Segurança e Otimização do Red Hat Linux

Um guia para sistemas de informação, configuração, otimização e para profissionais de segurança de rede

VOLUME 1

Título original:	**Securing and Optimizing Red Hat Linux**
Autor:	Gerhard Mourani
Email:	gmourani@videotron.ca
Versão:	1.2
Última revisão:	25 de março de 2000

Traduzido e adaptado por:	Edinaldo J.C. La-Roque / StarLink Conectividade Ltda.
Site:	www.conectividade.com.br
Email:	starlink@conectividade.com.br
Versão:	1.0
Última revisão:	05 de janeiro de 2001

Nota do Tradutor:

Este volume é a tradução parcial do livro **Securing and Optimizing Red Hat Linux** de Gerhard Mourani <gmourani@videotron.ca>.

Abaixo, uma tabela de referência cruzada entre esta tradução e o original:

Esta Tradução Parcial		Original	
Capítulo 1	Introdução ao Linux	Chapter 1	Introduction to Linux
Capítulo 2	Instalação do seu Servidor Linux	Chapter 2	Installation of your Linux Server
Capítulo 3	Segurança Geral do Sistema	Chapter 3	General System Optimization
Capítulo 4	Firewall de Rede	Chapter 7	Networking Firewall
Capítulo 5	Gerenciamento da Rede TCP/IP	Chapter 6	TCP/IP Network Management
Capítulo 6	Firewall de Rede com Suporte a Macaramento e Repasse	Chapter 8	Networking Firewall with Masquerading and Forwarding Support

O livro original contém 21 capítulos e esta tradução contém apenas 6.

Este material é usado na **StarLink Conectividade Ltda** como parte do material didático do curso:

LINUX - SEGURANÇA EM REDES TCP/IP (MÓDULO I)

Este material está disponível para download e livre distribuição, conforme autorizado por Gerhard Mourani, autor do original, a partir do site:

http://www.conectividade.com.br/download

Comentários, sugestões e apoio sobre esta tradução podem ser encaminhados para:

Edinaldo J. C. de La-Roque / StarLink Conectividade Ltda.
Av. Nazaré, 532 - salas 407/516
66.035-170 Belém PA

Email: starlink@conectividade.com.br
Site: www.conectividade.com.br

Índice

1. Introdução ao Linux

2. Instalação do seu servidor Linux

3. Segurança Geral do Sistema

4. Firewall de Rede

5. Gerenciamento da Rede TCP/IP

6. Firewall de Rede com Suporte a Mascaramento e Repasse

CAPÍTULO 1

Introdução ao Linux

Introdução

Quando eu comecei, a primeira pergunta que fiz a mim mesmo foi: Como instalar um servidor Linux e estar certo de que ninguém, nem de fora nem de dentro, possa acessá-lo sem permissão? Depois, fiquei imaginando se existia algum método similar ao do Windows para melhorar a performance do computador. Em seguida, iniciei uma pesquisa pela Internet e li vários livros para obter o máximo de informações sobre segurança e performance para o meu servidor. Após vários anos de pesquisas e estudos, finalmente descobri as respostas para as minhas perguntas. Todas essas respostas foram encontradas através de diferentes documentos, livros, artigos e sites pela Internet. Então, criei uma documentação, com base em minhas pesquisas, que pudesse me ajudar em minhas tarefas diárias. Através dos anos, esta documentação ficou maior e começou a se parecer mais com um livro do que com simples anotações dispersas. Decidi publicá-la na Internet para que qualquer um pudesse se beneficiar dela. Ao compartilhar essas informações, fiz minha parte na comunidade Linux, comunidade essa que tem respondido a várias de minhas necessidades computacionais com um sistema operacional mágico, confiável, robusto, poderoso, rápido e livre chamado Linux. Tive muito feedback, bem como, comentários sobre minha documentação, o que ajudou a melhorá-la. Também, acho que muitas pessoas gostariam de vê-la publicada por causa de seu conteúdo, para que possam aproveitar suas vantagens e ver o poder deste bonito sistema, que é o Linux, em ação.

Foram necessários muito tempo e esforço para criar este livro e assegurar que os resultados fossem os mais precisos possíveis. Se você encontrar quaisquer anormalidades ou resultados inconsistentes, erros, omissões ou qualquer coisa que não pareça certo, por favor mantenha-me informado para que eu possa investigar o problema e corrigir o erro. Sugestões para versões futuras também são bem-vindas e apreciadas.

Público-Alvo

Este livro é voltado para um público técnico e para administradores de sistemas que gerenciam servidores Linux, mas também inclui material para usuários domésticos e outros. Ele fala sobre como instalar e configurar um Servidor Red Hat Linux com toda a segurança e otimização necessárias para uma máquina específica Linux com alta performance. Já que estamos falando de configuração de segurança e otimização, usaremos uma distribuição de programas em código-fonte (tar.gz) sempre que possível, especialmente para softwares críticos de servidor como o Apache, o BIND/DNS, o Samba, o Squid, o OpenSSL, etc. O código-fonte nos dará atualização rápida dos bugs de segurança quando necessário, além de melhor compilação, personalização e otimização para nossas máquinas específicas, o que não se pode obter com pacotes RPM.

Estas instruções de instalação assumem

Que você tem um drive de CD-ROM em seu computador e o CD-ROM Oficial do Red Hat Linux. As instalações foram testadas no Red Hat Linux Oficial, versão 6.1.

Você precisa compreender o sistema de hardware no qual o sistema operacional será instalado. Após examinar o hardware, o restante deste documento guiará você, passo-a-passo, através do processo de instalação.

Sobre os produtos mencionados neste livro

Vários produtos serão mencionados neste livro – alguns comerciais, a maioria não-comercial com custo zero e que pode ser livremente usado e distribuído. Também, é importante dizer que não sou associado a nenhum deles e se menciono uma ferramenta é porque ela é útil. Você descobrirá que muitas empresas grandes utilizam a maioria dessas ferramentas em seu dia-a-dia.

Obtendo o livro e arquivos de exemplos de configuração

O livro Segurança e Otimização do Red Hat Linux agora está também disponível para download a partir da maioria dos sites web Linux populares. Versões com formatos livres deste livro podem ser encontradas na Internet através dos seguintes endereços listados abaixo:

- Do site web original (Open Network Architecture): http://pages.infinit.net/lotus1/
- Da homepage do The Linux Documentation Project : http://www.linuxdoc.org/docs.html#guide
- Da rede da O'Reilly: http://www.oreillynet.com/pub/t/20
- Do TuneLinux.COM: http://tunelinux.com/bin/page?general/optimization/

Existem outros sites web relacionados, porém não são de meu conhecimento. Se você hospedar este livro (Segurança e Otimização do Red Hat Linux) e quiser ser incluído na lista do próximo lançamento, por favor envie uma mensagem com as suas intenções.

Se você recebeu este livro como parte de uma distribuição impressa ou em um CD-ROM, por favor verifique a homepage da Documentação Linux http://www.linuxdoc.org/ ou o site web original http://pages.infinit.net/lotus1/ para ver se existe uma versão mais recente. Potencialmente, isto pode resguardá-lo de muitos problemas. Se você quiser traduzir este livro, por favor notifique-me para que eu possa ter o acompanhamento dos idiomas nos quais este livro foi publicado.

Os exemplos de arquivos de configuração deste livro estão disponíveis eletronicamente via http a partir deste URL:

http://pages.infinit.net/lotus1/opendocs/floppy.tgz

Em qualquer caso, extraia os arquivos digitando:

[root@deep tmp]# **tar xzpf floppy.tgz**

Caso você não consiga obter os exemplos diretamente da Internet, por favor entre em contato com o autor nos endereços de email abaixo:

gmourani@videotron.ca
gmourani@netscape.net

Uma nota sobre os direitos autorais

É importante observar que os direitos autorais deste livro foram alterados de Open Content (Conteúdo Aberto) para Open Publication License (Licença de Publicação aberta).

--

--

Basicamente, o que estamos dizendo é: faça o download do livro, imprima-o para dar aulas, mas não venda-o, pois o mesmo pertence à Gerhard Mourani e OpenDocs.

