| **GUIA PRÁTICO**

SERVIDOR
SEM COMPLICAÇÃO

Andrio P. Jasper
mascaraapj@gmail.com

“Somos o que repetidamente fazemos. A excelência, portanto, não é um feito, mas um hábito” – Aristóteles

Prefácio

A rede mundial de computadores surgiu no meio da guerra fria, criada com objetivos militares. Nas décadas de 1970 e 1980, a rede de computadores foi um importante meio de comunicação acadêmica, alem de ser utilizada para fins militares.

Nos últimos anos, houve uma rápida expansão e evolução, diante disso, nunca é demais falar sobre o Linux.

Este é um Guia para quem esta dando seus primeiros passos no Linux, e deseja configurar um servidor para controle de sua rede, pretendo mostrar como configurar um servidor Fedora, oferecendo os principais serviços para sua rede: Firewall, servidor DHCP, Webcache, DNS-Cache, controle de banda, controle de acesso, acesso remoto (SSH), relatórios, monitoramento.

Esse Guia foi elaborado com base em pesquisas na internet e experiência própria. Espero assim, ajudar a muitos.

As opções aqui descritas não são as únicas maneiras de criação de tal sistema. Ha muitas maneiras de se alcançar este objetivo.

Não dou qualquer garantia de que os passos aqui descritos vão funcionar com você.

O Linux é um enorme mundo a ser explorado, espero que possa usar este para um dos seus guias nessa longa jornada.

"Para alcançar conhecimento adicione coisas todos os dias , para alcançar sabedoria elimine coisas todos os dias."

SUMARIO

"Pense como uma pessoa de ação e aja como uma pessoa que pensa."
(Henri Louis Bergson)

1. – Introdução

Uma distribuição Linux é um conjunto de diversos programas (pacotes) aglomerados entre si com um kernel (núcleo do sistema) funcional.

Fedora é uma das mais populares e estáveis distribuições Linux que existem atualmente. Ele era, no começo, um fork para a comunidade, liberado e mantido pela gigante Red Hat que, na época, estava fechando seu sistema e concentrando-se no mercado corporativo. Isso significa que, desde o princípio, o Fedora já contava com o que há de mais moderno em tecnologia de software, assim como também contava com uma das mais competentes e dedicadas equipes em seu desenvolvimento. Se o que você procura é uma distribuição com poderes de ser um servidor estável, mas com as facilidades das ferramentas de configuração gráficas, ou se, simplesmente, deseja um desktop mais robusto, o Fedora será a sua melhor escolha.

Ele conta com um ciclo de desenvolvimento rápido. A cada seis meses, em média, um novo Fedora é liberado pelo Fedora Project para a comunidade. A própria comunidade em si é uma das mais ativas da internet e o Fedora conta com uma farta ajuda online, mesmo sem oferecer o suporte técnico direto da Red Hat.

O manuseio de pacotes é feito de forma inteligente e automática com a ajuda do YUM que cuida das atualizações e resolve as dependências de todos os pacotes, baixando o que for necessário ao sistema dos repositórios e gerenciando a instalação.

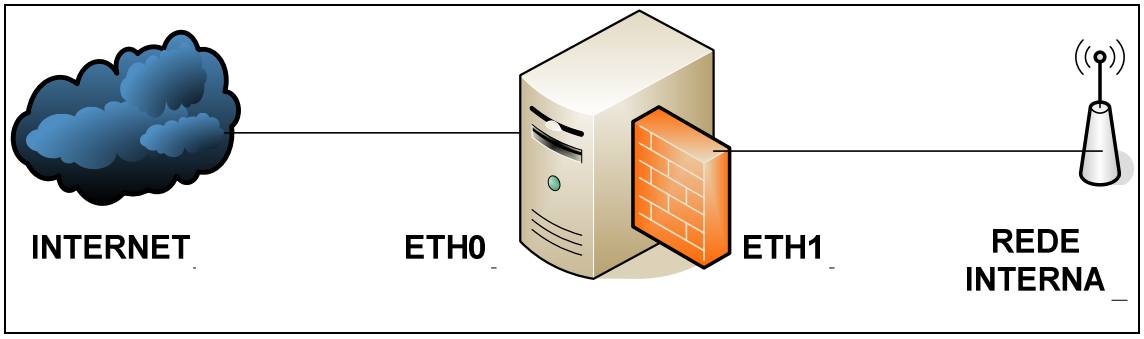
* 1º Fedora Core: "http://fedora.redhat.com/"
* 2º Red Hat Linux Enterprise "http://www.redhat.com/software/rhel/"
* 3º Fedora Core Brasil "http://www.fedora.org.br/"
* 4º Guia de Instalação “http://docs.fedoraproject.org/install-guide/f8/pt/”

1.1. - Requisitos

- - Fedora 11
- - Conexão com a internet
- - Hardware com 2 placas de rede (1 placa configurada para o acesso a internet, e a outra configurada para servir como Gateway da rede interna).

Nota: nesse, uso o hostname *servidor.lqm.farolbr* com endereço de gateway *172.167.0.1*. Essas configurações podem ser diferentes para você, então, tens que substituí-las sempre que for necessário.

1.2. - Cenário



Placa de rede eth0 (conexão externa - internet), configurado de acordo com sua conexão com a internet, aqui esta configurado assim:

```
# eth0
IP: 10.1.1.2
mask: 255.0.0.0
Gateway: 10.1.1.1
DNS1: 201.10.128.2
DNS2: 201.10.120.3
```

Placa de rede eth1 (conexão interna - rede), configurado ao seu gosto, aqui esta configurado assim:

```
# eth1

IP: 172.168.0.1
mask: 255.255.0.0
```

02. – Baixando e conferindo a Instalação do Fedora 11

Antes de iniciarmos a instalação, certifique-se de possuir a última versão estável do Fedora. O Fedora geralmente tem suas versões estáveis em números pares e instáveis em números ímpares. Atualmente essa versão estável é o Fedora 11.

Existem 3 tipos de arquiteturas suportadas pelo Fedora. São elas:

- i386 (32-bit) = Processadores AMD e Intel;
- x86_64 (64-bit) = Processadores AMD com suporte ao AMD64 e processadores Intel com suporte ao EM64T;
- ppc = Processadores IBM PowerPC.

Você poderá baixar em "Torrent" ou "Download direto via HTTP ou FTP". Para baixar é só visitar a página de downloads:

http://www.projetofedora.org/downloadav

Lembrando: baixe somente á versão correspondente ao seu processador.

A versão em DVD é única, apenas 1 arquivo. A versão em CDs tem em média 5 arquivos. Se baixar a versão em DVD, não precisará baixar as versões em CDs.

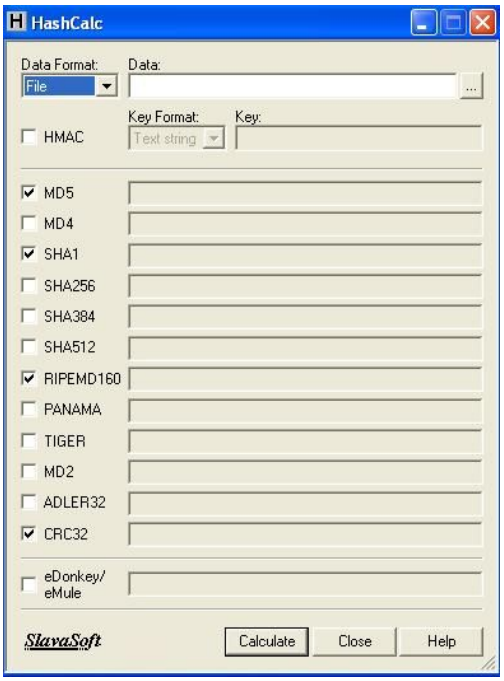
Efetuado o download do arquivo, é possível que ele venha corrompido ou incompleto, seja por problemas com a conexão ou do gerenciador de download usado. Então, depois que terminar o download, é sempre bom verificar a integridade do arquivo .ISO antes de gravar o DVD e acabar por gastar mídia à toa. Você pode detectar esse tipo de problema verificando o hash do arquivo.

Hash é um teste de algoritmo que soma todos os bits de um arquivo e nos devolve um algoritmo único. Se um único bit (número, letra) mudar, o algoritmo hash devolvido também mudará. Em resumo, uma mesma mensagem sempre resultará no mesmo algoritmo hash, não importando onde e quando você utilizar a função (desde que, obviamente, seja a mesma função hash).

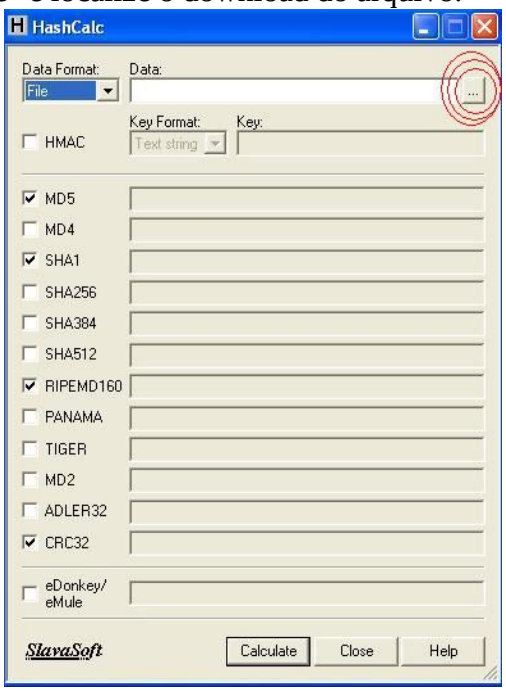
Para verificar o hash do arquivo utilize o programa HASHCAL, que pode ser encontrado no seguinte endereço:
http://www.baixaja.com.br/downloads/Windows/Development/Other/HashCalc_36898.html

Existem várias funções hash, algumas das mais utilizadas hoje são a MD5, a SHA-1 e a SHA-256. Iremos efetuar o cálculo usando o SHA1.

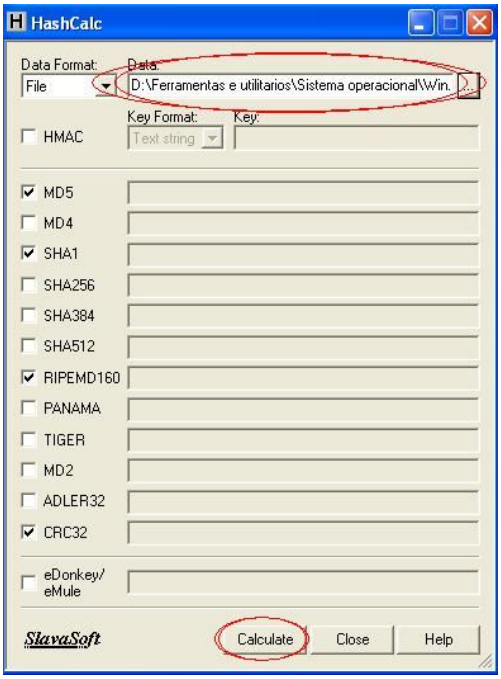
1. Já efetuado o download do HashCal, execute-o:



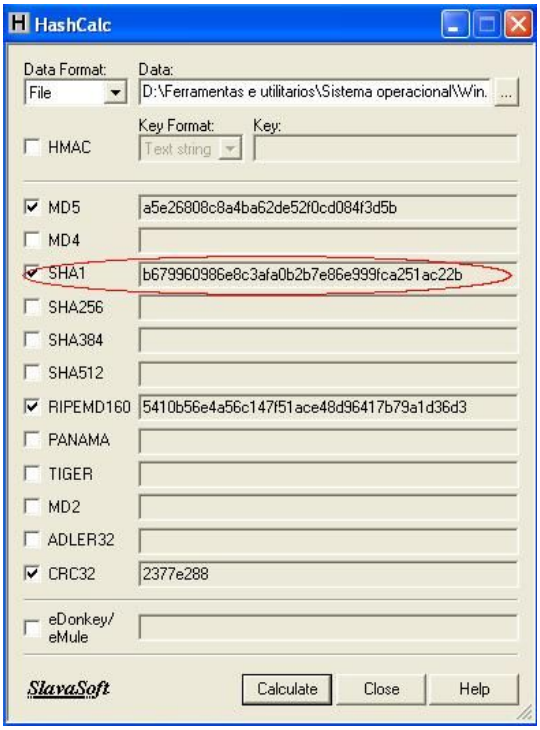
2. Clique no botão "find file" e localize o download do arquivo.



3. Após ter localizado o arquivo, o próximo passo é efetuar o calculo, para isso clique no botão "Calculate".



4. Após ter clicado em "Calculate", foram gerados os algoritmos hash nas funções selecionadas. Contudo iremos verificar apenas o algoritmo hash SHA1, compare o algoritmo hash SHA1 gerado com o apresentado abaixo:



Caso o algoritmo hash devolvido seja diferente dos algoritmos hash abaixo, aconselho a efetuar novamente o download.

