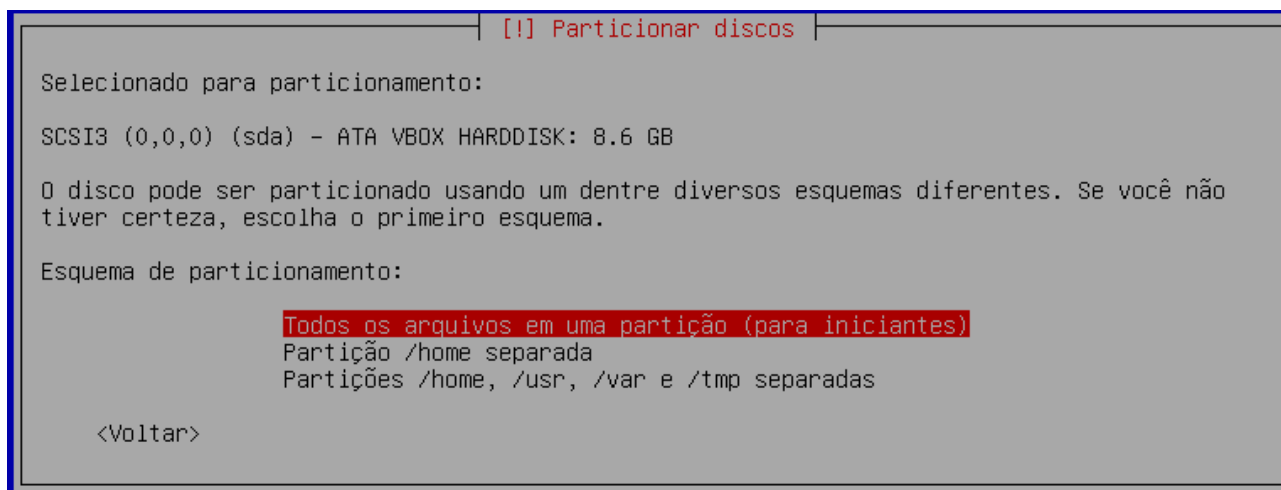
Fuso horário para o sistema



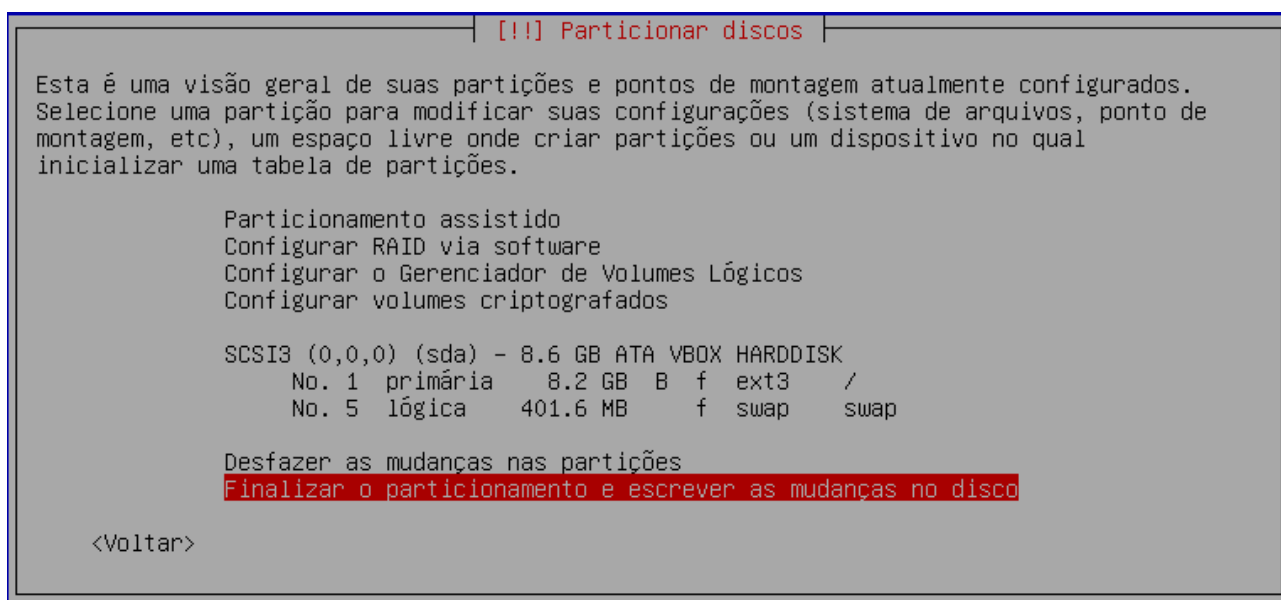
Instalação rápida (formata e utiliza o disco inteiro – instalação rápida)



