

Conectando sua rede interna com Linux, ipchains e ADSL

por Carlos Fernando Scheidecker Antunes

Escrito em 20 de Janeiro de 2001.
Última revisão : 22 de Março de 2001.
copyright (c) 2001 Carlos Fernando Scheidecker Antunes

Índice :

[Licença de uso](#)

[Público Alvo](#)

[1.0 Introdução](#)

- [1.1 Porque resolvi escrever esse artigo](#)
- [1.2 Dificuldades](#)
- [1.3 Software, hardware, serviços e provedor utilizados](#)
- [1.4 Vantagens](#)
- [1.5 Desvantagens](#)

[2.0 Conceitos](#)

- [2.1 Um pouco sobre telefonia tradicional](#)
- [2.2 O que é ADSL](#)
- [2.3 Conceitos de TCP/IP que você deve saber](#)
- [2.4 O que é Proxy](#)
- [2.5 O que é NAT](#)
- [2.6 O que é IP Masquerading](#)
- [2.7 O que é IP Forwarding ou Ipfwadm](#)
- [2.8 O que é IPChains](#)
- [2.9 Funcionamento do IPChains](#)
- [2.10 Esquema da rede](#)
- [2.11 Gateways](#)

[3.0 Instalação do hardware](#)

- [3.1 Instalação do Modem ADSL](#)
- [3.2 Máquina para Firewall Linux](#)

[4.0 Configuração do Firewall Linux](#)

- [4.1 Redes, subnets, gateways e IPs](#)
- [4.2 Configurando eth0, eth1, eth2, default gateway e DNS.](#)

[5.0 Script de firewall](#)

- [5.1 Alterando os atributos do script](#)

- [5.2 Criando o script de inicialização do firewall](#)
- [5.3 Inserindo o script /etc/rc.d/init.d/firewall na inicialização](#)
- [5.4 Rodando o firewall](#)
- [5.5 Para usuários do Slackware](#)

6.0 Medindo a velocidade do seu acesso

- [6.1 Considerações técnicas](#)
- [6.2 Técnica sugerida](#)

7.0 Configurando os Hosts da sua rede

- [7.1 Configurando Hosts Linux](#)
- [7.2 Configurando Hosts Windows 95/98](#)
- [7.3 Configurando Hosts Windows NT](#)

8.0 Sugestões

- [8.1 Cable Modem](#)
- [8.2 Modem comum sob linha telefônica](#)
- [8.3 Outros tipos de aplicações](#)

9.0 Informações adicionais

- [9.1 Leitura recomendada](#)
- [9.2 Como contatar o autor e obter os scripts gratuitamente](#)

10.0 Sobre o autor

11.0 Sistema S.E.N.

12.0 Links

13.0 Como obter e apreender mais sobre Linux

14.0 O que é Linux

15.0 Agradecimentos

Público Alvo

Este artigo destina-se a :

- Integradores que precisam de recursos técnicos para melhor atender seus clientes;
- ISPs : Provedores de acesso internet;
- Estudantes da área que desejam aprender mais sobre redes e conceitos avançados de conectividade;

- Empresas, escolas, entidades governamentais que precisam disponibilizar acesso internet de qualidade e alta velocidade na sua rede a custos baixos;
- Indivíduos que queiram conectar uma rede inteira à internet.

Licença de uso

Essa licença aplica-se ao uso do artigo intitulado "Conectando sua rede interna com Linux, IPchains e ADSL", de autoria de Carlos Fernando Scheidecker Antunes.

- Este artigo é fornecido gratuitamente.
- Nenhum tipo de garantia quanto à sua aplicação é oferecida.
- O autor não se responsabiliza por nenhum dano causado pela implementação do firewall. Use-o sob sua total responsabilidade.
- Nenhuma obrigação ou tipo de suporte são oferecidos por parte do autor.
- O artigo poderá ser copiado e divulgado desde que o autor seja notificado.
- Toda reprodução ou divulgação do artigo, em qualquer tipo de mídia, deve conter o nome do autor.
- O artigo não poderá ser modificado sem a expressa autorização, por escrito, do autor.
- O artigo poderá ser traduzido para outra língua desde que, autorizado pelo autor, seja preservada sua autoria bem como a integridade do texto.

1.0 Introdução

Neste artigo, veremos como conectar a sua rede interna à internet através de um firewall baseado em Linux. Atualmente, conectividade à internet tornou-se algo fundamental nas empresas, instituições educacionais, gabinetes públicos e escritórios em casa (SoHo). Quando a necessidade é maior, ou seja, conectar uma rede privativa inteira à internet, os custos tendem a crescer proporcionalmente. Bem, essa opinião pode não ser totalmente correta. Este artigo apresenta uma solução para isso incluindo :

- Instalação de hardware;
- Hardware e Software utilizados,
- Explicação de cada conceito utilizado,
- Implementação da solução.

Além disso, por este artigo será possível mostrar o Linux em ação para conectar não apenas uma, mas duas redes à internet em alta velocidade através de uma linha ADSL, com muito poucos recursos, software livre e um equipamento obsoleto. Tudo isso é viável graças à famosa conectividade, estabilidade e baixo (ou nenhum) custo do Linux.

Importante: Se na sua cidade não há ADSL, não se preocupe. Uma das propostas deste artigo é apontar o que se deve fazer para utilizar a solução com um cable modem e até com um modem convencional em linha discada para compartilhar uma única conexão internet com toda a sua rede. Claro que o desempenho irá variar de acordo com o comprimento de banda da sua conexão. Se você usa uma ADSL de 256k ou 512k, sua situação é

bem diferente de quem pode apenas trabalhar com uma linha discada e um banda teórica de 56k.

1.1 Porque resolvi escrever esse artigo.

Este artigo nasceu de uma solução que implementamos na empresa em que trabalho, um ASP chamado Sistema SEN. Na nossa empresa, queríamos reduzir a carga sobre o roteador e link dedicado, colocando todo o tráfego de internet dos nossos desktops em outra via que não a do nosso roteador. Uma outra grande vantagem que essa solução possibilitou foi uma nova rota para nossa rede interna no caso de o link principal ficar fora do ar e necessitarmos gerenciar ou obter alguma informação ou serviço de nossa rede interna. Quando finalmente habilitamos o firewall sob uma linha ADSL, resolvemos escrever um paper e distribuí-lo gratuitamente a nossos clientes de forma a facilitar e reduzir os custos das empresas ligadas a nós 24 horas por dia e aos nossos aplicativos via internet. Logo se percebeu que esse paper poderia beneficiar muitas empresas, não só as de nossos clientes, mas também escolas, profissionais liberais e integradores que precisassem vender seus serviços. O paper se transformou em artigo.

1.2 Dificuldades

Quando resolvemos implantar essa solução, deparamo-nos com várias dificuldades. A primeira era a falta de treinamento do pessoal da nossa operadora e do próprio provedor que não pôde fornecer-nos informações simples. Por exemplo: como devia ser o cabo par trançado ligado do modem ADSL à interface do computador, cross ou paralelo? essa pergunta era pertinente porque o manual do modem ADSL sequer é fornecido e, em geral, o uso de ADSL ainda é restrito pois o próprio provedor instala-o apenas em um equipamento que rode Windows. As equipes de instalação dos provedores são terceirizadas e possuem um treinamento extremamente básico para conectar e configurar apenas 1 host Windows. Os provedores e as operadoras poderiam vender muito mais linhas ADSL se houvesse treinamento ou algo publicado a respeito. Deflagrada essa carência, surgiu a idéia deste artigo que procura preencher essa deficiência, não só ajudando os provedores e as operadoras bem como fornecendo a solução para os integradores e empresas.

Espera-se que este artigo crie uma maior demanda para esses serviços uma vez que busca como conectar uma rede inteira à internet. Além das dificuldades de suporte por falta de treinamento do nosso provedor, havia também o trabalho maior: estudar como fazer, juntar todos os componentes e finalmente implementar a solução. Com relação ao modem e às perguntas que meu provedor e operadora deveriam estar capacitados a responder e não o fizeram, eu as resolvi fazendo uma ligação internacional ao fabricante do modem ADSL, Efficient Networks Inc localizado em Dallas, Texas. Além disso baixou-se, imprimiu-se e encadernou-se o manual do modem e enviaram-se dois e-mails a Efficient Networks. O segundo e-mail perguntava qual OS rodava no Modem. A resposta oficial recebida era que o OS era baseado em UNIX e não foi possível saber se era especificamente Linux, mesmo tendo ficado 37 minutos ao telefone e sendo transferido para 4 pessoas diferentes.

O resto da solução e das dificuldades foram resolvidas com pesquisas na internet, a leitura de um livro específico sobre Firewall no Linux, que indico a seguir, e minha experiência e prazer de trabalhar com Linux.

1.3 Software, hardware, serviços e provedor utilizados.

Como hardware, além da nossa rede interna, foi utilizado:

- a. Uma máquina Pentium 133mhz, com 64mb de memória, HD de 1.2Gb e três placas de rede 10/100mbps baseadas no chip RTL8139c. Esse equipamento estava obsoleto e encontrado na empresa. Para aproveitá-lo foi canibalizada a memória de outra unidade semelhante de forma a contabilizar 64mb; as placas de rede foram compradas ao custo de R\$ 35 cada e só foram necessárias

Artigo

- duas porque a unidade já possuía uma;
- b. O modem ADSL "cedido" por nossa operadora, um SpeedStream 5660 da Efficient Networks www.efficientnetworks.com que roda um kernel baseado em UNIX (qual será??). Nada foi pago por ele já que o "leasing" ou aluguel está incluso no serviço.
- c. Um metro de cabo padrão categoria 5, dois conectores RJ-45 climpados a ele no padrão paralelo EIA/TIA 568A conforme mostrado abaixo.

Como software utilizamos :

- a. Sistema Operacional : Distribuição Red Hat Linux 7.0. Inicialmente foi utilizado o Red Hat 6.2 para rodar o firewall e em seguida feito o upgrade. Note que qualquer distribuição de qualidade serve. Se você usa [Conectiva](#), [Mandrake](#), [Caldera](#), [Timpanogas](#), [Slackware](#), etc, pode implantar a solução deste artigo sem traumas. Iremos comentar as diferenças mais para frente. O mais importante na distribuição que irá instalar é a versão do Kernel. O ideal é que seja versão 2.2.16 pelo menos, já que versões menores que 2.2.11 têm um bug de fragmentação de pacotes IPchains. É importante notar que esse Firewall será construído usando IPchains que está apenas disponível em Kernels a partir do 2.1.x. Kernels 2.0.x usavam IPForward conforme iremos explicar mais adiante. Linux é uma solução excelente não apenas pelo baixo custo. Quando se fala em conectividade, o senso comum é utilizar OSes baseados no padrão POSIX ou UNIX com variações tanto proprietárias quanto livres como Linux e FreeBSD. Lembramos que a opção por Linux foi realizada primeiramente pela qualidade do OS e depois por seu baixo ou nenhum custo, se você obtiver uma cópia gratuitamente no servidor FTP da sua distribuição preferida. Para verificar qual o kernel do seu Linux (caso já tenha um em operação) digite o comando "uname -r" e verá algo do tipo 2.2.16-22 (versão do kernel que está no nosso Linux).
- b. Software de Firewall. Utilizaremos o IPchains. O ideal é usar a versão 1.3.9 ou superior (inexistente no momento em que foi escrito o artigo). Para saber qual a versão do seu IPchains digite "/sbin/ipchains --version" na linha de comando. Insistimos em que não use uma versão inferior a essa, uma vez que pode estar submetendo sua rede interna a riscos de segurança. Lembre que o IPchains é um software gratuito. Pode ser obtido através dos CDs da sua distribuição favorita como [Conectiva](#), [Caldera](#), [Timpanogas](#), [Red Hat](#), [Mandrake](#), etc, ou pode ser obtido no site www.rpmfind.com, no site da sua distribuição ou em outros sites na internet como www.tucows.com.

Provedor e operadora :

Como essa solução foi implantada em São Paulo, a operadora é a Telefonica e como provedor foi escolhido o Terra (Zaz), por conta das recomendações de pessoas que respeitamos quanto à qualidade do provedor. Verifique, na sua cidade, junto a sua operadora local se sua subestação está equipada para fornecer ADSL sobre a sua linha telefônica. Existe uma pequena taxa para converter o telefone para ADSL e uma taxa fixa por mês pelo serviço, que nos dias atuais, não passa de R\$200 mensais. Nossos clientes de fora de São Paulo têm informado preços abusivos de outras operadoras locais para o mesmo serviço que a Telefonica presta em São Paulo. Nesse ponto, a Telefonica está de parabéns pela qualidade e preços justos.

Como se pode observar, nada nessa lista consiste em algo de custo elevado ou difícil de obter. Você pode e deve utilizar uma máquina que não está mais usando porque está ultrapassada como um 486 ou um Pentium de primeira geração, por exemplo. Procure priorizar a quantidade de memória no seu Linux firewall e nem tanto o processador ou HD. No nosso caso utilizou-se 64mb de memória um processador Pentium 133MHz e um HD simples de 1.2Gb.

1.4 Vantagens

Considerando-se a necessidade citada pela maior parte das empresas, a solução apresentada nesse artigo resolve o problema, ou seja, a acessibilidade à internet a custos muito baixos. Muitas empresas acabam optando por servir seus sites e utilizar servidores de e-mails bem como hospedar seus domínios em servidores de terceiros. Nesses casos, a necessidade é possuir apenas conectividade à internet. A solução que apresentamos a seguir é voltada para isso. Se sua empresa já possui um link dedicado a essa atividade, você pode utilizar uma conexão extra com uma ADSL para poupar seu link e o processamento do seu roteador, deixando-o exclusivamente para os servidores. Esse foi exatamente o principal motivo por termos instalado um ADSL.

1.5 Desvantagens

A solução apresentada não resolve o seu problema se a necessidade é servir web pages, FTP, DNS autoritativo, e-mail, etc, com seus próprios servidores. Claro que você sempre pode enviar e-mails configurando o seu sendmail para isso. Mas um servidor de e-mail com várias contas e vários domínios requer um link dedicado e no mínimo 2 IPs fixos válidos. Esses 2 IPs são necessários para cadastrar dois DNS servers – Master e Slave –, para que você possa hospedar domínios, servir seus websites, contas de e-mail em mais de um domínio, etc.

2.0 Conceitos

A seguir, serão expostos os conceitos necessários para que você possa entender a solução apresentada neste artigo e modificá-la de modo a atender às suas necessidades.

2.1 Um pouco sobre telefonia tradicional

Você já notou que quando está falando ao telefone com outra pessoa que está ouvindo música ao mesmo tempo, a música que chega até você pelo telefone não possui boa qualidade? Isso ocorre porque a linha telefônica convencional utiliza um espectro de frequência de 0 a 4KHz, enquanto o ouvido humano pode reconhecer um espectro mais amplo. Por isso, música transmitida por telefone é diferente já que as frequências fora do espectro não chegam a outra pessoa do outro lado da linha.

2.2 O que é ADSL

ADSL, da sigla em inglês, Asymmetric Digital Subscriber Loop, é uma tecnologia de acesso de alta velocidade à internet que usa uma linha comum de cobre. ADSL pode providenciar velocidades entre 384kbps a 1.5mbps, sempre utilizando velocidades diferentes nos canais de saída e de entrada de dados, por isso o nome Asymmetric. Se você obtiver um ADSL de 256Kbps, note que a velocidade que terá entre seu computador e seu provedor para sua recepção de dados será de 256kbps, enquanto a sua velocidade de envio (upstream) não será tão elevada. ADSL é ótimo para acessar sites na internet, fazer download de ISOs de distribuições de Linux, acessar seu e-mail, logar remotamente em servidores via SSH, TELNET, etc. Mas no momento em que a necessidade é a contrária, ou seja, de servir informações, o correto é obter um link dedicado cuja velocidade de envio e recepção tem a mesma prioridade e a mesma relação. Portanto, ADSL é uma tecnologia que usa linhas telefônicas de cobre, provê transferência de dados em altas velocidades e permite usar a linha telefônica para voz ao mesmo tempo. É uma linha digital dedicada ideal para uma conexão IP e as taxas de dados funcionam em combinação de recepção/envio, sendo a taxa de recepção sempre privilegiada. Em São Paulo, a Telefonica oferece ADSLs de 256 e 512Kbps de recepção. Até o

fechamento desta matéria, não conseguimos obter a informação da taxa de envio.

Caberia aqui,então,perguntar como é possível usar o telefone e conectar-se à internet ao mesmo tempo com apenas uma linha telefônica? Isso acontece porque ADSL é uma tecnologia que trafega informações sobre a linha comum de cobre num espectro de frequência superior ao que é usado para voz. A voz utiliza de 0 a 4KHz, enquanto dados utilizam de 4KHz a 2MHz. É como se você tivesse duas linhas em uma só. Note que nem todas as estações estão equipadas para possibilitar tráfego de dados sobre a sua linha telefônica. Geralmente são estações mais novas que contam com novos equipamentos que fornecem essa possibilidade. Além disso, sua operadora precisa estar conectada à internet que é o caso da Telefonica. Uma dica : Antes de perguntar a sua operadora se seu prefixo telefonico tem ou não a opção de ADSL, sugiro fazer um levantamento de todos os prefixos que podem ser instalados no seu local e depois verificar com a operadora. Muitas pessoas ficam desesperadas porque ligam e recebem como resposta que o prefixo do telefone está habilitado. Por isso, facilite a sua vida e procure se informar antes conhecendo a telefonia da sua região.

Para ter-se uma idéia da vantagem desse serviço,nos Estados Unidos a tecnologia DSL é fornecida pelas operadoras nas seguintes modalidades :

Tipo	Taxa de Recepção (Downstream)	Taxa de envio (UpStream)
ADSL	de 1.5Mbps a 384Kbps	de 128kbps a 384kbps
HDSL (2 linhas)	1.5mbps	1.5mbps
SDSL (1 linha)	1.5mbps	1.5mbps
VDSL	de 13mbps a 52mbps	de 1.5mbps a 2.3mbps
IDSL ou ISDN	128kbps	128kbps
RADSL	384kbps	128kbps
UDSL	de 384kbps a 1mbps	de 128kbps a 384kbps

Note que não é em todas as regiões dos EUA que as modalidades acima estão disponíveis, porque isso também depende da estação local da sua linha telefônica.Lá, ao contrário do que muitos pensam, existem também dificuldades na parte de telecomunicações e dizemos isso por experiência própria.

Segundo o instalador da operadora que visitou nossa empresa,está ocorrendo uma média de 400 instalações de ADSL por dia, em São Paulo, taxa que poderia ser bem maior se a maioria não fosse utilizada para uso em casa por apenas um computador.

2.3 Conceitos de TCP/IP que você deve saber

Para muitos, essa parte pode parecer bastante repetitiva, mas foi incluída para facilitar o entendimento de iniciantes ao TCP/IP, notação de subnet, etc. TCP/IP é um conjunto de protocolos usados para a troca de informações em redes locais ou remotas incluindo a internet. Em uma rede TCP/IP cada equipamento possui um endereço único de 32 bits, muitas vezes, referido apenas como "IP". O endereço é composto de 4 octetos, cada octeto (ou byte) equivale a 8 bits. Ao contrário das pessoas, o computador não usa a base decimal e sim a binária. Portanto a notação 10 significa 2 em decimal. Uma maneira simples de entender isso é pensar que cada bit está sempre na base 2. Veja a notação binária 101, ou seja, o número 5. Sempre lendo (ao contrário) da direita para a esquerda : o primeiro bit seria o equivalente a 2 elevado a zero que é 1 se estiver setado ou 0 se não estiver setado. O segundo bit, 0, significa 2 elevado a 1 ou zero. Como não está setado, equivale a 0. O terceiro bit seria 2 elevado a 2 igual 4. Portanto 101 em binário equivale a $4+0+1 = 5$ em decimal.

Normalmente, a notação de endereçamento à internet se escreve em decimal, assim 191.1.0.23, por exemplo. O mesmo endereço em binário seria equivalente a 10111111.00000001.00000000.00010111. Vamos ver o

Artigo

primeiro octeto 191 ou $10111111 = 128+0+32+16+8+4+2+1 = 191$.

Tabela de valores de bits

posição	fórmula	valores possíveis
primeiro 00000001	2 elevado a zero	0 ou 1
segundo 00000010	2 elevado a um	0 ou 2
terceiro 00000100	2 elevado a dois	0 ou 4
quarto 00001000	2 elevado a três	0 ou 8
quinto 00010000	2 elevado a quatro	0 ou 16
sexto 00100000	2 elevado a cinco	0 ou 32
sétimo 01000000	2 elevado a seis	0 ou 64
oitavo 10000000	2 elevado a sete	0 ou 128

A fórmula seria 2^x onde x vai de 0 a 7. O número 5, por exemplo, seria representado pela soma do primeiro e terceiro bit setados.

Uma subnet é uma coleção de endereços de rede que podem comunicar-se diretamente entre si sem precisar de um roteador. A comunicação é direta entre todos os Hosts na mesma subnet. O que estamos demonstrando neste artigo é como construir um roteador Linux ou um gateway para conectar a sua rede à internet. A subnet mask é usada para dividir os 32 bits de um IP em duas partes: o endereço da rede e os endereços dos Hosts. A subnet mask simplesmente informa ao host qual a parte do IP referente à rede e qual é a parte do IP referente aos Hosts. Dessa forma o Host irá ou não recorrer ao seu roteador ou gateway.

Você verá que, quando estivermos usando ipchains para implementar o nosso firewall, haverá notações de rede do tipo 192.168.0.0/24 ou 192.168.1.0/26. Essa é a notação da rede mais a sua subnet mask escrita pela quantidade de bits setados.