Fedora 11 - i386 (32 bits) - Hash: SHA256

6e812e782e52b536c0307bb26b3c244e1c42b644235f5a4b242786b1ef375358 *Fedora-11-i386-DVD.iso

48bf00b8aa4d13da9bb13a1a82d835e90ab65ff32d282b58dffae66e70773630 *Fedora-11-i386-disc1.iso
530a4f4486216680bcc68e4b9ccbd667ed1278d668199f90242e5139d000183a *Fedora-11-i386-disc2.iso
b3a8c355c4f78303ea3eea92a4a537c43ddead23bef2a52d0e1f209986ac3811 *Fedora-11-i386-disc3.iso
8318dc3af01bc3f864d6b52c55242444d60fbdbac6ad924190724a2324302730 *Fedora-11-i386-disc4.iso
114152bbbcbe1ad1f5fca4de17b6762a2b86e68c56192b54814f0e0ffe70402b *Fedora-11-i386-disc5.iso
e296683a4702d3ccd6e15faf159c2a9c3f00325bf2a7a28434a3441d68e9e434 *Fedora-11-i386-disc6.iso
b61cf796fa1602ca003b340ca8073d783576507e88db3499d86640b0d20034cd *Fedora-11-i386-netinst.iso

Fedora 11 - x86 (64 bits)- Hash: SHA256

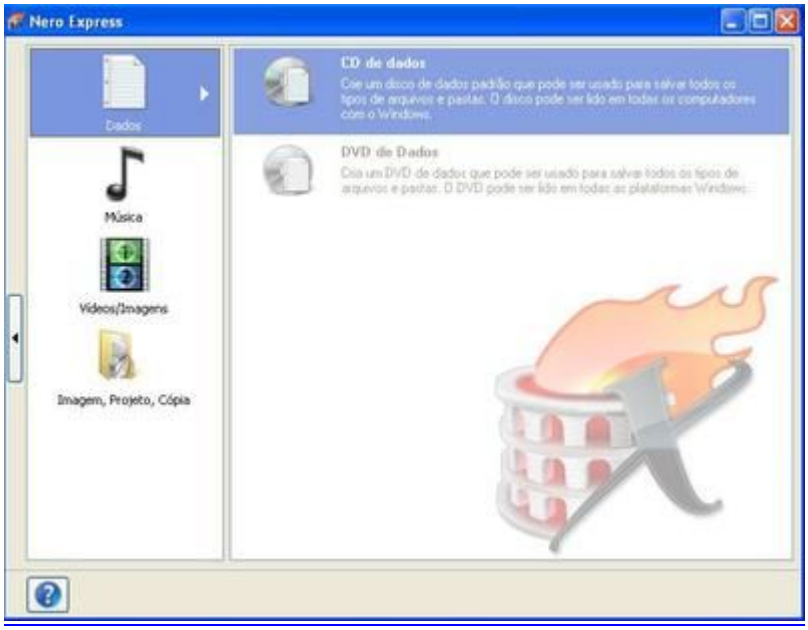
9f733ef43d470217a08dd3f4214deecccfc9e6d5041dc8eef47d990c419a6884 *Fedora-11-x86_64-DVD.iso
bc61803ba2bd50c1a1f8f1165480fee34ec25f831e93718a6ccebea754995fb1 *Fedora-11-x86_64-disc1.iso
dc2e01e16001d8f99acfe26af32fcf4797df12772d14e8254d53f9ad63ddb878 *Fedora-11-x86_64-disc2.iso
bf2889b356ff22623d3fd6fb5a1c8424dc24ed121a4a5634d7d1cd44de6b27d0 *Fedora-11-x86_64-disc3.iso
d69a4329d46958f7028272eeba91eea19a0902fef6f60ef0bac1c6cdd531d15c *Fedora-11-x86_64-disc4.iso
1acdebdc07e185d9f2792c4a1c1a9961129ae3f0c63794d37589703de0eefcbe *Fedora-11-x86_64-disc5.iso
53a74d293543928bfefb53a064a0d981f83b3743954b5e2517c2a687b567cbc5 *Fedora-11-x86_64-disc6.iso
b85a0eafd895754f6a65a3021bba84bb153d8ad41788a229cf5c51ca9c6fba5e *Fedora-11-x86_64-netinst.iso

03 – Gravando o seu Fedora

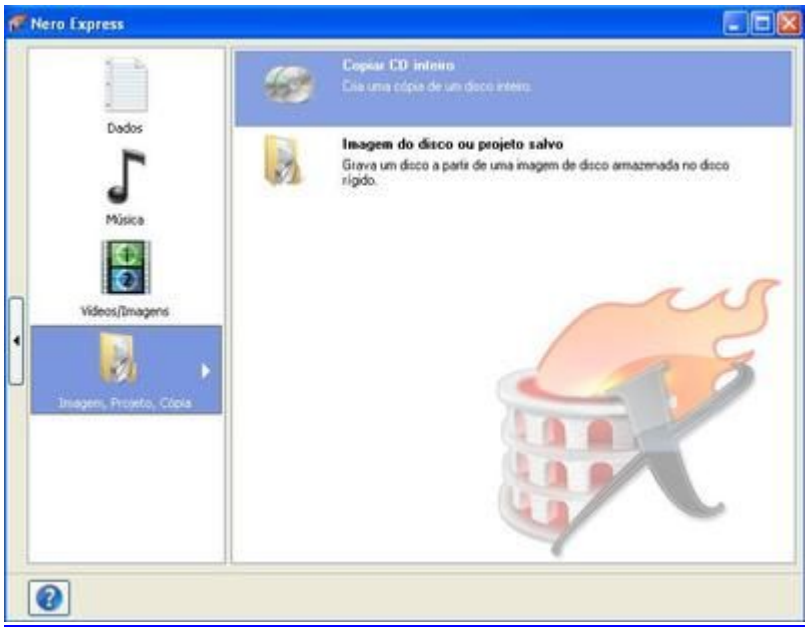
O processo de gravação de uma imagem .iso é um pouco diferente do processo de gravação de um CD/DVD normal. Algumas vezes, ao baixar o arquivo .iso, ele fica parecendo um arquivo do winrar (já que o .iso é um extensão aceita pelo winrar), porém não descompacte-o, iremos efetuar a gravação assim mesmo.

Irei descrever o processo de gravação de arquivo .iso através do Nero Express 8. Antes de iniciarmos, certifique-se de que a mídia de CD/DVD se encontra em seu drive:

1. Abra o Nero Express, geralmente encontrado no seguinte caminho: Iniciar - todos os programas - Nero 8 - Nero Express.

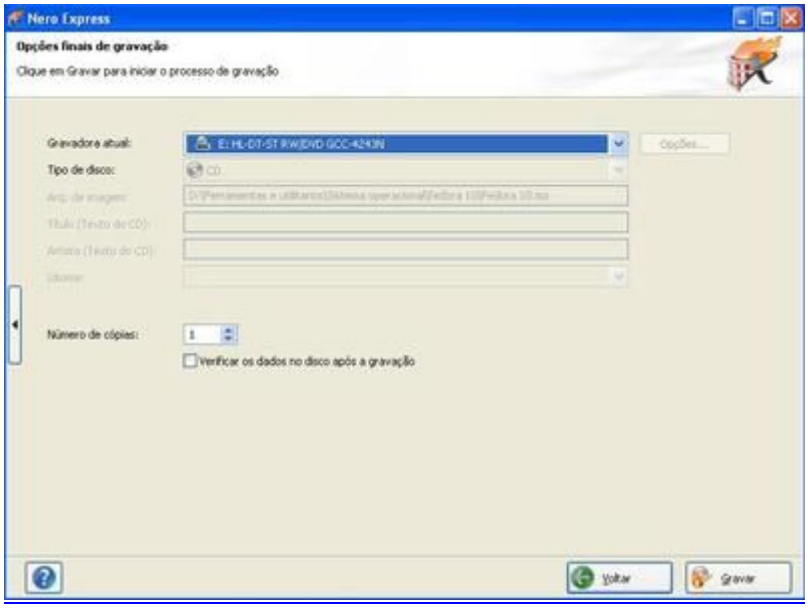


2. Clique em no botão "Imagem, Projeto, Cópia", localizado no canto inferior na aba a esquerda.



3. Clique em "Imagem do disco ou projeto salvo", será aberta uma janela para você localizar onde se encontra o arquivo que deseja gravar (localize o download do Fedora 11):

4. Nessa etapa você encontrará 2 opções interessantes: selecionar o "número de cópias" que deseja gravar e se deseja "verificar os dados após a gravação", aconselho a marcar a opção 2 (assim teremos certeza que não ocorreu nenhum erro no processo de gravação). Feito isso, clique em "Gravar" (sua gravação terá início).



Agora é só esperar a gravação terminar e terá sua mídia CD/DVD do Fedora 11 pronta para a instalação.

04 – Dando boot no CD/DVD

Com o CD/DVD já gravado, o próximo passo é configurar o setup da placa-mãe para dar boot através do DVD. Praticamente todos os micros vem configurados para dar boot preferencialmente através do floppy (disquete).

Existem 2 maneiras de fazer com que o computador dê boot pelo CD:

4.1. - Pressionando F8

1. Pressione a tecla "F8" durante o teste de memória (primeira tela no PC).
2. Aparecerá um menu com várias opções para boot, selecione o CDROM.
3. Ao iniciar o micro aparecerá a frase " Boot from CDROM" e logo após ler o CD de instalação aparecerá "Pressione qualquer tecla para continuar". Pressione então qualquer tecla, caso não faça isso, ele voltará a carregar o Windows ou outro sistema que estiver instalado no HD. Esta alteração apenas faz com que ele passe a procurar primeiro no drive de CD/DVD.

4.2. - Alterando o Setup

1. Neste caso teremos que acessar o setup da sua placa mãe, geralmente pressionando a tecla "DEL" durante o teste de memória (primeira tela no PC) você entrará no setup (caso não consiga, procure saber como acessar o setup da sua placa mãe).
2. Procure pela seção "Boot" e coloque o CDROM como dispositivo primário.
3. Tudo pronto, agora é só salvar a configuração acessando o menu exit, escolhendo a opção "Save & Exit setup".
4. Ao reiniciar o micro, aparecerá a frase "Boot from CDROM" e logo após ler o CD de instalação aparecerá "Pressione qualquer tecla para continuar". Pressione então qualquer tecla, caso não faça isso ele voltará a carregar o Windows ou outro sistema que estiver instalado no HD. Esta alteração apenas faz com que ele passe a procurar primeiro no drive de CD/DVD.

"Não confunda jamais conhecimento com sabedoria. Um o ajuda a ganhar a vida; o outro a construir uma vida." (Sandra Carey)

05 - Iniciando a instalação do Fedora

Antes de iniciarmos a instalação, certifique-se de que o CD/DVD do Fedora esteja inserido no seu drive de CD/DVD.

1. Reinicie seu computador, logo após reinicializar o boot iniciará pelo CDROM e aparecerá a tela abaixo:

Nessa primeira tela encontramos as seguintes opções:

- Install or Upgrade an Existing System - é a opção que iremos usar: o instalador gráfico;
- Install or Upgrade an Existing System (text mode) - fará a instalação em modo texto;
- Rescue Installed System - faz recuperar um Fedora já instalado em seu computador, caso ele tenha se "Corrompido";
- Boot from a local drive - inicializa uma instalação local do seu disco rígido.

Então daremos "ENTER" em "Install or Upgrade an Existing System", caso contrário ele iniciará automaticamente em 60 segundos.

2. Logo após a tela de carregamento ele perguntará se você quer fazer um teste de mídia (CD ou DVD) antes de prosseguir com a instalação. Caso você tenha conferido o SHA1SUM e tenha certeza de que suas mídias não estão com problemas, selecione "Skip" (com as teclas direcionais do teclado) e siga adiante. Caso queira testá-la, basta selecionar "OK" e pressionar a tecla "Enter" para verificar se o CD está OK ou se apresenta algum problema. Aguarde, irá demorar um pouquinho!

3. Depois da checagem ou de pular a mesma (Skip), o Anaconda será carregado (Anaconda é o instalador gráfico, caso ele não consiga identificar a sua placa de vídeo, será carregado um instalador em modo texto). Feito isso, a primeira tela a ser mostrada é a de boas vindas:

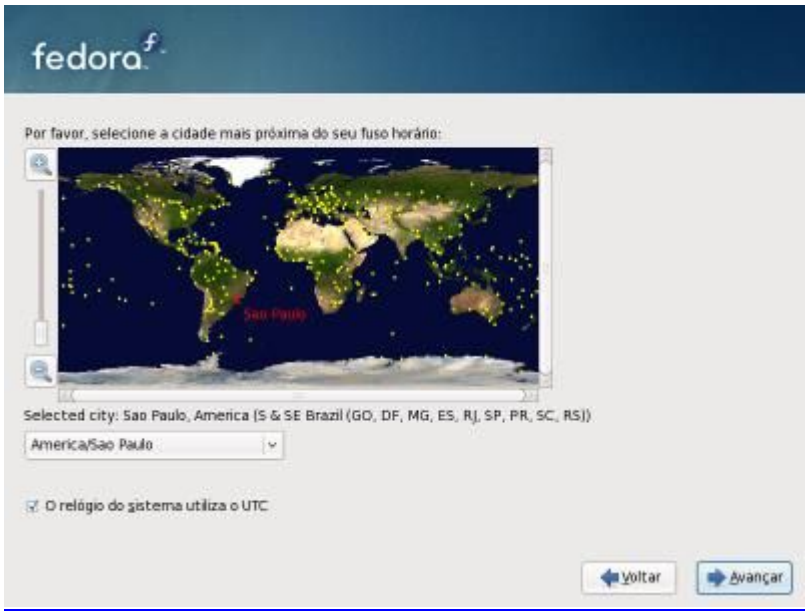
Nesta tela não temos o que fazer, então clique em "Next" para iniciar o processo de configuração de instalação

4. Agora iremos selecionar o idioma do sistema. Selecione "Portuguese (Brazillian)", que corresponde ao Português do Brasil e clique em next. O idioma que você selecionar aqui será o idioma padrão do sistema uma vez que estiver instalado.

5. A tela seguinte pede pra selecionar o layout do teclado. Se o seu teclado possuir a tecla "Ç", escolha a opção "Português Brasileiro (ABNT2)". Caso não possua esta tecla, provavelmente seu teclado é tipo padrão internacional. Neste caso escolha "Estados Unidos (Internacional)" e clique no botão "Avançar".

6. A tela seguinte pede para nomear o computador para identificá-lo na rede. Coloque o nome do seu domínio e clique no botão "Avançar".

7. Na tela seguinte selecionaremos o fuso-horário. Você poderá procurar no mapa ou selecionar na lista abaixo.



8. Na próxima tela temos um passo simples, a escolha da senha do root (o administrador, necessário para executar tarefas que alteram funções do sistema). A senha é "case sensitive", ou seja, diferencia maiúsculas de minúsculas.

9. Na próxima tela vamos escolher o tipo de instalação, você poderá selecionar opções de partições, HDs e outros. Esse é um dos passos mais importantes, portanto preste muita atenção. Nesta etapa particionaremos o HD de forma personalizada, ao invés de deixar o próprio sistema fazer isso. Selecione "Criar Layout Personalizado" e clique em "Avançar.