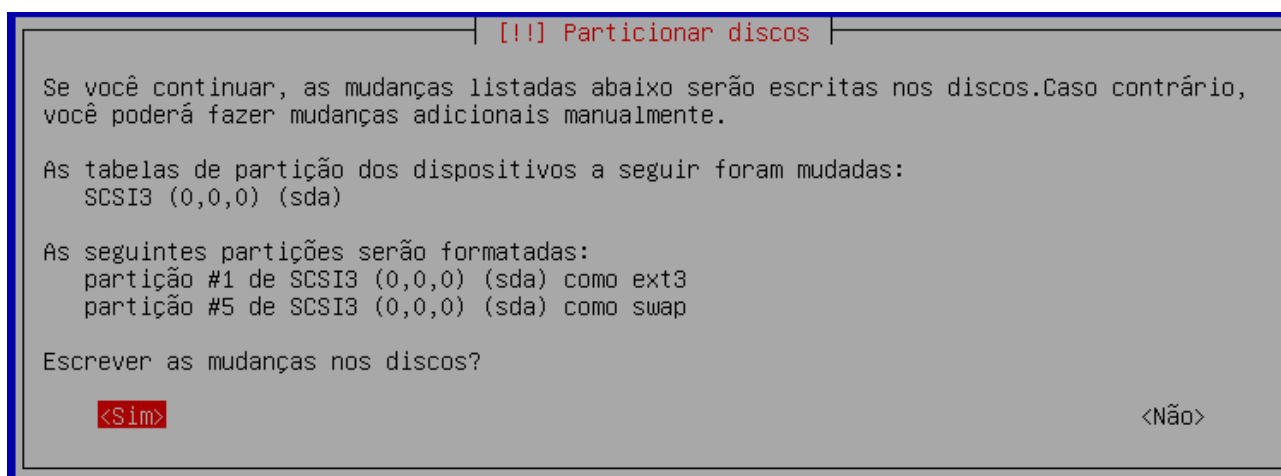
Disco onde será instalado o sistema operacional



Formato das partições do disco (primeira opção não é muito recomendada pois não é tolerante a falhas. Para usuários experientes o ideal é separar a instalação em discos diferentes)



Finalizar estilo de partições usadas na instalação



Formatação dos discos ou partições a serem usadas na instalação

Após esse procedimento será iniciado a instalação do Debian. Após a conclusão da instalação será necessário reiniciar o computador.

```
Debian GNU/Linux 6.0 firewall tty1
firewall login: _
```

Tela de login do Debian 6.0

2 COMANDOS BÁSICO DO EDITOR VIM

Para configurar os arquivos é necessário saber alguns comandos básico do editor VIM.

Abrir um arquivo com o editor vim

root@firewall:~# vim /caminho/arquivo.conf

Iniciar inserção de texto

[TECLA INSERT]

Retornar ao modo de comandos

[TECLA ESC]

Movimentação dentro do arquivo

[SETA PARA CIMA]

[SETA PARA BAIXO]

[SETA PARA DIREITA]

[SETA PARA ESQUERDA]

Para salvar o arquivo

[TECLA SHIFT] :w

Para salvar o arquivo e sair do editor

[TECLA SHIFT] :wq

Com Debian instalado, será iniciado as configurações para que o firewall e o proxy possa funcionar de maneira satisfatória.