Em TCP/IP, o último endereço de uma rede ou de uma sub-rede é seu broadcast, enquanto o primeiro endereço é o endereço de rede.

Sub-rede (subnet) é a forma que se criou para dividir uma rede. Assim, se você possui 1 rede de 62 hosts, deve utilizar uma máscara (subnet mask) de 26 bits.

Note que o endereçamento IP (IPV4) é constituído por 32 bits, portanto, quando se fala em subnet mask de 24 bits, seria o equivalente a indicar 11111111.11111111.11111111.00000000 ou 255.255.255.0 em decimal. Já uma subnet mask de 26 bits ou /26 seria equivalente a 11111111.11111111.11111111.1100000000, ou seja 255.255.255.192. Para tanto basta contar a quantidade de bits setados.

Vamos supor um rede 192.168.1.0 de máscara 26 bits. O primeiro endereço válido seria 192.168.1.1 e o último seria 192.168.1.62. Essa rede possui 62 endereços, mas o endereço (rede) 0 é reservado por ser o primeiro endereço, bem como o último endereço (BCast) 63 é reservado por ser o endereço de broadcast. Portanto, os endereços válidos vão de 192.168.1.1 a 192.168.1.62 e são esses os endereços que você usaria em seus hosts.

Para discriminar qual parte de um endereço é relativa a uma rede, foi criado o conceito de classes. Existem cinco formas de endereços ou classes.

Artigo

A classe A tem sua rede definida em seu primeiro octeto sendo os três restantes direcionados aos hosts. Por exemplo: 25.0.0.0 seria um exemplo de rede da classe A.

A classe B tem sua rede definida em seus dois primeiros octetos, por exemplo, 130.26.0.0.

A classe C tem sua rede definida em seus três primeiros octetos, por exemplo, 192.168.2.0. Essa é a classe de rede que você irá utilizar e também é a classe utilizada em serviços ADSL.

Existem ainda as classes D e E.

Na prática o que irá acontecer é que você irá utilizar redes de classe C, seja internamente como já deve estar usando ou através da sua operadora que lhe irá conferir um(1) endereço IP ao modem ADSL que irá pertencer a uma rede classe C.

No caso, ao instalar nosso ADSL, a operadora nos forneceu o "IP" do modem, sua subnet mask e o endereço do gateway (geralmente o primeiro IP de host válido de uma subnet). Ao instalar o seu firewall, você precisará conhecer qual é o IP do modem, qual o IP do gateway e qual é a subnet mask.

Vamos simular o que um provedor de ADSL faria. Primeiro, ele pegaria uma rede classe C e a dividiria em algumas sub-redes sendo que cada sub-rede teria um gateway. Supondo que a rede classe C que o provedor irá utilizar seja 192.168.0.0 e que ele irá dividi-la em 7 sub-redes, seria semelhante a :

	Rede	Broadcast	Subnetmask
Rede 1	192.168.0.0	192.168.0.63	255.255.255.192
Rede 2	192.168.0.64	192.168.0.95	255.255.255.224
Rede 3	192.168.0.96	192.168.0.127	255.255.255.224
Rede 4	192.168.0.128	192.168.0.159	255.255.255.224
Rede 5	192.168.0.160	192.168.0.191	255.255.255.224
Rede 6	192.168.0.192	192.168.0.223	255.255.255.224
Rede 7	192.168.0.224	192.168.0.255	255.255.255.224

Supondo que o IP do seu modem ADSL seja 192.168.0.5, então a rede e a subnet mask seriam 192.168.0.0/26, o gateway seria provavelmente 192.168.0.1 e o broadcast 192.168.0.63. Isso é que será necessário conhecer da rede da sua ADSL. Se o IP do seu modem ADSL fosse 192.168.0.67 nessa rede acima, provavelmente seu gateway seria 192.168.0.65, a rede e subnet seriam 192.168.0.64/27 e o broadcast seria 192.168.0.95.

O importante é conhecer os conceitos básicos de TCP/IP, subnet e classes de redes para que você possa implantar o seu firewall corretamente.

2.4 O que é Proxy

O termo servidor Proxy vem de uma palavra em inglês que significa procuração. Em termos técnicos, servidor de Proxy é um software que tem a "procuração" de um ou mais hosts para buscar na internet uma informação solicitada. No Linux o servidor Proxy mais conhecido, eficiente e gratuito é o Squid. Muitos integradores instalam um servidor Proxy e configuram os hosts clientes para acessar o Proxy. Esse artigo não pretende discutir apenas como instalar um servidor Proxy com ADSL para dar acesso de sua rede interna à internet, apesar de muitas empresas e integradores fazerem isso. O objetivo é ir além, proporcionando uma solução mais barata, bem mais completa e eficiente. O problema de se ter um servidor Proxy é ficar limitado aos protocolos que esse servidor suporta. Por exemplo: se um servidor Proxy só suporta os protocolos de http,

https e ftp e um usuário tenta logar num servidor remoto via SSH, ou tenta abrir uma sessão de ICQ ou ainda ver um vídeo, pode não conseguir se o servidor Proxy não suportar esses protocolos. O Proxy tem a vantagem de atuar como um grande cache. Se você abre a [home page do Linux](#), na segunda vez que acessá-la ou se outra pessoa na rede for acessá-la, tudo que já estiver armazenado no espaço em disco do Proxy será enviado ao seu browser sem que o Proxy tenha feito um novo download na internet, economizando tempo e dinheiro. Se instalar apenas um servidor com Proxy conectado via ADSL, sua rede estará limitada aos serviços suportados pelo Proxy. Essa solução seria inferior, em termos de performance, à proposta neste artigo. Além disso, alguns servidores comerciais Proxy funcionam muito mal com páginas dinâmicas tipo ASP, PHP, etc. Portanto, cuidado! É claro que poderá unir as duas coisas : montar seu firewall no Linux e ainda disponibilizar um servidor Proxy Squid para "economizar" e agilizar o acesso para alguns serviços que o squid suporta. Se você não possui um serviço de ADSL na sua região, pode montar esse nosso firewall com uma linha discada e também instalar o Squid para agilizar o processo, já que a sua banda será bastante limitada com um modem convencional.

2.5 O que é NAT

NAT : Network Address Translation ou tradução de endereço de rede é o processo de tradução de endereços muito encontrado em roteadores. Existem implementações em Windows, Linux e Solaris de servidores NAT. O NAT é muito semelhante, em termos operacionais ao IP Masquerading. Sua única limitação do NAT é requerer um subnet. Com IP Masquerading pode-se utilizar apenas 1 IP válido seja ele dinâmico ou fixo.

2.6 O que é IP Masquerading

IP Masquerading é uma forma de tradução de endereços como o NAT. Isso significa que o IP Masquerading permite que uma rede ou um host com IP não válido se comunique com a internet através de um servidor Linux que "traduz" ou mascara o IP inválido com o IP válido do servidor.

2.7 O que é IP Forwarding ou Ipfwadm

Ipfwadm é o antecessor do ipchains implementado antes do kernel 2.2.x e baseado na implementação da BSD. A solução que estamos propondo utiliza o ipchains que é mais moderno, rápido, seguro e eficiente.

2.8 O que é IPCHAINS

Como Ip forwarding, IPChains é uma ferramenta para filtragem de pacotes. Na internet ou TCP/IP, toda a comunicação é baseada em troca de pacotes. Por exemplo: se você faz um download de um arquivo de 100Kbytes, irá receber mais de 68 pacotes de 1460 bytes cada. O header (ou cabeçalho) de um pacote contém as informações que identificam para onde o pacote vai, o endereço do remetente e o tipo do pacote. O corpo do pacote (body) é onde ficam os dados transportados. O protocolo TCP (que é usado para web, e-mail, logins remotos, etc.) usa o conceito de conexão antes de enviar qualquer pacote. Os pacotes iniciais de uma comunicação TCP enviam uma requisição de comunicação e uma confirmação caso a mesma seja estabelecida. O IPChains é um filtro de pacotes atuando como juiz. IPChains decide, baseado no header do pacote, se ele será negado (deny), aceito (accept) ou rejeitado (reject) nesse caso avisando o outro lado que houve rejeição. No Linux o processo de filtrar pacotes é incluso no Kernel. IPChains é um ferramenta que permite construir um firewall para decidir o que fazer com os pacotes que são transmitidos e recebidos trabalhando em conjunto com o Kernel. IPChains é um pacote que pode ser obtido gratuitamente, via internet, ou já deve estar incluso na sua distribuição Linux. Se o seu Linux é baseado em RPM, como o Red Hat, Conectiva, Timpanogas, Mandrake ,etc, digite o comando "rpm -ql ipchains" para verificar se o pacote IpChains foi instalado. Se o seu IPChains já está instalado, verifique a sua versão digitando o comando "/sbin/ipchains --version". O ideal é utilizar a versão 1.39 ou uma superior a ela.

2.9 Funcionamento do IPChains

A maneira mais fácil de entender esse funcionamento é colocar alguns exemplos e explicá-los. Além disso, providenciamos um guia de referência rápida, por meio da tabela 2.1, exposta a seguir.

Exemplo :

```
/sbin/ipchains -A forward -j MASQ -i eth0 -s 192.168.0.0/24 -d 0.0.0.0
```

Explicações :

-A forward = adiciona regra de encaminhamento;

-j MASQ = política de mascarar o IP com o IP do servidor;

-i eth0 = pela interface eth0;

-s 192.168.0.0/24 = que tenha origem na rede 192.168.0.0 de subnet 255.255.255.0;

-d 0.0.0.0 = destino a internet.

O que essa regra faz é mascarar todos os pacotes provenientes da rede 192.168.0.0 com o IP da eth0 encaminhando-os à internet.

Exemplo 2 :

```
/sbin/ipchains -A input -s 0.0.0.0/32 0:7000 -j DENY
```

Explicações :

O que o exemplo 2 faz é negar toda a entrada de pacotes originários da internet nas portas 0 a 7000.

-A input = adiciona regra de entrada

-s 0.0.0.0/32 origem (source) = determina a origem, nesse caso a internet com subnet 255.255.255.255 ou /32 (32 bits).

0:7000 = especifica todas as portas entre 0 e 7000

-j DENY = política de DENY, ou seja negar.

Exemplo 3 :

```
/sbin/ipchains -A input -s 0.0.0.0/32 80 -p TCP -i eth1 -j ACCEPT -l
```

Explicações :

Esse exemplo é mais completo por especificar a interface eth1 e o protocolo TCP. Nesse caso conexões provenientes da internet na porta 80, protocolo TCP para interface eth1 são aceitas. Além disso serão logadas através do parâmetro -l.

-A input = adiciona regra de entrada

-s 0.0.0.0/32 origem (source) = determina a origem, nessa caso a internet com subnet 255.255.255.255 ou /32 (32 bits).

80 = especifica porta 80, ou seja a porta que geralmente utiliza-se http.

-p TCP = apenas para o protocolo TCP.

-i eth1 = na interface especificada eth1.

-j ACCEPT = política de aceitação.

-l = logar atividade.

Exemplo 4 :

```
/sbin/ipchains -A output -d 0.0.0.0/32 4444 -j DENY -l
```

Explicações :

Esse exemplo bloqueia toda a saída da sua rede para a internet que esteja usando a porta 4444.

-A output = adiciona regra de saída.

-d 0.0.0.0/32 = destino internet.

4444 = porta 4444.

-j DENY = política de DENY (negar).

-l = logar atividade.

O exemplo 4 é útil para quando não se quer que os funcionários utilizem serviços como Napster, ICQ, jogos ou outros tipos de jogos. É importante conhecer a porta do serviço e também conhecer seu protocolo.

Veja mais exemplos e seu comentários no script rc.firewall.

Tabela 2.1 IP Chains Referencia Rapida

Built-in Chains

ipchains fornece 3 built-in-chains. Todos os pacotes começam com uma dessas chains e, dependendo das regras, pode terminar passando por todas as 3.

input Pacotes chegando através de um network device na sua máquina de uma origem externa. Pacotes gerados localmente vêm sempre do loopback device ou "lo".

forward Pacotes que apenas estão passando pela sua máquina ou redirecionados. Se tanto o destino quanto a origem do pacote são remotos o pacote é

enviado para o forwarding firewall.

output Pacotes deixando a sua máquina sob um network device para uma origem externa. Ou, se enviado para o loopback device, o pacote reaparece na chain de input.

Criando e destruindo chains

Chain (ou corrente em português) especifica o nome da chain. Pode ter até 8 letras de comprimento e, para prevenir conflitos com possíveis built-in target names futuros, deve conter pelo menos 1 letra minúscula.

-N Chain Cria uma nova chain definida pelo usuário.

-X [chain] Deleta uma chain vazia definida pelo usuário, ou todas as chains definidas pelo usuário. Todas as regras referentes a

uma chain definida pelo usuário deve ser deletada antes da chain definida pelo usuário.

Adicionando ou removendo regras

-v (verbose): Quando usado com o seguinte grupo de comandos, irá fazer com que a regra seja ecoada para o stdout.

[Regra], como especificada na linha de comando, consiste em nenhum ou mais predicados seguidos por nenhuma ou mais ações. Predicados e ações estão listados a seguir.

[Índice] é usado para especificar uma regra de acordo com a sua posição na chain. A primeira regra numa chain tem o índice 1.

-A [-v] [Regra] Adiciona uma regra a chain

-D [-v] [Índice] Deleta uma regra na chain pela posição [Índice].

-D [-v] [Regra] Deleta primeira regra na chain que contenha a [Regra].

-F [chain] Descarta todas as regras da chain (ou todas as chains). Equivalente a deletar todas as regras uma a uma.

-I [-v] [Índice Regra] Insere [Regra] na chain precedendo a regra de índice [Índice]. Portanto, se o índice é 1, a regra inserida fica sendo a primeira regra na chain.

-R [-v] [Índice regra] Substitui (replace) a regra no índice [Índice] na chain com a regra [Regra].

Targets (Alvos)

Cada regra tem um alvo que determina o que fazer com um pacote quando enquadrado. Se um pacote chega ao final de uma chain sem se enquadrar em nenhuma das regras, a política de target padrão (default) da chain é usada. Essas são as políticas.

ACCEPT Permite que o pacote passe através do firewall

REJECT Rejeita o pacote. Se não for um pacote ICMP, envia um reply ICMP Host Unreachable para o remetente.

DENY não aceitar o pacote, não responder (reply). Simplesmente ignora o remetente.

MASQ (para chain forward apenas). Deixa o pacote passar, porém mascara ele. Substitui o remetente do pacote pelo endereço local e substitui a porta de origem no cabeçalho com o número temporário gerado localmente.

REDIRECT (para chain input apenas. Envia o pacote a um soquete local ou processa. Pode ser usado com pacotes TCP e UDP em chains de input ou chains definidas pelo usuário.

RETURN Equivalente a ignorar as demais chains, podendo chamar uma política de target built-in ou retornar a uma chain do usuário. Seria o equivalente ao return dentro de uma função em C.

(no target especificed) O byte da regra e o contador do pacote serão incrementados, porém o pacote será passado para a próxima regra na chain mesmo se for enquadrado nessa regra. Normalmente utilizado para contabilidade.

Se um target for usado incorretamente (MASQ de uma input chain por exemplo), o pacote será descartado e uma mensagem será enviada ao log do sistema, syslog.

Comandos de Masquerading

-M L [-v] Lista as conexões de masquerading correntes.
 -v ira fazer com que as informações reelecionadas aos números da sequencia delta sejam descartadas também.

-M -S tcp Configura os valores de timeout de masquerading.
tcpfin udp Os parametros especificam o timeout em segundos para sessoes TCP (tcp), sessoes apos recepcão do pacote FIN (tcpfin), e pacotes UDP respectivamente. Um timeout de 0 ira manter os timeouts anteriores. Os Defaults são 15,2 e 5 minutos.

Informação

-h Imprime um sumário dos comandos

-h icmp Lista nomes ICMP conhecidos a ipchains

--version Informa a versão do ipchains.

Utilitários Chain

-P chain Troca a política de uma chain built-in para [target].
target [target] precisa ser ACCEPT, DENY, REJECT ou MASQ para chains forward. Nenhum outro tipo de target pode ser usado como política built-in de uma chain.

-Z [-L] Zerar o byte do pacote e os contadores na chain (ou todas as chains). -Z pode ser usado em combinação com -L para leitura de contadores e depois apaga-los, assegurando que nenhum pacote não prosseguirá como não contabilizado. No entanto, ao fazer isso, você deve zerar todas as suas chains. você não pode zerar automaticamente e listar uma unica chain.

-L [-vxn] Lista as regras numa chain (ou todas as chains).
[chain] -v especifica modo verbose, -x expande os números (mostra valores sem as abreviações K, M, e G),
 -n faz o ipchains imprimir IPs numericos ao inves de fazer lookups de nomes. Pode ser usado com -Z acima.

-C [-v] Testa um pacote numa chain. pkt e formado como se fosse chain pkt uma regra exceto pelo fato de conter pelo menos -s, -d, -p (precisa ter um protocolo especificado, não pode ser generico), e a flag -i (ao menos que -f seja usado para criar um fragmento). -v faz com que um trace do caminho do pacote seja impresso no stdout.

Ações

-j target Pula para (jump-to), especifica o target a ser chamado
[port] quando a regra combinar. Target pode ser uma das listas acima, ou o nome de uma chain definida pelo usuário.

você não pode pular para uma chain built-in.
para facilitar pense assim -j [política] ou
-j [target].

- l Faz com que os pacotes que combinarem com a regra sejam logados no syslog. Muito cuidado com isso porque pode fazer seu arquivo de log crescer além da capacidade do seu disco.
- m [valor] número a marcar no pacote. Usado em conjunto com a implementação do Serviço de Qualidade nos kernels 2.1. Se [valor] começar com + ou -, então o valor será somado ou subtraído do valor marcado no pacote, e não substituindo-o.
- o [tam maximo] Copia o pacote para o device do espaço do usuário. [tam maximo] limita o números de bytes a serem copiados.
- t and xor Muda o bit do tipo de serviço do pacote (TOS – Type Of Service). O TOS do pacote será ANDed com and e depois XORed com xor. Os dois parametros são valores de 8-bits hexadecimais. A RFC1349 especifica que o LSB do campo TOS não pode ser alterado, portanto ipchains irá recusar qualquer regras que violem isso. A RFC1349 também especifica que apenas 1 bit no campo TOS pode ser alterado por vez. Regras que alterarem mais de 1 bit por vez serão aceitas mas um aviso será enviado para o stdout.

Predicados

- p [!] Especifica um protocolo. Pode ser um nome do protocolo como protocolo TCP, UDP, ICMP ou ALL (para todos) (não importa letras maiúsculas ou minúsculas), ou o número IP do protocolo sendo 0 para todos. Exemplo, 22 ou ssh podem ser usados para ssh. A lista dos protocolos podem ser encontradas no arquivo /etc/services. O símbolo [!] significa NOT. Ou seja ! ssh. Para, não a SSH.
 - s [!] end O endereço de origem a ser combinado ou [!] para NOT esse endereço. -s significa SOURCE (origem). Onde [end] e o endereço ip (address). Por exemplo 192.168.0.10.
 - d [!] end O endereço de destino a ser combinado ou [!] para NOT esse endereço. -d significa DESTINATION (destino). Onde [end] e o endereço ip (address). Por exemplo 192.168.0.10.
- Obs. Tanto o endereço -s quanto -d podem ser especificados pelo nome (por exemplo, localhost, www.conectiva.com.br) ou o IP, por exemplo 192.168.0.10. Para um endereço IP, você pode significar o quanto da rede ou endereço e significativa especificando a netmask.
- Por exemplo :
- As duas notações são válidas :
- 192.168.0.10/255.255.255.0 ou
192.168.0.10/24 (sendo 24 equivale a uma subnet de 24 bits, ou seja 255.255.255.0). Nessa caso estamos falando de todos os endereços entre 192.168.0.0 até 192.168.0.255. Ou seja, a subnet inteira.
- [[!] porta] Quando usado com protocolos TCP ou UDP, por exemplo :
-p tcp ou -p udp, uma porta ou intervalo de portas podem ser especificados. Simplesmente especifique o número da porta ou o nome. Por exemplo 80 ou www. Um intervalo pode ser determinado usando um : entre a porta menor e a porta maior. Exemplo 0:65535.
 - [[!] -y Quando utilizado com o protocolo TCP, especifica pacotes SYN do TCP apanes. Irá combinar com pacotes TCP requisitando uma conexão TCP.
 - [[!] -f Combina o segundo até o último fragmento de um pacote fragmentado. Nenhuma porta pode ser especificada quando o flag -f é utilizado.