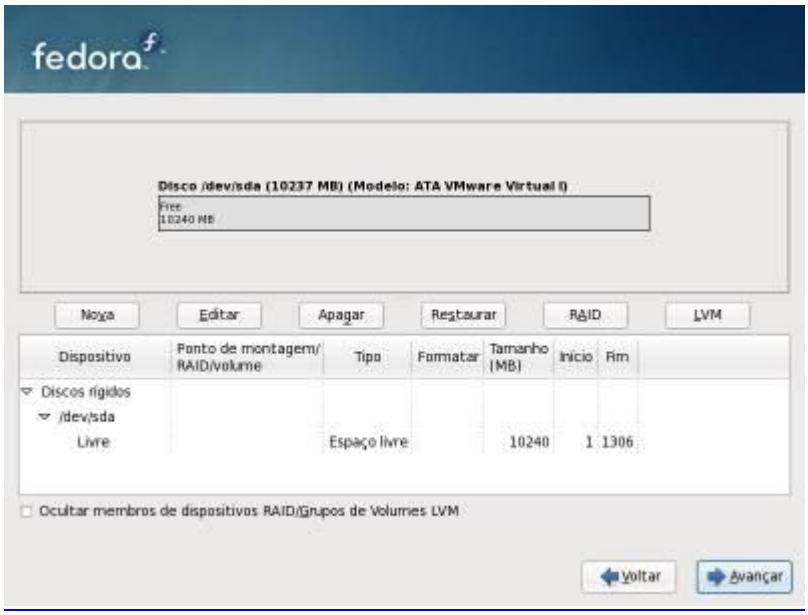
As opções que encontramos são as seguintes:

- Apagar todas partições nos discos selecionados e criar layout padrão: Se você escolher esta opção, todos os dados do seu computador serão apagados e um layout (particionamento) padrão será criado automaticamente;
- Remover partições Linux nos discos selecionados e criar layout padrão: Ao escolher esta opção, qualquer partição Linux do disco selecionado será removida e ao mesmo tempo, se você possuir outro tipo de Sistema Operacional instalado, ele NÃO será apagado. Após isso um layout (particionamento) padrão será criado automaticamente;
- Usar espaço livre nos discos selecionados e criar layout padrão: Escolhendo esta opção você instalará o Fedora na partição vazia de seu disco. Um layout (particionamento) padrão será criado automaticamente;

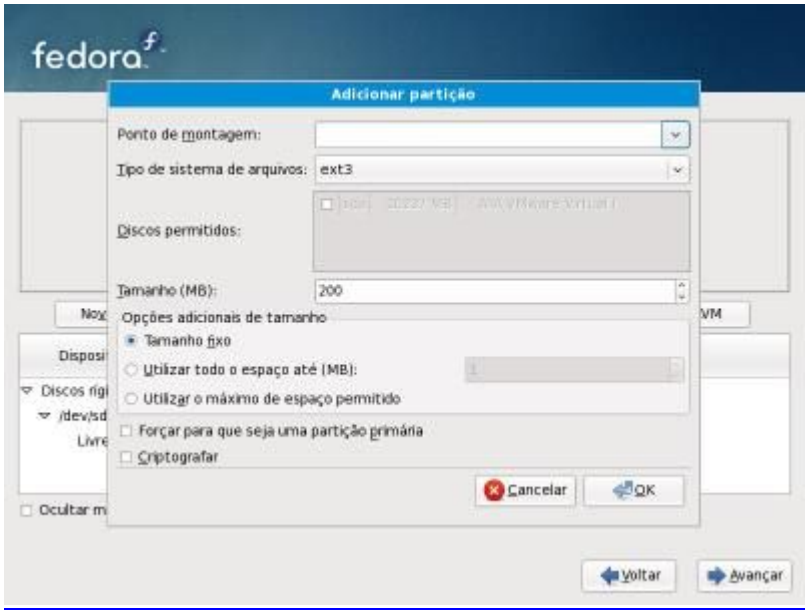
  Criar layout personalizado: Escolha essa opção caso entenda um pouco das partições do Linux.

"A verdadeira sabedoria consiste em saber como aumentar o bem-estar do mundo." (Benjamin Franklin)

10. Na próxima tela verifique que o sistema reconhece a partição onde está instalado o Windows. Neste caso, estou usando o VMWare.



Essa tela é uma das principais da instalação, é nela que você particionará todo o seu HD. Clicando em "Nova" é possível adicionar uma nova partição.



a. Primeiro vamos criar a partição "/" (raiz) para instalar o sistema. Em "Ponto de Montagem" selecione "/" (barra). Em "Tipo de Sistema de Arquivos" deixe como está "ext3". Em "Tamanho (MB)" insira uma partição pequena para o "/", algo em torno de metade do tamanho do seu HD.

1024 KB é igual a 1 MB

1024 MB é igual a 1 GB

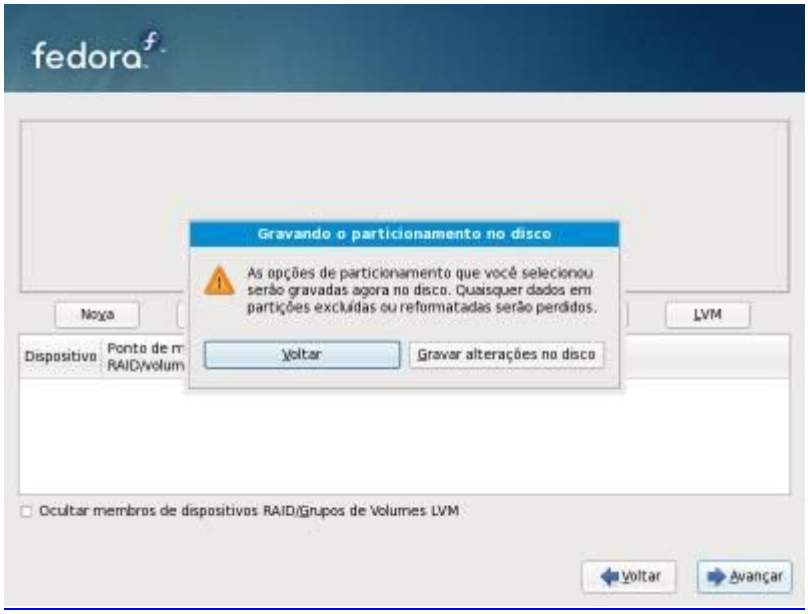
b. Vamos criar a partição "/boot" para armazenar os arquivos de boot. Em "Ponto de Montagem" selecione "/boot". Em "Tipo de Sistema de Arquivos" deixe como está "ext3". Em "Tamanho (MB)" insira o tamanho “200" (após inserir o tamanho da partição, clique em OK).

c. Agora vamos criar a partição "Swap". Em "Tipo de Sistema de Arquivos" selecione "swap". Em "Tamanho (MB)" deixe o dobro da sua memória (após inserir o tamanho da partição, clique em OK).

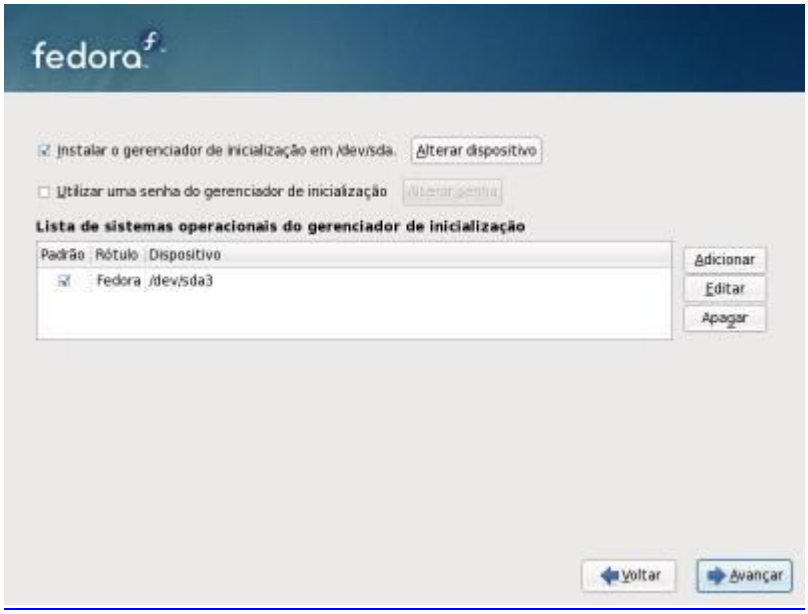
d. Vamos criar a partição "/var" para armazenar os arquivos do sistema. Em "Ponto de Montagem" selecione "/var". Em "Tipo de Sistema de Arquivos" deixe como está "ext3". Em "Tamanho (MB)" insira o restante do seu HD (após inserir o tamanho da partição, clique em OK), se der erro, diminua em 1 o tamanho (MB).

Após todas as partições criadas, clique em "Avançar".

11. Aparecerá uma mensagem alertando que as opções de particionamento que você selecionou serão gravadas no disco, selecione "Gravar alterações em disco".

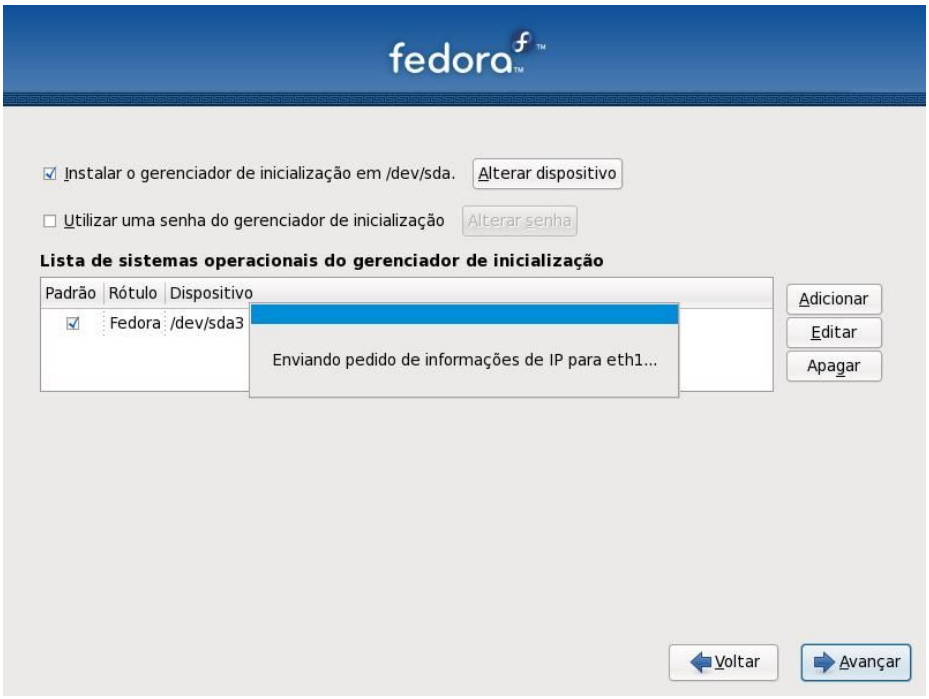


12. Na próxima tela você verá o "Gerenciador de Inicialização (GRUB)", que será instalado em "/dev/hda. Clique em "Avançar" para prosseguir:

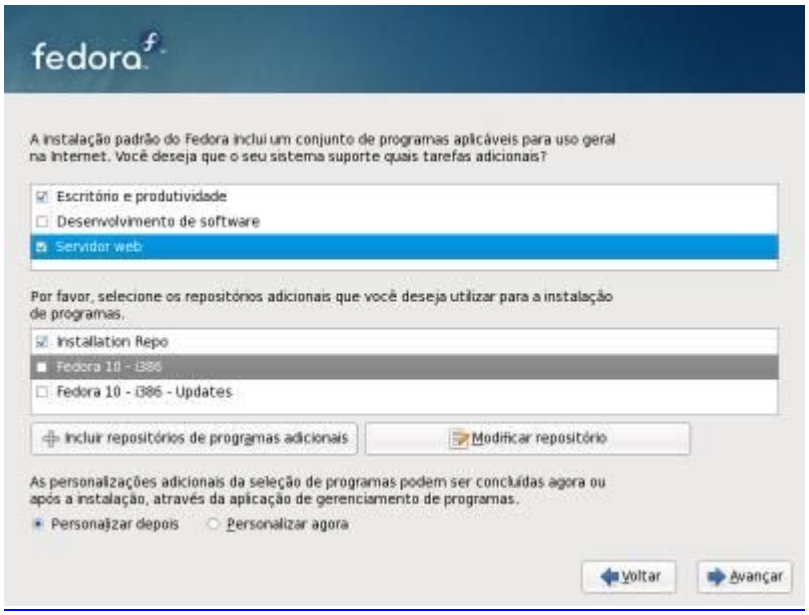


13. Será pedido para configurar as interfaces de rede, configure-as conforme seu ambiente; caso essa tela não apareça, poderemos configurar as conexões de rede quando o sistema já estiver instalado (no meu caso, estarei configurando conforme o ITEM “1.2. – Cenário”).

O instalador salvara as informações ao se configurar as interfaces e clicar em “OK”.



14. Na próxima tela veremos as opções de pacotes, disponíveis inicialmente em três categorias, você pode selecionar a opção que lhe deseja e até adicionar outros repositórios personalizados, clicando no botão correspondente abaixo.



Clicando em "Personalizar agora" e "Avançar", você poderá personalizar os pacotes, como por exemplo selecionar o ambiente GNOME ou KDE. Contudo, para um usuário iniciante que utilizará o micro para tarefas básicas, deixe como está, pois já contém muitos aplicativos para uso do dia-a-dia (Office, Multimídia, Internet etc). Clique em "Avançar".

15. Na próxima tela o Anaconda resolverá todas as dependências necessárias e iniciará a instalação:

Aguarde enquanto todos os mais de 800 pacotes são instalados. Geralmente não passa de 30 minutos, mas pode demorar até uma hora, dependendo da sua máquina e dos grupos de pacotes escolhido.

16. Após instalar o Fedora 11 você deve definir algumas configurações básicas. Logo após iniciar o sistema, a seguinte tela aparecerá:

Esta é a primeira tela que você verá do sistema. Não há nada para se fazer aqui, apenas clique no botão "Avançar".

17. Na próxima tela veremos os termos de uso nos quais o Fedora foi lançado. Se você concorda, clique em "Avançar".

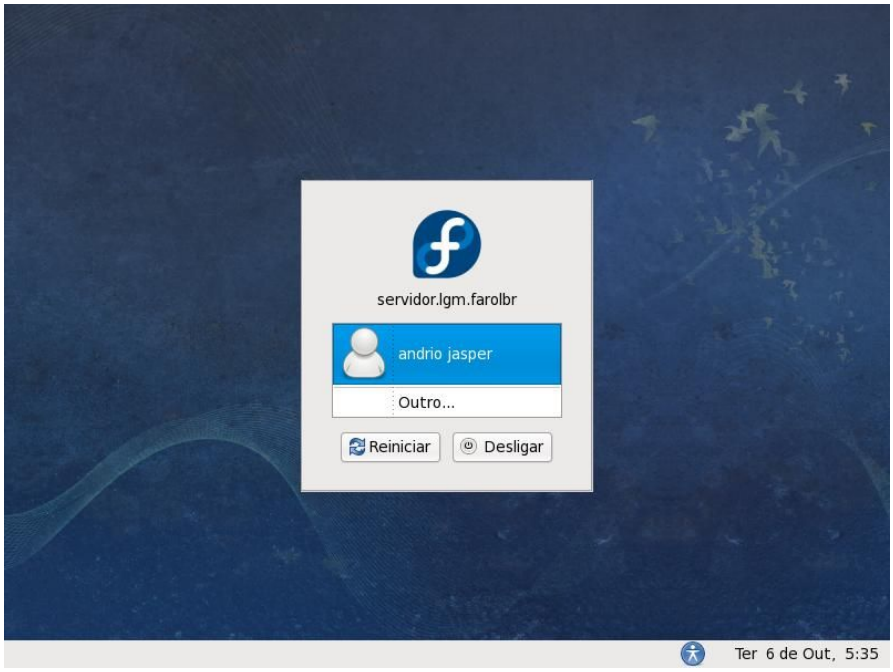
18. Na próxima tela crie sua conta de usuário. Recomendo digitar o nome de usuário em letras minúsculas. Após preencher tudo, clique em "Avançar".