Reconhecimentos

Eu gostaria de agradecer à Michel Méral que desenhou todos os bonitos animais em meu livro, à Robert L. Ziegler por permitir que eu incluísse o seu software de firewall e a todos os usuários Linux em todo o mundo por seus comentários e sugestões.

Chave Pública GPG de Gerhard Mourani

-----CHAVE PÚBLICA PGP – INÍCIO DE BLOCO-----
Versão: GnuPG c1.0.0 (GNU/Linux)
Comentário: Para informações, consulte http://www.gnupg.org

-----CHAVE PÚBLICA PGP – FIM DE BLOCO

Parte I Referência Relativa à Instalação

Nesta Parte:

Introdução ao Linux
Instalação do seu servidor Linux

Capítulo 1 Introdução ao Linux

Neste Capítulo:

O que é o Linux ?
Algumas boas razões para se usar Linux
Vamos dissipar alguns temores, incertezas e dúvidas sobre o Linux

Introdução ao Linux

O que é o Linux ?

O Linux é um sistema operacional cuja criação foi iniciada na Universidade de Helsinki, na Finlândia, por um jovem estudante chamado Linus Torvalds. Naquele tempo, o estudante estava trabalhando em um sistema UNIX que executava em uma plataforma cara. Devido ao seu baixo orçamento e sua necessidade de trabalhar em casa, ele decidiu criar uma cópia do sistema UNIX e conseguiu executá-lo em uma plataforma menos cara como um IBM PC. Ele começou o seu trabalho em 1991, quando liberou a versão 0.02 e trabalhou firmemente até 1994, quando a versão 1.0 do Kernel do Linux foi liberada. A versão atual completa neste momento é a 2.2.X (liberada em 25 de janeiro de 1999), e o desenvolvimento prossegue.

O sistema operacional Linux é desenvolvido sob a Licença Pública Geral da GNU (também conhecida como GNU GPL) e o seu código-fonte está livremente disponível para todos que queiram fazer download pela Internet. A versão do Linux em CD-ROM também está disponível em várias lojas e as empresas que o fornecem cobram um preço por ele. O Linux pode ser usado para uma grande variedade de propósitos, incluindo rede, desenvolvimento de software e como uma plataforma de usuário final. Geralmente, o Linux é considerado uma alternativa excelente e de baixo custo com relação a outros sistemas operacionais mais caros porque você pode instalá-lo em vários computadores sem pagar a mais por isso.

Algumas boas razões para se usar Linux

Não há taxas de licenciamento ou royalties e o código-fonte pode ser modificado para satisfazer suas necessidades. Os resultados podem ser vendidos para se obter lucros, porém os autores originais detém os direitos autorais e você tem de fornecer o código-fonte das suas modificações.

Devido ao fato de vir com o código-fonte do kernel e ser completamente portável, o Linux roda em várias CPUs e plataformas mais do que qualquer sistema operacional de computador.

Os rumos atuais da indústria de software e hardware são forçar o consumidor a comprar computadores mais rápidos, com maiores capacidades de memória de sistema e disco rígido. O Linux não é afetado por estes rumos da indústria devido à sua capacidade de ser executado em quaisquer computadores, como velhos computadores baseados em x486 com quantidades limitadas de RAM.

O Linux é um sistema operacional multitarefa real similar ao seu irmão UNIX. Ele usa o que há de mais moderno em tecnologia de gerenciamento de memória para controlar todos os processos do sistema. Isto significa que se um processo travar, você poderá matá-lo e continuar trabalhando com segurança.

Um outro benefício é que o Linux é praticamente imune à todos os tipos de vírus que encontramos em outros sistema operacionais. Até agora, encontramos somente dois vírus que se fizeram efetivos em sistemas Linux.

Vamos dissipar alguns temores, incertezas e dúvidas sobre o Linux

É um Sistema Operacional de brinquedo.

As empresas Fortune 500, os governos e os consumidores usam o Linux cada vez mais como uma solução efetiva de custo. O Linux foi e continua sendo usado por grandes empresas como a IBM, a Amtrak, a NASA e outras mais.

Não há suporte.

Toda distribuição Linux vem com mais de 12.000 páginas de documentação. As distribuições comerciais, tais como RedHat Linux, Caldera, SuSE e OpenLinux oferecem um suporte inicial a usuários registrados e pequenos negócios, e contas corporativas podem obter suporte 24/7 através de empresas de suporte comercial. Como um sistema operacional de Fonte Aberto, não há necessidade de se esperar seis meses até que um serviço seja liberado e a comunidade Linux online conserta vários bugs sérios em questão de horas.

CAPÍTULO 2

Instalação do seu servidor Linux

Capítulo 2 Instalação do Seu Servidor Linux

Neste Capítulo:

Instalação do Linux
Conheça o seu hardware
Criando o disco de boot e fazendo o boot
Classe e método de instalação
Configuração do disco (Disk Druid)
Componentes a serem instalados
Seleção de pacotes individuais
Como usar os comandos RPM
Iniciando e parando os serviços (daemons)
Softwares que devem ser desinstalados após a instalação do servidor
Softwares que devem ser instalados após a instalação do servidor
Programas instalados no seu servidor
Coloque algumas cores no seu terminal
Atualização dos softwares mais recentes

Instalação do Linux

Preparamos este capítulo de forma que a sequência original do CD-ROM do Red Hat Linux 6.1 seja seguida. Cada seção abaixo se refere e irá guiá-lo através de diferentes telas que aparecerão durante a configuração do seu sistema após a inserção do disco de boot do Red Hat Linux em seu computador. Será interessante ter a máquina, na qual você deseja instalar o Linux, pronta e perto de você quando você estiver seguindo os passos descritos abaixo.

Conheça o seu hardware !

1) Quantos discos rígidos você tem ?
2) Qual o tamanho de cada disco rígido (3.2 GB) ?
3) Caso você tenha mais de um disco rígido, qual é o primário ?
4) Que tipo de disco rígido você tem (IDE, SCSI) ?
5) Quanto de RAM você tem (256 MB de RAM) ?
6) Você tem um adaptador SCSI ? Caso positivo, qual o fabricante e o modelo ?
7) Você tem um sistema RAID ? Caso positivo, qual o fabricante e o modelo ?
8) Que tipo de mouse você tem (PS/2, Microsoft, Logitech) ?
9) Quantos botões o seu mouse possui (2/3) ?
10) Caso tenha um mouse serial, a que porta ele está conectado (COM1) ?
11) Qual o fabricante e o modelo de sua placa de vídeo ? Quanta RAM de vídeo você tem (4 MB) ?
12) Que tipo de monitor você tem (marca e modelo) ?
13) Você estará conectado a uma rede ? Caso afirmativo, quais os seguintes dados:
    a. Seu endereço IP ?
    b. Seu netmask ?
    c. Seu endereço de gateway ?
    d. O endereço IP do seu servidor de nomes de domínio (DNS) ?
    e. Seu nome de domínio ?
    f. Seu nome de host ?
    g. Os tipos de suas placas de rede (marca e modelo) ?

Criando o disco de boot e fazendo o boot

A primeira coisa a fazer é criar um disco de instalação, também conhecido como disco de boot. Caso você tenha comprado o CD-ROM oficial do Red Hat Linux, você encontrará este disco com o nome de "Boot Diskette" na caixa do Red Hat Linux e você não precisará criá-lo. De tempos em tempos, você pode descobrir que a instalação poderá falhar com a imagem de disco padrão que vem com o CD-ROM oficial do Red Hat Linux. Caso isto ocorra, será necessário um disco revisado para que a instalação funcione adequadamente. Para estes casos, imagens especiais estão disponíveis na página web Errata do Red Hat Linux para resolver o problema (http://www.redhat.com/errata). Já que esta é uma ocorrência relativamente rara, você economizará tempo se tentar usar as imagens de disco padrão primeiramente e consultar a Errata somente se você experimentar algum problema em completar a instalação.