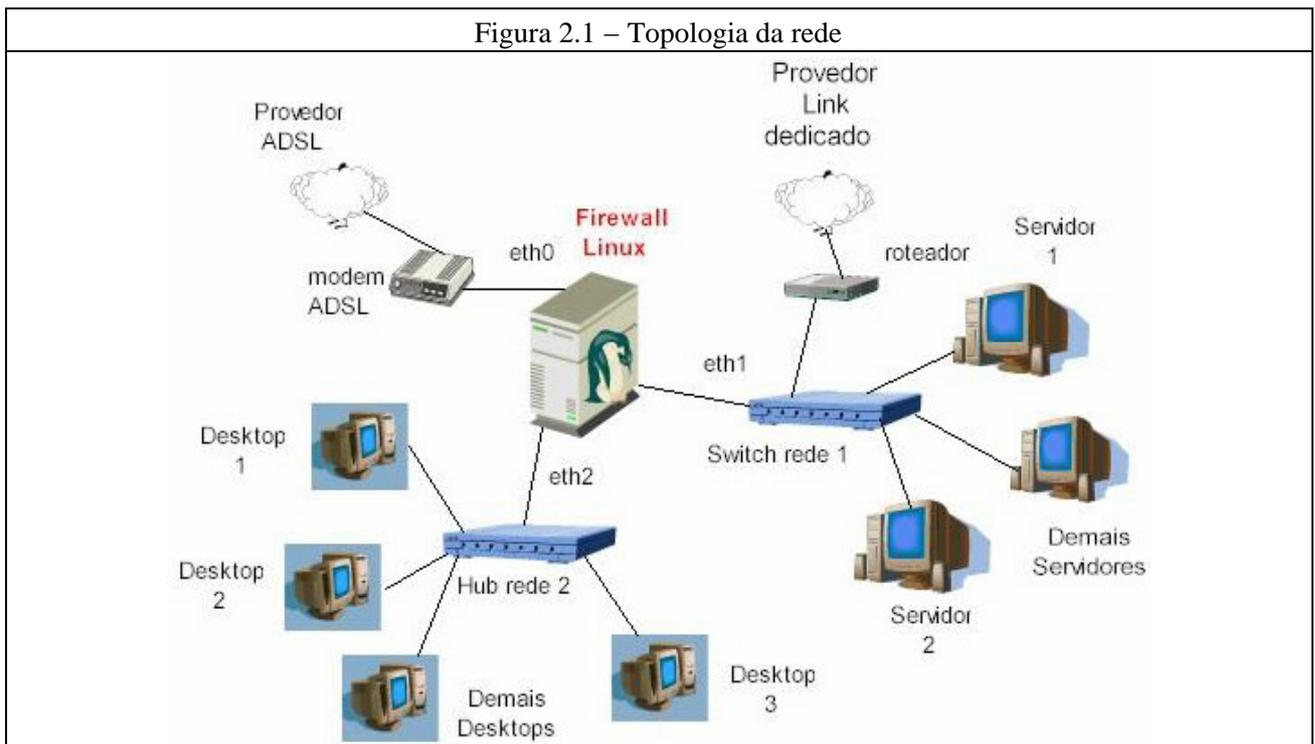
-i [!] nome Especifica a interface de rede pelo nome (de acordo com o nome listado no comando ifconfig). A interface de input e' a interface por onde entram os pacotes, a interface de forward e output sao as interfaces por onde os pacotes saem. Um nome de interface terminado com + ira combinar com todas as interfaces daquele tipo. Por exemplo eth+ para : eth0, eth1, eth2 etc. ppp+ para ppp0, ppp1, etc. Pode-se especificar um interface que não existe no seu sistema ou não esta ativa, por exemplo ppp1. Nenhum pacote ira combinar com a regra ate que a interface ppp1 esteja ativa.

-b Bidirecional, is vai fazer com que a regra funcione não importa qual seja a direcao do pacote. E equivalente a repetir a regra invertendo o endereço de origem (-s) e destino (-d). Na verdade, seria como inserir duas regras em 1 so. Talvez, para não confundir seja melhor declarar as duas regras a declarar apenas 1.

obs. A exclamacao ! significa NOT. Por exemplo "! -s 162.168.0.11" ira combinar com qualquer pacote menos 1 originado em 162.168.0.11. A mesma regra pode ser usada para portas, protocolo, interface e demais predicados acima com essa opcao discriminada.

2.10 Esquema da rede

A figura 2.1 ilustra um modelo da rede de acordo com a solução deste artigo. O firewall Linux possui 3 interfaces : a eth0 está ligada diretamente ao modem ADSL, a eth1 está conectada ao switch da rede 1 que possui os servidores e está conectada ao link dedicado; na rede 2 estão os desktops e workstations.



2.11 Gateways

O Firewall Linux está conectado à internet via modem ADSL. Para a rede 2, o IP da eth2 do Linux é o gateway dessa rede. No caso da rede 1, há dois gateways : o default é o roteador e o segundo é o Firewall Linux. Para o Firewall Linux, o gateway é o primeiro endereço válido da subnet do ADSL fornecido pela

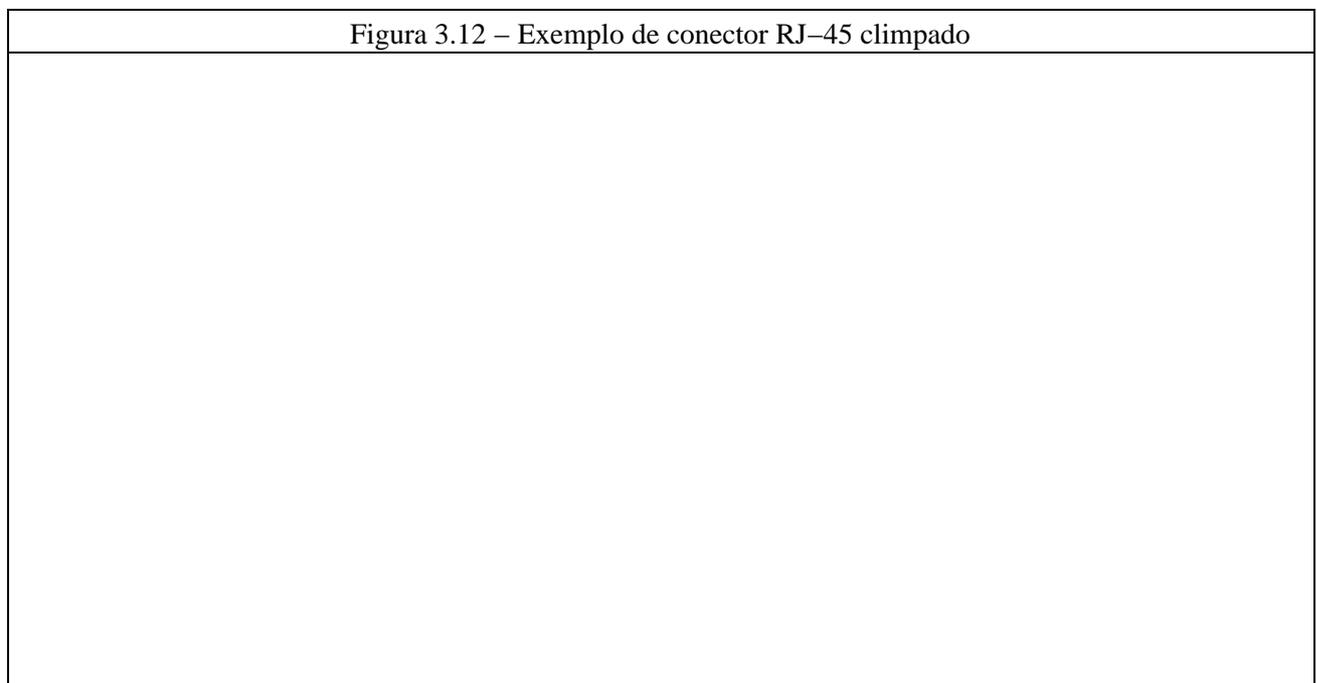
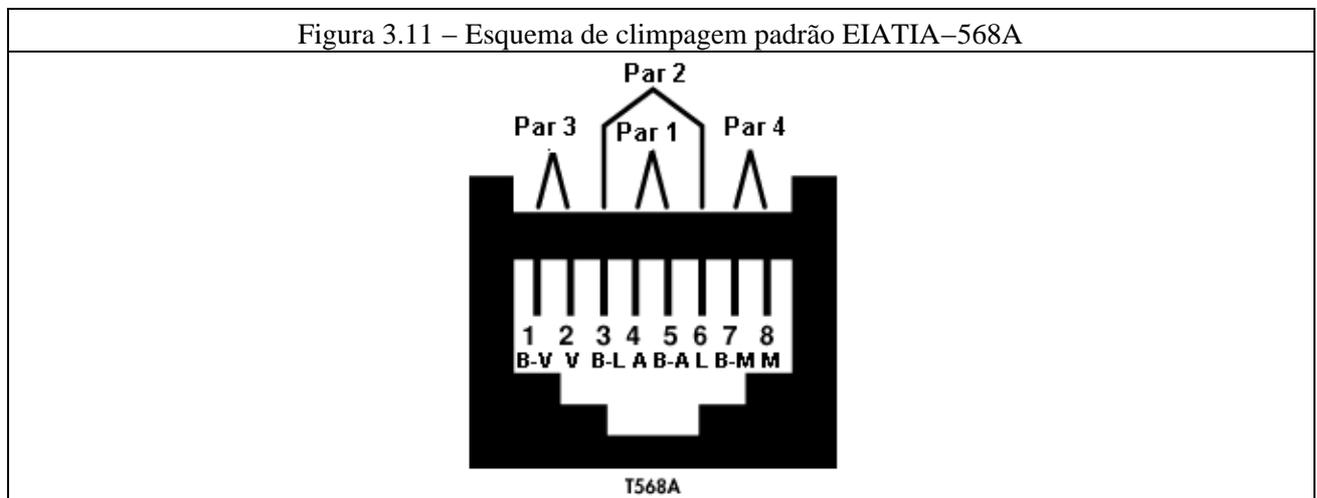
operadora.

3.0 Instalação do hardware

3.1 Instalação do Modem ADSL

Nesta secção iremos explicar como foi efetuada a instalação da máquina Linux e do ADSL.

O modem ADSL, um SpeedStream 5600 da Efficient Networks, vem acompanhado de 2 cabos par trançado e uma fonte de energia externa. O manual não nos foi fornecido, mas o obtivemos na internet. O cabo que liga o SpeedStream 5660 direto na interface eth0 do Firewall Linux deve ser paralelo, ou seja, os dois conectores RJ-45 devem ser climpados na mesma seqüência. Se você pretende ligar o seu ADSL direto num Hub ou switch, terá de usar um cabo cross. O esquema de climpagem do cabo par trançado está ilustrado na figura 3.11. O ideal é utilizar cabo categoria 5. No nosso caso foi utilizado o da Lucent Technologies (uma divisão da AT&T) e confeccionados mais dois cabos adicionais para conecta-los ao Hub da rede 2 e ao switch da rede 1.



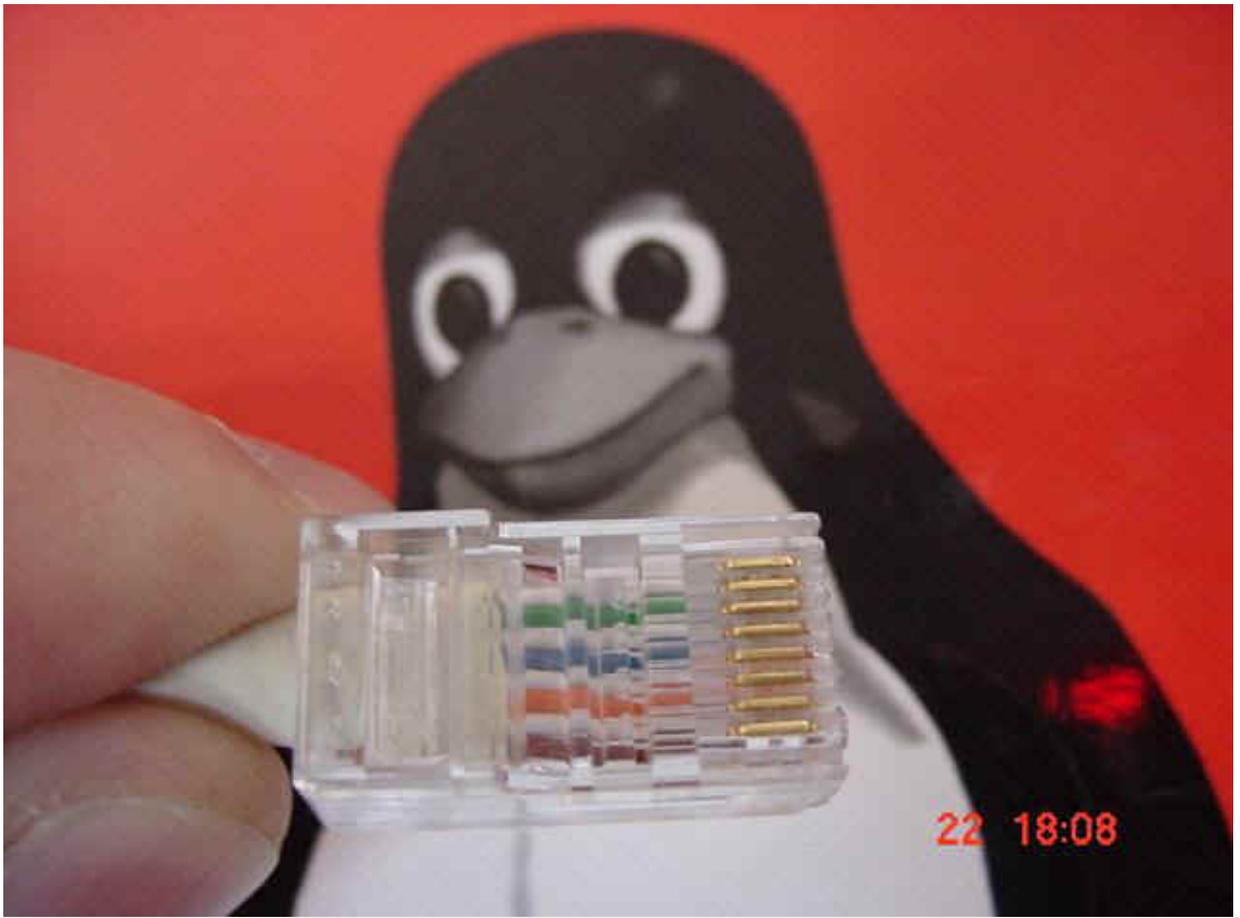


Figura 3.13 – Ferramentas para climpar



A operadora (Telefonica) instalou uma pequena caixa DSL (Figura 3.14) com 3 saídas RJ-11, 2 para voz (Voice 1 e Voice 2) e outra para dados (data) que será ligada direto na entrada RJ-11 do modem ADSL. Há também uma entrada para a linha (line). A linha telefônica convertida para ADSL deve ser conectada nessa caixa DSL no conector de entrada line.

Figura 3.14 – Caixa DSL



Figura 3.15 – Modem ADSL



No modem, ligados o cabo telefonico (RJ-11) conectado na entrada da linha cuja ponta está conectada na saída (data) da caixa DSL. Conectamos o par trançado RJ-45 na entrada e-net e a outra ponta na eth0 do Firewall Linux.

3.2 Máquina para Firewall Linux

O hardware necessário para se montar um Linux Firewall não é muito difícil de conseguir e nem é necessário adquirir algo caro para isso.

A máquina que utilizamos foi um Pentium 133MHz com 64mb de RAM, 1.2Gb de disco, um interface de vídeo Diamond 4Mb e 3 NICs com chipset RTL8139C de 10/100Mbps custando estes últimos R\$ 35,00 cada.

É possível fazer o mesmo com um 486, 16Mb de RAM (aconselhamos 32mb) e um HD de pouca capacidade. A distribuição do Linux utilizada é a Red Hat, mas pode-se utilizar Conectiva, Mandrake, Timpanogas, SuSe, Slackware, etc.

Figura 3.21 – Pentium 133MHz com 3NICs, 1.2Gb de disco e 64MB RAM

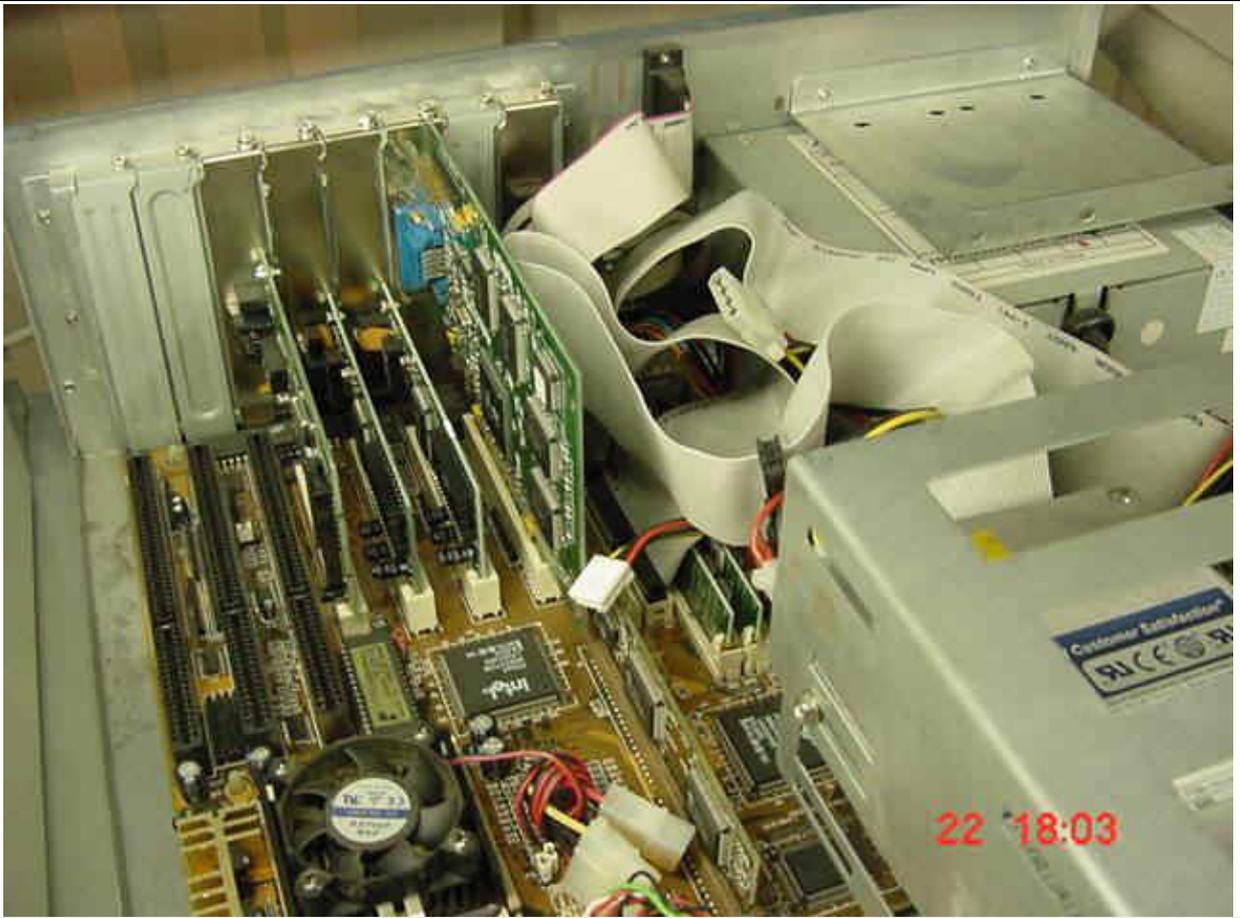


Figura 3.22 –Vista traseira



Figura 3.23 – Em operação com o script de Firewall carregado



4.0 Configuração do Firewall Linux

Esta seção descreve como configurar a parte de rede, montar o script e criar os scripts de inicialização do Firewall. Por uma questão de ilustração, iremos adotar IPs reservados para descrever os endereços referentes ao ADSL que naturalmente não são esses.

4.1 redes, subnets, gateways e IPs

A rede e subnet ADSL será 192.168.0/26; o IP na eth0 é 192.168.0.13 e o default gateway 192.168.0.1. A rede interna 1 e subnet será 192.168.1.0/24 onde 192.168.1.1 é o IP na eth1. A rede interna 2 e a subnet serão 192.168.2.0/24 onde 192.168.2.20 é o IP na eth2. Para os hosts da rede interna 1 o IP da eth1 será o gateway; para os hosts da rede interna 2 o IP da eth2 será um dos gateways.

4.2 Configurando eth0, eth1, eth2, default gateway e DNS.

Pode-se utilizar o Linuxconf para configurar suas NICs ou fazê-lo manualmente editando os arquivos `ifcfg-eth*` no diretório `/etc/sysconfig/network-scripts/` e o arquivo `/etc/sysconfig/network`.

É necessário informar os endereços dos servidores DNS de seu provedor para poder resolver o endereço de sites como www.pecas-on-line.com.br. Para configurar os servidores DNS, edite o arquivo `/etc/resolv.conf` e informe o IP do master e secondary DNS servers fornecidos pelo seu provedor.

tabela 4.1 – configuração das NICs, gateway e endereços dos servidores DNS

```
arquivo /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE="eth0"
IPADDR="192.168.0.13"
NETMASK="255.255.255.192"
ONBOOT="yes"
BOOTPROTO="none"
IPXNETNUM_802_2=""
IPXPRIMARY_802_2="no"
IPXACTIVE_802_2="no"
IPXNETNUM_802_3=""
IPXPRIMARY_802_3="no"
IPXACTIVE_802_3="no"
IPXNETNUM_ETHERII=""
IPXPRIMARY_ETHERII="no"
IPXACTIVE_ETHERII="no"
IPXNETNUM_SNAP=""
IPXPRIMARY_SNAP="no"
IPXACTIVE_SNAP="no"
```

```
arquivo /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
DEVICE="eth1"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
ONBOOT="yes"
BOOTPROTO="none"
IPXNETNUM_802_2=""
IPXPRIMARY_802_2="no"
IPXACTIVE_802_2="no"
IPXNETNUM_802_3=""
IPXPRIMARY_802_3="no"
IPXACTIVE_802_3="no"
IPXNETNUM_ETHERII=""
IPXPRIMARY_ETHERII="no"
IPXACTIVE_ETHERII="no"
IPXNETNUM_SNAP=""
IPXPRIMARY_SNAP="no"
IPXACTIVE_SNAP="no"
```

```
arquivo /etc/sysconfig/network-scripts/ifcfg-eth2
```

```
DEVICE="eth2"
IPADDR="192.168.2.20"
NETMASK="255.255.255.0"
ONBOOT="yes"
BOOTPROTO="none"
IPXNETNUM_802_2=""
IPXPRIMARY_802_2="no"
IPXACTIVE_802_2="no"
IPXNETNUM_802_3=""
IPXPRIMARY_802_3="no"
IPXACTIVE_802_3="no"
IPXNETNUM_ETHERII=""
IPXPRIMARY_ETHERII="no"
IPXACTIVE_ETHERII="no"
IPXNETNUM_SNAP=""
IPXPRIMARY_SNAP="no"
```

```

IPXACTIVE_SNAP="no"

arquivo /etc/sysconfig/network

NETWORKING=yes
HOSTNAME="speedy"
GATEWAY="192.168.0.1"
GATEWAYDEV="eth0"
FORWARD_IPV4="yes"

arquivo /etc/resolv.conf

nameserver 200.246.248.1
nameserver 200.246.248.10

```

Após editar os arquivos, reinicialize a rede com o comando `"/etc/rc.d/init.d/network restart"`.