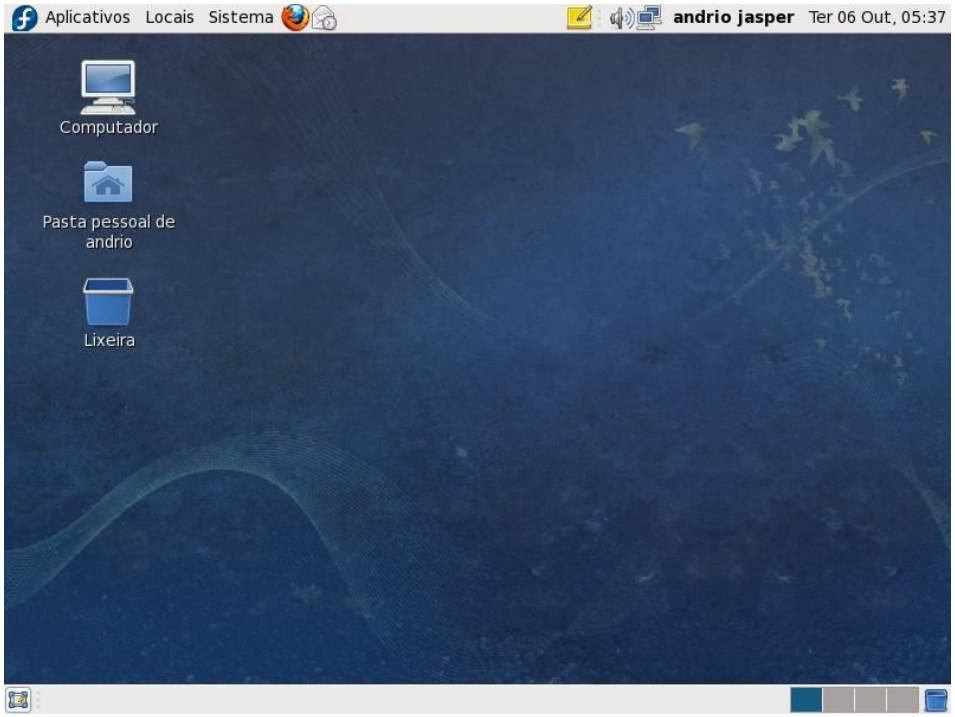
19. Certifique-se que a data e hora estão corretas.

20. Depois de selecionar data e horário, você poderá contribuir com o desenvolvimento do projeto Fedora. Selecionando para enviar ou não, avance. Caso aceite enviar, o utilitário se encarregará de enviar informações e configurações de hardware e se estão funcionando perfeitamente ou não, para o projeto, ajudando o mesmo a analisar onde o Fedora está sendo usado, melhorando a detecção e o funcionamento em determinados hardwares. Vale lembrar que não são enviadas informações pessoais.

21. Enfim, estamos terminados com a instalação do Fedora 11. Não foi nada difícil, ao contrário, o Fedora se destaca por uma instalação bem simples, estável e eficaz.

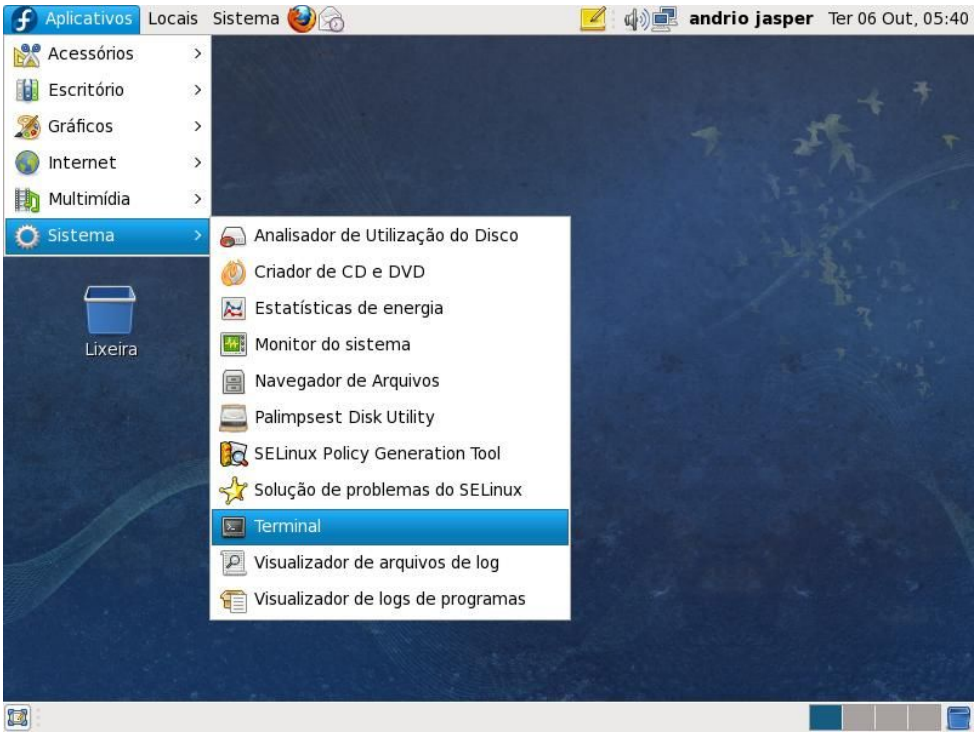
Depois de finalizado você irá para a tela de login, onde deverá inserir seu nome de usuário e senha (aconselho a nunca se logar como root!):



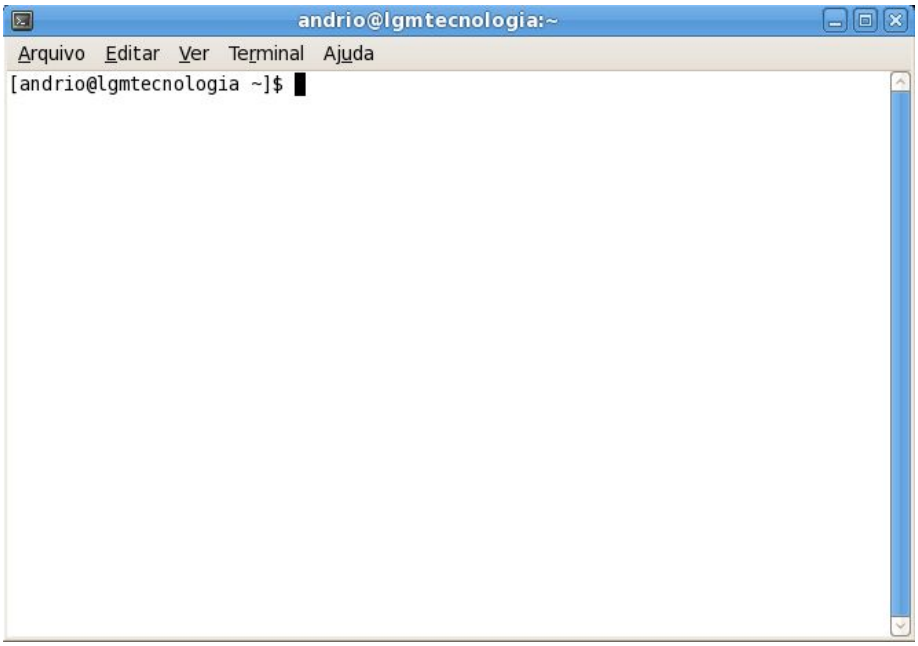


06 - Comandos básicos para administração do sistema

Assim como o DOS no Windows, é possível inserir comandos no sistema através de uma aplicação de terminal. Esse recurso pode ser facilmente localizado em qualquer distribuição.



Quando um terminal é acessado, uma informação aparece no campo de inserção de comandos. É importante saber interpretá-la. Para isso, veja os exemplos abaixo:



Observação: dependendo de sua distribuição e de seu shell, a linha de comandos pode ter um formato ligeiramente diferente do que é mostrado nos exemplos.

Nos exemplos, a palavra existente antes do símbolo @ diz qual o nome do usuário que está usando o terminal (lembre-se de que no Linux é necessário ter um usuário para utilizar o sistema). Os nomes que aparecem depois do @ indicam o computador que está sendo acessado seguido do diretório.

O caractere que aparece no final indica qual o poder do usuário. Se o símbolo for #, significa que usuário tem poderes de administrador (root). Por outro lado, se o símbolo for $, significa que este é um usuário comum, incapaz de acessar todos os recursos que um administrador acessa. Independente de qual seja, é depois do caractere que o usuário pode digitar os comandos.

A relação a seguir mostra os comandos seguidos de uma descrição:

6.1. - Comandos básicos

ls [-al]: listagem do diretório.

cp [-ir]: copiar arquivos.

mv [-i]: mover ou renomear arquivos.

rm [--]: deletar arquivos.

mkdir/rmdir: cria/deleta diretórios.

ln -s path link: cria links simbólicos (symlinks) para arquivos ou diretórios.

6.2. - Outros comandos

file: determina o tipo do arquivo (/etc/magic).

cat: exibe o conteúdo do arquivo na tela.

head / tail: exibe linhas no inicio / fim do arquivo.

less / more: lista o conteúdo do arquivo.

man filename: manual online do programa.

ctrl+alt+del/reboot: reinicia o sistema.

shutdown -h now/halt: desliga o computador.

6.3. - Combinações

CTRL+C: sai (kill) do programa.

CTRL+ALT+BackSpace: sai (kill) do servidor X.

CTRL+L: limpa a tela.

CTRL+A / E: move o cursor para o início / fim da linha.

CTRL+U / K: deleta da posição do cursor até o início / fim da linha.

CTRL+H: deleta palavra anterior ao cursor.

CTRL+R: busca comando digitado no history do bash.

CTRL+D: logout (para isto altere ou unset a var. $IGNOREEOF).

6.4. - Mais no terminal

stty -a: lista configurações do terminal.

reset: reseta o terminal (volta ao normal).

(SHIFT)PGUP/PGDN: barra de rolagem do bash.

TAB: auto-completa os comandos digitados no terminal.

MOUSE2/3: cola o texto selecionado (gpm).

CTRL+S (Scroll Lock): desabilita o vt.

CTRL+Q (Scroll Lock): habilita o vt (tente isto caso o terminal trave).

ALT+Fx: muda de console. CTRL+ALT+Fx: muda de console em modo gráfico.

Alterar data do sistema:

$ date 0109143001 (09/01/2001 14:30)

$ date -s "mm/dd/aaaa hh:mm:ss"

6.5. - Usuários

w: informações gerais sobre usuários logados e seus processos.

who: informações dos usuários atuais (do utmp)

last: listagem do histórico de logins (/var/log/wtmp)

lastlog: retorna informações sobre últimos logins.

adduser – Cria usuário

Exemplo:

adduser marina – Cria o usuário marina no grupo marina mesmo que este grupo não exista adduser –g vendedores marina - Cria o usuário marina no grupo vendedores

adduser –g diretoria –G vendas,marketing matheus - Cria o usuário matheus usando como grupo principal o grupo diretoria, mas também fazendo parte dos grupos vendas e marketing

adduser –d /home/contas lourdes - Cria o usuário lourdes com /home/contas como seu diretório home

adduser –d /home/noplace –g email –s /bin/nologin alfredo – Cria o usuário alfredo, no diretório /home/noplace, no grupo email, sem shell.

O objetivo deste comando é criar um usuário que não pode se logar no sistema

passwd – Defina uma senha para o usuário

Exemplo:

passwd marina – será solicitada a senha

usermod – Modifica os parâmetros de um usuário já criado

Exemplo:

usermod –l joao joaovalmir

Sua síntese é igual a do adduser

groupadd – Cria um grupo de usuário

Exemplo: groupadd vendas

userdel– Exclui um usuário

Exemplo:

userdel marina – Remove apenas o usuário

userdel -r marina – Remove o usuário e sua pasta Home

6.6. - Processos

CTRL+Z: suspende o processo temporariamente.

jobs: lista as tarefas rodando em fore/background.

bg/fg: manda processo para o back/foreground.

nice/renice: altera prioridades.

ps -auxw: lista todos os processos do sistema:

PID (process id), TTY (terminal ou ? caso seja um daemon), STAT (estado do processo), TIME (tempo de CPU consumido), COMMAND (o comando executado).

pstree -p: idem.

time: calcula o tempo decorrente do início ao término de um processo.

time updatedb

real 1m42.233s

user 0m0.490s

sys 0m10.290s

6.7. - Matando processos

kill: as opções mais comuns são (onde id é o mesmo que PID):

kill -HUP id-do-processo: reinicia processo.

kill -9 id-do-processo: mata processo.

killall processo: mata processo pelo nome.

killall -HUP processo: reinicia processo pelo nome.

6.8. - Sistema

lsdev, lspci: listagem do hardware/dispositivos pci.

pnpdump: retorna configuração das placas ISA PnP.

init

O init é o primeiro processo iniciado no Linux, logo após a carga do kernel do sistema. Quando é disparado, o init continua a carga do sistema, geralmente executando vários scripts que irão verificar e montar sistemas de arquivos, configurar teclado e iniciar servidores, entre outras tarefas.

O init utilizado no Linux permite que existam diversos níveis de execução no sistema. Um nível de execução é uma configuração de software do sistema que define quais processos devem ser inicializados e quais não devem, e também de que modo são inicializados.

O administrador do sistema é quem define qual será o nível de execução em que o sistema e os processos serão executados

Não existe uma regra que diga o que deve ser inicializado em cada nível de execução, mas em geral, utiliza-se o padrão descrito abaixo:

init 0 - Desliga o sistema (Não pode ser colocado como padrão)

init 1 - Sistemas funcionando no init 1 estão em modo monousuário, com um conjunto mínimo de processos ativos. O sistema de arquivos raiz (root) está montado em modo de leitura. Este nível de execução é normalmente utilizado quando a inicialização normal falha por alguma razão.

init 2 - A maior parte dos serviços estão ativos, com exceção dos processos de rede.

init 3 - Este é o nível normal de operação, com todos os processos ativos.

init 4 - Este nível não é utilizado na maior parte das distribuições.

init 5 - Semelhante ao init 3, com todos os processo ativos, porém com interface gráfica.

init 6 - Reinicia o sistema. (Não pode ser colocado como padrão)

6.9. - Permissões

As permissões dos arquivos são definidas através dos comandos chmod, chown e chgrp.

Estrutura do comando:

chmod

Ao listar as informações de um arquivo ou diretório, o formato é o seguinte: drwxrwxrwx.

Respectivamente: diretório (d), permissão do dono (read/write/execute), do grupo (read/write/execute) e de outros (read/write/execute).
Por exemplo, para transformar um arquivo em executável:

- **chmod +x nome_do_arquivo** (executável para todos)
- **chmod g+x nome_do_arquivo** (executável para o grupo)

Para alterar o usuário e o grupo de um arquivo ou diretório:

- **chown root.root /sbin/firewall.sh** (-R: recursivamente)

6.9.1. - Outros exemplos:

chmod 755 (executável): -rwxr-xr-x

chmod 4700 (suid) set user id para programas que precisam rodar com permissão de root: -rws------

Para calcular o valor numérico das permissões, basta considerar o valor do executavel como 1, de escrita como 2 e de leitura como 4, que seria o equivalente decimal aos bits:
rwx = 111 (todos bits ligados) = 2**2 + 2**1 + 2**0 = 7
Dessa forma, uma permissao de leitura e escrita (4+2) para o owner, e de leitura apenas para os outros teria o valor 644. Para calcular a umask, que seria a máscara de permissão aplicada na criação de um novo arquivo, basta então subtrair 666 (ou 777 para diretórios) resultando em umask 022.