Primeiramente é preciso verificar as interfaces de rede com o comando abaixo:

root@firewall:~# ifconfig

A interface que estiver conectada na internet deverá conter um endereço ip. Caso não tenha nenhum endereço ip é necessário executar o comando abaixo:

root@firewall:~# dhclient

Caso não consiga um endereço ip, verifique as conexões e cabos de rede.

Teste a comunicação do firewall com a internet com o comando abaixo:

```

root@firewall:~# ping -c 3 www.google.com.br
PING www.l.google.com (74.125.234.82) 56(84) bytes of data.
64 bytes from gru03s07-in-f18.1e100.net (74.125.234.82): icmp_req=1 ttl=54 time=
28.8 ms
64 bytes from gru03s07-in-f18.1e100.net (74.125.234.82): icmp_req=2 ttl=54 time=
28.8 ms
64 bytes from gru03s07-in-f18.1e100.net (74.125.234.82): icmp_req=3 ttl=54 time=
28.6 ms

--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 28.610/28.737/28.801/0.165 ms
root@firewall:~# _

```

root@firewall:~# ping -c 3 www.google.com.br

Se obtiver um resultado semelhante ao da foto acima, o firewall consegue se comunicar com a internet.

O próximo passo é a instalação de alguns serviços, utilizando os comandos abaixo.

Atualizando os repositórios:

root@firewall:~# apt-get update -y

Instalando os serviços:

root@firewall:~# apt-get install apache2 squid dhcp3-server bind9 vim ntp -y --force-yes

Após a instalação dos serviços será necessário a configuração básica para o funcionamento correto do firewall.

3 CONFIGURANDO IP ESTÁTICO PARA REDE LOCAL

Para que os serviços do firewall funcione é preciso que a interface local esteja com endereço ip estático. Abaixo segue as configurações para ip estático.

root@firewall:~# vim /etc/network/interfaces

As configurações devem ficar idêntias a figura abaixo.

allow-hotplug eth0

Carregará automaticamente a interface e buscará um ip automático fornecido por outro equipamento como modem ADSL por exemplo.

allow-hotplug eth1

iface eth1 inet static

address 192.168.0.1

netmask 255.255.255.0

network 192.168.0.0

broadcast 192.168.0.255

Acima as configurações para endereço estático na interface eth1 que será usada para rede local.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

allow-hotplug eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
```

4 CONFIGURANDO DHCP

O primeiro passo é configurar o serviço de dhcp para que possa fornecer os endereços ip's para os cliente na rede local. Para isso devemos editar o arquivo dhcpd.conf.

```
root@firewall:~# mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.original
```

```
root@firewall:~# vim /etc/dhcp/dhcpd.conf
```

Coloque o conteúdo abaixo dentro do arquivo dhcpd.conf.

```
ddns-update-style interim;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 192.168.0.1, 8.8.8.8, 8.8.4.4;
# Utilize a linha abaixo caso faça parte de algum domínio.
#option domain-name "example.com";

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.1 192.168.0.254;
}
```

Salve o arquivo e saia.

Agora devemos iniciar o serviço para verificar se tudo está funcionando perfeitamente.