Teste a sua rede "pingando" os outros endereços pelo firewall. Por exemplo, "ping" o endereço do gateway do ADSL para verificar que a rede do ADSL está OK. Ping um endereço ativo da rede interna 1 para ver se a eth1 está funcionando devidamente e faça o mesmo para a rede 2.

```

ping -c 15 192.168.0.1 (testa a rede ADSL)
ping -c 15 192.168.1.2 (testa a rede interna 1)
ping -c 15 192.168.2.11 (testa a rede interna 2)

```

Rode o ifconfig (tabela 4.2) para verificar se a sua rede está ok.

tabela 4.2 – resultado do ifconfig
<pre> eth0 Link encap:Ethernet HWaddr 00:E0:7D:92:72:AF inet addr:192.168.0.13 Bcast:192.168.0.63 Mask:255.255.255.192 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:38678 errors:0 dropped:0 overruns:0 frame:0 TX packets:32489 errors:0 dropped:0 overruns:0 carrier:0 collisions:1 txqueuelen:100 Interrupt:11 Base address:0x6200 eth1 Link encap:Ethernet HWaddr 00:E0:7D:92:72:EE inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:48198 errors:0 dropped:0 overruns:0 frame:0 TX packets:46249 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 Interrupt:10 Base address:0x6300 eth2 Link encap:Ethernet HWaddr 00:C0:DF:07:DD:7B inet addr:192.168.2.20 Bcast:192.168.2.63 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:96398 errors:0 dropped:0 overruns:0 frame:0 TX packets:64799 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 Interrupt:9 Base address:0x6400 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:3924 Metric:1 RX packets:14 errors:0 dropped:0 overruns:0 frame:0 </pre>

```
TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
```

5.0 Script de firewall

Este é o script de firewall (tabela 5.1). Observe os comentários para adequá-los a sua rede e estude as regras de firewall para aprender mais sobre ipchains.

tabela 5.1 – script de firewall /etc/rc.d/rc.firewall

```
#!/bin/sh

# -----
# VERSAO="1.02"
# ULTALT="Janeiro 2001"
# IPCHAINS FIREWALL por Carlos Fernando Scheidecker Antunes
# e-mail nando@antunes.eti.br
#
# Esse firewall possibilita conectividade das suas redes internas 1 e 2 para
# a internet e vice versa com varias medidas de seguranca.
# Alem disso, permite a conectividade entre as duas redes internas.
# Esse script de Firewall e derivado do firewall que construi para rodar
# na empresa usando um ip fixo via ADSL de 256kbps. Esse firewall foi
# montado num servidor Linux usando IPCHAINS com 3 NICs, eth0 conectado
# ao modem ADSL, eth1 conectado a rede interna 1 e eth2 conectado a rede
# interna 2.
#
# Pode ser usado com IP variaveis (fornecidos por DHCP) no caso de
# cable modem ou ip discado normal ao seu provedor.Tudo esta devidamente
# documentado para facilitar de acordo com o seu tipo de acesso.
#
# Esse script e o resultado de pesquisas na internet e estudo de publicacoes
# sobre o assunto.
#
# Condicoes de uso :
#
#     Nao me responsabilizo ou dou qualquer garantia com
#     relacao ao uso desse script.A responsabilidade de
#     uso do script e TOTAL do usuario sendo que nao irei
#     me responsabilizar por nenhum dano direto ou
#     indireto. Use-o sob sua responsabilidade.
#     Esse script e fornecido gratuitamente e nao me
#     obriga a fornecer qualquer tipo de assistencia ou
#     suporte.Fique a vontade para enviar seus comentarios
#     ou agradecimentos por e-mail.
#
# A configuracao abaixo e voltada para uso com DSL com caracteristicas :
#
# a) A interface externa, conectada ao DSL e a " eth0"
# b) O endereco IP externo e fixo, IP da eth0
# c) A rede interna 1 e acessivel via "eth1"
# d) A rede interna 2 e acessivel via "eth2"
# e) Os enderecos das redes internas estao dentro dos limites
#     de rede privada segundo a RFC1918.
#     Rede interna 1 : 192.168.1.0/24
#     Rede interna 2 : 192.168.2.0/24
# f) Por uma questao de protecao, estaremos usando
#     endereco da rede externa como sendo 192.168.0.0/26 (reservado)
#     Altere o endereco de acordo com os IPs validos fornecidos pelo
#     seu provedor.
#
# Recomendacoes :
# - Utilizar Kernel maior ou igual a 2.2.16. Versoes anteriores
#   possuem bugs de seguranca que podem comprometer seu sistema.
#   Para saber qual e a sua versao utilize o comando "uname -r".
# -----
# Para utilizar ou modificar o script para adequar ao seu uso voce
# precisa, basicamente, alterar as seguintes variaveis :
# EXTIF = Interface externa, eth0 no meu caso mas pode ser ppp0 no seu.
# EXTIP = IP da interface externa, caso seja fixo. Para ip variavel veja
```

```

#      comentarios abaixo.
#      EXTBROAD = Endereco de BroadCast da rede externa, pode ser obtido rodando
#      ifconfig. O endereco de BroadCast e o ultimo endereco IP de
#      uma subnet.Especificar esse endereco apenas se seu ip for
#      fixo.
#      EXTGW    = Endereco do gateway da rede externa. Deve ser obtido com
#      seu provedor ou via script abaixo.
# Rede Interna 1
#      INTIF    = Interface interna 1, eth1 no meu caso
#      INTIP    = IP da interface interna 1
#      INTLAN   = Endereco da rede interna 1 com subnet mask
# Rede Interna 2
#      INTIF2   = Interface interna 2, eth2 no meu caso
#      INTIP2   = IP da interface interna 2
#      INTLAN2  = Endereco da rede interna 2 com subnet mask
#-----
#*****
# Inicializando
#*****
echo -e "\n\nCarregando IPCHAINS Firewall $VERSAO de $ULTALT"
echo "-----"

#-----
# Declaracao de variaveis
#-----

# Interface e enderco de loopback
#
LOOPBACKIF="lo"
LOOPBACKIP="127.0.0.1"

# Interface Externa.
#
# Para usuarios de PPP a interface externa deve ser algo como ppp0.
# Para usuarios com mais de um modem, ou interface ppp veja codigo
# abaixo. O firewall deve ser executado depois do script
# /etc/ppp/ip-up.
#
#if [ "x$1" != "x" ]; then
#   EXTIF=$1
#else
#   EXTIF="ipp0"
#fi
#
# Interface Externa
EXTIF="eth0"

# Verificar se a interface externa esta habilitada :
if ! /sbin/ifconfig | grep $EXTIF > /dev/null; then
  echo -e "\n\nInterface Externa nao esta habilitada.Abortando."
  exit 1;
fi
echo Interface Externa: $EXTIF

# IP da interface externa :
#   A maioria dos acessos discados ppp atribui enderecos dinamicos
#   ao modem.
# Para usuarios de cable modem :
#   No caso de cable modems, alguns provedores utilizam DHCP e
#   alteram seu endereco de IP pelo menos uma vez ao dia. Nesse
#   caso, crie um script para parar e reinicializar o seu firewall
#   e programe-o atraves do crond.
# No caso de IPs dinamicos e necessario colocar uma regra no firewall
# para entender/obter o novo endereco IP toda vez que um novo IP for
# fornecido pelo provedor. Especialmente util para usuarios de cable modem.
# Utilize o DHCPd editando o arquivo ifup em /sbin. Veja man pages.
#
# Script para obter o endereco da interface externa em caso de ip dinamico :
#
# EXTIP=`ifconfig $EXTIF | awk '/inet addr/ { gsub(".*:", "", $2) ; print $2 }'`
#
#if [ "$EXTIP" = '' ]; then

```

```

# echo "Abortando.Nao foi possivel determinar o IP da $EXTIF .Problema de DHCP ou PPP?"
# exit 1
#fi
# Rede Externa
EXTIP="192.168.0.13"
echo IP Externo: $EXTIP

# Funcao para obter o Endereco do broadcast da rede externa
# "apenas para IPs dinamicos"
#
#EXTBROAD=`ifconfig $EXTIF | awk '/inet addr/ { gsub(".*:", "", $3) ; print $3 }`
#
# Rede Externa
EXTBROAD="192.168.0.63"
echo BroadCast Externo: $EXTBROAD

# Funcao para obter Gateway da rede Externa
#
#EXTGW=`/sbin/route -n | grep -A 4 UG | awk '{ print $2}`
# Rede Externa
EXTGW="192.168.0.1"
echo Default GW: $EXTGW

echo " --- "

# Interface Interna 1.
INTIF="eth1"
echo Interface Interna 1: $INTIF

# IP da interface interna 1
INTIP="192.168.1.1"
echo IP Interno 1: $INTIP

# IP e subnet mask da rede interna 1
INTLAN="192.168.1.0/24"
echo Rede Interna 1: $INTLAN

echo " --- "

# Interface Interna 2.
INTIF2="eth2"
echo Interface Interna 2: $INTIF2

# IP da interface interna 2
INTIP2="192.168.2.20"
echo IP Interno 2: $INTIP2

# IP e subnet mask da rede interna 2
INTLAN2="192.168.2.0/24"
echo Rede Interna 2: $INTLAN2

echo " --- "

# IP e mascara para todos os enderecos internet
UNIVERSE="0.0.0.0/0"

# Mascara de IP para todas as transmissoes de broadcast
BROADCAST="255.255.255.255"

# Portas IP altas nao privilegiadas.
UNPRIVPORTS="1024:65535"

# Portas do sistema X Windows (TCP).
XWINDOWS_PORTS="6000:6010"

# Caso voce precise especificar uma lista de hosts externos
# permitidos ou uma lista de subnets permitidas.
#
# Caso voce deseje permitir uma rede inteira, basta colocar
# o ultimo octeto com .0 e a subnet mask. Por exemplo :
#
# HOSTSEG="200.204.0.0/26"

```

```

#
#HOSTSEG="200.204.0.40"
#echo Host Seguro 1 IP: $HOSTSEG
#HOSTSEG2="200.204.0.41"
#echo Host Seguro 2 IP: $HOSTSEG2
#HOSTSEG3="200.204.0.42"
#echo Host Seguro 3 IP: $HOSTSEG3
#HOSTSEG2="200.204.0.43"
#echo Host Seguro 4 IP: $HOSTSEG4

# Enderecos IP para Port Forwarding
#
# Port forwarding, habilita trafico externo a conectar diretamente a sua
# maquina mascarada interna, acessivel apenas na rede interna.
# Uma aplicacao seria o acesso a um servidor FTP protegido atrs de uma
# mascara. Variaveis PORTFW, descomentar se for necessario.
#
#PORTFWIP1="192.168.1.20"
#echo IP PortForward 1 : $PORTFWIP1
#PORTFWIP2="192.168.2.12"
#echo IP PortForward 2 : $PORTFWIP2
#PORTFWIP3="192.168.1.21"
#echo IP PortForward 3 : $PORTFWIP3

# TCP/IP addresses of INTENRAL hosts network allowed to directly
# connect to the Linux server. All internal hosts are allowed
# per default.
# Enderecos da rede interna que terao acesso a esse firewall. O padrao e
# todos os hosts da rede interna estao habilitados.
#
# Coloque o IP e crie variaveis com nomenclatura HOST<rede><numero>IP
#
#HOST11IP="192.168.1.10"
#echo IP do Host Interno 1 da rede 1 : $HOST11IP
#HOST21IP="192.168.2.10"
#echo IP do Host Interno 1 da rede 2 : $HOST21IP

# Log do sistema firewall.
#
# Descomenta a linha " " e comente a "-1" para desabilitar o log.
#
# O arquivo de log pode ser encontrado no arquivo /var/log/messages.
# Caso voce so queria o log em algumas regras, simplesmente apague
# "$LOGGING" nas regras que nao deseja logar.
#
# LOGGING=" "
LOGGING="-1"

echo " --- "

echo "-----"

#-----
# Seccao de Debug do Firewall
#-----
# Se voce esta tendo problemas com seu firewall, descomente as linhas
# abaixo e reinicialize seu script.
#
# O arquivo de debug encontra-se em /tmp/rc.firewall.dump
#-----
#
#echo " - Debugging."
#echo IP de Loopback : $LOOPBACKIP > /tmp/rc.firewall.dump
#echo Nome da interface de Loopback : $LOOPBACKIF >> /tmp/rc.firewall.dump
#echo Nome da interface interna 1 : $INTIF >> /tmp/rc.firewall.dump
#echo IP da interface interna 1 : $INTIP >> /tmp/rc.firewall.dump
#echo Endereco da rede interna 1 : $INTLAN >> /tmp/rc.firewall.dump
#echo Nome da interface interna 2 : $INTIF2 >> /tmp/rc.firewall.dump
#echo IP da interface interna 2 : $INTIP2 >> /tmp/rc.firewall.dump
#echo Endereco da rede interna 2 : $INTLAN2 >> /tmp/rc.firewall.dump
#echo ----- >> /tmp/rc.firewall.dump
#echo Nome da interface Externa : $EXTIF >> /tmp/rc.firewall.dump

```

```

#echo IP da interface Externa : $EXTIP >> /tmp/rc.firewall.dump
#echo IP de broadcast da interface Externa : $EXTBROAD >> /tmp/rc.firewall.dump
#echo IP do default gateway da Interface Externa : $EXTGW >> /tmp/rc.firewall.dump
#echo ----- >> /tmp/rc.firewall.dump
# Liste os HOSTSEG, Hosts seguros
#echo Host Externo seguro : $HOSTSEG >> /tmp/rc.firewall.dump

#-----
# Geral
#-----
# Efetua processamentos gerais como configurar a rota de multicast
# e hackeamento de endereco DHCP.
#
# Multicast serve para transmitir dados para aplicacoes multimidia.
# Opcao de Multicast e opcional.
#
#echo " - Adicionando rota de multicast."
#sbin/route add -net 224.0.0.0 netmask 240.0.0.0 dev $EXTIF

# Desabilitando ataques de IP Spoofing.
#
#
echo " - Desabilitando ataques de IP Spoofing."
for file in /proc/sys/net/ipv4/conf/*/rp_filter
do
    echo "2" > $file
done

# Descomente se estiver usando um endereco dinamico
#*
#echo " - Habilitando hackeamento de endereco TCP/IP dinamico."
#echo "1" > /proc/sys/net/ipv4/ip_dynaddr

# Habilitando protecao a Cookie TCP SYN
#
echo " - Habilitando protecao a Cookie TCP SYN."
echo "1" > /proc/sys/net/ipv4/tcp_syncookies

# Certifique que as configuracoes de diversos ICMP sanity estao presentes.
#
echo " - Habilitando configuracoes de ICMP."

# Desabilitando protecao a echo de broadcast ICMP.
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# Habilitando protecao a mensagem de "bad error"
echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

# Desabilitando redirecionamentos de ICMP
for file in /proc/sys/net/ipv4/conf/*/accept_redirects; do
    echo "0" > $file
done
#

# Certifique que pacotes roteados na origem foram descartados
# Se estiver rodando IPRROUTE2, sera necessario desabilitar isso.
#
echo " - Certifique que pacotes roteados na origem foram descartados "
for file in /proc/sys/net/ipv4/conf/*/accept_source_route; do
    echo "0" > $file
done

# Logar pacotes spoofed, roteados na origem ou redirecionados.
#
echo " - Logar pacotes spoofed, roteados na origem ou redirecionados "
for file in /proc/sys/net/ipv4/conf/*/log_martians; do
    echo "1" > $file
done

#-----
# Configuracoes de Tipo de Servico (TOS - Type of Service)

```

```

#-----
# Voce pode dizer a internet como lidar com o seu trafico.
#
#     -t 0x01 0x10 = Delay Minimo
#     -t 0x01 0x08 = Throughput Maximo
#     -t 0x01 0x04 = Confiabilidade Maxima
#     -t 0x01 0x02 = Custo Minimo
#
# Por exemplo :
#
# Configuracao para FTP, SSH e TELNET
# /sbin/ipchains -A output -p tcp -d 0/0 21:23 -t 0x01 0x10
#
# Configuracao para Web WWW
# /sbin/ipchains -A output -p tcp -d 0/0 80 -t 0x01 0x10
#-----
# Timeouts de Masquerading
#-----
# Determinar valores de timeout para a sessao de masquerading.
#
# Explicacao : 7200 = 7200 segundos (2 hrs) para sessoes TCP
#              10   = 10 segundos para trafico TCP/IP apos recebimento
#                do pacote "FIN"
#              60   = 60 segundos para timeout do trafico UDP
# Para usuarios de ICQ aumente o valor para trafico UDP para 180 segundos
#
echo " - Alterando timeouts de IP masquerading."
/sbin/ipchains -M -S 7200 10 60
#-----
# Modulos de Masquerading
#-----
# A maioria de aplicativos TCP/IP funcionam bem atras de um servidor
# IP masquerading Linux. Alguns aplicativos precisam de modulos
# especiais para gerenciar o trafico de entrada e saida devidamente.
# Apenas descomente os modulos que ira efetivamente utilizar.
# O modulo FTP sera carregado.
#
# Verifique os modulos presentes no seu sistema no diretorio
# /lib/modules/<versao do seu kernel>/ipv4/
#-----
echo " - Carregando modulos de masquerading."

#/sbin/modprobe ip_masq_cuseeme
#/sbin/modprobe ip_masq_ftp
#/sbin/modprobe ip_masq_irc
#/sbin/modprobe ip_masq_quake
#/sbin/modprobe ip_masq_raudio
#/sbin/modprobe ip_masq_vdolive
#/sbin/modprobe ip_masq_icq
#-----
# Politicas default
#-----
# Configure todas as politicas default (padrao) para REJEITAR (REJECT)
# e descarte todas as regras antigas.
#-----
# Alterar politicas padrao para rejeitar REJECT
#
# Fazemos isso para, posteriormente, permitir qual o trafico que iremos
# permitir para OUT (saida) e In (entrada). Qualquer outro tipo de trafico,
# a nao ser que seja especificamente determinado, sera bloqueado.
#
echo " - Configurar politicas padrao para REJECT"
/sbin/ipchains -P input REJECT
/sbin/ipchains -P output REJECT
/sbin/ipchains -P forward REJECT

echo " - Descartar todas as regras antigas e configurar todas as "

```

```

echo "    politicas default para REJECT."
#
/sbin/ipchains -F input
/sbin/ipchains -F output
/sbin/ipchains -F forward

#*****
# Regras de entrada (input)
#*****
echo "-----"
echo "Regras de Entrada (Input) : "

#-----
# Trafico de entrada na rede Interna
#-----
# Essa parte controla o fluxo do trafico de entrada (input) dentro
# da rede interna.
# Todo o trafico da rede local e valido.
# Se voce precisar controlar qual trafico e permitido tera que configurar
# linhas individuais com ACCEPT para cada endereco IP.
#
# Voce pode desejar permitir apenas trafico numa direcao mas nao na contraria.
# Uma aplicacao seria permitir acesso a um servidor Web externo mas nao o
# acesso proveniente desse servidor. O correto e usar a flag -y.
#-----
echo " - Determinar filtros de trafico de entrada (INPUT) na rede interna."

# Servidor DHCP
#
# Se voce configurou um servidor DHCP na sua maquina Linux para servir
# enderecos IP a rede interna, voce tera que habilitar essa seccao.
#
# Esse e um exemplo de como permitir o fluxo do trafico de entrada na
# rede interna.
#
# echo "    Parametro Opcional : Servidor DHCPd"
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p udp -s $UNIVERSE bootpc -d $BROADCAST/0 bootps
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $UNIVERSE bootpc -d $BROADCAST/0 bootps
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p udp -s $UNIVERSE bootpc -d $BROADCAST/0 bootps
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $UNIVERSE bootpc -d $BROADCAST/0 bootps

#-----
# Acesso explicito a partir dos hosts da rede interna.
#-----
# Esse e um exemplo de como permitir apenas que hosts especificos
# na rede interna possam acessar os servicos de firewall.
#
# Exemplos de permissao para acesso de FTP, dados de FTP, SSH e TELNET.
#-----
#echo " - Configurando flitros de input para hosts especificos na rede interna."

# Host1 : Permita que o ip do host interno $HOST11IP conecte ao servidor linux
#
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ftp
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ftp-data
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ssh
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP telnet
# mesma coisa para rede 2 dentro da rede 2
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP ftp
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP ftp-data
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP ssh
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP telnet

# Host2 : Permita que o ip do host interno $HOST12IP conecte ao servidor linux
#
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ftp
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ftp-data
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ssh
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP telnet
# mesma coisa para rede 2
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP ftp