Passo 1

Antes de criar o disco de boot, insira o CD Oficial nr 1 do Red Hat Linux 6.1 em seu computador que esteja rodando o sistema operacional Windows. Quando o programa pedir o nome do arquivo, você digita **boot.img** para o disco de boot. Para criar disquetes no MS-DOS, você precisará usar este comandos (assumindo que o CD-ROM está no drive D: e que contenha o CD Oficial do Red Hat Linux 6.1):

- Abra o Pronto de Comandos do Windows: Iniciar | Programa | Prompt de Comando

```
C:\> d:
D:\> cd \dosutils
D:\dosutils> rawrite

Enter disk image source file name: ..\images\boot.img
Enter target diskette drive: a:
Please insert a formatted diskette into drive A: and press –ENTER--:

D:\dosutils>
```

O programa rawite.exe pede o nome de arquivo da imagem de disco: Digite **boot.img** e insira um disquete no drive A. Ele então pedirá pelo disquete a ser gravado: Digite **a:**. Depois, coloque uma etiqueta no disco: **Disco de Boot do Red Hat Linux 6.1**.

Passo 2

Já que vamos iniciar a instalação diretamente do CD-ROM, você precisa reinicializar com o disco de boot. Insira o disco de boot que você criou no drive A:, no computador onde você deseja instalar o Linux, e reinicialize o computador. No pronto boot:, pressione **Enter** para continuar com a inicialização e siga os três passos simples abaixo:

- Escolha o seu idioma
- Escolha o seu tipo de teclado
- Selecione o seu tipo de mouse

Classe e Método de Instalação (Tipo de Instalação)

O Red Hat Linux 6.1 define quatro classes ou tipos diferentes de instalação. Elas São:

- GNOME Workstation
- KDE Workstation
- Server
- Custom

Estas classes (GNOME Workstation, KDE Workstation e Server) dão a você a opção de simplificar o processo de instalação com muita perda de flexibilidade de configuração que não desejamos ter.

Por esta razão, recomendamos enfaticamente o **"Custom"**, pois isto lhe permitirá escolher quais serviços devem ser adicionados e como o sistema será particionado.

A idéia é carregar o mínimo de pacotes, enquanto se mantém o máximo de eficiência. Quanto menos software residente, menores serão as explorações e os buracos potenciais de segurança.

- Selecione **"Custom"** e clique em **Next**.

Configuração do Disco (Disk Druid)

Partimos do pressuposto que você está instalando o seu novo servidor Linux em um disco rígido novo, sem nenhum outro sistema de arquivos ou sistema operacional previamente instalado. Uma boa estratégia de particionamento é criar uma partição separada para cada um dos principais sistemas de arquivos. Isto melhora a segurança e evita negação de serviços acidental (DoS) ou a exploração de programas SUID.

A criação de múltiplas partições oferecem as seguintes vantagens:

- Proteção contra ataques de negação de serviços (DoS).
- Proteção contra programas SUID.
- Boot mais rápido.
- Gerenciamento fácil de backup e atualização.
- Habilidade de controlar melhor os sistemas de arquivos montados.

Advertência: Caso já exista um sistema de arquivos ou sistema operacional no disco rígido do computador onde você deseja instalar o seu Linux, recomendamos enfaticamente que você faça um backup do sistema atual antes de proceder com o particionamento do disco.

Passo 1

Por questões de performance, estabilidade e segurança, você deve criar, em seu computador, algo parecido com as seguintes partições listadas abaixo. Para esta configuração de particionamento, estamos supondo o fato de que você tem um disco rígido SCSI de 3.2 GB. É claro que você precisará ajustar os tamanhos das partições conforme suas próprias necessidades e tamanho de disco.

As partições que devem ser criadas em seu sistema:

/boot	5 MB	Imagens de kernel são mantidas aqui.
/usr	1000 MB	Deve ser grande, já que todos os programas binários do Linux são instalador aí.
/home	500 MB	Proporcional ao nr de usuários que você pretende hospedar (exemplo: 10 MB por usuário vezes o nr de usuários - 50 = 500 MB).
/chroot	400 MB	Caso você queira instalar programas em ambientes fechados chroot (exemplo: DNS).
/cache	400 MB	Esta é a partição de cache de um servidor proxy (exemplo: Squid).
/var	200 MB	Contém arquivos que mudam quando o sistema está rodando normalmente (exemplo: arquivos de log).
<Swap>	150 MB	Nossa partição de swap. A memória virtual.
/tmp	100 MB	Nossa partição de arquivos temporários.
/	315 MB	Nossa partição raíz.

Podemos criar mais duas partições especiais: **/chroot** e **/cache**. A partição /chroot pode ser usada para o servidor DNS, o servidor Apache e outros programas futuros no estilo chroot. A partição /cache pode ser usada para um servidor Proxy Squid. Se você não pretente instalar um servidor Proxy Squid, você não precisa criar a partição /cache.

Colocar **/tmp** e **/home** em partições separadas é muito mais obrigatório se os usuários tiverem uma conta shell no servidor (proteção contra programas SUID). A divisão destes sistemas de arquivos em partições separadas também impedem que usuários encham quaisquer sistemas de arquivos críticos (ataque de negação de serviços - DoS). Colocar **/var** e **/usr** em partições separadas também é uma idéia muito boa. Isolando-se a partição **/var**, você protege a sua partição raíz de um estouro (ataque de negação de serviços - DoS).

Em nossa configuração de partição, reservaremos 400 MB de espaço em disco para programas chroot, como o Apache, o DNS e outros softwares. Isto é necessário porque os arquivos do diretório raíz de documentos do Apache (DocumentRoot) e outros programas binários relacionados ao Apache serão instalados nesta partição, caso você decida rodar o servidor web Apache em um ambiente fechado chroot. Observe que o tamanho do diretório chroot do Apache é proporcional ao tamanho de seus arquivos em "DocumentRoot". Se você não pretente instalar e utilizar o Apache em seu servidor, você pode reduzir o tamanho desta partição para algo em torno de 10 MB para o servidor DNS que você sempre precisa ter em um ambiente fechado chroot por razões de segurança.

Tamanho mínimo das partições

Somente para informação, estes são os tamanhos mínimos, em megabyte, que as partições da instalação do Linux devem ter para um funcionamento adequado. Os tamanhos das partições listadas abaixo são realmente pequenos. Esta configuração pode caber em um disco rígido muito antigo de 512 MB de tamanho e que podemos encontrar em velhos computadores x486. Eu mostro estas partições a você só para dar um idéia:

/	35 MB
/boot	5 MB
/chroot	10 MB
/home	100 MB
/tmp	30 MB
/usr	232 MB
/var	25 MB

Disk Druid

O Disk Druid é um programa que particiona o disco rígido para você. Escolha **Add** para adicionar uma nova partição, **Edit** para editar, **Delete** para apagar uma partição e **Reset** para resetar a partição ao seu estado original. Quando você adiciona uma partição, uma nova janela aparece e lhe mostra parâmetros a serem escolhidos. Os diferentes parâmetros são:

Mount Point:	onde você deseja montar a sua nova partição.
Size (Megs):	o tamanho de sua nova partição em magabyte.
Partition Type:	Linux native para o sistema de arquivos Linux e Swap para a partição Linux de Swap.

Caso você tenha um HD SCSI, o nome do dispositivo será **/dev/sda** e caso você tenha um HD IDE, o nome será **/dev/hda**. Se você estiver em busca de performance e estabilidade altas, um disco SCSI é altamente recomendado.

O Linux se refere às partições do disco usando uma combinação de letras e números. Ele usa um esquema de nomes que é mais flexível e comunica mais informações do que os modelos utilizados por outros sistemas operacionais. Aquí está um resumo:

Primeiras Duas Letras - As primeiras duas letras do nome da partição indicam o tipo de dispositivo no qual a partição reside. Normalmente, você verá ou **hd** (para discos IDE) ou **sd** (para disco SCSI).

A Próxima Letra - Esta letra indica em que dispositivo a partição está. Por exemplo, **/dev/hda** (o primeiro disco rígido IDE) e **/dev/hdb** (o segundo disco IDE).

Tenha em mente estas informações, pois tornarão as coisas mais fáceis de se entender quando você estiver configurando as partições que o Linux precisa.