6.10. - Como se encontrar no sistema

6.10.1. - Localizar arquivo por nome:

find [path...] -name [nome_do_arquivo]

find . -name slackware.png

find / -name "*.png" -print (arquivos png do dir. atual)

find /home -size +5000k -print (arquivos com mais de 5Mb)

6.10.2. - Local de um binário:

whereis (ou which) [nome_do_arquivo]

which gcc

gcc: /usr/bin/gcc

6.10.3. - Localizar texto em arquivo:

grep [param] [texto] [arquivo]

grep -ni man /var/log/packages/grep.tgz (-i : case insensitive, -n : número da linha)

(use ' '(aspas simples) no [texto] para procurar palavra exata.)

ls -l | grep '^-..x' (lista executáveis)

ls -l | grep '^d' (lista diretórios - '^' indica a primeira letra da linha)

Outros:

cd - : alternar entre diretórios

pwd: listar caminho atual

6.11. - Operações com texto:

comm/diff: compara dois arquivos.

ispell: verficador ortográfico (-d br: dicionário em português).

sort: ordena em ordem crescente, alfabética, etc.

uniq: remove linhas duplicadas.

cut: retorna area delimitada (-c5: quinto caracter).

wc: conta linhas, palavras e bytes.

fold: ajusta o texto para a largura especificada.

nl: numera as linhas de um arquivo.

fmt: reformata as linhas de um arquivo.

expand/unexpand: converte tabs em espaços e vice-versa.

tr: remove e substitui caracteres (-d a-d para remover as letras entre a-d, tr a-d A-D para torná-las maiúsculas).

6.12. - Compactando arquivo

gzip – Compacta arquivos

Exemplo:

gzip lista – Remove o arquivo lista e cria o arquivo compactado lista.gz

OBS: O comando gzip deve ser usado com cautela, pois o arquivo original é apagado e uma cópia compactada é criada.

gunzip – Descompacta arquivos

Exemplo:

gunzip lista.gz – Remove o arquivo lista.gz e cria o arquivo lista

OBS: O comando gunzip deve ser usado com cautela, pois o arquivo original é apagado e uma

cópia descompactada é criada.

bzip2 – Compacta arquivos

Exemplo:

bzip2 lista – Remove o arquivo lista e cria o arquivo compactado lista.bz2

OBS: O comando bzip2 deve ser usado com cautela, pois o arquivo original é apagado e uma cópia compactada é criada.

bunzip2 – Descompacta arquivos

Exemplo:

bunzip2 lista.bz2 – Remove o arquivo lista.bz2 e cria o arquivo lista

OBS: O comando bunzip2 deve ser usado com cautela, pois o arquivo original é apagado e uma cópia descompactada é criada.

tar - Agrupar ou desagrupar arquivos

O utilitário tar é um dos mas antigos e seu propósito original era armazenar e recuperar arquivos de unidades de fita magnética. Seu nome vem de tape archive. Atualmente, você pode usar tar para armazenar arquivos em um único contêiner, para extrais arquivos do contêiner e para outras manipulações de contêiner. Para propósito didático, estamos definindo contêiner como o arquivo que contém outros arquivos dentro.

Exemplo:

tar –czvf backup.tar.gz *- Cria o contêiner backup.tar.gz contendo todos os arquivos do diretório atual.

tar –xzvf backup.tar.gz *- Extrai do contêiner backup.tar.gz todos os arquivos para diretório atual.

OBS: É importante observar que o comando tar não destrói os arquivos originais e não acrescenta automaticamente nenhuma extensão. Compacta arquivos (Este é compatível com o WinZip muito utilizado para lidar com arquivos compactados multi-plataforma)

Compactando

zip –r squid.zip squid.conf

zip –r bkp.zip /home/* /etc/squid/squid.conf /etc/rc.d/rc.local

Descompactando

unzip bkp.zip

6.13. - O editor vi(m)

O vi é um editor de textos ASCII poderoso e muito usado na interface de caractere do Linux para a edição de arquivos e programas. Seu uso não é muito simples a primeira vista, mas a edição de enormes scripts pode ser feita usando poucos comandos.

O vi tem basicamente dois modos: o modo de operação e o modo de inserção.

Modo de operação: Neste modo o vi aguarda comandos que vão realizar alguma ação.

Modo de inserção: Neste modo tudo o que for digitado é considerado texto. Para entrar no modo de inserção, basta apertar a tecla INSERT ou o comando “”i””.

Para editar um arquivo no vi basta chama-lo assim: Vi nome_do_arquivo

6.13.1. - Comandos Principais do VI:

Ação	Comando
Abrir Arquivo	:e arquivo
Salvar Arquivo	:w
Salvar Arquivo Como	:w arquivo
Salvar e Sair	:wq
Sair sem salvar	:q!
Gravar conteúdo se alterado	:ZZ
Para marcar um texto para cópia ou corte	v, setas de direção
Para copiar texto marcado	y
Para cortar texto marcado	c
Para colar texto marcado	p
Copiar uma linha	yy
Copiar até o final do arquivo	yG
Apagar texto à frente (DEL)	x
Apagar texto para trás (BACKSPACE)	SHIFT+x
Apagar uma linha	dd
Apagar até o final do arquivo	dG
Apagar até o final da linha	D
Localizar texto à frente	/texto
Localizar novamente	/
Localizar texto para trás	?texto
Localizar novamente	?
Desfazer alterações	u
Refazer alterações	CTRL+r
Formatar Alinhamento Centralizado	:ce

6.14. - Yum

O Yum e um software que e utilizado por padrão pelo Fedora no gerenciamento de pacotes que estão instalados, que serão atualizados, ou que podem ser removidos do seu sistema. Com uma pequena coleção de parâmetros a serem adicionados, suas funcionalidades podem se estender.

Para usar o YUM e necessário que você esteja como root, pois ele exige privilégios administrativos e para ter certeza de obter um melhor rendimento, esteja certo de ter instalado os repositórios do YUM recomendados.

Para ver uma lista de softwares disponíveis:

yum list available

Para instalar um software:

yum install nomedopacote

Para atualizar um software:

yum update nomedopacote

Para instalar todas as atualizações disponíveis:

yum update

Para verificar as atualizações disponíveis:

yum check-update

Para procurar por um pacote:

yum search nomedopacote

Para remover um pacote:

yum remove nomedopacote

7. – Conexão de rede

Uma das principais diferenças entre as distribuições Linux esta na configuração da rede. Na pratica, tudo se resume ao bom e velho ifconfig, mas as varias distribuições tentam se diferenciar com métodos mais amigáveis de configurações.

O Fedora utiliza o NetworkManager para gerenciamento da rede. O Fedora foi na verdade a principal distribuição por trás do desenvolvimento do NetworkManager, antes que ele fosse incluído no Ubuntu e em outras distribuições.

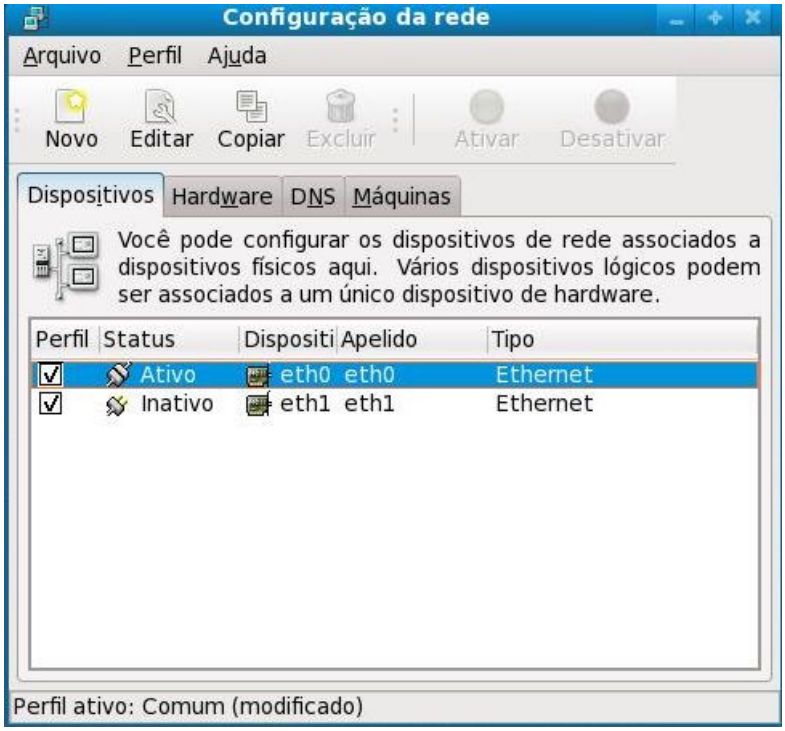
ifconfig – Este comando exibe as configurações existentes nas interfaces de rede
Exemplo:
ifconfig – Mostra todas as interfaces
ifconfig eth0 – Mostra apenas a configuração da eth0
ifup eth0 – inicia a interface eth0
ifdown eth0 – para/derruba a interface eth0

O "esqueleto" está no pacote initscripts; nele está:

- O diretório /etc/sysconfig/network-scripts, onde se localizam os scripts
- Os utilitários de controle (ifup para iniciar uma interface, ifdown para pará-la)

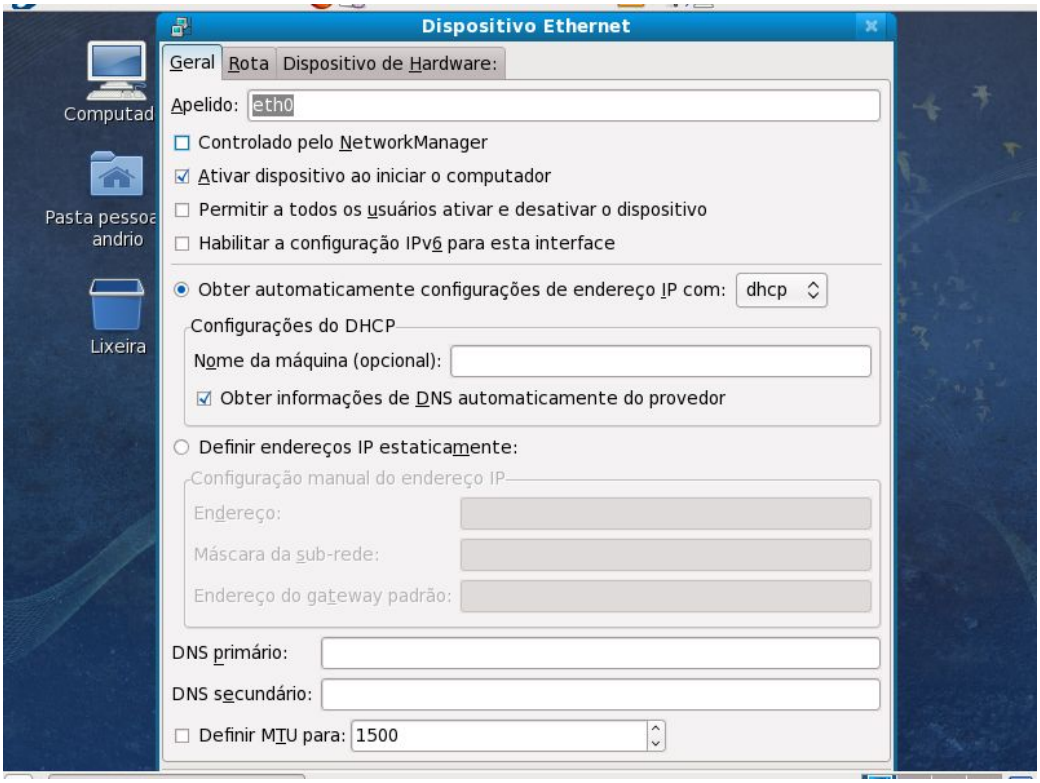
7.1. - Desabilitando NetworkManager

Para quem prefere a configuração manual, está disponível o "system-config-network" (Sistema > Administração > Rede), que permite desativar o NetworkManager e especificar a configuração manualmente. Basta desmarcar o "Controlado pelo NetworkManager" nas propriedades da interface:



Clique em cima do dispositivo e depois em **editar:**

Desative: Controlado pelo NetworkManager

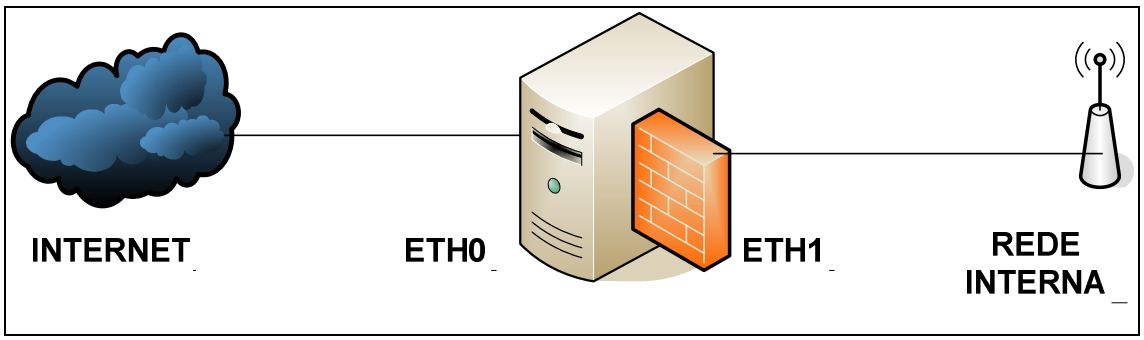


Reinicie o Servidor.

7.2. - Configurando conexão de rede

Este é um comando que exibe varias opções de configuração do linux dentre elas a configuração de redes.

Irei configurar da seguinte forma:



Placa de rede eth0 (conexão externa - internet), configurado de acordo com sua conexão com a internet, aqui esta configurado assim:

```
# eth0
IP: 10.1.1.2
mask: 255.0.0.0
Gateway: 10.1.1.1
DNS1: 201.10.128.2
DNS2: 201.10.120.3
```

Placa de rede eth1 (conexão interna - rede), configurado ao seu gosto, aqui esta configurado assim:

```
# eth1

IP: 172.168.0.1
mask: 255.255.0.0
```

Abra o terminal e passe para super usuário

Comando:

su –

Entre no setup, comando:

setup

Opção: Configuração de rede

Opção: Edit a device params

Selecione a interface correspondente:

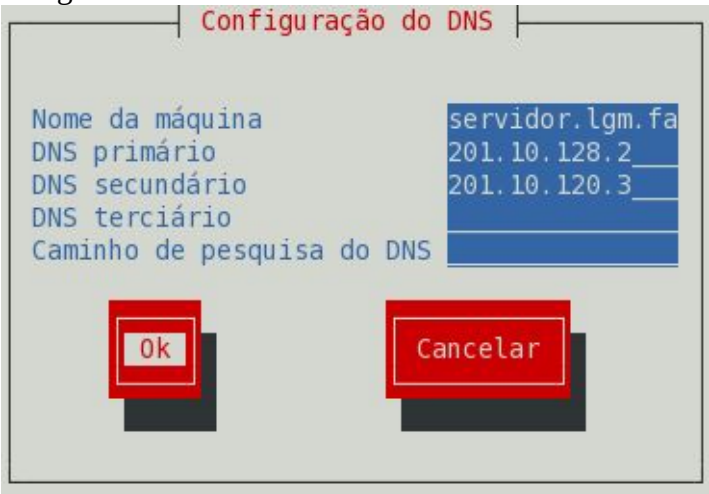
Configure a **Interface externa (eth0)** conforme seu cenário, no meu caso ficou assim:

Após configurar, clique em “Ok”. Selecione a outra **Interface interna(eth1)** e configure-a para ser o Gateway da rede interna. No meu caso, ficou assim:

Após configurar, clique em “Ok”, “Salvar”

Pronto, configuramos as interfaces, temos que configurar agora o DNS.