```
root@firewall:~# /etc/init.d/isc-dhcp-server start
```

Caso não retorne nenhum erro, o serviço foi iniciado com sucesso. Para ter certeza de que está funcionando, utilize um computador cliente conectado diretamente na placa da rede local do firewall com cabo crossover e verifique se o cliente possui um endereço ip. Caso tenha um endereço está tudo normal. Caso dê algum erro verifique as configurações do dhcpd.conf.

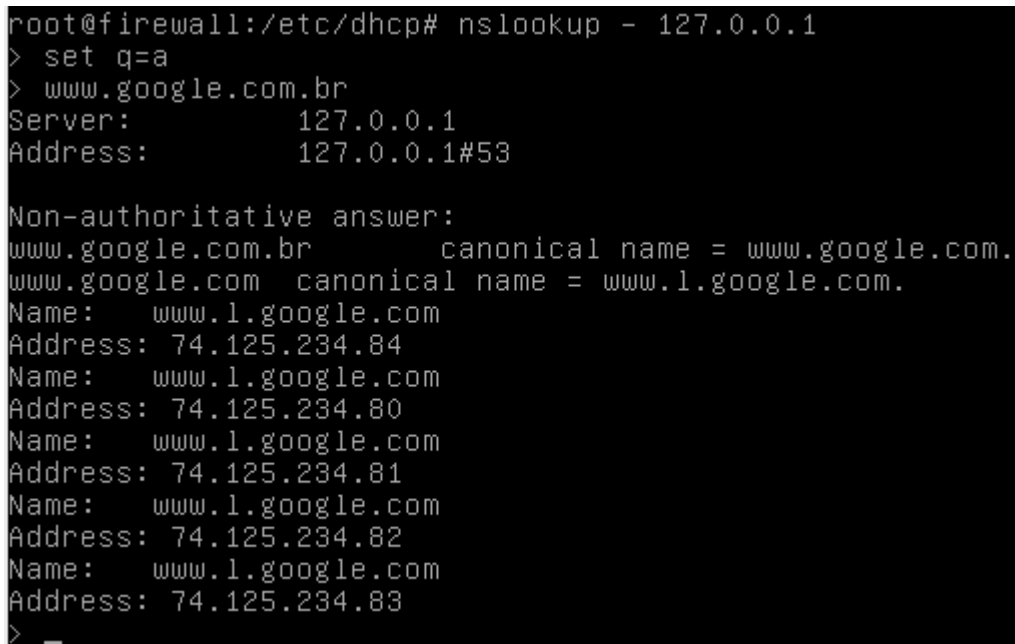
5 INICIANDO BIND

Com o serviço de dhcp funcionando o próximo passo é iniciar o serviço de resolução de nomes DNS.

```
root@firewall:~# service bind9 start
```

Execute o comando abaixo e veja se obterá o resultado semelhante a figura

```
root@firewall:~# nslookup - 127.0.0.1
```

A terminal window with a black background and white text. The prompt is root@firewall:/etc/dhcp#. The command nslookup - 127.0.0.1 is entered. The output shows the server address as 127.0.0.1 and the address as 127.0.0.1#53. It then shows a non-authoritative answer for www.google.com.br, listing several IP addresses for www.l.google.com.

```
root@firewall:/etc/dhcp# nslookup - 127.0.0.1
> set q=a
> www.google.com.br
Server:          127.0.0.1
Address:         127.0.0.1#53

Non-authoritative answer:
www.google.com.br canonical name = www.google.com.
www.google.com canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 74.125.234.84
Name:   www.l.google.com
Address: 74.125.234.80
Name:   www.l.google.com
Address: 74.125.234.81
Name:   www.l.google.com
Address: 74.125.234.82
Name:   www.l.google.com
Address: 74.125.234.83
> _
```

Nome resolvido com sucesso.

Nosso serviço de DNS está funcionando perfeitamente, precione CTRL + C para sair e voltar ao shell do linux.

6 CONFIGURANDO SQUID

Para que os cliente possam navegar na interne, é necessário configurar o squid para possibilitar esse acesso. Devemos configurar o arquivo squid.conf dentro da pasta /etc/squid.

```
root@firewall:~# mv /etc/squid/squid.conf /etc/squid/squid.conf.original
```

```
root@firewall:~# vim /etc/squid/squid.conf
```

Adicione o conteúdo abaixo para configuração do squid.

```
http_port 3128 transparent
visible_hostname Firewall
# Proxy transparent com autenticacao não funciona
error_directory /usr/share/squid/errors/Portuguese/
```

```

cache_mem 64 MB
maximum_object_size_in_memory 64 KB
maximum_object_size 512 MB
minimum_object_size 0 KB
cache_swap_low 50
cache_swap_high 70
cache_dir ufs /var/spool/squid 2048 16 256
cache_access_log /var/log/squid/access.log
#cache_store_log /var/log/squid/store.log
#cache_swap_log /var/log/squid/cache_swap.log
refresh_pattern ^ftp: 15 20% 2280
refresh_pattern ^gopher: 15 0% 2280
refresh_pattern . 15 20% 2280