Uma partição de swap

A partição de swap é usada para dar suporte à memória virtual. Se o seu computador tiver 16 MB de RAM ou menos, você deve criar uma partição de swap. Mesmo que você tenha mais memória, uma partição de swap ainda é recomendada. O tamanho mínimo de sua partição de swap deveria ser igual à RAM de seu computador ou 16 MB (o que for maior). A grosso modo, o maior tamanho de partição de swap utilizável é 1 GB (a partir do kernel 2.2, arquivos de swap de 1 GB são suportados), de forma que a criação de partições de swap maiores do que isso resultarão em perda de espaço. Observe, contudo, que você pode criar e utilizar mais de uma partição de swap (embora isto seja necessário somente para instalações de servidores muito grandes).

Observação: Tente colocar as suas partições de swap próximas do início de seu disco. O início do disco está fisicamente localizado na porção mais externa dos cilindros, de maneira que a cabeça de escrita/leitura pode cobrir mais terreno por revolução.

Agora, como um exemplo:

Para criar as partições listadas abaixo em nosso sistema (estas serão as partições que precisaremos para a instalação de nosso servidor), os comandos do Disk Druid seriam:

Add
Mount Point: **/boot** ← nosso diretório /boot.
Size (Megs): **5**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/usr** ← nosso diretório /usr.
Size (Megs): **1000**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/home** ← nosso diretório /home.
Size (Megs): **500**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/chroot** ← nosso diretório /chroot.
Size (Megs): **400**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/cache** ← nosso diretório /cache.
Size (Megs): **400**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/var** ← nosso diretório /var.
Size (Megs): **200**
Partition Type: **Linux Native**
Ok

Add
Mount Point: ← nosso partição /Swap (ponto de montagem em branco).
Size (Megs): **150**
Partition Type: **Linux Swap**
Ok

Add
Mount Point: **/tmp** ← nosso diretório /tmp.
Size (Megs): **100**
Partition Type: **Linux Native**
Ok

Add
Mount Point: **/** ← nosso diretório /.
Size (Megs): **316**
Partition Type: **Linux Native**
Ok

Após ter completado o particionamento de seu disco, você deverá ver algo parecido com as seguintes informações em sua tela. Nossos pontos de montagem se parecerão assim:

Mount Point	**Device**	**Requested**	**Actual**	**Type**
/boot	sda1	5M	5M	Linux Native
/usr	sda5	1000M	1000M	Linux Native
/home	sda6	500M	500M	Linux Native
/chroot	sda7	400M	400M	Linux Native
/cache	sda8	400M	400M	Linux Native
/var	sda9	200M	200M	Linux Native
<Swap>	sda10	150M	150M	Linux Swap
/tmp	sda11	100M	100M	Linux Native
/	sda12	316M	315M	Linux Native

Drive	**Geom [C/H/S]**	**Total (M)**	**Free (M)**	**Used (M)**	**Used (%)**
sda	[3079/64/32]	3079M	1M	3078M	99%

Observação: Estamos usando um disco rígido SCSI, pois as primeiras letras do dispositivo são **sd**.

Agora que você particionou e escolheu os pontos de montagem para os seus diretórios, selecione **Next** para continuar. Após ter criado suas partições, o programa de instalação perguntará quais partições deverão ser formatadas. Escolha as partições que você deseja inicializar, selecione a opção "**Check for bad blocks during format**" (teste de blocos defeituosos durante a formatação) e pressione **Next**. Isto formatará as partições e as tornará ativas para que o Linux possa usá-las.

Na próxima tela, você verá a configuração do LILO onde terá a opção de instalar o registro de boot do LILO no:

- Registro Mestre de Boot (Master Boot Record - MBR), ou no
- Primeiro setor da partição de boot

Geralmente, se o Linux for o único SO na sua máquina, você deve escolher "Master Boot Record (MBR)". Depois disso, você precisará configurar a sua LAN e o relógio. Após terminar de configurar o relógio, você precisará informar uma senha de root para o seu sistema e fazer a configuração da autenticação.

Para a configuração da autenticação, não esqueça de selecionar:

- Ativar senha MD5 (Enable MD5 passwords)
- Ativar senhas Shadow (Enable Shadow passwords)

Não precisa ativar o NIS (Enable NIS), já que não estaremos configurando o serviço NIS neste servidor.

Componentes a Serem Instalados (Seleção de Grupos de Pacotes)

Após ter configurado suas partições e ter selecionado-as para formatação, você está pronto para selecionar os pacotes para instalação. O Linux é um sistema operacional poderoso que, por default, executa vários serviços úteis. No entanto, a maioria desses serviços são desnecessários e representam um risco de segurança em potencial.

De maneira ideal, cada serviço deveria rodar em um único host dedicado somente àquele serviço. Muitos sistemas operacionais Linux são configurados por default mais para oferecer uma gama abrangente de serviços e aplicações do que para oferecer um serviço de rede em particular, de maneira que você precisa configurar o servidor eliminando os serviços desnecessários. A execução somente de serviços essenciais em um host em particular pode melhorar a segurança de sua rede de várias formas:

- Outros serviços não poderão ser usados para atacar o host e prejudicar ou remover serviços de rede desejados.

- Serviços diferentes podem ser administrados por indivíduos diferentes. Isolando-se os serviços, de forma que cada host e serviço tenha um único administrador, você minimiza a possibilidade de conflito entre os administradores.

- O host pode ser configurado para melhor atender às exigências de um serviço em particular. Serviços diferentes poderiam exigir configurações de hardware e software diferentes, o que poderia levar à vulnerabilidades ou restrições de serviços desnecessárias.

- Reduzindo-se os serviços, o número de arquivos de log e os registros nos arquivos de log são reduzidos, de forma que a detecção de comportamentos inesperados torna-se mais fácil.

Uma instalação adequada do seu servidor Linux é o primeiro passo para um sistema estável e seguro. Você primeiro tem que escolher que componentes de sistema você deseja ter instalados. Selecione os componentes e depois parta para a seleção individual dos pacotes de cada componente, selecionando a opção **Select individual packages** na tela de configuração do seu Red Hat.

Já que estamos configurando um servidor Linux, não precisamos instalar uma interface gráfica (XFree86) em nosso sistema (interface gráfica em um servidor significa mais processos, menos cpu, menos memória, riscos de segurança e assim por diante). Geralmente, a interface gráfica é utilizada somente em estações de trabalho. Selecione os seguintes pacotes para instalação:

- Networked Workstation (Estação de Trabalho em Rede)
- Network Management Workstation (Estação de Trabalho para Gerenciamento de Rede)
- Utilities (Utilitários)

Após selecionar os componentes que você deseja instalar, você pode selecionar ou desselecionar pacotes.

Observação: Selecione a opção **Select individual packages** (muito importante) para que você possa ter a possibilidade de selecionar ou desselecionar pacotes.

Seleção de Pacotes Individuais

O programa de instalação apresenta uma lista de grupos de pacotes disponíveis. Selecione o grupo a ser examinado.

Os componentes listados abaixo devem ser desselecionados do grupo de menus por razões de segurança, otimização e outras razões descritas abaixo:

Applications/File:	git
Applications/Internet:	finger, ftp, fwhois, ncftp, rsh, rsync, talk, telnet
Applications/Publishing:	ghostscript, ghostscript-fonts, mpage, rhs-printfilters
Applications/System:	arpwatch, bind-utils, knfsd-clients, procinfo, rdate, rdist, screen, ucd-snmp-utils
Documentation:	indexhtml
System Enviroment/Base:	chkfontpath, yp-tools
System Enviroment/Daemons:	XFree86-xfs, lpr, pidentd, portmap, routed, rusers, rwho, tftp, ucd-snmp, ypbind
System Enviroment/Libraries:	XFree86-libs, libpng
User Interface/X:	XFree86-75dpi-fonts, urw-fonts

Antes de fazer a descrição de cada programa que queremos desinstalar, alguém poderá perguntar: Por que eu preciso desinstalar do servidor os programas finger, ftp, fwhois e telnet? Primeiro de tudo, sabemos que esses programas, por sua natureza, são inseguros. Agora imagine que um cracker tenha acessado o seu novo servidor Linux. Ele poderá usar os programas finger, ftp, fwhois e telnet para consultar ou acessar outros nós da sua rede. Se esses programas não estiverem instalados no seu servidor Linux, ele será obrigado a usar esses programas externamente ou tentar instalar os programas no seu servidor, em cujo caso você poderá rastreá-lo com uma ferramenta como o Tripwire.