Opção: Edit DNS Configuration



Configure o "DNS primário" e o "DNS secundário" de acordo com o DNS do seu provedor.

Após configurar, clique em "Ok", "Salvar".
Salvar & sair
Sair

8. - SELinux, IPTABLES(Introdução, NAT)

8.1. - SELinux

O SELinux é uma implementação de segurança do Fedora, que por padrão, deveria oferecer uma maior segurança.

Porem, normalmente causa mais problemas do que vantagens (eu tive alguns problemas, alguns serviços não estavam funcionando, foi então, que descobri que os serviços estavam corretamente configurados, mas o SELinux estava causando problemas).

Alem do mais, em minha opinião, você não precisa dele para configurar um sistema seguro.

Portando, aconselho a desabilitá-lo.

Para maiores informações sobre o Selinux:

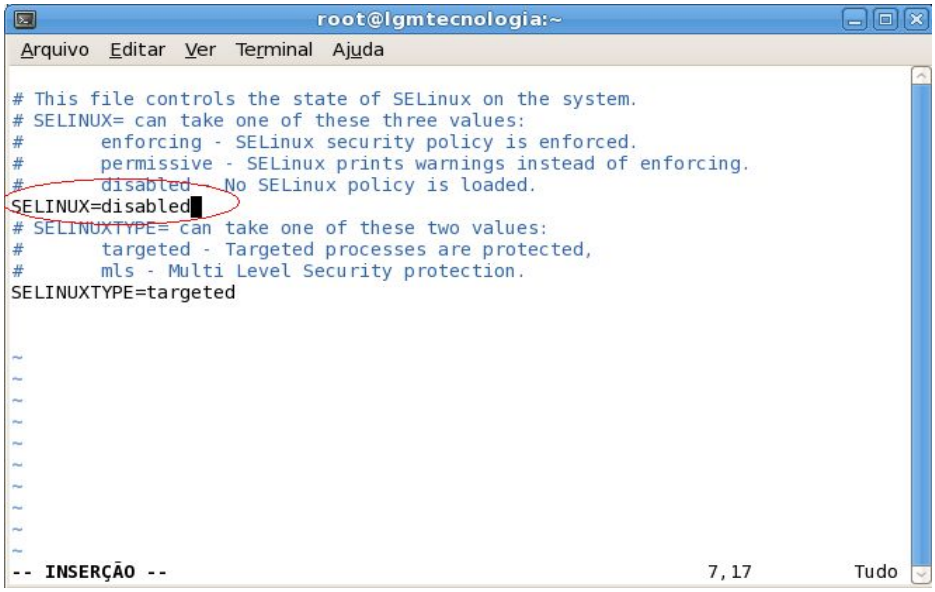
http://docs.fedoraproject.org/install-guide/f7/pt_BR/sn-firstboot-selinux.html

O config do SELinux pode ser encontrado em: /etc/selinux/config

Edite-o, mude o SELINUX=enforcing para SELINUX=disabled:

vim /etc/selinux/config

Deixe-o assim:



Reinicie o sistema:

reboot

ou

init 6

8.2. - Introdução ao Firewall

Firewall é uma extensão de segurança dado a um software/dispositivo que tem como seu principal objetivo aplicar uma política de segurança entre seu computador e a internet, ou, a um ponto especifico de controle de sua rede.

Explicando de uma maneira genérica, o firewall é como os seguranças da Casa Branca: só deixa entrar aqueles que são permitidos (total acesso) barram os que não são permitidos (acesso negado) ou direcionam os conhecidos a um determinado local (acesso parcial).

Nesse, abordaremos o iptables, na qual esta presente nos kernels atuais.

O iptables é um firewall statefull, nivel de pacotes, e funciona baseado no endereço/porta de origem/destino do pacote, prioridade, etc.

Podemos usar o iptables para uma gama de possibilidades, dependendo apenas da sua imaginação.

8.2.1. - Tabelas e Chains

Existem 3 tabelas disponíveis no Iptables: filter, nat, mangle.

Tabelas - São os locais usados para armazenar os chains

Chains - São os locais onde são armazenados os conjuntos de regras definidas pelo usuário.

Nota: os nomes dos chains são case-sensitive, o chain output é completamente diferente de OUTPUT.

filter: Tabela padrão, contem 3 chains:

- INPUT (para pacotes destinado a própria máquina)
- OUTPUT (para pacotes gerados localmente)
- FORWARD (qualquer pacote que atravessa o firewall, oriundo de uma máquina e direcionado a outra).

nat: Usada para dados que geram outra conexão.

- PREROUTING (para alterar pacotes recebidos antes do roteamento)
- OUTPUT (para alterar localmente pacotes gerados antes do roteamento)
- POSTROUTING (para mudar o endereço de origem das conexões para algo diferente).

mangle: Usada em ações especiais para o tratamento do tráfego que atravessa os chains.

- PREROUTING - Consultado quando os pacotes precisam ser modificados logo que chegam.
- POSTROUTING - Consultado quando os pacotes precisam ser modificados apos o tratamento de roteamento.
- INPUT - Consultado quando os pacotes precisam ser modificados antes que chegam a máquina(o próprio servidor... antes de ser tratado por qualquer outro chain).
- OUTPUT - Consultado quando os pacotes precisam ser modificados antes de sair da máquina
- FORWARD - Consultado quando os pacotes precisam ser modificados antes de serem redirecionado para outra interface

8.3. - NAT

"O NAT não é um protocolo nem um padrão. O NAT é apenas uma série de tarefas que um roteador (ou equipamento equivalente) deve realizar para converter endereços IPs entre redes distintas.

Um equipamento que tenha o recurso de NAT (sigla em inglês: Network Address Translation ou Tradução de Endereço de Rede) deve ser capaz de analisar todos os pacotes de dados que passam por ele e trocar os endereços desses pacotes de maneira adequada.
Vejamos agora como é fácil fazer um compartilhamento de acesso (NAT) no Linux com uma pequena ajuda do iptables"

Para fazer um nat basta você editar o arquivo rc.local que está em /etc/rc.d e adicionar as seguintes linhas ao seu conteúdo:

```
# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Nota: que a placa de rede que se conecta a internet é eth1, isso pode mudar de acordo com sua configuração, podendo variar para eth0, ppp0, etc.

Como queremos que apenas as regras que adicionamos sejam executadas, antes de tudo, é necessário limpar quaisquer regras do firewall existente.
Adicione as seguintes linhas antes da regra que compartilha Conexão:

```
# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"
```

Ficando o nosso script da seguinte forma:

```
# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
```

```
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
```

8.4. - LINKs EXTRAS

http://pt.wikipedia.org/wiki/SELinux

http://www.vivaolinux.com.br/artigo/Criando-um-firewall-simples-e-compartilhando-a-conexao-usando-o-IPtables/

http://focalinux.cipsga.org.br/guia/avancado/ch-fw-iptables.htm

http://www.vivaolinux.com.br/artigo/IPTABLES-Conceitos-e-aplicacao/

9. - Servidor DHCP

O dhcp permite que todos os micros da rede recebam automaticamente as suas configurações de rede, sem que você precise ficar configurando os endereços de rede em cada.

Ou seja, quando um cliente for inicializado e não tive rum endereço IP configurado, ele manda uma mensagem para toda a rede em busca de um endereço IP. Todos os computadores receberão essa mensagem, porém o único que poderá atender a ela é o servidor DHCP.

No fedora, a sua instalação pode ser feita através do yum:

yum install dhcp

O arquivo de configuração do dhcpd pode ser encontrado em: /etc/dhcp/dhcpd.conf

Para iniciar e parar o servidor dhcp, use os comandos:

service dhcpd start

service dhcpd stop

Independente da distribuição Linux, o arquivo de configuração é igual. Vejamos 2 exemplo:

9.1. - DHCP sem IP Fixo

vim /etc/dhcp/dhcpd.conf

```
# /etc/dhcp/dhcpd.conf

# Atualização do dns
ddns-update-style none;

# Tempo padrão de empréstimo de ip
default-lease-time 600;

# Tempo Maximo para empréstimo de ip
max-lease-time 7200;

# Este é o servidor autoritário, caso haja outro na rede
authoritative;

# A sua Subrede
subnet 172.168.0.0 netmask 255.255.0.0 {

# determina a faixa de endereços IP que será usada pelo servidor
range 172.168.0.10 172.167.0.254;

# endereço do default gateway da rede, ou seja, endereço da placa de rede que esta ligado a rede interna.
option routers 172.168.0.1;

# Servidores DNS que serão usados pelas estações.
option domain-name-servers 208.67.222.222,208.67.220.220;

# Endereço de broadcast
option broadcast-address 172.168.0.255;
}
```

9.2. - DHCP com IP Fixo

vim /etc/dhcp/dhcpd.conf

```
# /etc/dhcp/dhcpd.conf

# Atualização do dns
ddns-update-style none;

# Tempo padrão de empréstimo de ip
default-lease-time 600;

# Tempo Maximo para empréstimo de ip
```

```
max-lease-time 7200;

# Nega cliente sem o mac cadastrado
deny unknown-clients;

# Este é o servidor autoritário, caso haja outro na rede
authoritative;

# A sua Subrede
subnet 172.168.0.0 netmask 255.255.0.0 {

# endereço do default gateway da rede, ou seja, endereço da placa de rede que esta ligado a rede interna.
option routers 172.168.0.1;

# Servidores DNS que serão usados pelas estações.
option domain-name-servers 208.67.222.222,208.67.220.220;

# Endereço de broadcast
option broadcast-address 172.168.0.255;
}

#andrio/0002
# especificação um nome para o cliente
host andrio {

# especificação do MAC address da placa do cliente.
hardware ethernet 00:12:31:b3:6f:4C;

# especificação de um endereço que o cliente devera receber
fixed-address 172.168.0.9;

# especificação da mascara que o cliente ira receber
option subnet-mask 255.255.255.0;
}
```

9.3. - LINKs EXTRAS

http://pt.wikipedia.org/wiki/DHCP

http://www.gdhpress.com.br/servidores/leia/index.php?p=cap2-5

http://www.fedora.org.br/article102.html

10. - DNS Cache (Bind)

Bind é o servidor DNS mais utilizado, especialmente em sistemas Unix/Linux.
Nesse artigo, abordaremos a instalação e configuração de forma fácil e funcional da aplicação Bind, e assim servir de cache DNS. Dando um ganho de desempenho nas pesquisas DNS e uma pequena economia no Link.

No fedora, a sua instalação pode ser feita através do yum:
yum install bind

O arquivo de configuração do bind pode ser encontrado em: /etc/named.conf
Para iniciar e parar o servidor bind, use os comandos:
service named start
service named stop

10.1. - Configuração do DNS Cache

Edite o arquivo named.conf e deixe-o como abaixo:

vim /etc/named.conf

```
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
directory "/var/named";

# Cache DNS
dump-file "/var/named/data/cache_dump.db";

# Estatísticas DNS (sucessos, falhas, etc)
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";

# mude "172.168.0.0/16 para a faixa usada em sua rede.
allow-query { 172.168.0.0/16; localhost; };
allow-recursion {172.168.0.0/16; 127.0.0.1; };
forward only;
```

```
# aqui você ira colocar os dns de sua operadora ou outros dns, caso a requisição da rede
interna não encontre o dns pesquisado
# então, será pesquisado nos dns abaixo
forwarders { 189.38.95.95; 208.67.222.222; 200.176.2.12; 200.225.157.104; 201.10.128.2;
200.176.2.10; 189.38.95.96; 208.67.220.220; 200.225.157.105; 201.10.120.3; 200.192.112.8;
};
tcp-clients 1000;
version "[Not Available]";
};

logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};

zone "." IN {
type hint;
file "named.ca";
};

include "/etc/named.rfc1912.zones";
```

Reinicie o servidor bind:

service named restart

Pronto, seu DNS Cache já deve estar funcionando.

10.2. - Dicas BIND

1. - Para que sua rede possa pesquisar o dns diretamente no seu servidor (Gateway), teremos que editar o dhcpd.conf.

Volte no arquivo de configuração do dhcp, procure e altere: option domain-name-servers coloque o endereço da placa que ira atender a rede interna(Gateway rede interna)... no meu caso, fica assim:

option domain-name-servers 172.168.0.1;

2. - Caso você tenha seguido o script do Bind aqui descrito, o comando a seguir irá gravar dentro do arquivo /var/named/data/cache_dump.db toda a cachê do DNS, lembrando que esse

cachê zera cada vez que o serviço é parado e reiniciado. Após rodar o comando, edite o arquivo e mate sua curiosidade.

rndc dumpdb

10.3. - LINKs EXTRAS

http://pt.wikipedia.org/wiki/BIND

http://www.vivaolinux.com.br/artigo/DNS-Cache-no-Bind9/?pagina=1

http://www.vivaolinux.com.br/artigo/Monitoramento-de-utilizacao-do-DNS?pagina=1

https://www.isc.org/software/bind

11. - Web Cache (Squid)

Squid é um servidor Proxy e cache q permite reduzir a utilização do Link.

Podemos usar o Squid para varias funções: autenticação de usuários, restrições de acesso, auditoria, cache, etc.

Nesse, abordaremos a instalação e configuração de forma fácil e funcional do Squid para WEB Cache.

No Fedora, a sua instalação pode ser feita através do yum:

yum install squid

O arquivo de configuração do Squid pode ser encontrado em: /etc/squid/squid.conf

Para iniciar e parar o servidor Squid, use os comandos:

service squid start

service squid stop

Para criar os diretórios swap:

squid -z

Mas antes disso, certifique-se de ter configurado o Squid e de ter criado os diretórios swap.

11.1. - Configuracao do WEB Cache

Edite o arquivo named.conf e deixe-o como abaixo(comentei ele para facil entendimento):

vim /etc/squid/squid.conf

```
# squid.conf
# Andrio P. Jasper
# mascaraapj@gmail.com
#---------------------------------------------
# Opções para suportar Proxy transparente.
#nao esquecer de trocar a faixa de ip pela da sua rede
http_port 172.168.0.1:3128 transparent

#diz ao Squid que ele deve buscar os dados diretamente na origem
hierarchy_stoplist cgi-bin ?