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 22 995 993 465
acl Safe_ports port 21 80 138 139 443 563 70 210 280 488 59 777 901 1025-65535
acl purge method PURGE
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

# Validação da rede local
acl redelocal src 192.168.0.0/24

# Bloqueio de sites por dominio
#acl sites url_regex -i "/etc/squid/bloqueados/sites"
#http_access deny sites

#acl porno url_regex -i "/etc/squid/bloqueados/porno"
#http_access deny porno

# Bloqueio de arquivos por extensão
#acl extensao urlpath_regex -i "/etc/squid/bloqueados/extensao"
#http_access deny extensao

# Controle de banda de acesso a internet
# 15728640 = 15Mb de banda total contratada junto a operadora = 1,5MB/s
# 1048576 = 1Mb de banda controlada = 128Kb/s de velocidade máxima de download por
usuário
# 2097152 = 2mb de banda controlada = 256Kb/s de velocidade máxima de donwload por
usuário
#delay_pools 1

```

```
#delay_class 1 2
#delay_parameters 1 15728640/15728640 1048576/1048576
#delay_parameters 1 -1/-1 15728640/15728640 1048576/1048576 # 0 -1/-1 é ilimitado o uso da banda
#delay_parameters 1 32000/32000 1048576/1048576
#delay_access 1 allow redelocal
```

```
http_access allow localhost
http_access allow redelocal
http_access deny all
```

Com o arquivo do squid configurado, precisamos iniciar o serviço com o comando abaixo:

Finalizando serviço do squid
root@firewall:~# /etc/init.d/squid stop

Iniciando serviço do squid
root@firewall:~# /etc/init.d/squid start

Caso não exiba nenhum alerta, o squid está configurado de maneira correta. Caso retorne algum erro, verifique o arquivo de configuração do squid.

7 CONFIGURANDO SCRIPT FW.SH

Para otimização do firewall , devemos criar um script que execute as regras automaticamente quando o sistema operacional for reiniciado. Para isso devemos criar um arquivo de nome fw.sh dentro da pasta do squid.

root@firewall:~# vim /etc/squid/fw.sh

Adicione o conteúdo abaixo:

```
#!/bin/bash
    echo Inicializando regras do firewall
    sleep 0

IF_WAN=eth0 # INTERFACE DE SAIDA PARA INTERNET
LAN=192.168.0.0/24 # ENDEREÇO PARA REDE LOCAL LAN

# LIMPA REGRAS DO FIREWALL
    iptables -F INPUT ACCEPT
    iptables -F OUTPUT ACCEPT
    iptables -F FORWARD ACCEPT
    iptables -F
    iptables -t nat -F

    echo "nameserver 127.0.0.1" > /etc/resolv.conf
    echo "nameserver 8.8.8.8" >> /etc/resolv.conf
    echo "nameserver 8.8.4.4" >> /etc/resolv.conf
```



```
# ATIVA O SISTEMA DE ROTEAMENTO DE PACOTES
echo 1 > /proc/sys/net/ipv4/ip_forward

# ATIVA O MODO DE MASQUERADE
iptables -t nat -A POSTROUTING -o $IF_WAN -j MASQUERADE #
Mascaramento de rede

# FORÇA A NAVEGACAO PELA PORTA 3128
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 80 -s $LAN -j REDIRECT
--to 3128 # Forca navegacao na 3128
#iptables -t nat -A PREROUTING -p tcp -s $LAN --dport 1863 -j DROP

# BLOQUEANDO SITE COM HTTPS
#cat /etc/squid/bloqueados/bloq_https | while read SITES;
# do
#   iptables -A FORWARD -p tcp -d $SITES -j ACCEPT
# done
```

Salve o arquivo e saia.

Agora adicione o arquivo para execução automática dentro do arquivo rc.local.

```
root@firewall:~# vim /etc/rc.local
```

Adicione a linha abaixo antes da linha exit 0.