```

Artigo

```
#!/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP ftp-data
#!/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP ssh
#!/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP telnet

#-----
# Trafico proveniente da interface externa
#-----
# Essa regra ira controlar o trafico especifico cuja entrada e permitida
# proveniente da interface externa.
#
#-----
#
echo " - Configurando filtro de entrada para trafico proveniente da interface externa."

# Clientes de DHCP.
#
# Se seu provedor nao lhe designou um IP fixo, seu IP e dinamico.
# Portanto, voce tera que habilitar as linhas abaixo. Geralmente para
# usuarios de cable modem ou modems convencionais essa e a situacao.
##*
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p udp -s $UNIVERSE bootps -d $BROADCAST/0 bootpc
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE bootps -d $BROADCAST/0 bootpc

# FTP : Pemite usuarios externos (da internet) conectar ao seu servidor linux
# para servicos FTP.
#
# echo " Parametro opcional : Servidor FTP"
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP ftp
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP ftp-data

# IRC : Permite usuarios externos (na internet) conectar ao seu servidor Linux
# para servicos IRC.
# Verifique se o seu IRCD esta definido na tabela de servicos no arquivo
# /etc/services
#
# echo " Parametro Opcional : servidor IRC"
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP ircd

# HTTP : Permite usuarios externos (na internet) conectar ao seu servidor Linux.
#
# echo " Parametro Opcional : servidor HTTP"
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP http

# HTTPS : Permite usuarios externos (na internet) conectar ao seu servidor Linux.
#
# echo " Parametro Opcional : servidor HTTPS"
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP https

# Advanced ICMP: Some users prefer that their UNIX box NOT ping, etc.
# This is easy enough to do but be sure you know what you
# are doing.
# ICMP avancado : Alguns administradores preferem que seu servidor Linux
# nao permita ping, etc.
#
# Consulte o paper sobre filtragem de ICMP para saber mais :
# http://www.sys-security.com/archive/papers/ICMP\_Scanning\_v2.0.pdf
#
# Quando um firewall e configurado para rejeitar trafico de ICMP,
# o trafico resultante de reply e automaticamente rejeitado.
# Rode "/sbin/ipchains -h icmp" para verificar codigos de icmp suportados.
#
# Nao responda (reply) a ECHO REPLYs (tipo 0) vindos pela internet.
#
# echo " Parametro Opcional : Filtro de entrada de ICMP ECHO-REPLY"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type echo-reply $LOGGING
#
# Nao responder a requisicoes TCP/UDP TRACEROUTE da internet.
#
# echo " Parametro Opcional : Filtro de entrada TCP/UDP TRACEROUTE"
#
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 33434 $LOGGING
```

Artigo

```
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIP 33434 $LOGGING
#
# Nao responder a requisicoes TCP/UDP TRACEROUTE da Internet para clientes
# MS que utilizam ICMP ECHO e nao TCP/UDP.
#
# echo "          Parametro Opcional : Filtro de entrada ICMP TRACEROUTE (MS)"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type
destination-unreachable $LOGGING
#
# Nao responder a DESTINATION-UNREACHABLE (tipo 3) da internet.
#
# echo "          Parametro Opcional : filtro de entrada ICMP DESTINATION-UNREACHABLE"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type
destination-unreachable $LOGGING
#
# Nao responder a SOURCEQUENCH (tipo 4) da internet.
#
# echo "          Parametro Opcional : filtro de entrada ICMP SOURCEQUENCH"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type source-quench
$LOGGING
#
# Nao responder a nenhuma forma de refirecionamento de pacotes (tipo 5)
#
# echo "          Parametro Opcional : filtro de entrada ICMP REDIRECT"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type redirect $LOGGING
#
# Nao permitir requisicoes de PING (tipo 8) da internet.
#
# echo "          Parematro Opcional : filtro de entrada ICMP ECHO"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type echo-request
$LOGGING
#
# Nao responder a pacotes do tipo (Time to Live expirado) TTL-Expired.
#
# echo "          Parametro Opcional : filtro de entrada ICMP TTL-EXPIRED"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type time-exceeded
$LOGGING
#
# Nao responder a pacotes do tipo ICMP PARAMETER-PROBLEM.
#
# echo "          Parametro Opcional : filtro de entrada ICMP PARAMETER-PROBLEM"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type
parameter-problem $LOGGING
#
# Nao responder a pacotes ICMP TIMESTAMP (tipos 13 e 14)
#
# echo "          Parametro Opcional : filtro de entrada ICMP TIMESTAMP"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type timestamp-request
$LOGGING
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type timestamp-reply
$LOGGING
#
# Nao responder a pacotes ICMP ADDRESS MASK (tipo 17 e 18).
#
# echo "          Parametro Opcional : filtro de entrada ICMP ADDRESS-MASK"
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type
address-mask-request $LOGGING
#!/sbin/ipchains -A input -j REJECT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIP --icmp-type address-mask-reply
$LOGGING

# ICMP Geral : Permite pacotes ICMP a partir de todos enderecos externos.
#
# Desabilitar pacotes ICMP por regras de firewall pode fazer muito mais
# que apenas barrar usuarios pingando a sua maquina. Muitos aspectos
# do TCP/IP e seus aplicativos relacionados baseiam-se em varias mensagens
# ICMP. Sem ICMP, tanto seu servidor Linux quanto os hosts internos da sua
# rede podem nao funcionar.
#
# Se desejar filtrar pacotes ICMP, faca-o descomentando o tipo de trafico
# que deseja barrar nas linhas acima e nao na linha a seguir.
#
# Essa linha aceita pacotes ICMP originarios da Internet para o IP da
```

```

# sua interface externa.
#
/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p icmp -s $UNIVERSE -d $EXTIF

# NNTP : Permite hosts externos conectarem o seu servidor Linux para
#        servicos de news NNTP.
#
# echo "          Parametro Opcional : servidor NNTP"
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIF nntp

# NTP : Permite hosts externos conectarem o seu servidor Linux para
#        servicos NTP.Alguns clientes de NTP utilizam trafico TCP
#        enquanto outros utilizam UDP.
#
# echo "          Parametro Opcional : servidor NTP"
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIF ntp
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIF ntp

# TELNET : Permite hosts externos conectarem seu servidor Linux para
#        acesso TELNET.
#
# echo "          Parametro Opcional : servidor TELNET"
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIF telnet

# Servidor SSH: Permite hosts externos conectarem seu servidor Linux para
#        acesso seguro secure shell SSH.
#
# echo "          Parametro Opcional : servidor SSH"
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIF ssh

#-----
# Rejeicoes especificas de entrada pela interface externa
#-----
# Essas regras rejeitam trafico especifico que voce nao deseja dentro
# do seu sistema.
#-----
echo " - Rejeitar entradas (inputs) especificos."

# Recusar pacotes via interface externa com endereco de loopback
#*
/sbin/ipchains -A input -j DENY -i $EXTIF -s $LOOPBACKIP

# Interface remota alegando ser maquina local.Caso de IP spoofing.
/sbin/ipchains -A input -j REJECT -i $EXTIF -s $INTLAN -d $UNIVERSE $LOGGING

# De acordo com RFC1918 e IANA
# Filtro de enderecos reservados
#
# Filtrar todo o trafico externo originario do espaco reservado de enderecos.
# Rode "whois IANA*@arin.net" e "whois RESERVED*@arin.net" para obter
# maiores informacoes.
#
# Reservado-1
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 0.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-9
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 1.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-10
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 10.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-23
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 23.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-31
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 31.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-7 (65.0.0.0 - 95.255.255.255)
#

```

Artigo

```
# 65.0.0.0 - 65.255.255.255
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 65.0.0.0/8 -d $UNIVERSE $LOGGING
# 66.0.0.0 - 67.255.255.255
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 66.0.0.0/7 -d $UNIVERSE $LOGGING
# 68.0.0.0 - 71.255.255.255
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 68.0.0.0/6 -d $UNIVERSE $LOGGING
# 72.0.0.0 - 79.55.255.255
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 72.0.0/5 -d $UNIVERSE $LOGGING
# 80.0.0.0 - 95.255.255.255
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 80.0.0.0/4 -d $UNIVERSE $LOGGING

# Reservado-8 (96.0.0.0 - 126.255.255.255)
# A mascara a seguir inclui tambem a rede 127.0.0.0.
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 96.0.0.0/3 -d $UNIVERSE $LOGGING

# Loopback
# Incluso acima no Reservado-8

# Reservado-3
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 128.0.0.0/16 -d $UNIVERSE $LOGGING

# BuracoNegro3 = BLACKHOLE3
#
# Desabilitado pelo fato que todas as funcoes de reverso de DNS , exceto
# a funcao de endereco, nao irao funcionar corretamente.
#
# /sbin/ipchains -A input -j REJECT -i $EXTIF -s 128.9.64.26/32 -d $UNIVERSE $LOGGING

# Inclui NET-TEST-B
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 128.66.0.0/16 -d $UNIVERSE $LOGGING

# IANA-RESERVED e RFC1918 (172.19-31.0.0)
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 172.16.0.0/12 -d $UNIVERSE $LOGGING

# Reservado-4
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 191.255.0.0/16 -d $UNIVERSE $LOGGING

# ROOT-NS-LAB - 192.0.0.0/24
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 192.0.0.0/24 -d $UNIVERSE $LOGGING

# NET-ROOTS-NS-LIVE - 192.0.1.0/24
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 192.0.1.0/24 -d $UNIVERSE $LOGGING

# NET-TEST - 192.0.2.0/24
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 192.0.2.0/24 -d $UNIVERSE $LOGGING

# RFC1918
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 192.168.0.0/16 -d $UNIVERSE $LOGGING

# Reservado-13
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 197.0.0.0/16 -d $UNIVERSE $LOGGING

# Reservado-14
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 201.0.0.0/8 -d $UNIVERSE $LOGGING

# Reservado-5
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 223.255.255.0/24 -d $UNIVERSE $LOGGING

# Para uso futuro com classes E e F.
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 240.0.0.0/5 -d $UNIVERSE $LOGGING
/sbin/ipchains -A input -j REJECT -i $EXTIF -s 248.0.0.0/5 -d $UNIVERSE $LOGGING

# Multicast : Desabilitar trafico Multicast.
#
# echo "          Parametro Opcional : Ignorar MULTICAST"
# /sbin/ipchains -A input -j REJECT -i $EXTIF -s $UNIVERSE -d 224.0.0.0/4

# NFS: Rejeita trafico NFS de e para maquinas externas.
#
# Procure nao habilitar trafico externo de NFS para evitar problemas de
```

Artigo

```
# segurança.
#
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 2049
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE 2049 -d $EXTIP

# SMB e CIFS: Rejeita trafico SMB e CIFS de e para maquinas externas.
#
# Procure nao habilitar trafico externo de Samba (Windows 3.x, 9x e NT) ou
# CIFS (Windows 2000) para evitar problemas de segurança.
#
# Portas: 137 TCP/UDP (NetBIOS name service)
#         138 UDP      (NetBIOS datagram service) - filtra TCP
#         139 TCP      (NetBIOS session service) - filtra UDP
#         445 TCP/UDP (MS CIFS em Windows 2000)

echo "      - Rejeitar silenciosamente trafico TCP/UDP de SMB e CIFS pela interface externa."
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 137
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIP 137
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTBROAD 137
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTBROAD 137
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 138
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIP 138
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTBROAD 138
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTBROAD 138
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 139
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIP 139
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTBROAD 139
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTBROAD 139
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP 445
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTIP 445
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTBROAD 445
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE -d $EXTBROAD 445
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE 137 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE 137 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE 138 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE 138 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE 139 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE 139 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p tcp -s $UNIVERSE 445 -d $EXTIP
/sbin/ipchains -A input -j REJECT -i $EXTIF -p udp -s $UNIVERSE 445 -d $EXTIP

#-----
# Trafico de entrada para todas as Interfaces
#-----
# Isso ira controlar o trafico de entrada em todas as interfaces.
#-----
echo "      - Configurando filtros de entrada para servicos publicos em todas as interfaces."

# AUTH: Permite o protocolo de autenticacao em todas as interfaces
#       mas desabilita no arquivo /etc/inetd.conf. A razao disso
#       e que algumas pilhas TCP/IP nao lidam corretamente com
#       requisicoes de autorizacao rejeitadas.
#
# Trafico para e apartir da sua maquina
/sbin/ipchains -A input -j ACCEPT -p tcp -s $UNIVERSE -d $UNIVERSE auth
/sbin/ipchains -A input -j ACCEPT -p tcp -s $UNIVERSE auth -d $UNIVERSE

# DHCP/BOOTP : Rejeita todo trafico.
#
#/sbin/ipchains -A input -j REJECT -p udp -s $UNIVERSE bootpc

# DNS: Se voce e um provedor de acesso e esta rodando um DNS
#      de IPs validos, e necessario abrir as portas do DNS em
#      todas as interfaces e permitir lookups.
#
# echo "      Parametro Opcional : servidor DNS"
#/sbin/ipchains -A input -j ACCEPT -p tcp -s $UNIVERSE -d $UNIVERSE domain
#/sbin/ipchains -A input -j ACCEPT -p udp -s $UNIVERSE -d $UNIVERSE domain

# RIP: Rejeita todo o trafico RIP.Muitas redes mal configuradas
#      propagam protocolos de roteamento de rede ate o limite da rede.
```

Artigo

```
# A linha a seguir permite que voce filtre RPI.
#
#/sbin/ipchains -A input -j REJECT -p udp -s $UNIVERSE -d $UNIVERSE route

# SMTP: Se voce esta rodando um servidor SMTP valido, deve permitir
# o trafico de SMTP em todas as interfaces.
#
# echo " Parametro Opcional : servidor SMTP"
#/sbin/ipchains -A input -j ACCEPT -p tcp -s $UNIVERSE -d $UNIVERSE smtp

# Proxy SQUID com filtro de lixo
#
# Se voce esta usando o Squid com filtro de Banners, voce tera que
# habilitar as linhas a seguir para fazer o redirecionamento IPCHAINS
# para a porta 3128 do Squid.
#
#echo " Parametro Opcional : Proxy transparente SQUID"
#/sbin/ipchains -A input -j ACCEPT -i $LOOPBACKIF -p tcp -d $LOOPBACKIP/32 www
#/sbin/ipchains -A input -j ACCEPT -i $INTIF -p tcp -s $INTLAN -d $INTIP/32 www
#/sbin/ipchains -A input -j REDIRECT 3128 -i $INTIF -p tcp -s $INTLAN -d $INTLAN/0 www $LOGGING
# Rede 2
#/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -p tcp -s $INTLAN2 -d $INTIP2/32 www
#/sbin/ipchains -A input -j REDIRECT 3128 -i $INTIF2 -p tcp -s $INTLAN2 -d $INTLAN2/0 www $LOGGING

#-----
# Rejeicoes de entrada especifica em qualquer interface.
#-----
# AS regras abaixo rejeitam trafico especifico que voce nao quer fora
# do seu sistema.
#-----
#echo " - Rejeitar trafico para dominios especificos."

# Nao permitir que qualquer host interno tenha acesso aos seguintes sites :
#
#
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 63.160.54.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 128.11.92.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 199.95.206.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 199.95.207.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 199.95.208.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 199.95.210.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 204.178.112.160/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 204.253.104.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 208.10.202.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 208.203.243.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 208.211.225.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 208.228.86.0/24
#/sbin/ipchains -A input -j REJECT -i $INTIF -p tcp -s $UNIVERSE -d 209.67.38.0/24

# Suponha que voce nao quer receber nenhum e-mail de um servidor.
# Use o codigo abaixo, colocando o endereco valido apos o flag -d
#
#/sbin/ipchains -A input -j REJECT -p tcp -s $UNIVERSE 25 -d 152.163.159.0/24
#/sbin/ipchains -A input -j REJECT -p tcp -s $UNIVERSE 25 -d 205.188.157.0/24

#-----
# Permite INPUT de hosts externos
#-----
# Isso controla acesso externo de hosts especificos. O exemplo permite
# FTP, Secure Shell, POP3 e TELNET de um servidor especificado dentro do
# firewall. Alem das regras de input voce precisa permitir o trafico desse
# servidor para fora. Veja as regras de output mais abaixo.
#
#-----
#echo " - Configurando filtros de entrada para hosts externos."

#
#echo " Permite INPUT de $HOSTSEG para ftp, ssh, POP3 e TELNET."
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG -d $EXTIP ftp
#/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG -d $EXTIP ftp-data
```

Artigo

```
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG -d $EXTIP ssh
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG -d $EXTIP pop-3
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG -d $EXTIP telnet

#echo "    Permite INPUT de $HOSTSEG2 para ftp, ssh, POP3 e TELNET."
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG2 -d $EXTIP ftp
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG2 -d $EXTIP ftp-data
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG2 -d $EXTIP ssh
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG2 -d $EXTIP pop-3
#!/sbin/ipchains -A input -j ACCEPT -i $EXTIF -p tcp -s $HOSTSEG2 -d $EXTIP telnet
#
# copie o bloco para mais hosts apos $HOSTSEG2

# Permite que todas as interfaces internas acessem a internet
# -----
# Interface local e maquinas locais podem ir a qualquer lugar.
#
# A razao principal dessa regra estar no final da seccao de INPUT
# e certificar que todas as linhas DENY/REJECT do firewall sejam
# testadas antes de permitir todo o trafico interno.
# Se voce desejar pode voltar ao topo dessa seccao e especificar
# quais os hosts que podem sair, depois comente a linha abaixo
# de modo que so os hosts permitidos podem sair para a internet.
#
# Rede Interna 1
/sbin/ipchains -A input -j ACCEPT -i $INTIF -s $INTLAN -d $UNIVERSE
#*
# Rede Interna 2
/sbin/ipchains -A input -j ACCEPT -i $INTIF2 -s $INTLAN2 -d $UNIVERSE

# Interface de Loopback e valida.
#
/sbin/ipchains -A input -j ACCEPT -i $LOOPBACKIF -s $UNIVERSE -d $UNIVERSE

# Portas altas :
#
# Habilita todas as portas altas nao privilegiadas para todo o trafico
# TCP/UDP de reply.
#
# O uso da flag "! -y" (not -y) filtra todo trafico TCP que nao possui
# o bit SYN configurado. Isso significa que qualquer trafico que tentar
# negociar com seu servidor numa porta alta sera rejeitado. Apenas
# trafico de retorno ou trafico baseado em UDP sera aceito em portas
# altas. Nao utilizar filtro SYN na porta 20 para secoes ativas de FTP.
# Por isso, deve-se especificar isso.
#
echo " - Habilitando toda a entrada de trafico de REPLY (TCP/UDP) em portas altas."
/sbin/ipchains -A input -j ACCEPT ! -y -p tcp -s $UNIVERSE -d $EXTIP $UNPRIVPORTS
/sbin/ipchains -A input -j ACCEPT -p tcp -s $UNIVERSE ftp-data -d $EXTIP $UNPRIVPORTS
/sbin/ipchains -A input -j ACCEPT -p udp -s $UNIVERSE -d $EXTIP $UNPRIVPORTS

#-----
# Capturar todas as regras de INPUT
#-----
#
echo " - Capturar todas as regras de input finais."

# Todos os outros tipos de entradas sao negadas e logadas.
/sbin/ipchains -A input -j REJECT -s $UNIVERSE -d $UNIVERSE $LOGGING

#*****
# Regras de Output (saida)
#*****
echo "-----"
echo "Regras de Output:"

#-----
# Trafico de saida (Outgoing) da rede interna
#-----
```