#diz ao Squid para não armazenar em cache o conteúdo dos CGI's
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY

#memória usada pelo squid
cache_mem 128 MB

#esvazia o cache
cache_swap_low 75
cache_swap_high 78

#tamanho Maximo para gravação no cache Squid
maximum_object_size 150 MB

#tamanho mínimo para gravação no cache Squid
minimum_object_size 0 KB

# Tamanho Maximo dos objetos mantidos em memória.
maximum_object_size_in_memory 2048 KB

# política de substituição dos objetos quando se esgota o espaço destinado ao cache em disco.
# lru: mantem os objetos referenciados recentemente.
# heap GDSF: otimiza o "hit rate" por manter objetos pequenos e
# e populares no cache, guardando assim um numero maior de objetos.
# heap LFUDA: otimiza o "byte hit rate" por manter objetos populares
# no cache sem levar em conta o tamanho. Se for utilizado este, o
# maximum_object_size devera ser aumentado para otimizar o LFUDA.
cache_replacement_policy heap LFUDA

#define a política de substituição dos objetos em memória
#da mesma forma como o cache_replacement_policy
memory_replacement_policy heap GDSF
```

```
#determina onde e como será feito o cache e o tamanho
#a cada 1GB (1024), deve separar 15mb de memória
cache_dir aufs /var/spool/squid 10000 64 128

# Log de requisições.
cache_access_log /var/log/squid/access.log

# Log de objetos guardados. Pode ser desativado.
cache_store_log none

# Log do cache.
cache_log /var/log/squid/cache.log

#Pode ser usada para especificar uma lista de servidores DNS no
#lugar no /etc/resolv.confdns_nameservers Endereço_IP
#nao esquecer de trocar a faixa de dns pela da sua faixa
# caso tenha um servidor dns instalado na mesma maquina, deixe assim: dns_nameservers
127.0.0.1
dns_nameservers 127.0.0.1
dns_nameservers 201.10.120.3

#TAG's referentes ao processo de autenticação.
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

auth_param basic casesensitive off

## Aumentando o tempo do CACHE WINDOWS UPDATE
refresh_pattern -i w?xpsp[0-9]\.microsoft\.com/ 0 100% 20160 reload-into-ims
refresh_pattern -i w2ksp[0-9]\.microsoft\.com/ 0 100% 20160 reload-into-ims
refresh_pattern -i windowsupdate.com/.*\.(cab|exe|dll|msi) 0 100% 43200 reload-into-ims
refresh_pattern -i microsoft.com/.*\.(cab|exe|dll|msi) 10080 100% 43200 reload-into-ims
refresh_pattern -i download\.macromedia\.com/ 0 100% 20160 reload-into-ims

#configuram como serão tratados os tempos de vida dos objetos no cache
refresh_pattern ^ftp: 15 20% 2280
refresh_pattern ^gopher: 15 20% 2280
refresh_pattern (/cgi-bin/|\?) 0 0% 0
refresh_pattern . 0 20% 4320

#O cache pode ser configurado para continuar com o download de requisições abortadas
quick_abort_min -1 KB
quick_abort_max 0 KB
quick_abort_pct 100%

#Tempo de vida para resultados mal sucedidos de resolução DNS.
negative_ttl 2 minutes
```

```
#Tempo de vida para resultados bem sucedidos de resolução DNS. não deixe inferior a 1
minuto.
#Padrão de 6 horas.
positive_dns_ttl 5 minutes

#Alguns clientes podem parar o envio de pacotes TCP enquanto deixam o recebimento em
aberto.
#Algumas vezes o Squid não consegue diferenciar conexões TCP totalmente fechadas e
parcialmente fechadas.
#Mudando essa opção para off fará com que o Squid imediatamente feche a conexão quando a
leitura do socket
#retornar "sem mais dados para leitura"
half_closed_clients off
read_timeout 60 seconds
pconn_timeout 120 seconds

#Estas ACL's fazem parte da configuração padrão do Squid e é o mínimo
#recomendável para seu uso não sendo necessária nenhuma alteração nas mesmas
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSl_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 #unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

##não se esquecer de trocar a faixa de ip pela da sua rede
acl rede src 172.168.0.0/255.255.0.0

#Definição de regras de acesso referentes as ACL's da parte da configuração
#padrão do Squid, também não é necessária nenhuma alteração, portanto apenas
#acrescente as suas próprias regras a estas;
http_access allow localhost
http_access allow rede
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

#Ela diz ao Squid que se nenhuma das regras anteriores for
#aplicada o acesso será então negado
http_access deny all
```

```
# Usuário sob o qual ira rodar o Squid.
cache_effective_user squid
# Grupo sob o qual ira rodar o Squid.
cache_effective_group squid

#Mostra o nome do servidor configurado nas mensagens de erro
visible_hostname servidor.lgm.farolbr

#Desligando essa variável, faz com que o Squid descarregue a memória não
#utilizada, chamando uma função interna free() do Squid
memory_pools off

#Por padrão o Squid irá incluir o ip ou nome da sua máquina nas solicitações HTTP.
#Para o site visitado não interessa para ele qual seu ip interno, o importante é que você visitou
o site.
forwarded_for off

#mensagens de erro em Português
error_directory /usr/share/squid/errors/Portuguese

#essa opção como off mostra no log o endereço completo.
strip_query_terms off
ie_refresh on

# Resolve um problema com conexões persistentes que ocorre com certos servidores,
detect_broken_pconn on

#o Squid irá trabalhar com 2 requisições paralelamente
pipeline_prefetch on
```

Edite o script do firewall rc.local (/etc/rc.d.rc.local) e adicione a regra de redirecionamento do trafego para o Squid.
Ficando o nosso script da seguinte forma:

```
# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
```

```
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# Redireciona todo trafego http(80) que não seja para a conectividade social, para o Squid (3128),
iptables -t nat -A PREROUTING -i eth1 -p TCP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT --to-port 3128
iptables -t nat -A PREROUTING -i eth1 -p UDP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT --to-port 3128

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
```

11.2. – Restringindo acesso

Em um ambiente de trabalho encontramos alguns funcionários que acabam passando a maior parte do tempo no Orkut, diminuindo o desenvolvimento da empresa.

Podemos usar o Squid de forma bem simples para bloquear sites indesejáveis.

Faremos isso em 2 passos:

1. Criamos a “acl” onde iremos especificar os endereços.
2. Bloqueamos ou liberamos a “acl” através do parâmetro “http_access”

Nota: você pode incluir diversas “acls” diferentes dentro da configuração do Squid, desde que use um nome diferente para cada uma. De certa forma, elas são similares às variáveis, que usamos ao programar em qualquer linguagem.

Podemos usar a mesma lógica de regras para bloquear o acesso a determinados usuários(hosts).

Exemplo:

Vamos criar uma “acl” onde iremos bloquear os endereços: orkut.com, twitter.com.

O nome dessa “acl”será site_bloqueado.

```
acl site_bloqueado orkut.com twitter.com
http_access deny site_bloqueados
```

Existe um porem: muitos sites podem ser acessados tanto com o "www" quanto sem o "www". Se os dois estiverem hospedados em servidores diferentes, o Squid ira consider que são sites diferentes, de forma que ao bloquear apenas o "www.orkut.com" os usuários ainda conseguirão acessar o site através do "orkut.com" e vice-versa.

Se preferir, poderá criar um arquivo onde ira conter todos os sites que deverão ser bloqueados pelo squid. Porem, a regra muda um pouquinho, vejamos:

Crie um arquivo de texto

touch /etc/squid/sites_bloqueados

E adicione no arquivo, todos os domínios que deseja bloquear (um por linha):

```
orkut.com
www.orkut.com
twitter.com
www.twitter.com
playboy.abril.com.br
```

Veja como ficou a regra do squid para esse outro caso:

acl sites_bloqueados url_regex -i "/etc/squid/ sites_bloqueados”

http_access deny sites_bloqueados

Em alguns ambientes de trabalho é muito mais fácil bloquear todos os sites e ir liberando somente os permitidos. Para esse caso, apenas invertemos a lógica da regra.

Ao invés de negarmos o acesso: http_accesss **deny**

Liberamos o acesso: http_accesss **allow**

Lembre-se: o Squid processa as regras seqüencialmente, as páginas que forem bloqueadas pela acl "sites_bloqueados" não chegam a passar pela regra que autoriza os acessos da rede local. Adicione as regras antes da regra que libera o acesso para a rede local, exemplo:

```
#Estas ACL's fazem parte da configuração padrão do Squid e é o mínimo
#recomendável para seu uso não sendo necessária nenhuma alteração nas mesmas
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSl_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 #unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
```

acl sites_bloqueados url_regex -i "/etc/squid/ sites_bloqueados”
http_access deny sites_bloqueados

##não se esquecer de trocar a faixa de ip pela da sua rede
acl rede src 172.168.0.0/255.255.0.0

11.3. - Dicas SQUID

1. - Para ver quem esta acessando a web através do Squid em tempo real (IP da maquina, Site cessado e Status do Acesso) digite no terminal:

tail -f /var/log/squid/access.log | awk '{print$3 " - " $4 " - " $7 }'

2. - Para limpar o cache, digite os passos abaixo no terminal:

service squid stop

cd /var/spool/squid

rm -rf *

squid -z

service squid start

11.3. - LINKs EXTRAS

http://www.guiadohardware.net/dicas/squid-sarg-monitorando-acesso-web-sua-lan.html

http://www.vivaolinux.com.br/etc/squid.conf-5

http://br.geocities.com/cesarakg/installing-configuring-squid.html

http://pt.wikipedia.org/wiki/Squid

http://www.squid-cache.org/

http://www.gdhpress.com.br/servidores/leia/index.php?p=cap2-9

12. – Thunder Cache

Aguardando finalização da versão 3.0

13. - Acesso remoto (SSH)

Todo servidor necessita de manutenção seja ele que sistema operacional ele use. No Linux temos um serviço muito interessante chamado SSH (Secure SHell).
O SSH é uma maneira extremamente segura de se conectar no servidor mesmo que está conexão seja vinda da internet.
O SSH é tão bom que apenas precisaremos alterar algumas linhas para torná-lo ainda, mas seguro.

O ssh ja vem por padrão no Fedora.
Arquivo de configuração do SSH, sshd_config pode ser encontrado em "/etc/ssh/sshd_config"

Apenas as linhas abaixo precisam ser alteradas:

- 1°: Port 22: está linha indica a porta na qual o ssh vai funcionar a padrão é 22, mas o ideal é ser mudada para uma porta a sua escolha.

OBS: Cuidado para não escolher uma porta que está sendo utilizada por outro serviço.

- 2°: PermitRootLogin no: está linha indica se o root pode se logar no sistema através deste serviço. Isso não é uma boa idéia pois é um alvo em potencial para ataques pois é um usuário que o Hacker sabe que existe no seu sistema.

- 3°: LoginGraceTime 120: Define o tempo máximo que o usuário tem para digitar a senha e logar no sistema.

- 4°: AllowUsers andrio: Permite o login somente dos usuários configurado, dificultando ainda mais o trabalho de um hacker. No meu caso, permiti apenas o login do usuario andrio

- 5°: MaxStartups 5:80:10: Desta forma ele rejeita 80% das tentativas de conexão

13.1. - Informações SSH

Para iniciar e parar o servidor SSH, use os comandos:
service sshd start

service sshd stop

Logando no sistema via SSH:
#ssh (login)@(ip) –p (numero da porta)
#ssh andrio@172.168.0.1 –p 2250

Para fazer o sistema sempre iniciar o SSH caso ele seja reiniciado.
Comando:
setup
Opção: Serviços do Sistema
Opção: sshd
OK e SAIR

14. - Controle de acesso (MACxIP)

O controle de acesso por MACxIP é feito com a ajuda do iptables.
O Cliente devera ter sempre o mesmo IP, basta configurar o DHCP com ip fixo ou configurar o micro do cliente manualmente.

Funcionara da seguinte forma:

- -- teremos um arquivo que ira conter todos os IPs e MACs da rede.
- -- iremos alterar a política padrão de ACCEPT para DROP (assim estaremos bloqueando TUDO),
- -- adicionaremos 2 regras no script do firewall, essas ultimas serão responsável por liberar o acesso aos cadastrados.

14.1. - Configurando o acesso (MACxIP)

Atualmente, nosso rc.local (/etc/rc.d.rc.local), esta da seguinte forma:

```
# Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
```

```
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# Redireciona o trafego http(80) para o Squid (3128)
iptables -t nat -A PREROUTING -i eth1 -p TCP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128
iptables -t nat -A PREROUTING -i eth1 -p UDP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Criaremos o arquivo que conterá os IPs e MACs, e adicionaremos os IPs e MACs, cada cliente em uma linha, da seguinte forma:

#IP;MAC;Marcação pacote;nome do cliente

vim /etc/macxip

```
172.168.0.9;00:12:31:b3:6f:4C;10019;andrio
```

Agora, editamos o rc.local (/etc/rc.d.rc.local), deixando-o da Seguinte forma:

```
# Paramentros do Controle de acesso
MACLIST=/etc/macxip
echo " Configurações necessárias.....[ OK ]"

# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"
```

```
# Definindo Política Padrão
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# # Controle de ACESSO # #
# Diretivas do BD IP, MAC e Port
for i in `cat $MACLIST`; do
IPSOURCE=`echo $i | cut -d ';' -f 1`
MACSOURCE=`echo $i | cut -d ';' -f 2`
CBQMARK=`echo $i | cut -d ';' -f 3`

# Controle de Acesso IPxMAC
iptables -t filter -A FORWARD -d 0/0 -s $IPSOURCE -m mac --mac-source
$MACSOURCE -j ACCEPT
iptables -t filter -A INPUT -s $IPSOURCE -d 0/0 -m mac --mac-source $MACSOURCE
-j ACCEPT
done

# Redireciona o trafego http(80) para o squid (3128)
iptables -t nat -A PREROUTING -i eth1 -p TCP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128
iptables -t nat -A PREROUTING -i eth1 -p UDP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
```

- Execute o script do firewall e seu controle de acesso IPxMAC já estará funcionando.
- Para bloquear um determinado cliente, basta mudar os 2 primeiros "00" do MAC do mesmo, dessa forma, o novo mac cadastrado não ira bater com o mac real do cliente(MAC 00:12:31:b3:6f:4C é diferente do MAC 11:12:31:b3:6f:4C)

Pode ser necessário adicionar mais 3 linhas de regras no script, para manter/aceitar as conexões estabilizadas. adicione-as logo abaixo das regras de "Política Padrão"

```
# Aceita os Pacotes que realmente devem entrar
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Como deixamos o firewall restritivo, é bom adicionar a regra abaixo, responsável por aceitar toda conexão loopback.