Applications/File (Aplicações/Arquivo):

- O pacote GIT oferece um browser extensível de sistema de arquivos, um visualizador de arquivos ASCII/hexadecimal, um visualizador/matador de processos e outros utilitários correlatos e shell scripts. **[Desnecessário]**

Applications/Internet (Aplicações/Internet):

- O pacote finger é um utilitário que permite que usuários vejam informações sobre os usuários do sistema. **[Desnecessário]**

- O pacote ftp oferece um cliente FTP de linha de comando padrão UNIX. **[Riscos de segurança]**

- O programa fwhois permite consultas à bancos de dados whois. **[Riscos de segurança]**

- O pacote Ncftp é um cliente FTP melhorado. **[Riscos de segurança, desnecessário]**

- O pacote rsh permite que usuários executem comandos em máquinas remotas, login em outras máquinas e copiem arquivos entre máquinas (rsh, rlogin e rcp). **[Riscos de segurança]**

- O pacote ntalk oferece os programas daemon e cliente para o protocolo de conversação pela Internet, o que lhe permite bater papo com outros usuários em sistemas UNIX diferentes. **[Riscos de segurança]**

- O Telnet é um protocolo popular para efetuar login em sistemas remotos através da rede, porém é inseguro (transfere senhas em texto plano). **[Riscos de segurança]**

Applications/Publishing (Aplicações/Editoração):

- O pacote ghostscript é uma série de softwares que oferecem um interpretador PostScript(TM) e um interpretador de arquivos em Formato de Documento Portável (PDF). **[Desnecessário]**

- O pacote ghostscript-fonts pode ser usado pelo interpretador ghostscript durante a conversão de textos. **[Desnecessário]**

- O utilitário do pacote mpage aceita arquivos em texto plano ou documentos PostScript(TM) como entrada, reduz o tamanho do texto e imprime os arquivos em uma impressora PostScript com várias páginas em cada folha de papel. **[Desnecessário, não há impressoras instaladas no servidor]**

- O pacote rhs-printfilters contém uma série de filtros de impressão, que servem primariamente para serem usados com o utilitário printtool da Red Hat. **[Desnecessário, não há impresoras instaladas no servidor]**

Applications/System (Aplicações/Sistema):

- O pacote arpwatch contém utilitários para monitorar o tráfico em redes Ethernet ou FDDI e construir um banco de dados com pares de endereços Ethernet/IP. **[Desnecessário]**

- O pacote bind-utils contém uma coleção de utilitários para descobrir informações sobre hosts Internet. **[Vamos compilá-lo mais adiante neste livro]**

- O pacote knfsd-clients contém o programa showmount que consulta o daemon de montagem em um host remoto para obter informações sobre o servidor NFS no host remoto. **[Riscos de segurança e serviços NFS não serão instalados neste servidor]**

- O pacote procinfo captura informações sobre o seu sistema a partir do kernel. **[Desnecessário, outros métodos existem]**

- O utilitário do pacote rdate pode recuperar a data e a hora de uma outra máquina da sua rede. **[Riscos de segurança]**

- O pacote rdist é um programa que mantém cópias idênticas de arquivos em múltiplos hosts. **[Riscos de segurança]**

- O pacote screen é um programa útil para usuários que façam telnet para uma máquina ou são conectados via terminal burro, mas que querem fazer mais do que apenas um login. **[Desnecessário]**

- O pacote ucd-snmp-utils contém vários utilitários para uso com o projeto de gerenciamento de rede ucd-snmp. **[Desnecessário, riscos de segurança]**

Documentation (Documentação):

- O pacote indexhtml contém a página HTML e os gráficos para a página de bem-vindo mostrada pelo seu browser web em Sistemas X-Window. **[Desnecessário, não precisamos de interface gráfica]**

- O Serviço de Informação de Rede (Network Information Service – NIS) é um sistema que fornece e centraliza informações de rede (nomes de login, senhas, diretórios base e informações de grupos) para todas as máquinas em uma rede. **[Riscos de segurança, não o usaremos em nosso servidor]**

System Enviroment/Daemons (Ambiente de Sistema/Daemons):

- O pacote Xfree86-xfs é um servidor de fontes para o Xfree86 que pode também servir fontes para outros servidores X remotos. **[Desnecessário, não usaremos interface gráfica em nosso servidor]**

- O pacote lpr oferece os utilitários básicos de sistema para o gerenciamento dos serviços de impressão. **[Desnecessário e nenhuma impressora será instada no servidor]**

- O pacote pidentd contém o identd que monitora conexões TCP/IP específicas e retorna ou o nome do usuário ou outras informações sobre o processo ao qual pertence a conexão. **[Desnecessário, pouquíssimas coisas na rede EXIGEM que o remetente esteja rodando o identd, porque muitas máquinas não o tem e porque muitas pessoas o desligam]**

- O pacote portmapper gerencia conexões RPC, que são usadas por protocolos como o NFS e o NIS. **[Desnecessário, riscos de segurança, e os serviços NIS/NFS não serão instalados neste servidor]**

- O daemon de roteamento do pacote routed mantém as tabelas de roteamento atualizadas pela manipulação do tráfico RIP entrante e pelo broadcast do tráfico RIP sainte relativo às rotas do tráfego de rede. **[Desnecessário, riscos de segurança e é limitado]**

- O programa do pacote rusers permite aos usuários descobrir quem está logado em várias máquinas na rede. **[Riscos de segurança]**

- O pacote rwho mostra quem está logado em todas as máquinas da rede que estejam rodando o daemon rwho. **[Riscos de segurança]**

- O pacote tftp ou Protocolo Trivial de Transferência de Arquivos (Trivial File Transfer Protocol – TFTP) permite que usuários transfiram arquivos de e para uma máquina remota. Normalmente, é utilizado para boot remoto de estações de trabalho diskless. **[Desnecessário, riscos de segurança]**

- O pacote ucd-snmp ou SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede) é um protocolo utilizado para gerenciamento de rede. **[Desnecessário, riscos de segurança]**

System Enviroment/Libraries (Ambiente de Sistema/Bibliotecas):

- O pacote Xfree86-libs contém as bibliotecas compartilhadas que a maioria dos programas X precisam para serem executados adequadamente. **[Desnecessário, não usaremos interface gráfica]**

- O pacote libpng contém uma biblioteca de funções de criação e manipulação de arquivos de imagem no formato PNG. PNG é um formato de gráfico bitmap similar ao formato GIF. **[Desnecessário]**

User Interface/X (Interface de Usuário/X):

- pacote Xfree86-75dpi-fonts contém os fontes em 75 dpi (os fontes padrão) usados pela maioria dos sistema X-Window. **[Desnecessário, não usaremos interface gráfica]**

- O pacote urw-fonts contém as versões Livres dos fontes PostScript, Padrão 35, Tipo 1. **[Desnecessário, não usaremos interface gráfica]**

Neste ponto, o programa de instalação irá formatar todas as partições que você selecionou para formatação em seu sistema. Isto pode levar vários minutos dependendo da velocidade de sua máquina. Uma vez formatadas todas as partições, o programa de instalação começa a instalar os pacotes.

Como usar os Comandos RPM

Esta seção contém uma visão geral dos principais modos de se usar o RPM para instalar, desinstalar, atualizar, consultar, listar e verificar os pacotes RPM em seu sistema Linux. Você deve se familiarizar agora com esses comandos RPM porque estaremos usando eles com frequência ao longo deste livro.

- Para instalar um pacote RPM, use o comando:
  [root@deep /]# **rpm -ivh foo-1.0-2.i386.rpm**

Observe que pacotes RPM tem nomes de arquivos como **foo-1.0-2.i386.rpm**, que incluem o nome do pacote (**foo**), a versão (**1.0**), a release (**2**) e a arquitetura (**i386**).

- Para desinstalar um pacote RPM, use o comando:
  [root@deep /]# **rpm -e foo**

Observe que usamos o nome do pacote **foo**, não o nome do arquivo original do pacote "**foo-1.0-2.i386.rpm**".