```
sh /etc/squid/fw.sh
```

Com isso o firewall carregará as regras na inicialização automaticamente.

8 CONFIGURANDO SINCRONIZAÇÃO DO RELÓGIO

Para que o relógio do firewall fique sempre atualizado vamos adicionar um script para automatização desse serviço.

Crie um arquivo com nome de clock.sh dentro da pasta /etc/squid.

```
root@firewall:~# vim /etc/squid/clock.sh
```

Adicione a linha abaixo.

```
ntpdate -u pool.ntp.org
```

Agora adicione o arquivo para execução automática dentro do arquivo rc.local.

```
root@firewall:~# vim /etc/rc.local
```

Adicione a linha abaixo antes da linha exit 0.

```
sh /etc/squid/clock.sh
```

Com isso o firewall irá sincronizar o relógio automaticamente na inicialização, porém o computador deve estar conectado com a internet para que isso funcione.

Adicione o script para execução todos os dias em um determinado horário, nesse caso será colocado todos os dias às 23:00 Hrs.

Execute o comando abaixo.

```
root@firewall:~# crontab -e
```

Adicione a linha abaixo.

```
00 23 * * * * /etc/squid/clock.sh
```

A partir desse momento serão gerados relatórios todos os dias às 23:00 Hrs.

9 INSTALANDO E CONFIGURANDO SARG (RELATÓRIO DO SQUID)

Para se ter controle do que devemos bloquear é necessário que saibamos quais os conteúdos que estão sendo acessados e para isso o squid fará a coleta dessas informações, porém para bloquear algum site precisamos ver quais foram acessados, então o sarg será nosso gerenciador de relatórios emitidos pelo squid.

Para instalar o sarg vamos seguir os passos abaixo:

Primeiro devemos editar o arquivo source.list.

```
root@firewall~:# vim /etc/apt/source.list
```

Adicione a linha abaixo:

```
deb http://backports.debian.org/debian-backports squeeze-backports main
```

Salve o arquivo e saia.

Agora temos que atualizar os repositórios com o comando abaixo e instalar com o comando à seguir.

```
root@firewall~:# apt-get update -y  
root@firewall~:# apt-get install sarg -y --force-yes
```

Após esse procedimento o sarg terá sido instalado com sucesso. Para testar rode o comando abaixo e veja o resultado:

```
root@firewall~:# sarg
```

```
root@firewall:/etc/squid# sarg
SARG: No records found
SARG: End
root@firewall:/etc/squid# _
```

Essa mensagem mostra que não existem nenhuma informação no cache do squid, só será possível ver os relatórios a partir do momento que os cliente começarem a utilizar a internet, pois o cache do squid está em branco até o momento.

Para adicionar o script para gerar relatórios diários siga os passos abaixo.

root@firewall:~# vim /etc/squid/relatorio.sh

Adicione as linhas abaixo

```
clear
DATA=`date +%d/%m/%Y`
sarg -g e -d $DATA-'$DATA'
```

Salve e feche o arquivo de relatório.

Digite o comando abaixo:

root@firewall:~# crontab -e

Adicione a linha abaixo.

00 23 * * * * /etc/squid/relatorio.sh

A partir desse momento serão gerados relatórios todos os dias as 23:00 Hrs.

10 CONFIGURANDO SARG

Por padrão o sarg não possui senha de acesso, que no quesito segurança isso não é aconselhável, pois qualquer computador poderia acessar os relatórios.

Por medidas de segurança será colocado senha de acesso aos relatórios do sarg.

Vamos editar o arquivo de configuração do http.

root@firewall~:~# vim /etc/apache2/sites-enabled/000-default

Altera a linha abaixo:

<VirtualHost *:80>

Para

<VirtualHost *:8082>

Adicione as linhas abaixo de DocumentRoot no final do arquivo de configuração.

<Directory "/var/www/squid-reports/">

```
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
AuthType Basic
AuthName "Acesso Restrito"
AuthUserFile "/etc/squid/.sargpasswd"
Require valid-user
</Directory>
```

Salve as configurações e feche-o.

Abra o arquivo ports.conf na pasta do apache2 e altere conforme abaixo:

```
root@firewall~:# vim /etc/apache2/ports.conf
```

Devemos alterar a linha abaixo

```
NameVirtualHost *:80
Listen 80
```

Para

```
NameVirtualHost *:8082
Listen 8082
```

Salve as configurações, feche o arquivo e reinicie o serviço apache2 com o comando abaixo.