Artigo

```
# Essas regras contem politicas para todo trafico de saida da rede
# interna. Todo trafico para fora e permitido.
#
#-----
echo " - Configurando filtros de output para todo o trafico da rede interna."

# Filtrar pacotes via interface externa com endereco de loopback
#*
/sbin/ipchains -A output -j DENY -i $EXTIF -s $LOOPBACK $LOGGING

# Interface local, qualquer origem para a rede local 1 e valida.
/sbin/ipchains -A output -j ACCEPT -i $INTIF -s $UNIVERSE -d $INTLAN

# Interface local, qualquer origem para a rede local 2 e valida.
#*
/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -s $UNIVERSE -d $INTLAN2

# Interface de Loopback e valida.
/sbin/ipchains -A output -j ACCEPT -i $LOOPBACKIF -s $UNIVERSE -d $UNIVERSE

# DHCP: Se voce configurou um servidor DHCP nessa maquina Linux, voce tera
# que habilitar as seguintes regras :
#
# echo "          Parametro Opcional : servidor DHCPd"
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p udp -s $INTIP/32 bootps -d $BROADCAST/0 bootpc
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $INTIP/32 bootps -d $BROADCAST/0 bootpc
#*
# Rede 2
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p udp -s $INTIP2/32 bootps -d $BROADCAST/0 bootpc
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $INTIP2/32 bootps -d $BROADCAST/0 bootpc

# HTTP: Como permitir trafico interno HTTP a um servidor intranet de Web
# sem permitir o acesso externo.
#
# echo "          Parametro Opcional : servidor WWW"
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $INTIP/32 http -d $INTLAN

# APC PowerChute para Linux. Esse e o software de gerenciamento de nobreaks
# da marca APC que uso internamente. Serve para desligar e verificar o nobreak.
# Esse software manda um broadcast para a rede interna procurando pelo daemon
# upsd.
#
# echo "          Parametro Opcional : servidor UPSd"
# /sbin/ipchains -A output -j ACCEPT -i $INTIF -p udp -s $INTIP/32 -d $BROADCAST 5456
#*
# Rede 2
# /sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p udp -s $INTIP2/32 -d $BROADCAST 5456

#-----
# Output da rede interna.Acesso de hosts internos ao firewall.
#-----
# As regras abaixo permitem a apenas hosts especificados o acesso
# aos servicos desse firewall.
#
# Abaixo, esta demonstrado como permitir acesso FTP, SSH e TELNET.
#
#-----
#echo " - Estabelecendo filtros para output de hosts da rede interna."

# Host1 da rede 1 HOST11IP
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ftp
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ftp-data
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP ssh
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST11IP -d $INTIP telnet

# Host2 da rede 1 HOST12IP
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ftp
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ftp-data
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP ssh
#/sbin/ipchains -A output -j ACCEPT -i $INTIF -p tcp -s $HOST12IP -d $INTIP telnet
```

```

# Host1 da rede 2 HOST21IP
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP2 ftp
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP2 ftp-data
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP2 ssh
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST21IP -d $INTIP2 telnet

# Host2 da rede 2 HOST22IP
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP2 ftp
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP2 ftp-data
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP2 ssh
#/sbin/ipchains -A output -j ACCEPT -i $INTIF2 -p tcp -s $HOST22IP -d $INTIP2 telnet

#-----
# Trafico de saida na interface externa
#-----
# Essa regra controla o trafico que pode sair pela interface externa.
#-----
echo " - Configurando filtros de input para trafico com a interface externa."

# Cliente DHCP : Se o seu servidor Linux esta conectado via Cablemodem, ou seja,
#                acesso dedicado por cabo e seu provedor nao lhe forneceu um IP
#                fixo e sim um endereco dinamico que muda de acordo com
#                intervalos determinados, sera necessario descomentar as
#                regras abaixo.
#
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $UNIVERSE bootpc -d $UNIVERSE bootps
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p udp -s $UNIVERSE bootpc -d $UNIVERSE bootps

# FTP : Permite trafico FTP se o seu servidor Linux for um servidor FTP tambem.
#
# echo "          Parametro Opcional : servidor FTP"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp -d $UNIVERSE
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp-data -d $UNIVERSE

# IRCd : Permite trafico se o seu servidor Linux servir IRC.
#        Obs : ircd deve estar especificado no arquivo de servicos
#                localizado em etc/services
#
# echo "          Parametro Opcional : servidor IRC"
# /sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ircd -d $UNIVERSE

# HTTP : Permite trafico HTTP. Seu Linux e um servidor de documentos WWW
#
# echo "          Parametro Opcional : servidor WWW"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP http -d $UNIVERSE

# HTTPS : Permite trafico HTTP. Seu Linux e um servidor de documentos seguros WWW
#
# echo "          Parametro Opcional : servidor WWW seguro HTTPS"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP https -d $UNIVERSE

# NTP : Permite atualizacoes NTP. Seu Linux e um servidor NTP.
#        Alguns clientes NTP usam TCP e outros usam UDP.
#
# echo "          Parametro Opcional : servidor NTP"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ntp -d $UNIVERSE
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p udp -s $EXTIP ntp -d $UNIVERSE

# TELNET: Permite trafico TELNET.
#
# echo "          Parametro Opcional : servidor TELNET"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP telnet -d $UNIVERSE

# SSH : Permite trafico de saida de SSH, se o seu Linux estiver rodando o SSHd.
#        Nesse caso, voce pode acessar o seu Linux pela internet (interface externa)
#        via SSH. No meu caso, eu faco isso.
#*
# echo "          Parametro Opcional : servidor SSH"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ssh -d $UNIVERSE
#-----

```

```

# Trafico de saida em todas as interfaces
#-----
# As regras abaixo controlam o trafico de saida para todas as interfaces.
# As regras sao apenas para especificar o que pode ser usado, uma vez que
# a regra geral esta acima como REJECT.
#-----
echo " - Configurando filtros de output para todas as interfaces."

# AUTH : Permite que o protocolo de autenticacao AUTH e ident funcionem com
# todas as interfaces.
# Trafico PARA a sua maquina DA sua maquina.
/sbin/ipchains -A output -j ACCEPT -p tcp -s $UNIVERSE auth -d $UNIVERSE
/sbin/ipchains -A output -j ACCEPT -p tcp -s $UNIVERSE -d $UNIVERSE auth

# DNS : Caso esteja rodando um servidor Linux DNS autoritativo, voce precisa
# habilitar as regras a seguir.
#
# echo " Parametro Opcional : Servidor DNS"
#/sbin/ipchains -A output -j ACCEPT -p tcp -s $EXTIP domain -d $UNIVERSE
#/sbin/ipchains -A output -j ACCEPT -p udp -s $EXTIP domain -d $UNIVERSE

# ICMP avancado : Alguns administradores preferem que seu servidor Linux
# nao seja pingado com PING.
# Consulte http://www.sys-security.com/archive/papers/ICMP\_Scanning\_v2.0.pdf
# sobre como filtrar trafico ICMP.
#
# Rode "/sbin/ipchains -h icmp" para saber sobre codigos ICMP.
#
# Nao responder a ICMP ECHO REPLYs (tipo 0) da Internet.
#
# echo " Parametro Opcional : Saida de ICMP ECHO REPLY filtrada"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type echo-reply
#
# Nao responder a requisicoes de TRACEROUTE via TCP/UDP da Internet
#
# echo " Parametro Opcional : Trafico de saida TRACEROUTE TCP/UDP filtrado"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 33434 $LOGGING
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 33434 $LOGGING
#
# Nao responder a requisicoes de TRACEROUTE via ICMP ECHO para clientes MS
#
# echo " Parametro Opcional : Trafico de saida TRACEROUTE ICMP ECHO (MS) filtrado"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type echo-request
$LOGGING
#
# Nao responder a DESTINATION-UNREACHABLE (tipo 3) da Internet
#
# echo " Parametro Opcional : Trafico de saida ICMP DESTINATION-UNREACHABLE filtrado"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type
destination-unreachable $LOGGING
#
# Nao responder a SOURCEQUENCH (tipo 4) da Internet
#
# echo " Parametro Opcional : Trafico de saida ICMP SOURCEQUENCH filtrado"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type source-quench
$LOGGING
#
# Nao responder a qualquer tipo de pacote ICMP REDIRECT (tipo 5)
#
echo " Parametro Opcional : trafico de saida ICMP REDIRECT filtrado"
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type redirect $LOGGING
#
# Nao permitir PING (tipo 8) da Internet
#
# echo " Parametro Opcional : trafico de saida ICMP ECHO filtrado"
#/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type echo-request
$LOGGING
#
# Nao responder a pacotes Time To Live Expired (tipo 11) da Internet
#
echo " Parametro Opcional : trafico de saida ICMP TTL-EXPIRED filtrado"
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type

```

```

ttl-zero-during-reassembly $LOGGING
#
# Nao responder a pacotes PARAMETER-PROBLEM (tipo 12) da internet
#
echo "          Parametro Opcional : Trafico de saida ICMP PARAMETER-PROBLEM filtrado"
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type parameter-problem
$LOGGING
#
# nao responder a pacotes ICMP TIMESTAMP (tipo 13 e 14)
#
echo "          Parametro Opcional : trafico de saida ICMP TIMESTAMP filtrado"
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type timestamp-request
$LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type timestamp-reply
$LOGGING
#
# Nao responder a pacotes ICMP ADDRESS MASK (tipo 17 e 18)
#
echo "          Parametro Opcional : Trafico de saida ICMP ADDRESS-MASK filtrado"
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type
address-mask-request $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p icmp -s $EXTIP -d $UNIVERSE --icmp-type
address-mask-reply $LOGGING

# ICMP Geral : Permite trafico de ICMP para fora
#
# Cuidado ao desabilitar pacotes ICMP com regras de firewall. Muitos
# aspectos do protocolo TCP/IP e aplicativos derivados dependem de
# mensagens ICMP. Portanto, ao fazer isso tenha certeza do que esta
# realmente filtrando. Sem ICMP, tanto o seu servidor Linux quanto
# as maquinas conectadas a ele podem nao funcionar.
#
# Aceita trafico ICMP da Internet
/sbin/ipchains -A output -j ACCEPT -p icmp -s $UNIVERSE -d $UNIVERSE

# NNTP : Permite trafico de News baseado em NNTP.
#
# echo "          Parametro Opcional : servidor NNTP"
#/sbin/ipchains -A output -j ACCEPT -p tcp -s $EXTIP nntp -d $UNIVERSE

# SMTP : Se seu servidor Linux e um servidor SMTP ou funciona como um relay
#         voce precisa descomentar a linha abaixo.
#
# echo "          Parametro Opcional : servidor SMTP"
#/sbin/ipchains -A output -j ACCEPT -p tcp -s $EXTIP smtp -d $UNIVERSE

#-----
# Saida para Hosts externos especificos
#-----
# Essas regras permitem saida para hosts especificos que denominamos
# $HOSTSEG. Abaixo, POP3 e SSH sao permitidos para Hosts especificados.
# Alem das regras de saida (OutPut) tambem sao necessarias as regras de
# Input. Veja acima.
#
#-----
echo " - Configurando filtros de saida para hosts externos especificos."

# Host 1 = HOSTSEG
#
#echo " Permitindo output de ftp, ssh, pop-3 e telnet para $HOSTSEG"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp -d $HOSTSEG $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp-data -d $HOSTSEG $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ssh -d $HOSTSEG $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP pop-3 -d $HOSTSEG $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP telnet -d $HOSTSEG $UNPRIVPORT

#echo " Permitindo output de ftp, ssh, pop-3 e telnet para $HOSTSEG2"
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp -d $HOSTSEG2 $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp-data -d $HOSTSEG2 $UNPRIVPORTS
#/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ssh -d $HOSTSEG2 $UNPRIVPORTS

```

Artigo

```
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP pop-3 -d $HOSTSEG2 $UNPRIVPORTS
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP telnet -d $HOSTSEG2 $UNPRIVPORT

#echo " Permitindo output de ftp, ssh, pop-3 e telnet para $HOSTSEG3"
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp -d $HOSTSEG3 $UNPRIVPORTS
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ftp-data -d $HOSTSEG3 $UNPRIVPORTS
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP ssh -d $HOSTSEG3 $UNPRIVPORTS
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP pop-3 -d $HOSTSEG3 $UNPRIVPORTS
#!/sbin/ipchains -A output -j ACCEPT -i $EXTIF -p tcp -s $EXTIP telnet -d $HOSTSEG3 $UNPRIVPORT

#-----
# Rejeicoes especificas de output (saida)
#-----
# Essas regras rejeitam trafico especifico que voce nao quer saindo
# da sua rede.
#-----
echo " - Rejeita trafico de saida especificados."

# Rejeita trafico de saida para a rede interna atarves da interface
# de saida.
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d $INTLAN $LOGGING
# Rede 2
#*
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d $INTLAN2 $LOGGING

# Rejeita trafico de saida originado da rede interna atraves da interface
# externa
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $INTLAN -d $UNIVERSE $LOGGING
# Rede 2
#*
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $INTLAN2 -d $UNIVERSE $LOGGING

# Filtragem dos enderecos reservados RFC1918 e IANA
#
# Filtra todo o trafico vindo da interface externa cujo enderecamento
# seja baseado em enderecos reservados.
# Para saber mais rode "whois IANA*@arin.net" e
# "whois RESERVED*@arin.net".
#
# Reservado-1
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 0.0.0.0/8 $LOGGING

# Reservado-9
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 1.0.0.0/8 $LOGGING

# Reservado-10
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 10.0.0.0/8 $LOGGING

# Reservado-23
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 23.0.0.0/8 $LOGGING

# Reservado-31
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 31.0.0.0/8 $LOGGING

# Reservado-7 (65.0.0.0 - 95.255.255.255)
#
# 65.0.0.0 - 65.255.255.255
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 65.0.0.0/8 $LOGGING
# 66.0.0.0 - 67.255.255.255
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 66.0.0.0/7 $LOGGING
# 68.0.0.0 - 71.255.255.255
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 68.0.0.0/6 $LOGGING
# 72.0.0.0 - 79.55.255.255
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 72.0.0.0/5 $LOGGING
# 80.0.0.0 - 95.255.255.255
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 80.0.0.0/4 $LOGGING

# Reservado-3
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 128.0.0.0/16 $LOGGING

# BLACKHOLE3
```

Artigo

```
#!/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 128.9.64.26/32 $LOGGING

# Inclui NET-TEST-B
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 128.66.0.0/12 $LOGGING

# IANA-BBLK-RESERVED e RFC1918 (172.19-31.0.0)
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 172.16.0.0/12 $LOGGING

# Reservado-4
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 191.255.0.0/16 $LOGGING

# ROOT-NS-LAB - 192.0.0.0/24
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 192.0.0.0/24 $LOGGING

# NET-ROOTS-NS-LIVE - 192.0.1.0/24
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 192.0.1.0/24 $LOGGING

# NET-TEST - 192.0.2.0/24
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 192.0.2.0/24 $LOGGING

# RFC1918
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 192.168.0.0/16 $LOGGING

# Reservado-13
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 197.0.0.0/8 $LOGGING

# Reservado-14
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 201.0.0.0/8 $LOGGING

# Reservado-5
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 223.255.255.0/24 $LOGGING

# Para uso futuro das classes E e F :
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 240.0.0.0/5 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -s $UNIVERSE -d 248.0.0.0/5 $LOGGING

# Samba e CIFS. Rejeita trafico Samba e CIFS de maquinas externas.
#
# NUNCA habilite trafico SMB/CIFS pela internet a nao ser que tenha
# absoluta certeza do que esta fazendo. Se voce realmente precisa
# dessa funcionalidade use um IP seguro ou sistema VPN.
#
# Portas: 137 TCP/UDP (NetBIOS name service)
#         138 UDP      (NetBIOS datagram service) - TCP filtrado por seguranca
#         139 TCP      (NetBIOS session service) - UDP filtrado por seguranca
#         445 TCP/UDP (MS CIFS no Windows 2000)

echo "      - Rejeitando trafico TCP/UDP para Samba na interface externa."
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF -d $UNIVERSE 137
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF -d $UNIVERSE 137
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF -d $UNIVERSE 138
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF -d $UNIVERSE 138
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF -d $UNIVERSE 139
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF -d $UNIVERSE 139
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF -d $UNIVERSE 445
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF -d $UNIVERSE 445
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF 137 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF 138 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF 138 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF 139 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF 139 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIF 445 -d $UNIVERSE
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIF 445 -d $UNIVERSE

# Filtrando todo o trafico de saida que e declarado inseguro ou de alguma
# maquina interna que possa estar infectada com algum cavalo de troia (Trojan).
#
# RPC. Usado para NFS ou outro mecanismo inseguro
#
```

```

/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE sunrpc $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP sunrpc -d $UNIVERSE $LOGGING

# Mountd - Usado para NFS
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 635 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 635 -d $UNIVERSE $LOGGING

# PPTP - Bloco nao autorizado de saida a VPNs
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 1723 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 1723 $LOGGING

# Winsock remoto - Bloqueia maquinas Windows internas de realizar operacoes estranhas.
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 1745 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 1745 $LOGGING

# NFS - Bloqueia NFS devido a falta de seguranca
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 2049 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 2049 -d $UNIVERSE $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 2049 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 2049 -d $UNIVERSE $LOGGING

# Software PcAnywhere - Bloqueia sessoes de saida remota nao autorizadas
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 5631 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 5631 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 5632 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE 5632 $LOGGING

# Xwindows - Bloqueia sessoes Xwindows nao autorizadas ou inseguras
#
# Veja a parte de variaveis acima para intervalo de portas (6000:6007 padrao)
# O X pode usar mais portas que apenas o intervalo de 6000 a 6007.
#
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE $XWINDOWS_PORTS $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE $XWINDOWS_PORTS $LOGGING

# VPNs de IPs seguros - Bloqueia VPNs nao autorizadas
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 500 -d $UNIVERSE/0 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE/0 500 $LOGGING

# MySQL - Bloqueia sessoes nao autorizadas de SQL
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 3306 -d $UNIVERSE/0 $LOGGING

# EggDrop IRC - Bloqueia bots nao autorizados
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 3456 -d $UNIVERSE/0 $LOGGING

# Bloqueia as portas de rede conhecidas para Torjans.
#
# O protocolo TCP/IP pode usar portas altas aleatoriamente. Por isso, o filtro
# abaixo nao garante que voce nao tenha uma maquina interna infectada. Essa lista nao e
# completa mas possui as portas mais comuns.
#
# Consulte http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html
# para uma lista completa.

# NetBus.
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 12345 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE 12346 $LOGGING

# NetBus Pro.
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE/0 20034 $LOGGING

# BackOffice
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE/0 31337 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP -d $UNIVERSE/0 31338 $LOGGING

# Win Crash Trojan.
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE/0 5742 $LOGGING

```

```

# Socket De Troye.
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE/0 30303 $LOGGING

# Cavalo de Troia desconhecido (Master's Paradise [CHR])
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP -d $UNIVERSE/0 40421 $LOGGING

# Trinoo UDP flooder - Essa porta pode mudar com o tempo
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 27665 -d $UNIVERSE/0 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 27444 -d $UNIVERSE/0 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 31335 -d $UNIVERSE/0 $LOGGING

# Shaft distributed flooder - Essa porta pode mudar com o tempo
/sbin/ipchains -A output -j REJECT -i $EXTIF -p tcp -s $EXTIP 20432 -d $UNIVERSE/0 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 18753 -d $UNIVERSE/0 $LOGGING
/sbin/ipchains -A output -j REJECT -i $EXTIF -p udp -s $EXTIP 20433 -d $UNIVERSE/0 $LOGGING

#-----
# Permite todas as portas altas de retornar trafico.
#
echo " - Habilitando todo o trafico de saida REPLY (TCP/UDP) nas portas altas."
/sbin/ipchains -A output -j ACCEPT -p tcp -s $EXTIP $UNPRIVPORTS -d $UNIVERSE
/sbin/ipchains -A output -j ACCEPT -p udp -s $EXTIP $UNPRIVPORTS -d $UNIVERSE

#-----
# Capturar todas as regras
#-----
echo " - Output final, capturar todas as regras."

# Qualquer outro tipo de saida sera negada e logada. Essa regra
# deve capturar tudo inclusive Samba que ainda nao foi bloqueado.
#
/sbin/ipchains -A output -j REJECT -s $UNIVERSE -d $UNIVERSE $LOGGING

*****
# Regras de encaminhamento (Forwarding)
*****
#
echo "-----"
echo "Regras de Forwarding :"

#-----
# Habilita forwarding e masquerading de TCP/IP originario da rede interna
#-----

# Usuarios de Diald :
#
# Essa regra sera necessaria para permitir que a interface SLIP s10
# receba trafico quando estiver subindo a s10.
#
#/sbin/ipchains -A forward -j MASQ -i s10 -s $INTLAN -d $UNIVERSE/0

#-----
# Port Forwarding
#-----
# Port forwarding permite o direcionamento de trafico externo para uma
# maquina interna mascarada. Um uso disso seria usuarios externos
# acessando um servidor web atras de uma mascara.
#
# Para usar PORTFW voce precisa descomentar e editar a seccao $HOSTSEG
# acima.
#
# Consulte o howto de IP-MASQUERADING para detalhes sobre Port Forwarding.
#
# Nao utilizar portas maiores que 1023 para redirecionamento.
#
#-----
#echo " Habilitando Port Forwarding nos hosts internos."
#/usr/sbin/ipmasqadm portfw -f

```

```

#echo " Redirecionando trafico SSH na porta 26 para $PORTFWIP1"
#/usr/sbin/ipmasqadm portfw -a -P tcp -L $EXTIP 26 -R $PORTFWIP1 22
#
#echo " Redirecionando trafico SSH na porta 26 para $PORTFWIP2"
#/usr/sbin/ipmasqadm portfw -a -P tcp -L $EXTIP 26 -R $PORTFWIP2 22
#
#echo " Redirecionando trafico SSH na porta 26 para $PORTFWIP3"
#/usr/sbin/ipmasqadm portfw -a -P tcp -L $EXTIP 26 -R $PORTFWIP3 22

#-----
# Habilita forwarding e masquerading TCP/IP a partir da rede interna
#-----

# Habilita IP Forwarding no kernel do Linux
#
# Existem dois metodos para habilitar essa opcao. O primeiro e editar
# o arquivo /etc/sysconfig/network e alterar a linha FORWARD_IPV4 para
# FORWARD_IPV4=true
#
# O segundo pode ser executado a qualquer momento.
# Basta alterar o arquivo /proc/sys/net/ipv4/ip_forward atraves
# do comando abaixo
#
echo " - Habilitando IP forwarding."
echo "1" > /proc/sys/net/ipv4/ip_forward

# Masquerade da rede interna 1 na interface local para internet.
#
echo " - Habilitando IP Masquerading na rede interna 1 para internet."
/sbin/ipchains -A forward -j MASQ -i $EXTIF -s $INTLAN -d $UNIVERSE

# Masquerade da rede interna 2 na interface local para internet.
#
echo " - Habilitando IP Masquerading na rede interna 2 para internet."
/sbin/ipchains -A forward -j MASQ -i $EXTIF -s $INTLAN2 -d $UNIVERSE

# Masquerading da Rede interna 1 para a Rede interna 2
#
echo " Habilitando IP Masquerading da Rede Interna 1 para a Rede Interna 2"
/sbin/ipchains -A forward -j MASQ -i $INTLAN2 -s $INTLAN -d $INTLAN2

# Masquerading da Rede interna 2 para a Rede interna 1
#
echo " Habilitando IP Masquerading da Rede Interna 2 para a Rede Interna 1"
/sbin/ipchains -A forward -j MASQ -i $INTLAN -s $INTLAN2 -d $INTLAN

# Habilitando "Always Defrag" para sistemas Masqueraded
#
echo " - Habilitando IP Always Defrag para a rede interna."
echo "1" > /proc/sys/net/ipv4/ip_always_defrag

# Desabilitando o patch LooseUDP que alguns jogos via internet usam.
#
#
echo " - Desabilitando o patch LooseUDP por seguranca."
echo "0" > /proc/sys/net/ipv4/ip_masq_udp_dloose

# Capturar todas as regras, qualquer outro tipo de forwarding e negado.
#
/sbin/ipchains -A forward -j REJECT -s $UNIVERSE -d $UNIVERSE $LOGGING

# Final
#
echo "-----"
echo -e "IPCHAINS Firewall $VERSAO $ULTALT implementado.\n\n"

```

5.1 Alterando os atributos do script

O script rc.firewall acima deve ser copiado para /etc/rc.d/. Torne o script executável apenas pelo root com o comando "chmod 700 /etc/rc.d/rc.firewall".