- Para atualizar um pacote RPM, use o comando:
  [root@deep /]# **rpm -Uvh foo-1.0-2.i386.rpm**

Com este comando, o RPM desinstala automaticamente a versão antiga do pacote foo e instala a nova. Utilize sempre "rpm –Uvh" para instalar pacotes, já que funciona bem mesmo que não haja versões anteriores do pacote instalado.

- Para consultar um pacote RPM, use o comando:
  [root@deep /]# **rpm -q foo**

Este comando irá imprimir o nome do pacote, o número da versão e da release para o pacote foo instalado. Use este comando para verificar se um pacote está ou não instalado em seu sistema.

- Para mostrar informações sobre um pacote, use o comando:
  [root@deep /]# **rpm -qi foo**

Este comando mostra informações sobre um pacote, incluindo nome, versão e descrição do programa instalado. Use este comando para obter informações sobre um pacote instalado.

- Para listar os arquivos de um pacote, use o comando:
  [root@deep /]# **rpm -ql foo**

Este comando irá listar todos os arquivos de um pacote RPM instalado. Funciona somente quando o pacote já está instalado em seu sistema.

- Para verificar a assinatura de um pacote RPM, use o comando:
  [root@deep /]# **rpm -checksig foo**

Este comando verifica a assinatura PGP do pacote especificado para assegurar a sua integridade e origem. Sempre utilize este comando primeiramente antes de instalar novos pacotes RPM em seu sistema. Também, o software GnuPG ou o Pgp deve estar instalado em seu sistema antes que você possa usar este comando.

Iniciando e parando os serviços (daemons)

O programa **init**, também conhecido como controlador de inicialização de processos, é responsável por iniciar todos os processos normais e autorizados que são necessários no momento do boot de seu sistema. Isto pode incluir o daemon do APACHE, os daemons de REDE, e qualquer coisa mais que deva ser executada quando sua máquina faz o boot. Cada um desses processos tem um script no diretório "/etc/rc.d/init.d/" escrito para aceitar um argumento que pode ser "start", "stop" ou "restart". De fato, você pode executar esses scripts manualmente com um comando como:

Por exemplo:

- Para iniciar o Servidor Web httpd manualmente no Linux.
  [root@deep /]# **/etc/rc.d/init.d/httpd start**
  Starting httpd: [OK]

- Para parar o Servidor Web httpd manualmente no Linux.
  [root@deep /]# **/etc/rc.d/init.d/httpd stop**
  Shutting down httpd: [OK]

- Para reiniciar o Servidor Web httpd manualmente no Linux.
  [root@deep /]# **/etc/rc.d/init.d/httpd restart**
  Shutting down httpd: [OK]
  Starting httpd: [OK]

Dê uma verificada dentro do seu diretório "/etc/rc.d/init.d" para encontrar serviços disponíveis e utilize os argumentos start | stop | restart para manipulá-los.

Softwares que devem ser desinstalados após a instalação do Servidor

O Red Hat Linux instala em seu sistema outros programas pré-estabelecidos por default e não lhe dá a opção de desinstalá-los durante a configuração da instalação. Por esta razão, você deve desinstalar os seguintes softwares de seu sistema após a instalação de seu servidor:

pump	kernel-pcmcia-cs	setserial	redhat-release
mt-st	linuxconf	kudzu	gd
eject	getty_ps	raidtools	pciutils
mailcap	setconsole	gnupg	rmt
apmd	isapnptools	redhat-logos	

Use o seguinte comando RPM para desinstalá-los:

- O comando para desinstalar software é:
  [root@deep /]# **rpm -e <nome_do_software>**

Onde <nome_do_software> é o nome do software que você deseja desinstalar, por exemplo, (foo).

Programas como apmd, kudzu e sendmail são daemons que rodam como processos. É melhor parar esses processos antes de desinstalá-los do sistema.

- Para parar esses processos, use os seguintes comandos:
  [root@deep /]# **/etc/rc.d/init.d/apmd stop**
  [root@deep /]# **/etc/rc.d/init.d/sendmail stop**
  [root@deep /]# **/etc/rc.d/init.d/kudzu stop**

Agora, você pode desinstalá-los com segurança e todos os outros pacotes, todos juntos, conforme mostrado abaixo:

Passo 1
Remova os pacotes especificados.
[root@deep /]# **rpm -e --nodeps pump mt-st eject bc mailcap apmd kernel-pcmcia-cs linuxconf getty_ps setconsole isapnptools setserial kudzu raidtools gnupg redhat-logos redhat-release gd pciutils rmt**

Passo 2
Remova o arquivo linux.conf-installed manualmente.
[root@deep /]# **rm -f /etc/conf.linuxconf-installed**

Observação: Este é um arquivo de configuração relacionado ao software de configuração linuxconf que deve ser removido manualmente.

O programa **hdparm** é necessário para discos rígidos IDE, mas não para discos rígidos SCSI. Se você tiver um disco rígido IDE em seu sistema, você deve manter este programa (hdparm). Porém, se você não tiver um disco rígido IDE, você pode removê-lo de seu sistema.

- Para remover o hdparm de seu sistema, use o seguinte comando:
  [root@deep /]# **rpm -e hdparm**

Os programas **kbdconfig**, **mouseconfig**, **timeconfig**, **authconfig**, **ntsysv** e **setuptool**, nesta ordem, configuram o idioma e o tipo de seu teclado, o tipo do seu mouse, o fuso horário default, o seu NIS e senhas shadow, os seus numerosos links simbólicos no diretório "/etc/rc.d/" e o utilitário de menu em modo texto que lhe permite acessar todas essas características. Após essas configurações terem sido ajustadas durante o estágio de instalação do seu servidor Linux, é raro que você precise mudá-las novamente. Assim, você pode desinstalá-las e, caso no futuro você precise alterar o seu teclado, mouse, fuso horário default, etc novamente, tudo o que você tem a fazer é instalar o programa com o RPM a partir do CD-ROM original.

- Para você remover de seu sistema todos os programas acima, use o seguinte comando:
  [root@deep /]# **rpm -e kbdconfig mouseconfig timeconfig authconfig ntsysv setuptool**

O programa **Sendmail** é sempre necessário em seus servidores para mensagens em potencial enviadas ao usuário root por diferentes serviços de software instalados em sua máquina.

O **Sendmail** é um programa Agente de Transporte de Correio (Mail Transport Agent – MTA) que envia mensagem de correio de uma máquina para outra. Pode ser configurado de diferentes maneiras. Pode servir como um agente de entrega interna para um Servidor Concentrador de Correio (Mail Hub Server) ou pode ser configurado para funcionar como um Concentrador Central de Correio para todas as máquinas Sendmail de sua rede. Desta forma, dependendo do que você quer fazer com o Sendmail, você deve configurá-lo para responder às suas necessidades específicas. Por esta razão, você deve desinstalar o Sendmail e consultar a parte deste livro que fala sobre instalação e configuração do Sendmail.