```
root@firewall~:# /etc/init.d/apache2 restart
```

Agora precisamos definir a senha no arquivo .sargpasswd com o comando abaixo:

```
root@firewall~:# htpasswd -c /etc/squid/.sargpasswd root
```

```
[root@localhost etc]# htpasswd -c /etc/squid/.sargpasswd root
New password:
Re-type new password:
Adding password for user root
[root@localhost etc]# _
```

Digite a senha e repita a senha novamente. Pronto, o sarg já possui um usuário e senha, que poderá ser diferente do usuário root do sistema, nesse caso utilizamos o mesmo usuário e a mesma senha.

Abra o arquivo sarg.conf dentro da pasta /etc/sarg e altere as linhas abaixo:

```
Linhas originais
#output_dir /var/www/html/squid-reports
output_dir /var/lib/sarg
```

Após serem alteradas
output_dir /var/www/squid-reports
#output_dir /var/lib/sarg

11 INSTALANDO WEBMIN (GERENCIADOR DE CONFIGURAÇÕES WEB)

Uma ferramenta que ajuda muito é o webmin, que possui sua interface toda baseada na web e permite que o administrador configure diversos parâmetros usando essa ferramenta. Para instalar use o comando abaixo:

Download do webmin

```
root@firewall~:# wget  
http://prdownloads.sourceforge.net/webadmin/webmin_1.570_all.deb
```

```
root@firewall~:# dpkg -i webmin_1.570_all.deb
```

Será mostrado alguns erros de dependência para isso use o comando abaixo.

```
root@firewall~:# apt-get install -f
```

Inicie o serviço

```
root@firewall~:#service webmin stop  
root@firewall~:#service webmin start
```

Para iniciar o webmin, abra o navegador de internet e digite o ip do firewall seguido da porta 10000 como no exemplo abaixo:

<https://192.168.0.1:10000>

Nesse momento será solicitado o usuário e senha do sistema, digite seu usuário root e a respectiva senha para ter acesso as configurações.

12 INICIALIZANDO SERVIÇOS NA INICIALIZAÇÃO

Para inicializarmos os serviços na inicialização do Linux, precisamos instalar o chkconfig com o comando abaixo:

```
root@firewall~# apt-get install chkconfig -y --force-yes
```

Agora devemos colocar os serviços a serem iniciados com os comandos abaixo:

```
root@firewall~# chkconfig apache2 on  
root@firewall~# chkconfig bind9 on  
root@firewall~# chkconfig squid on  
root@firewall~# chkconfig webmin on
```

13 REINICIANDO SISTEMA

Após conclusão de todos os passos, devemos reiniciar o Linux, se tudo ocorrer bem, seu firewall estará pronto para ser instalado em uma rede.

Reinicie o sistema com o comando abaixo:

```
root@firewall:~# reboot
```

14 ADICIONANDO BLOQUEIOS DE SITES

Como a proposta de um firewall é ter controle de acessos a determinados sites, de nada adiantaria ter configurado e não adicionar a lista dos sites que serão bloqueados os acessos. Devemos criar uma lista de sites e adicionar nos arquivos de listagem que serão criados a partir desse ponto.

Devemos criar alguns arquivos, e acioná-los no arquivo de configuração do squid.

Para criar os arquivos execute os comandos abaixo.

```
root@firewall:~# mkdir /etc/squid/bloqueados  
root@firewall:~# touch /etc/squid/bloqueados/porno  
root@firewall:~# touch /etc/squid/bloqueados/chat  
root@firewall:~# touch /etc/squid/bloqueados/sites  
root@firewall:~# touch /etc/squid/bloqueados/extensao
```

Poderá ser criados diversos outros tipo de arquivos, grupos, pastas separadas, fica de acordo com que for mais fácil de trabalhar.

Após criar os arquivos devemos adicionar os sites nos arquivos **porno**, **chat**, **sites** e as extensões que serão bloqueadas para download no arquivos **externsão**.

Adicione os site que serão bloqueados.