5.2 Criando o script de inicialização do firewall.

Criaremos agora o script /etc/rc.d/init.d/firewall (tabela 5.2) para inicializar o /etc/rc.d/rc.firewall.

tabela 5.1 – script de inicialização /etc/rc.d/init.d/firewall

```
#!/bin/sh
#
# chkconfig: 2345 11 89
#
# description: Carrega o rc.firewall.
#
# processname: firewall
# pidfile: /var/run/firewall.pid
# config: /etc/rc.d/rc.firewall
# probe: true

# -----
# # IpChains Firewall
# versao 1.02
#
# carrega o script /etc/rc.d/rc.firewall
#
# Esse script "firewall" deve ser colocado no diretorio /etc/rc.d/init.d
# - Alterar seus atributos comando "chmod 700 firewall"
# - Criar os scripts S11Firewall e K89Firewall nos run levels 345
# Comandos :
#         chkconfig --add firewall
#         chkconfig --level 345 firewall on
#
# obs : o script rc.firewall deve ter seus atributos alterados pelo comando
#       "chmod 700 rc.firewall" dentro do diretorio /etc/rc.d/
#
# -----

# biblioteca Source function.
. /etc/rc.d/init.d/functions

# Verificar se a rede esta rodando.

# Essa linha nao funciona mais com o bash2
#[ ${NETWORKING} = "no" ] && exit 0
#
# [ "XXXX${NETWORKING}" = "XXXXno" ] && exit 0

# [ -x /sbin/ifconfig ] || exit 0

# Menu de opcoes :
case "$1" in
start)
    /etc/rc.d/rc.firewall
    ;;
stop)
    echo -e "\nDescartando firewall e configurando politicas padrao para ACCEPT\n"
    /sbin/ipchains -P input REJECT
    /sbin/ipchains -P output REJECT
    /sbin/ipchains -P forward REJECT

    /sbin/ipchains -F input
    /sbin/ipchains -F output
    /sbin/ipchains -F forward
    ;;
restart)
```

```

    $0 stop
    $0 start
    ;;
status)
    /sbin/ipchains -L
    ;;
*)
    echo "Sintaxe : firewall {start|stop|status}"
    exit 1
esac
exit 0

```

5.3 Inserindo o script /etc/rc.d/init.d/firewall na inicialização

Primeiramente, torne o script executável com o comando "chmod 700 /etc/rc.d/init.d/firewall". Agora, vamos criar os links de inicialização S11firewall e K89firewall nos run levels 345 com o chkconfig.

Para criar os links entre com os comandos :

```
"chkconfig --add firewall"
```

```
"chkconfig --level 345 on"
```

Obs : Caso precise desabilitar o firewall no boot, utilize o ntsysv. Para remover os links use o comando "chkconfig --del firewall".

5.4 Rodando o firewall

Rode o firewall com o comando "/etc/rc.d/init.d/firewall start". Diversas mensagens serão ecoadas pelo script rc.firewall (veja linhas que começam com echo). Na inicialização do sistema, no entanto, você não verá essas mensagens.

Obs : Para parar o seu firewall use "/etc/rc.d/init.d/firewall stop".

5.5 Para usuários do Slackware

Faça o procedimento de 5.1 deixando o script rc.firewall executável. Depois insira a seguinte linha ao final do script /etc/rc.d/rc.local :

```
/etc/rc.d/rc.firewall
```

Dessa forma, o script irá rodar toda a vez que o seu Slack for inicializado. Note que a forma de inicializar um máquina Slackware difere de sistemas como Red Hat, Mandrake, Conectiva, etc.

6.0 Medindo a velocidade do seu acesso

6.1 Considerações técnicas

Lembre-se: ao obter um ADSL de 256Kbps, sua velocidade de recepção não será necessariamente de 256Kbps. Será 256 com a sua operadora mas o que vale mesmo é a velocidade do seu provedor com a internet e a quantidade de usuários plugados naquele momento. Além disso, é necessário levar em conta o fator de

networking overhead que pode acarretar uma perda de 20%, dependendo da qualidade e arquitetura de rede do seu provedor. Considerando uma velocidade de 256Kbps, a média seria algo em torno de 205Kbps. Sua velocidade máxima, portanto, passa a ser medida a partir do gateway do seu provedor e não a partir do seu Firewall Linux.

Você notará que, em muitos casos, a velocidade com um determinado site fora do Brasil é bem menor do que com outro. Deve-se considerar também a relação (quantidade de tráfego / capacidade do link) do site acessado. Um exemplo, seria tentar fazer o download de uma ISO do Red Hat pelo ftp server da própria Red Hat e pelo ftp server da FreeSoftware. A última opção sempre tem sido mais veloz na nossa experiência prática. A quantidade de hops de roteamento até determinado host na internet é ainda outro fator a ser considerado. Lembre-se: quanto menos hops de roteamento, maior a velocidade no tráfego de pacotes entre dois hosts.

Para medir a velocidade entre o seu Firewall e seu provedor, verifique se o seu provedor possui um servidor FTP e tente fazer o download de algo cujo tamanho seja considerável, em torno de 10 megas, por exemplo. Existem vários sites na internet que medem a sua velocidade, mas na prática o ideal é fazê-lo você mesmo porque essas medições são muito relativas e dependem de diversas variáveis.

6.2 Técnica sugerida

Para medir sua velocidade, faça um download via FTP pela linha de comando do seu Firewall Linux. Após a conclusão do download, divida a quantidade de bytes do arquivo baixado pelo tempo da operação em mili-segundos.

7.0 Configurando os Hosts da sua rede

Esta seção descreve como configurar seus Hosts Windows 9X, Windows NT e Linux.

7.1 Configurando Hosts Linux.

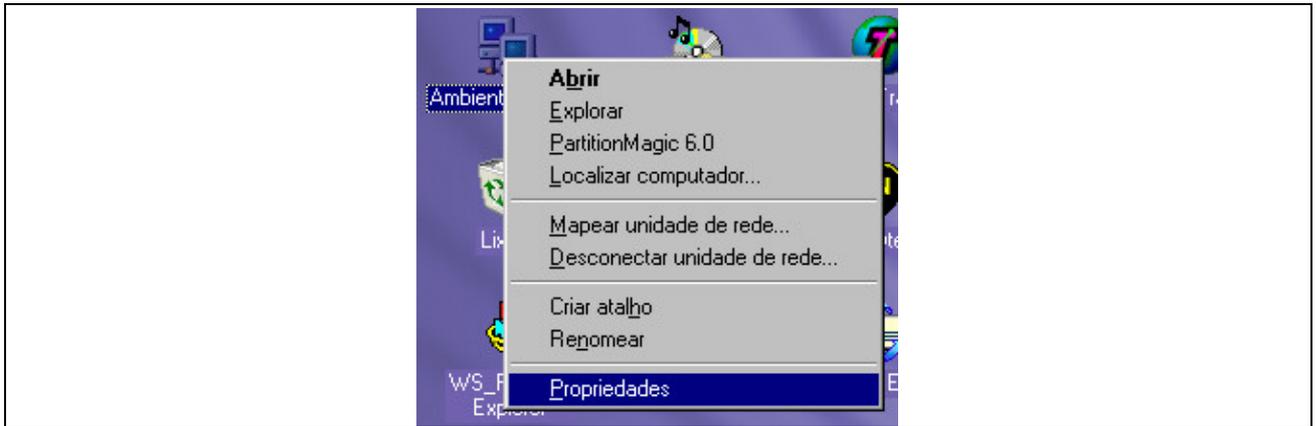
Seguindo o nosso exemplo, configure um desktop Linux na rede 2 (192.168.2.0/24) cujo IP é 192.168.2.11. Para esse host, o gateway será o IP da eth2 do Firewall Linux, ou seja, 192.168.2.20. Siga os mesmos procedimentos descritos em 4.2 editando o arquivo /etc/sysconfig/network-scripts/ifcfg-eth0, /etc/sysconfig/network e /etc/resolv.conf, cujos endereços dos DNS servers serão os mesmos.

7.2 Configurando Hosts Windows 95/98.

Um hosts Windows 98 na rede 2 de IP 192.168.2.12 terá como gateway o IP da eth2 do Firewall Linux que é 192.168.2.20. Os endereços dos DNS servers serão os do seu provedor conforme o arquivo /etc/resolv.conf.

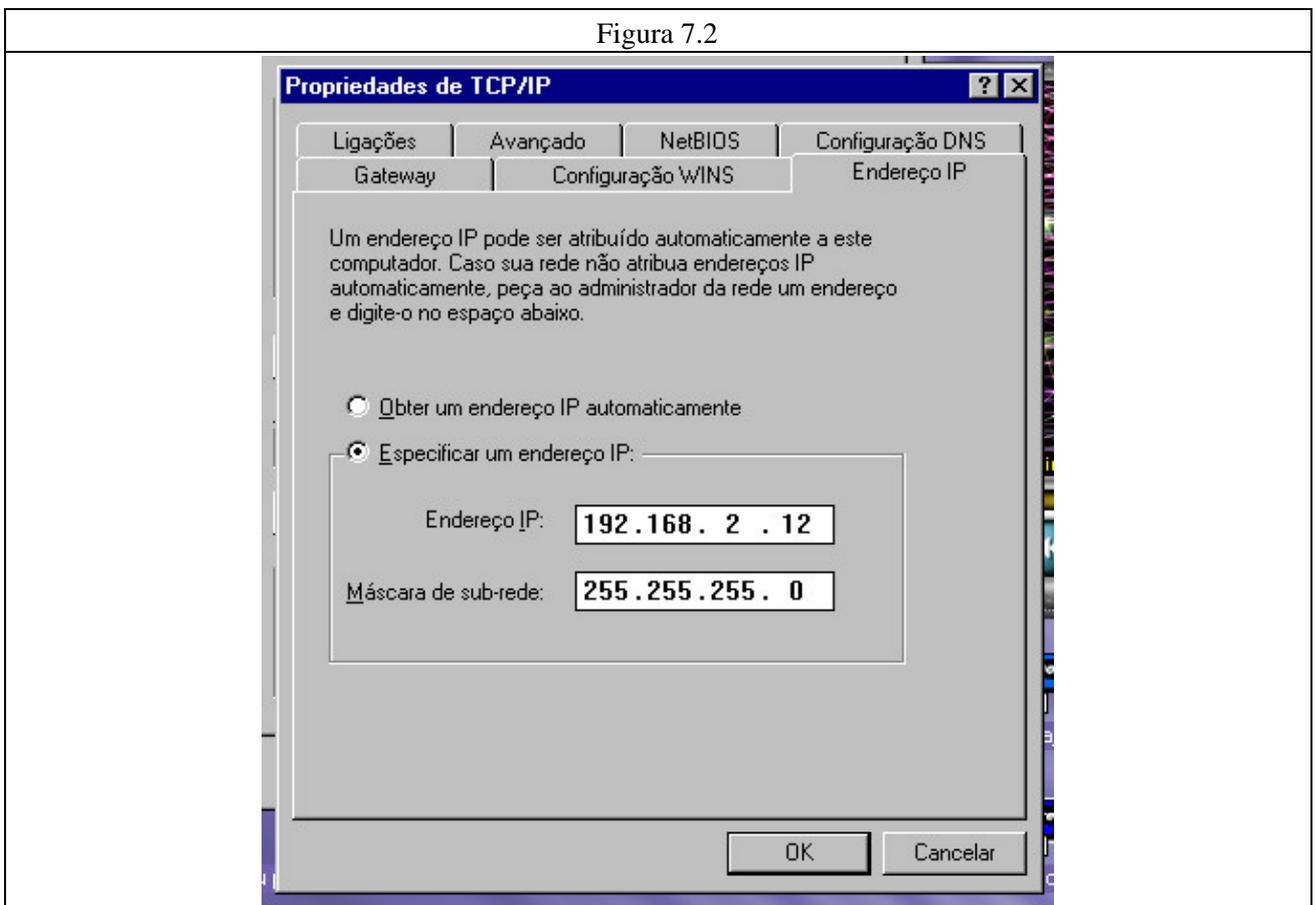
Clique com o botão direito do Mouse no ícone Ambiente de Rede e selecione propriedades. (figura 7.1)

Figura 7.1



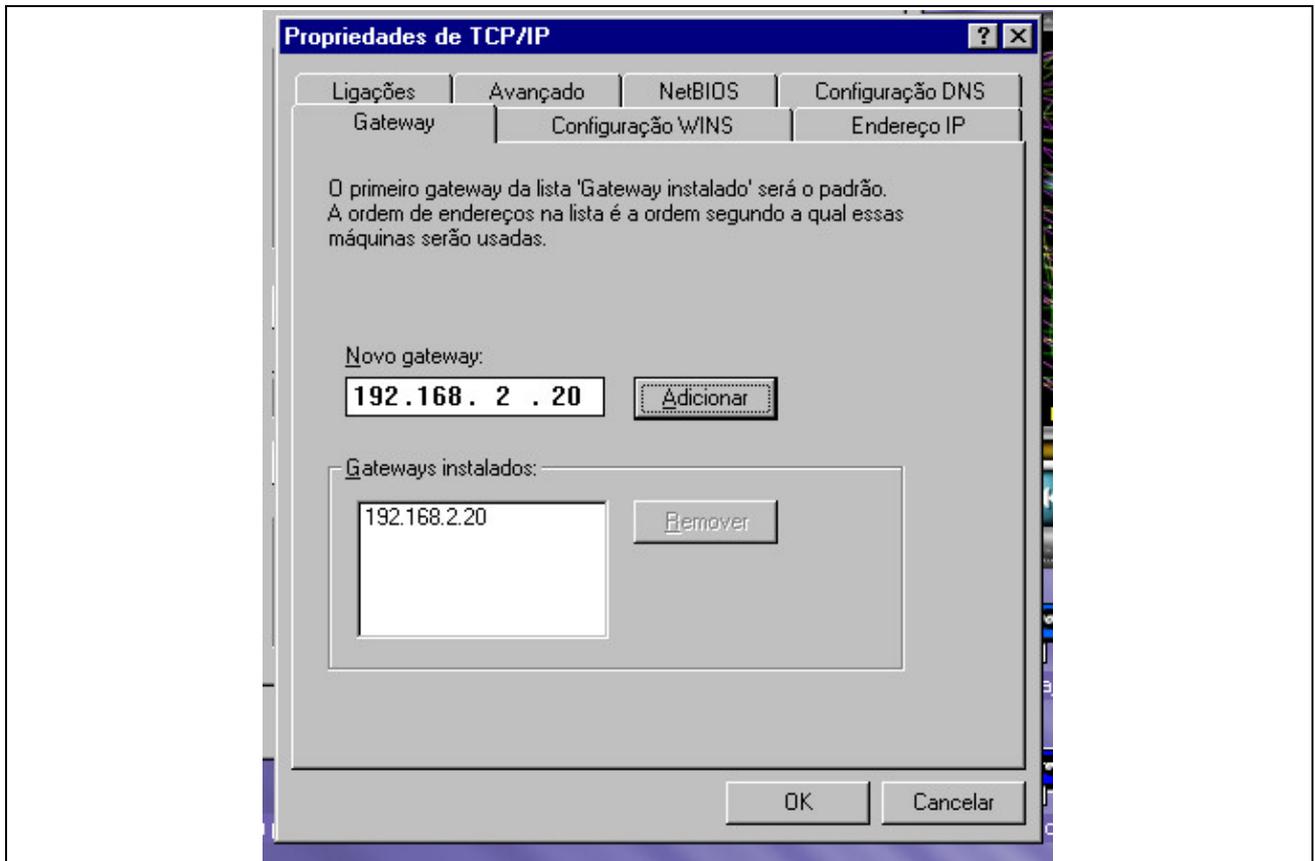
Selecione o protocolo TCP/IP da lista de componentes e entre o IP do host e sua subnet conforme figura 7.2

Figura 7.2



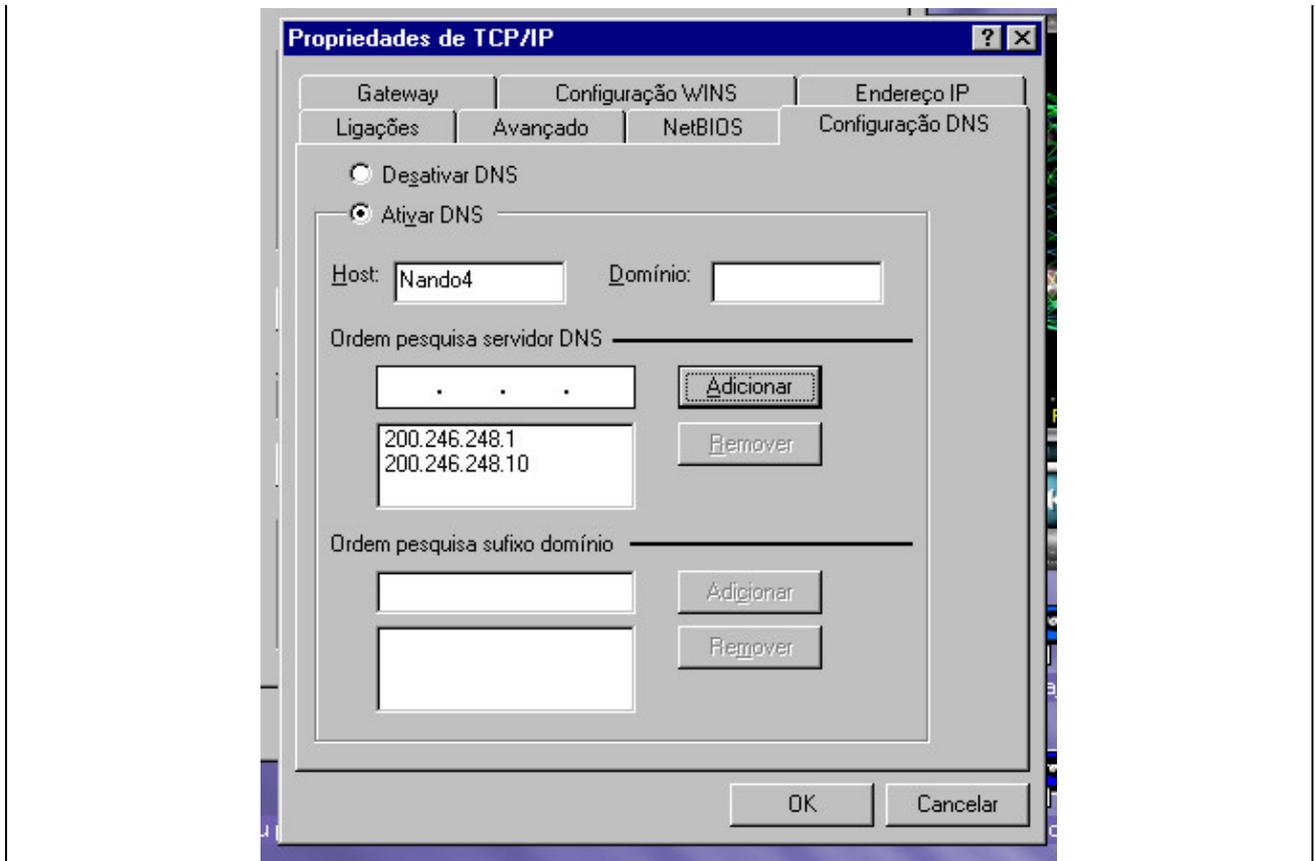
Selecione a pasta Gateway (Figura 7.3) e entre com o IP da eth2 do Firewall.

Figura 7.3



Entre com os IPs dos DNS do seu provedor (figura 7.4) na pasta Configuração DNS.