```
# Aceita todo o trafego vindo do loopback e indo pro loopback
```

```
iptables -t filter -A INPUT -i lo -j ACCEPT
```

14.2. - LINKs EXTRAS

http://under-linux.org/b1326-bloqueio-por-mac

15. - Controle de Banda

> “Imagine esta cena: você tem um ADSL e compartilha com seus vizinhos, mas um deles usa o Kazaa o dia todo deixando todo mundo lento ou pior, você tem um acesso coletivo em sua empresa, onde na sua maioria, os usuários apenas usam a conexão de maneira "superficial" (e-mail, icq, Kazaa, MSN, bate-papo, etc), ocupando assim toda a banda com coisas inúteis e você precisa fazer uma alteração urgente no servidor remoto, tendo que concorrer com todos usuários, ou pior, a diretoria de sua empresa está achando que a conexão está lenta (embora seu link seja de bom tamanho) e te pede uma solução barata para que eles possam navegar mais rapidamente. Esta cena não é muito difícil de acontecer, contudo ambas as situações podem ser elegantemente contornadas.
>
> A solução: Qualidade de Serviço (QoS)”

Artigo: http://www.vivaolinux.com.br/artigo/Controle-sua-banda-de-maneira-simples-e-inteligente-com-CBQ/

Nesse guia, irei mostrar como instalar o controle de banda Bandlimit e o CBQ, ficando ao seu cargo escolher qual lhe agrada.

15.1. – Bandlimit

Este Script tem como objetivo fazer limitação de banda, sendo baseado na idéia de Francisco Antonello (Skyzer) e Marcus Maciel de criar uma fácil solução para Limitação de Banda.
Feito em bash, este script não acompanha nenhuma distribuição, mais e facilmente encontrado na internet, pois é um simples front-end para os comandos do pacote iproute2 e iptables. Um projeto under-linux.

Abra o terminal
Passe para super usuário:
su –

Vai para a pasta /sbin:

cd /sbin

Faca o download o script do Bandlimit:
wget http://underlinux.com.br/downloads/bandlimit/rc.bandlimit-v0.4

Para uma melhor administração, altere o nome, de “rc.bandlimit-v0.4” para “bandlimit”

mv rc.bandlimit-v0.4 /sbin/bandlimit

De permissão para execução:

chmod +x /sbin/bandlimit

Crie o diretorio bandlimit dentro do seu /etc

mkdir /etc/bandlimit

Dentro deste diretorio crie os arquivos ips e interfaces

touch /etc/bandlimit/ips

touch /etc/bandlimit/interfaces

Depois edite o arquivo “ips” e o “interfaces”, colocando dentro do ips os ips que você deseja limitar, um por linha no seguinte formato

ip:download:upload

172.168.0.9:300:128

E no arquivo “interfaces”, as interfaces que você usa na sua maquina, um por linha também.

Exemplo:

eth0

eth1

Para iniciar o controle de banda, digite:

bandlimit start

Para parar o controle de banda, digite:

bandlimit stop

Para iniciar o controle de banda juntamente com o sistema, adicione “bandlimit start” no script do firewall antes das regras “Limpando Regras”.

15.2. - CBQ

No Fedora, não é necessário instalar o script do CBQ. Por padrão, ele já vem no sistema.
Importante saber:

- Os arquivos de limitação ficam (classes) ficam em: /etc/sysconfig/cbq/
- Os arquivos de limitação obedecem o formato predefinido: cbq-(clsid).(nome)
- O mesmo IP não pode estar em duas regras
- É necessário 2 arquivo de limitação para cada regra: 1 para download e outro para upload.
- Cada arquivo de limitação deve conter as regras abaixo, com 1 pequena diferença, um dos arquivos devera conter uma vírgula no final da RULE, o arquivo que conter a virgula será o que vai indicar o upload:

  DEVICE=(interface rede),(banda),(peso)

  RATE=(velocidade)

  WEITH=(peso/10)

  PRIO=(prioridade)

  RULE=(ip ou rede a ser controlada)

Opcional

BOUNDED=yes/no se setado para yes o usuário estará limitado mesmo que o link esteja com folga.

ISOLATED=yes/no se setado para yes indica que o cliente não poderá emprestar banda pra ninguém

Exemplo, regra para o usuário andrio:

vim /etc/sysconfig/cbq/cbq-0002.andrio

```
DEVICE=eth0,10Mbit,1Mbit
RATE=256
WEIGHT=64Kbit
PRIO=5
```

```
RULE=172.168.0.9
BOUNDED=yes
ISOLATED=no
```

vim /etc/sysconfig/cbq/cbq-0003.andrio

```
DEVICE=eth1,10Mbit,1Mbit
RATE=256
WEIGHT=64Kbit
PRIO=5
RULE=172.168.0.9,
BOUNDED=yes
ISOLATED=no
```

Nota: Qualquer regra seguida da virgula " , " controla o trafego de saída da sua rede

Com todas as regras prontas, vamos ativar o serviço.

Primeiro compilamos as novas regras

cbq compile

E depois iniciamos o cbq:

cbq start

Pronto, cbq funcionando.

Faca o teste.

Para um controle de upload mais efetivo, aconselho a marcar os pacotes de cada cliente.

Editamos o rc.local (/etc/rc.d.rc.local)

Adicione a opção MARK na regra do cliente que contiver a virgula ","

deixe-o assim:

```
# vim cbq-0003.andrio
DEVICE=eth0,10Mbit,1Mbit
RATE=256
WEIGHT=64Kbit
PRIO=5
RULE=172.168.0.9,
MARK=16709
BOUNDED=yes
ISOLATED=no
```

E o script do firewall, deixe-o da Seguinte forma:

```
# Parâmetros do Controle de acesso
MACLIST=/etc/macxip
echo " Configurações necessárias.....[ OK ]"

# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# Aceita os Pacotes que realmente devem entrar
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# # Controle de ACESSO # #
# Diretivas do BD IP, MAC e Port
for i in `cat $MACLIST`; do
IPSOURCE=`echo $i | cut -d ';' -f 1`
MACSOURCE=`echo $i | cut -d ';' -f 2`
CBQMARK=`echo $i | cut -d ';' -f 3`

# Controle de Acesso IPxMAC
iptables -t filter -A FORWARD -d 0/0 -s $IPSOURCE -m mac --mac-source $MACSOURCE
-j ACCEPT
iptables -t filter -A INPUT -s $IPSOURCE -d 0/0 -m mac --mac-source $MACSOURCE -j
ACCEPT

#Pacote Marcado - importante lembrar que todo trafego de saída deve ser controlado na
interface oposta do cliente.
# no meu caso= eth0
iptables -A PREROUTING -t mangle -i eth0 -s $IPSOURCE -j MARK --set-mark
$CBQMARK
done

# Redireciona o trafego http(80) para o squid (3128)
```

```
iptables -t nat -A PREROUTING -i eth1 -p TCP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128
iptables -t nat -A PREROUTING -i eth1 -p UDP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward

# Aceita todo o trafego vindo do loopback e indo pro loopback
iptables -t filter -A INPUT -i lo -j ACCEPT
```

15.1. - LINKs EXTRAS

http://www.vivaolinux.com.br/artigo/Limitando-banda-com-o-CBQ/

http://br-linux.org/artigos/dicas_cbq.htm

http://www.linuxnarede.com.br/artigos/fullnews.php?id=128

http://under-linux.org/wiki/BandLimit

http://under-linux.org/comunidade/underlinux/underlinux-bandlimit/

16. - Outras Regras

1- O Kernel conta com algumas opções interessantes, vamos adicioná-las em nosso script de firewall, deixando por fim... assim:

2- Entramos um problema no acesso remoto (ssh), pois deixamos nosso firewall restritivo, liberando acesso somente aos cadastrados. Vamos então adicionar + 1 regra que permitira o acesso remoto na porta do ssh.

```
# Parâmetros do Controle de acesso
MACLIST=/etc/macxip
echo " Configurações necessárias.....[ OK ]"

# # Limpando Regras
iptables -F
iptables -X
iptables -Z
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F -t nat
iptables -X -t nat
iptables -F -t mangle
iptables -X -t mangle
```

```
echo " Limpando Regras .....[ OK ]"

# Definindo Política Padrão
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
echo " Alterando política padrão.....[ OK ]"

# Aceita os Pacotes que realmente devem entrar
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Proteções #
# evita ataques como 'syn flood atack'
echo "1" > /proc/sys/net/ipv4/tcp_syncookies

# rejeita todas as requisição de ICMP ECHO, ou apenas aquelas destinadas a endereçamento broadcasting ou multicasting
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# ignora mensagens falsas de icmp_error_responses
echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

# Kill timestamps. These have been the subject of a recent bugtraq thread
echo "0" > /proc/sys/net/ipv4/tcp_timestamps

# Permite o redirecionamento seguro dos pacotes
echo "1" > /proc/sys/net/ipv4/conf/all/secure_redirects

# Evita problema de resposta tamanho zero
echo "0" > /proc/sys/net/ipv4/tcp_ecn

# Tempo em segundos para manter um fragmento IP na memória
echo "15" > /proc/sys/net/ipv4/ipfrag_time

# Tempo Maximo de Espera da Conexão sem Resposta
echo "1800" > /proc/sys/net/ipv4/tcp_fin_timeout

# conf/accept_redirects - essa opção decide se o kernel aceita redirecionar mensagens ICMP ou nao
# conf/accept_source_route - Desativar essa opção fecha as chances para que um cracker realize ataques do tipo IP Spoofing
# conf/send_redirects - Não envie mensagens de redirecionamento ICMP
# conf/*/log_martians - permite que pacotes de origem suspeita ou desconhecida (como pacotes forjados) sejam logados pelo próprio kernel.
# conf/*/rp_filter - verifica o Endereço de Origem do Pacote, prevenindo a sua maquina de ataques como 'IP Spoofing'.
for i in /proc/sys/net/ipv4/conf/*; do
echo "0" > $i/accept_redirects
```

```
echo "0" > $i/accept_source_route
echo "0" > $i/send_redirects
echo "1" > $i/log_martians
echo "1" > $i/rp_filter;
done

# Liberando todos os dados cacheados da memória
echo 3 > /proc/sys/vm/drop_caches

echo "2048" > /proc/sys/net/ipv4/tcp_max_syn_backlog
echo "4096" > /proc/sys/net/core/netdev_max_backlog
echo "3" > /proc/sys/net/ipv4/tcp_syn_retries

# permite determinar o nº de segundos que uma conexão precisa estar ociosa antes de o TCP enviar checagens de keep-alive
echo "1800" > /proc/sys/net/ipv4/tcp_keepalive_time
echo "30" > /proc/sys/net/ipv4/tcp_keepalive_intvl

# Permite ativar o TCP Selective Acknowledgements previsto pela RFC2018
echo "0" > /proc/sys/net/ipv4/tcp_sack

# permite ativar o TCP window scaling previsto pela RFC1323
echo "0" > /proc/sys/net/ipv4/tcp_window_scaling

# Confundir fingerprinting "
echo "255" > /proc/sys/net/ipv4/ip_default_ttl

# Esse parâmetro determina o nº de pacotes SYN+ACK enviados antes de o kernel liberar a conexão
echo "2" > /proc/sys/net/ipv4/tcp_synack_retries
echo " Carregando Proteções Adicionais.....[ OK ]"

# # Controle de ACESSO # #
# Diretivas do BD IP, MAC e Port
for i in `cat $MACLIST`; do
IPSOURCE=`echo $i | cut -d ';' -f 1`
MACSOURCE=`echo $i | cut -d ';' -f 2`
CBQMARK=`echo $i | cut -d ';' -f 3`

# Controle de Acesso IPxMAC
iptables -t filter -A FORWARD -d 0/0 -s $IPSOURCE -m mac --mac-source $MACSOURCE -j ACCEPT
iptables -t filter -A INPUT -s $IPSOURCE -d 0/0 -m mac --mac-source $MACSOURCE -j ACCEPT

#Pacote Marcado
iptables -A PREROUTING -t mangle -i eth1 -s $IPSOURCE -j MARK --set-mark $CBQMARK
done
```

```
# Redireciona o trafego http(80) para o Squid (3128)
iptables -t nat -A PREROUTING -i eth1 -p TCP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128
iptables -t nat -A PREROUTING -i eth1 -p UDP ! -d 200.201.0.0/16 --dport 80 -j REDIRECT
--to-port 3128

# Compartilha Conexão
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward

# Aceita todo o trafego vindo do loopback e indo pro loopback
iptables -t filter -A INPUT -i lo -j ACCEPT

# # SSH - mude a porta caso necessário
iptables -A INPUT -p tcp --dport 22 --syn -m state --state NEW -j ACCEPT
```

17. - Limite de Conexão (connlimit)

O Objetivo principal do uso do connlimit é sobre a limitação de softwares p2p. Analisando o tráfego desse tipo de software, percebemos que tinha que atacar diretamente o fato deles abrirem muitas conexões simultâneas, mas, em alguns casos não é interessante limitar todas as portas, principalmente se parte de seus clientes são empresas e precisam de acesso full, o que é necessário então é limitar somente o P2P.

Faremos 2 tipo de limitação:

Um somente para as portas nativas e outra para as portas não nativas

17.1 - Limitando Portas nativas

Crie uma tabela chamada CONNLIMIT, e coloque nessa tabela as principais portas: 20,21,23,25,53,110,443,1863,2210,31 28,5600,8080,8081

No final, ative o limite de 96 conexões simultâneo (--connlimit-above 96) para cada ip na rede (--connlimit-mask 32).

Nota: alterando o (--connlimit-mask 32) para (--connlimit-mask 24) vc ira limitar uma rede ao todo, ao total de conexões configuradas, aqui eu deixei em "32", pois assim eu limito ip por ip.

```
# Connlimit
# Controle de conexão
iptables -t mangle -N CONNLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 -m multiport --destination-port
20,21,23,25,53,110,443 -j CONNLIMIT
```

```
iptables -t mangle -A FORWARD -p TCP -d 0/0 -m multiport --destination-port
1863,2210,3128,5600,8080,8081 -j CONNLIMIT
iptables -t mangle -A CONNLIMIT -p TCP -m state ! --state RELATED -m connlimit --
connlimit-above 96 --connlimit-mask 32 -j DROP
echo " Connlimit porta nativa iniciado.....[ OK ]"
```

17.2 - Limitando Portas não nativas

Criei uma outra tabela chamada CONLIMIT, e limitei todas as outras portas para um total de 45 conexões simultâneas...

```
iptables -t mangle -N CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 1:19 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 -m multiport --destination-port 22,24 -j
CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 26:52 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 54:79 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 81:109 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 111:442 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 444:1862 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 1864:2209 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 2211:3127 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 3129:5599 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 5601:8079 -j CONLIMIT
iptables -t mangle -A FORWARD -p TCP -d 0/0 --dport 8082:65535 -j CONLIMIT
iptables -t mangle -A CONLIMIT -p TCP -m state ! --state RELATED -m connlimit --
connlimit-above 45 --connlimit-mask 32 -j DROP
echo " Connlimit portas não nativa iniciado.....[ OK ]"
```

Adicione essas regras antes da regra de Controle de acesso

17.3. - LINKs EXTRAS

http://linuxadm.blogspot.com/2007/05/limitando-o-trfego-p2p-com-layer7-e.html

http://under-linux.org/f88121-relato-de-uso-do-controle-de-conexoes-simultaneas-connlimit

Nenhum problema pode ser resolvido pelo mesmo estado de consciência que o criou.
(Albert Einstein)

18. - QOS

19. – Monitoramento

19.1. – Sarg

19.2. – Squid-Graph

19.3. – Iptstate

19.4. – Iptraf

19.5. – Ntop

19.6. – Comandos sistema

“Espero que este não seja o fim de sua aprendizagem, mas um bom começo.”