- Para remover o Sendmail de seu sistema, use o seguinte comando:
  [root@deep /]# **rpm -e sendmail**

- O pacote DHCP Pump permite que clientes diskless individuais em uma rede possam obter as suas próprias informações de configuração de rede IP a partir de servidores da rede. **[Desnecessário]**

- Os programas de gerenciamento de drives de fita mt (para drives de fita magnética) e st (para dispositivos de fita SCSI) podem controlar a rebobinação,

a ejeção, pular arquivos, blocos e mais. **[Necessário somente se você tiver backup em fita neste servidor]**

- O pacote eject contém o programa eject que permite ao usuário ejetar mídia removível (tipicamente CD-ROMs, discos flexíveis, discos Jaz ou Zip da Iomega) usando controle por software. **[Necessário somente se você tiver backup em fita neste servidor]**

- O programa Metamail, que usa o mailcap, lê o arquivo mailcap para determinar como deve mostrar material multimídia ou não-texto. **[Desnecessário]**

- Os utilitário do pacote apmd (Advanced Power Management Daemon) pode monitorar a bateria de seu notebook e advertir todos os usuários quando a bateria estiver fraca. **[Desnecessário para um servidor]**

- O pacote kernel-pcmcia-cs é para máquinas laptop (e alguns não-laptops) que suportam cartão de expansão PCMCIA. **[Desnecessário para um servidor]**

- O pacote linuxconf é uma ferramenta de configuração do sistema. **[Desnecessário, programa cheio de bugs]**

- O pacote getty_ps contém programas que são usados para aceitar logins na console ou em um terminal de seu sistema. **[Desnecessário]**

- O pacote setconsole é um utilitário básico de sistema para configuração dos arquivos "/etc/inittab", "/dev/systty" e "/dev/console" para manipular uma nova console. **[Desnecessário]**

- O pacote isapnptools contém utilitários para configuração de placas ISA Plug-and-Play (PnP). **[Desnecessário]**

- O pacote setserial é um utilitário básico de sistema para mostrar/configurar informações das portas seriais. **[Desnecessário]**

- O pacote kudzu é uma ferramenta de varredura de hardware executada por ocasião do boot do sistema para determinar que hardware foi adicionado ou removido do sistema. **[Desnecessário]**

- O pacote raidtools inclui as ferramentas que você precisa para configurar e manter um dispositivo RAID por software em um sistema Linux. **[Depende de você usar Raid ou não]**

- O pacote GnuPG é uma ferramenta para armazenamento e comunicação de dados com segurança. É uma substituição ao software PGP. Também pode ser usado para criptografar dados e criar assinaturas digitais. **[Nós o compilaremos mais adiante em nosso livro]**

- O pacote redhat-logos contém os arquivos do logo "Shadow Man" da Red Hat e o logo do RPM. **[Desnecessário em uma máquina servidora]**

- O pacote redhat-release contém o arquivo de release do Red Hat Linux. **[Desnecessário]**

- O pacote gd permite que seus códigos desenhem imagens rapidamente e grave o resultado como um arquivo ".gif". **[Desnecessário]**

- O pacote pciutils contém vários utilitários de inspeção e configuração de dispositivos conectados ao barramento PCI. **[Usaremos outros métodos]**

- O utilitário rmt fornece acesso remoto para fazer backup via rede. **[Riscos de segurança, já que o rmt depende do rsh para funcionar]**

Softwares que devem ser instalados após a instalação do Servidor

Para poder compilar programas em seu servidor, você deve instalar os seguintes pacotes RPM. Esta parte da instalação é muito importante e exige que você instale todos os pacotes correlatos descritos abaixo. Estes softwares estão no CD nr 1 do seu Red Hat Linux no diretório RedHat/RPMS e representam o software básico necessário para compilar programas no Linux.

Passo 1
Primeiro, montamos o CD-ROM e mudamos para o subdiretório RPMS do CD-ROM.

- Para montar o drive de CD-ROM e mudar para o diretório RPMS, use os seguintes comandos:
  [root@deep /]# **mount /dev/cdrom /mnt/cdrom/**
  [root@deep /]# **cd /mnt/cdrom/RedHat/RPMS**

Estes são os pacotes que precisamos para podermos compilar programas no sistema Linux. Lembre-se: estes são os pacotes mínimos que permitem a você compilar a maioria dos programas tar.gz disponíveis para Linux. Outros pacotes compiladores existem no CD-ROM da Red Hat, por isso verifique o arquivo README que vem com os programas tar.gz que você deseja instalar, caso você receba mensagens de erro durante a compilação de um software específico.

autoconf-2.13-5.noarch.rpm
m4-1.4-12.i386.rpm
automake-1.4-5.noarch.rpm
dev86-0.14.9-1.i386.rpm
bison-1.28-1.i386.rpm
byacc-1.9-11.i386.rpm
cdecl-2.5-9.i386.rpm
cpp-1.12-24.i386.rpm
cproto-4.6-2.i386.rpm
ctags-3.2-1.i386.rpm
egcs-1.1.2-24.i386.rpm
ElectricFence-2.1-1.i386.rpm
flex-2.5.4a-7.i386.rpm
gdb-4.18-4.i386.rpm
kernel-headers-2.2.12-20.i386.rpm
glibc-devel-2.1.2-11.i386.rpm
make-3.77-6.i386.rpm
patch-2.5-9.i386.rpm

Observação: É melhor instalar os softwares descritos acima todos juntos se você não quiser receber mensagens de erro de dependência durante a instalação dos RPMs.

Passo 2
Instale todos os softwares necessários acima com um único comando RPM.

- O comando RPM para instalar todos os softwares de uma vez é:
  [root@deep /]# **rpm -Uvh autoconf-2.13-5.noarch.rpm m4-1.4-12.i386.rpm automake-1.4-5.noarch.rpm dev86-0.14.9-1.i386.rpm bison-1.28-1.i386.rpm byacc-1.9-11.i386.rpm cdecl-2.5-9.i386.rpm cpp-1.12-24.i386.rpm cproto-4.6-2.i386.rpm ctags-3.2-1.i386.rpm egcs-1.1.2-24.i386.rpm ElectricFence-2.1-1.i386.rpm flex-2.5.4a-7.i386.rpm gdb-4.18-4.i386.rpm kernel-headers-2.2.12-20.i386.rpm glibc-devel-2.1.2-11.i386.rpm make-3.77-6.i386.rpm patch-2.5-9.i386.rpm**

Passo 3
Você deve sair e fazer login novamente para todas as alterações tenham efeito.

- Para sair da sua console, use o seguinte comando:
  [root@deep /]# **exit**

Após a instalação e compilação de todos os programas que você precisa em seu servidor, é uma boa idéia remover todos os objetos agudos (compiladores, etc) descritos acima, a menos que sejam necessários para algum sistema. Uma das razões é que se um cracker ganhar acesso ao seu servidor, ele não poderia compilar ou modificar seus programas binários. Também, isto vai liberar muito espaço e vai ajudar a melhorar a varredura regular de arquivos em seu servidor para verificação de integridade.

Quando você executa um servidor, você lhe dá uma tarefa especial para cumprir. Você nunca colocará todos os serviços que deseja oferecer em uma única máquina, ou você perderá velocidade (recursos disponíveis divididos pelo número de processos que estão executando no servidor) e diminuirá a sua segurança (com muitos serviços rodando na mesma máquina, se um cracker acessar este servidor ele poderá atacar diretamente todos os outros disponíveis).

Ter servidores diferentes fazendo tarefas diferentes simplificará a administração, o gerenciamento (você sabe que tarefa cada servidor está encarregado de executar, que serviços devem estar disponíveis, que portas devem estar abertas para acesso dos clientes e que portas devem estar fechadas, você sabe o que deverá ver nos arquivos de log, etc) e lhe dará mais controle e flexibilidade sobre cada um (servidor dedicado para correio, páginas web, banco de dados, desenvolvimento, backup, etc). Assim, ter um servidor, por exemplo, voltado somente para desenvolvimento e testes lhe permitirá não ser compelido a instalar programas compiladores no servidor cada vez que você quiser compilar e instalar um novo software nesta máquina e, logo após, ser obrigado a desinstalar o compilador e os objetos agudos.

Programas instalados no seu Servidor

Passo 1

Já que optamos por personalizar a instalação de nosso sistema Linux, esta é a lista de todos os programas que você deve ter em seu servidor após a completa instalação do servidor Linux. Esta lista deve coincidir exatamente com o arquivo **install.log** localizado no seu diretório "/tmp". Do contrário, você poderá ter problemas. Não esqueça de instalar todos os programas listados acima na seção "Softwares que devem ser instalados após a instalação do Servidor" para que você possa fazer compilação em seu Servidor.