Figura 7.4

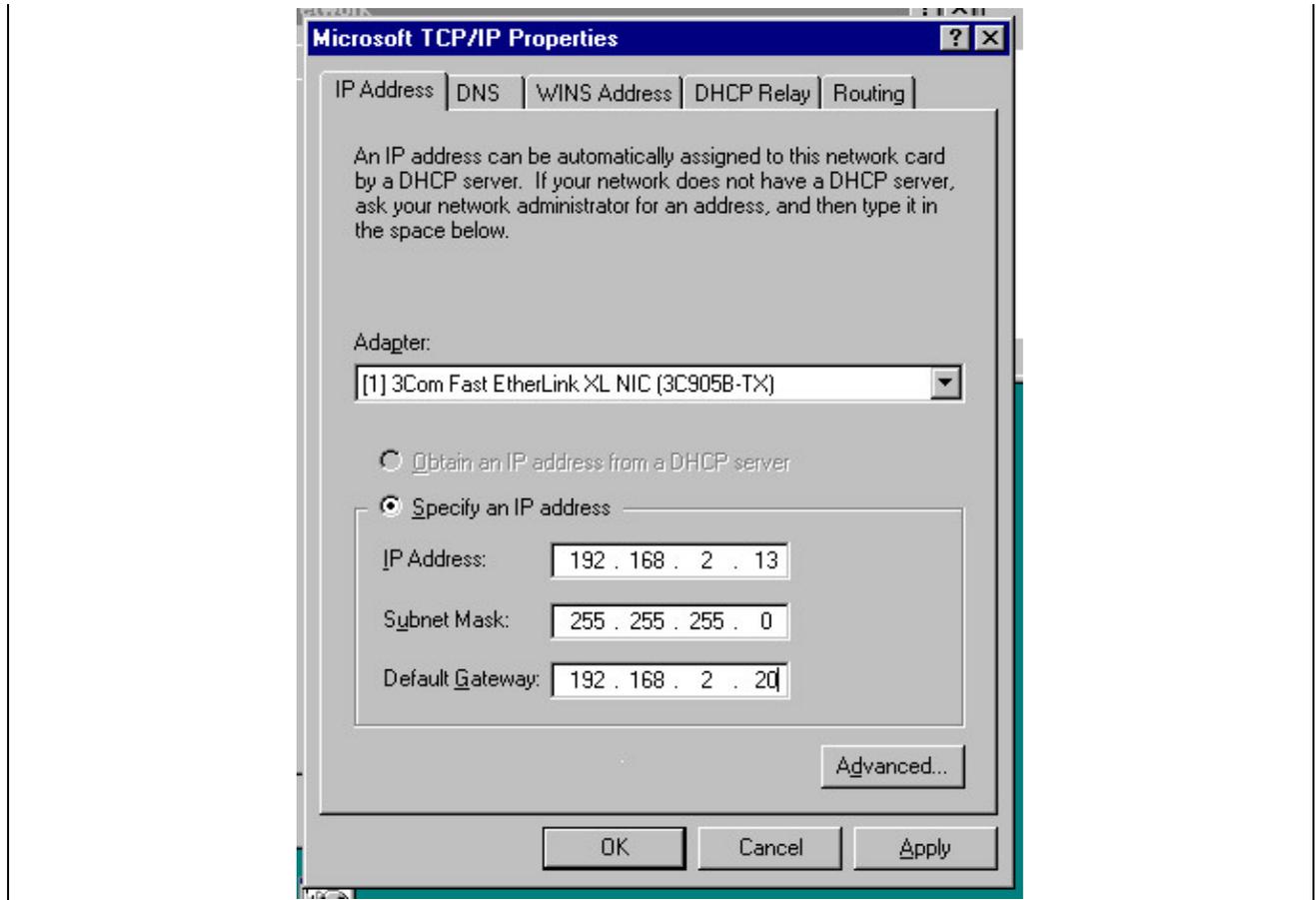


Clique em OK. Você será notificado pelo seu Host Windows que será necessário rebotar a máquina.

7.3 Configurando Hosts Windows NT

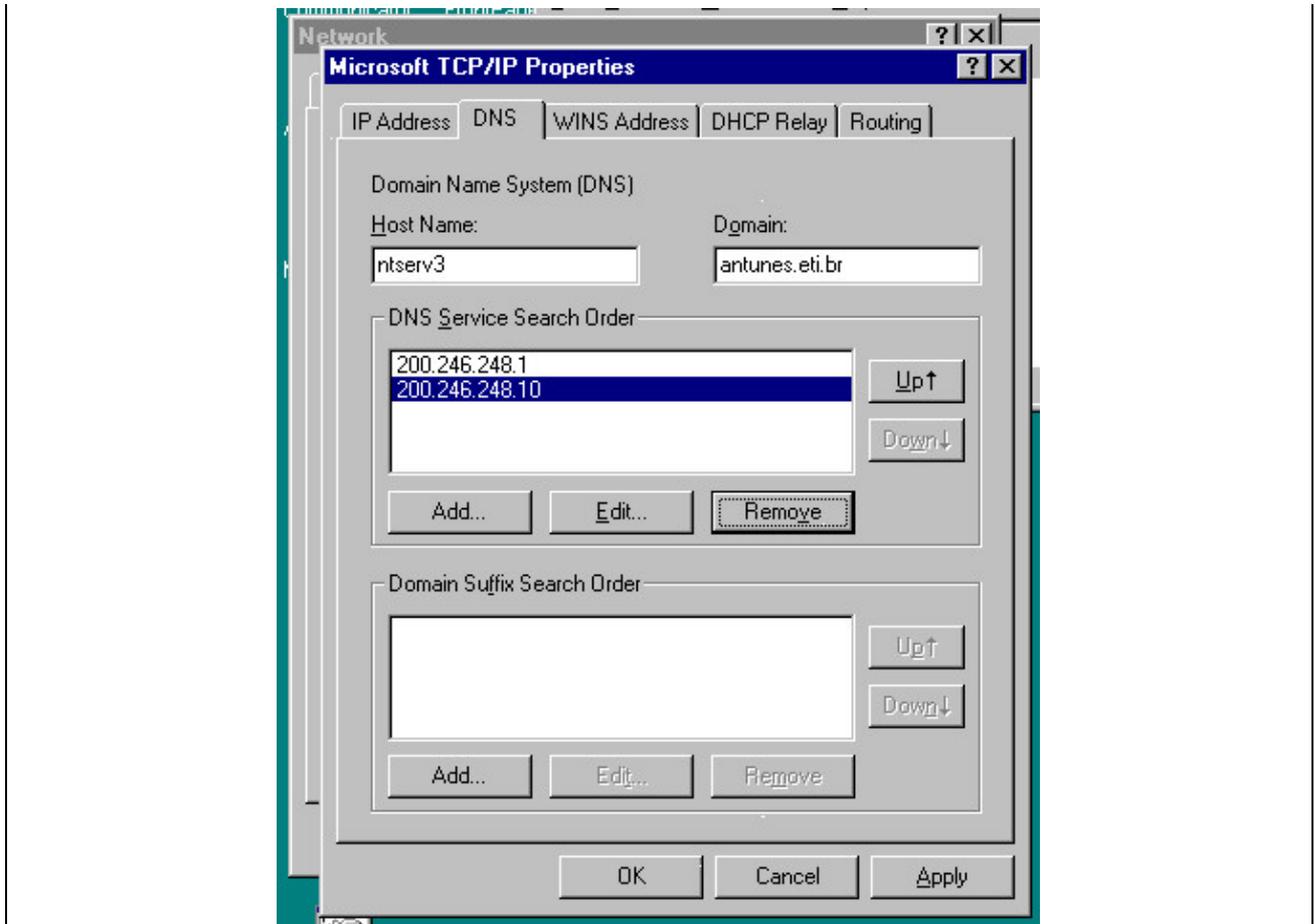
Clique sobre o ícone Network Neighborhood com o botão direito e selecione properties. Selecione a tab Protocols. Selecione o protocolo TCP/IP e clique no botão Properties. Selecione o adaptador desejado, digite o endereço IP, a Subnet e o Default Gateway (figura 7.5).

Figura 7.5



Clique no tab DNS e digite os endereços de DNS do seu provedor (figura 7.6).

Figura 7.6



Clique no botão Apply, clique em OK. O NT irá avisar que precisa rebootar a máquina.

8.0 Sugestões

8.1 Cable Modem

Para configurar a mesma solução, mas utilizando um cable modem, verifique os comentários inclusos no script `rc.firewall`. Note que os provedores de cable modem costumam alterar o IP do seu modem pelo menos 1 vez ao dia.

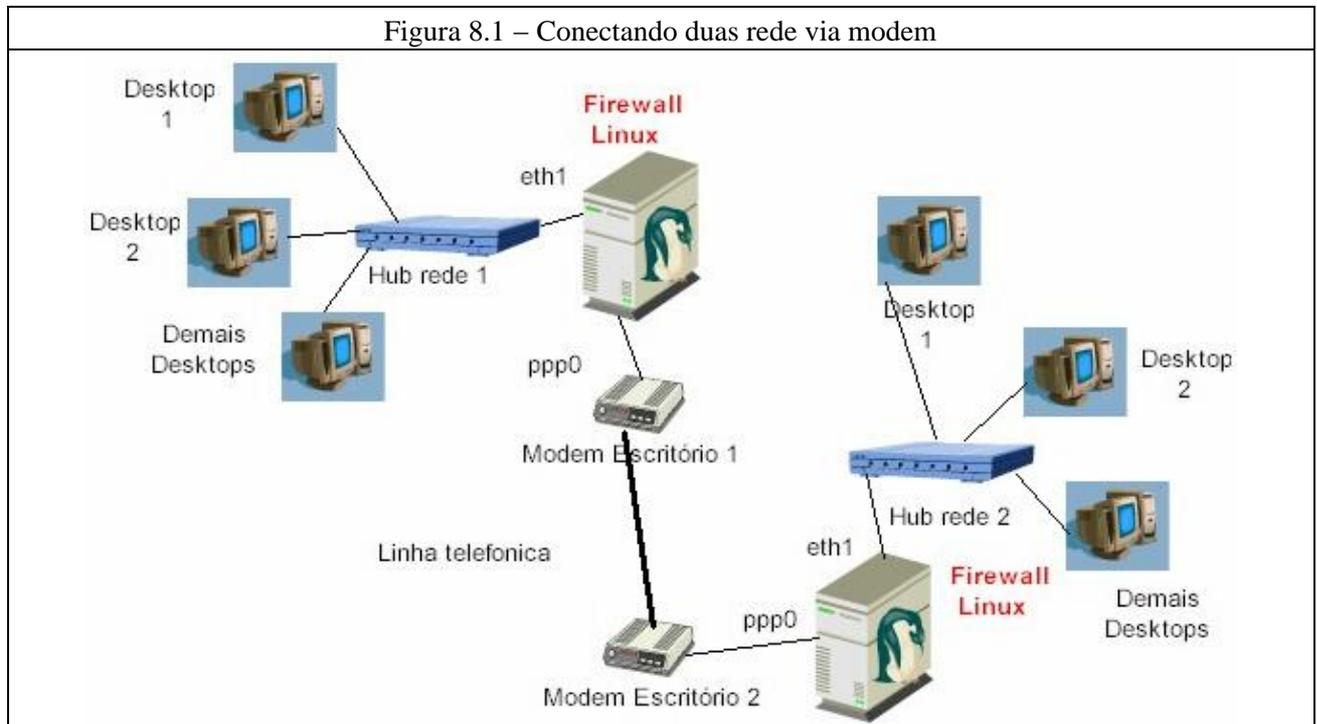
8.2 Modem comum sob linha telefônica

Para modems comuns, observe os comentários no `rc.firewall`. A interface externa passa a ser a `ppp0` e não mais `eth0`. Cada vez que conectar, seu provedor lhe fornecerá um IP diferente, veja os dados no script. Você poderá também utilizar o `Dial on Demand` ou `Diald`. Verifique o manual desse software para saber mais.

8.3 Outros tipos de aplicações

Independentemente de conectar a sua rede na internet, você pode utilizar os conceitos de firewall, gateway e routing que propomos neste artigo para apenas conectar a rede de dois escritórios separados via modem. Para isso, seria necessário possuir um Firewall Linux, nos dois lados, equipado com modem e que a sua rede interna, nos dois lados rode, TCP/IP. Estude com critério os comentários e a referência rápida sobre IPChains.

Essa situação está ilustrada na figura 8.1 a seguir:



9.0 Informações adicionais

9.1 Leitura Recomendada

Para saber mais sobre IPChains e Firewall recomendo :

Linux Firewalls, Robert L. Ziegler
New Riders, ISBN 0-7357-0900-9

Pode ser adquirido nas seguintes empresas :

www.livrariacultura.com.br

(que possui comentários de minha autoria),

www.temporeal.com.br

www.amazon.com.

9.2 Como contatar o autor e obter os scripts gratuitamente.

O autor pode ser contatado através do endereço nando@antunes.eti.br e fica à disposição para enviar os arquivos dos scripts apresentados neste artigo por e-mail. Ao requisitar os scripts, pede-se a gentileza de enviar seu nome completo, empresa em que atua, ramo de negócios e cargo que ocupa. Sugestões e comentários serão apreciados.

10.0 Sobre o autor



Sobre o Autor

Carlos Fernando Scheidecker Antunes teve sua educação e formação profissional no Brasil e nos EUA.

Trabalha com computadores desde 1984 e conheceu o Linux em 1995 quando estava em Utah.

Fundou em 1991, com seu pai Carlos Jorge Freire Antunes, a empresa Sistema SEN que é um ASP especializado em soluções internet para empresas.

Atualmente, trabalha também como consultor técnico do Peças on Line (www.pecas-on-line.com.br) e está de mudança para Salt Lake City, UT onde estenderá seus estudos em [The University of Utah](http://www.theuniversityofutah.edu).

Entre as atividades preferidas, está sua corrida diária de 8 Km, indispensável para quem trabalha num ritmo que chega a 18 horas diárias.

11.0 Sistema S.E.N.

O Sistema S.E.N. é um ASP (Application Service Provider) especializado em soluções internet. ASP é uma empresa que oferece acesso ou customiza aplicativos e serviços internet específicos, que de outra forma, teriam que ser desenvolvidos pelo próprio cliente. O Sistema S.E.N. traz a vantagem de que seus clientes não precisam investir em desenvolvimento, máquinas, infra-estrutura, mão-de-obra especializada e manutenção para que seus projetos rodem na internet. Basta possuir acesso à internet!

Se sua empresa é pequena, média ou um conglomerado multinacional, existem diversos pontos a considerar. O primeiro é o tempo para poder colocar um projeto em prática, o segundo é o custo e o terceiro é a funcionalidade. No Sistema S.E.N., as empresas podem implantar seus projetos rapidamente, sem precisar alterar sua estrutura ou adquirir softwares caros para migrar seus sistemas internos a fim de estarem compatíveis com a solução e-business desejada. Além disso, todo o gerenciamento e acompanhamento é fornecido pelo Sistema S.E.N.. Esse modelo de negócio está obtendo enorme sucesso nos EUA e tem sido muito proveitoso para os clientes da empresa nos últimos 11 anos em que atua no mercado. Por tudo isso os

proprietários de empresas ou altos executivos têm-se perguntado : "Com o advento da Internet, não seria mais interessante e efetivo empregar nossos esforços no nosso próprio negócio, em vez de contratar pessoal especializado, comprar tecnologia e desenvolver uma solução própria?". O Sistema S.E.N. irá ajudá-lo a fazer tudo o que você precisa mais rapidamente, a um custo menor e com mais segurança do que se fosse feito "*in house*". Os clientes do Sistema S.E.N. gastam suas energias melhorando seu próprio negócio, enquanto o e-business de suas empresas fica por nossa conta. Com nossa ajuda, sua empresa ficará totalmente concentrada no que faz melhor : o seu negócio. Enxuge sua empresa e consulte-nos sobre como podemos ajudá-lo.

O Sistema S.E.N. foi fundado em 1991, tendo sido pioneiro no Brasil ao implementar soluções e-business especialmente nas áreas comerciais, suporte a clientes, assistência técnica e pós-vendas de diversas empresas. O endereço de e-mail para contato é info@sistema-sen.com.br.

12.0 Links

- Peças on Line – Site gratuito para comercialização de autopeças www.pecas-on-line.com.br
- The University of Utah www.utah.edu fundada há 150 anos, é uma das pioneiras em Internet ao lado de Stanford e Berkley. Local de profissionais como Jim Clark (SGI e Netscape), David Evans (Evans & Sutherland), John Warnock (Adobe Systems), Nolan Bushnell (Atari), etc. A University of Utah foi um dos 4 primeiros nodes da Internet (ARPANET) em 1969 junto com Stanford, Berkley, UCLA. De lá saíram diversas empresas famosas na área. Está localizada a 50 minutos de Silicon Valley por avião.
- O estado de Utah www.utah.com capital Salt lake City. Conheça o estado que será sede das Olimpíadas de 2002 (Winter Games). Um lugar de qualidade de vida sem igual, ideal para esportes e turismo. Local histórico de recordes de velocidade na planície do grande lago salgado em Boneville, Salt Flats. O verdadeiro velho oeste americano.
- Red Hat Linux – Distribuição Linux utilizada neste artigo www.redhat.com ou servidor FTP (geralmente ocupado) [ftp.redhat.com](ftp://ftp.redhat.com) existem outros servidores espalhados no mundo inteiro.
- Free Software FTP server – Servidor de alta capacidade para download de ISOs e aplicativos Linux. ftp.freesoftware.com
- Ute Linux Timpanogas – Distribuição Linux de boa qualidade www.timpanogas.com. Essa empresa foi fundada por ex-profissionais da Novell em Utah e hoje dedica-se a criar sistema Linux/Novell.
- SlackWare Linux Project – Um pioneiro é distribuído gratuitamente www.slackware.com na internet ou encontra-se à venda no site www.cdrom.com ou na Livraria Tempo Real (abaixo).
- Conectiva Linux – Distribuição Linux Brasileira que oferece suporte e pacotes específicos www.conectiva.com.br
- The Linux Home Page – www.linux.org
- Efficient Networks – Fabricante de modems ADSL www.efficientnetworks.com
- Cyclades – Fabricante de hardware para conectividade de redes e internet www.cyclades.com.br
- CheapBytes – Site que vende CDs prontos de várias distribuições www.cheapbytes.com
- LinuxMall (Brasil) – Site que vende CDs prontos www.linuxmall.com.br
- Livraria Tempo Real – Revendedor de diversas distribuições Linux como SuSe, Slackware, Yellow Dog, etc. www.temporeal.com.br
- Livraria Cultura – www.livrariacultura.com.br
- RIO MP3 Player da Diamond – www.diamondmm.com Device que roda Linux.

13.0 Como obter e apreender mais sobre Linux

Linux é distribuído em CDs por diversas empresas (Red Hat, Conectiva, Timpanogas, Caldera, SuSe, Slackware, etc) que além do kernel incluem vários aplicativos como servidores de e-mail, http, servidores gráficos, etc.

Geralmente, as distribuidoras põem à disposição as imagens de seus CDs em arquivos ISO através de seus próprios servidores FTP ou espalhados em vários outros servidores na internet. As empresas distribuidoras, além de fornecer gratuitamente a imagem dos CDs para download, vendem pacotes prontos com CDs, manuais e contrato de suporte. Além disso, revistas distribuem CDs, e sites vendem CDs já gravados por valores muito pequenos.

Existem diversos manuais sobre Linux na internet, assim como revistas impressas e via internet, diversos livros publicados além das distribuidoras que fornecem suporte. Há também escolas homologadas pelas empresas distribuidoras que ministram cursos variados sobre Linux.

Existem dois livros em português que pude avaliar para poder indicar. Os dois são básicos, de baixo custo e muito interessantes para quem precisa apreender Linux.

– Linux Administração e suporte, editora Novatec, autor Chuck V. Tibet e ISBN 85–85184–95–7

– Dominando 110% Intranet em Ambiente Linux, editora Brasport, autor Antonio Marcelo e ISBN 85–74520–47–0

Ambos podem ser adquiridos online na www.temporeal.com.br

14.0 O que é Linux

Linux é um sistema operacional que foi criado inicialmente como hobby por um estudante finlandês chamado Linus Torvalds enquanto estava na Universidade de Helsinki, na Finlândia. Linux é um sistema no padrão POSIX/UNIX de alta qualidade que é desenvolvido e mantido constantemente por milhares de programadores em todo o mundo. Empresas e organizações como a Shell, Boeing, Toyota, NASA, governo americano, NSA, governos espalhados no mundo, etc. utilizam largamente Linux pela sua alta qualidade e estabilidade. A NASA possui um grande interesse no Linux e tem a maioria de seus técnicos em informática linuxers de carteirinha. Um curiosidade é a uso do Linux nos computadores de bordo do onibus espacial, projeto conhecido como Flying Linux. O Sr Torvalds começou a trabalhar no Linux em 1991 e hoje o kernel do sistema encontra-se na versão 2.4.x sendo constantemente revisto e ampliado. Linux foi desenvolvido sob a licença GNU–GPL (veja www.gnu.org) cujo código fonte é livremente acessível para qualquer pessoa. Porém, isso não significa que as distribuições Linux sejam gratuitas. As empresas que distribuem Linux agregam valor incluindo softwares, manuais e suporte ao produto. Linux roda em diversos equipamentos e plataformas, desde servidores SUN, Intel, Alpha, PowerPC (Mac), etc. até pequenos players MP3, como o RIO da Diamond (que utilizo em minhas corridas diárias). A utilização do Linux em pequenos devices, gadgets e computadores é denominada embedded system e existem várias empresas especializadas apenas nisso. Atualmente com a crise de energia americana, muitas empresas estão adotando Linux pela vantagem de ser um sistema operacional que gasta menos energia. Como se não bastassem as demais vantagens que já conhecemos.

15.0 Agradecimentos

Gostaria de agradecer a prof. Maria Helena Bruna e minha mãe Natália Maria Scheidecker Antunes pela revisão desse texto. Gostaria também de agradecer os diversos e-mails que temos recebido dos leitores satisfeitos. Acreditem, isso é que realmente impulsiona um trabalho como esse.