```
root@firewall:~# vim /etc/squid/bloqueados/porno
```

Salve o arquivo e saia.

Repita o processo nos outros arquivos.

```
root@firewall:~# vim /etc/squid/bloqueados/chat
```

Salve o arquivo e saia.

Repita o processo nos outros arquivos.

```
root@firewall:~# vim /etc/squid/bloqueados/sites
```

Salve o arquivo e saia.

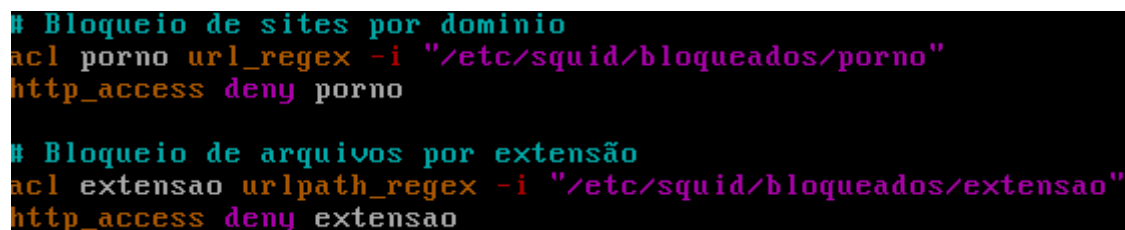
Adicione as extensões de arquivos que serão bloqueados..

```
root@firewall:~# vim /etc/squid/bloqueados/extensao
```

Salve o arquivo e saia.

Após criado a lista do que será bloqueado pelo firewall, devemos habilitar as linha dentro do arquivos do squid.

```
root@firewall:~# vim /etc/squid/squid.conf
```



```
# Bloqueio de sites por dominio
acl porno url_regex -i "/etc/squid/bloqueados/porno"
http_access deny porno

# Bloqueio de arquivos por extensão
acl extensao urlpath_regex -i "/etc/squid/bloqueados/extensao"
http_access deny extensao
```

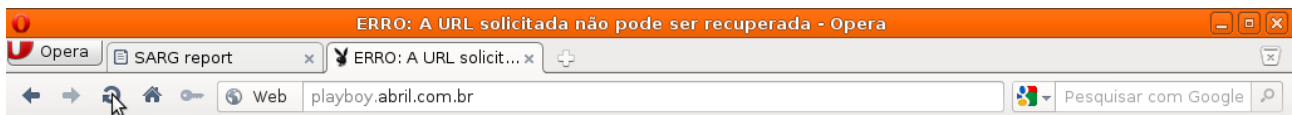
Reinicie o serviço do squid e teste no navegador se os sites da lista estão sendo bloqueados.

```
root@firewall:~# /etc/init.d/squid restart
```

Ao adicionar os site a serem bloqueados não é necessário reiniciar o squid, é necessário apenas recarregar as configurações com o comando abaixo:

```
root@firewall:~# /etc/init.d/squid reload
```

Se as configurações estiverem corretas será mostrado a imagem abaixo caso alguns usuário tente acessar algum dos sites que estiverem na lista dos bloqueados.



ERRO

A URL solicitada não pode ser recuperada

Na tentativa de recuperar a URL: <http://playboy.abril.com.br/>

O seguinte erro foi encontrado:

- **Proibido o Acesso.**

O controle de acessos impediu sua requisição. Caso você não concorde com isso, por favor, contate seu provedor de serviços, ou o administrador de sistemas.

Generated Thu, 08 Dec 2011 17:53:39 GMT by Firewall_Delta (squid/2.6.STABLE21)



Esta página de ACCESS DENIED poderá ser personalizada, basta editar o arquivo ERR_ACCESS_DENIED dentro da pasta /etc/share/squid/errors/Potuguese/ caso altere a linha no arquivo squid.conf para outro idioma deverá entrar na pasta equivalente ao idioma configurado no squid.conf