Installing setup.
Installing filesystem.
Installing basesystem.
Installing ldconfig.
Installing glibc.
Installing shadow-utils.
Installing mktemp.
Installing termcap.
Installing libtermcap.
Installing bash.
Installing MAKEDEV.
Installing SysVinit.
Installing XFree86-Mach64.
Installing chkconfig.
Installing apmd.
Installing ncurses.
Installing info.
Installing fileutils.
Installing grep.
Installing ash.
Installing at.
Installing authconfig.
Installing bc.
Installing bdflush.
Installing binutils.
Installing bzip2.
Installing sed.
Installing console-tools.
Installing e2fsprogs.
Installing rmt.
Installing cpio.
Installing cracklib.
Installing cracklib-dicts.
Installing crontabs.
Installing textutils.
Installing dev.
Installing gzip.
Installing hdparm.
Installing initscript.
Installing ipchains.
Installing isapnptools.
Installing kbdconfig.
Installing kernel.
Installing kernel-pcmcia-cs.
Installing kudzu.
Installing ld-so.
Installing less.
Installing libc.
Installing libstdc++.
Installing lilo.
Installing pwdb.
Installing pam.
Installing sh-utils.
Installing redhat-release.
Installing linuxconf.
Installing logrotate.
Installing losetup.
Installing lsof.
Installing mailcap.
Installing mailx.
Installing man.
Installing mingetty.
Installing mkbootdisk.
Installing mkinitrd.
Installing modutils.
Installing mount.
Installing mouseconfig.
Installing mt-st.
Installing ncompress.
Installing net-tools.
Installing netkit-base.
Installing newt.
Installing sendmail.
Installing setconsole.
Installing setserial.
Installing setuptool.
Installing shapecfg.
Installing slang.
Installing slocate.
Installing stat.
Installing sysklogd.
Installing tar.
Installing tcp_wrappers.
Installing tcpdump.
Installing tcsh.
Installing time.
Installing timeconfig.
Installing timed.
Installing tmpwatch.
Installing traceroute.
Installing utempter.
Installing util-linux.
Installing vim-common.
Installing vim-minimal.
Installing vixie-cron.
Installing which.
Installing zlib.


```
Installing diffutils.
Installing dump.
Installing ed.
Installing eject.
Installing etcskel.
Installing file.
Installing findutils.
Installing gawk.
Installing gd.
Installing gdbm.
Installing getty_ps.
Installing glib.
Installing gmp.
Installing gnupg.
Installing gpm.
Installing groff.
Installing ntsysv.
Installing passwd.
Installing pciutils.
Installing perl.
Installing procmail.
Installing procps.
Installing psmisc.
Installing pump.
Installing python.
Installing quota.
Installing raidtools.
Installing readline.
Installing redhat-logos.
Installing rootfiles.
Installing rpm.
Installing sash.
```

Passo 2

Após ter desinstalado todo o software que deve ser desinstalado após a instalação do nosso servidor Linux (consulte "Softwares que devem ser desinstalados após a instalação do Servidor") e depois da adição dos softwares RPM necessários para a compilação de programas em nosso servidor (Softwares que devem ser instalados após a instalação do Servidor) devemos verificar novamente a lista de todos os programas RPM instalados, mas desta vez com o seguinte comando:

- Para verificar a lista dos pacotes RPM instalados em seu sistema, use o comando:
  [root@deep /]# **rpm -qa > installed_rpm**

A opção "-qa" fará a consulta de todos os pacotes RPM instalados em seu sistema e o caractere especial ">" irá redirecionar a saída para o arquivo chamado "installed_rpm".

O conteúdo do arquivo **installed_rpm** deve se parecer exatamente com isto:

setup-2.0.5-1
filesystem-1.3.5-1
basesystem-6.0-4
ldconfig-1.9.5-15
glibc-2.1.2-11
shadow-utils-19990827-2
mktemp-1.5-1
termcap-9.12.6-15
libtermcap-2.0.8-18
bash-1.14.7-16
MAKEDEV-2.5-2
SysVinit-2.77-2
chkconfig-1.0.7-2
ncurses-4.2-25
info-3.12h-2
fileutils-4.0-8
grep-2.3-2
ash-0.2-18
at-3.1.7-11
m4-1.4-12
bdflush-1.5-10
binutils-2.9.1.0.23-6
bzip2-0.9.5c-1
sed-3.02-4
console-tools-19990302-17
e2fsprogs-1.15-3
byacc-1.9-11
cpio-2.4.2-13
cracklib-2.7-5
cracklib-dicts-2.7.-5
crontabs-1.7-7
textutils-2.0-2
dev-2.7.10-2
diffutils-2.7-16
dump-0.4b4-11
ed-0.2-12
bison-1.28-1
etcskel-2.0-1
file-3.27-3
findutils-4.1-32
gawk-3.0.4-1
cdecl-2.5-9
gdbm-1.8.0-2
autoconf-2.13-5
glib-1.2.5-1
gmp-2.0.2-10
cpp-1.1.2-24
gpm-1.17.9-3
groff-1.11a-9
gzip-1.2.4-14
initscripts-4.48-1
ipchains-1.3.9-3
cproto-4.6-2
ElectricFence-2.1-1
kernel-2.2.12-20
patch-2.5-9
ld-so-1.9.5-11
less-3.4.0-1
libc-5.3.12-31
libstdc++-2.9.0-24
lilo-0.21-10
pwdb-0.60-1
pam-0.68-7
sh-utils-2.0-1
automake-1.4-5
logrotate-3.3-1
losetup-2.9u-4
lsof-4.45-1
mailx-8.1.1-9
man-1.5g-6
mingetty-0.9.4-10
mkbootdisk-1.2.2-1
mkinitrd-2.3-1
modutils-2.1.121-14
mount-2.9u-4
ctags-3.2-1
ncompress-4.2.4-14
net-tools-1.53-1
netkit-base-0.10-37
newt-0.50-13
passwd-0.63-1
perl-5.00503-6
flex-2.5.4a-7
procps-2.0.4-2
psmisc-1.8-3
python-1.5.2-7
quota-1.66-8
gdb-4.18-4
readline-2.2.1-5
glibc-devel-2.1.2-11

rootfiles-5.2-5
rpm-3.0.3-2
sash-3.3-1
make-3.77-6
shapecfg-2.2.12-2
slang-1.2.2-4
slocate-2.0-3
stat-1.5-11
sysklogd-1.3.31-12
tar-1.13.11-1
tcp_wrappers-7.6-9
tcpdump-3.4-16
tcsh-6.08.00-6
time-1.7-9
timed-0.10-23
tmpwatch-2.0-1
traceroute-1.4a5-16
utempter-0.5.1-2
util-linux-2.9w-24
vim-common-5.4-2
vim-minimal-5.4-2
vixie-cron-3.0.1-39
which-2.8-1
zlib-1.1.3-5
dev86-0.14.9-1
egcs-1.1.2-24
kernel-headers-2.2.12-20

O segundo passo é necessário para certificar-se de que não esquecemos de remover os pacotes RPMs desnecessários, bem como, de adicionar alguns pacotes que nos permitem compilar programas no sistema. Se o resultado parecer-se com o nosso arquivo **installed_rpm** acima, então estamos prontos para brincar com o nosso servidor Linux.

Coloque algumas cores no seu terminal

Colocar algumas cores no seu terminal pode ajudar a distinguir pastas, arquivos, dispositivos, links simbólicos e arquivos executáveis dentre os demais. Minha opinião é que as cores nos ajudam a cometer menos erros e a navegar mais rápido em seu sistema.

Edite o arquivo **profile** (vi /etc/profile) e adicione as seguintes linhas:

```
# Cores para o comando ls
eval 'dircolors /etc/DIR_COLORS –b'
export LS_OPTIONS='-s -F -T 0 --color=yes'
```

Edite o arquivo **bashrc** (vi /etc/bashrc) e adicione a linha:

```
alias ls='ls --color=auto'
```

Então, faça logout e login. Depois disto, a nova variável ambiental COLORS estará configurada e o seu sistema a reconhecerá.

Atualização dos softwares mais recentes

Mantenha todos os softwares atualizados com a última versão (especialmente os softwares de rede), verifique as páginas de errata da distribuição Red Hat Linux disponível em http://www.redhat.com/corp/support/errata/index.html. As páginas de errata talvez sejam o melhor recurso para consertar 90% dos problemas mais comuns com o Red Hat Linux. Além disso, brechas de segurança para as quais existe um solução geralmente estão nas páginas de errata 24 horas após a Red Hat ter sido notificada. Você sempre deve verificar lá em primeiro lugar.

Os softwares que devem ser atualizados neste momento para o seu Red Hat Linux 6.1 são:

groff-1_15-1_i386.rpm
sysklogd-1_3_31-14_i386.rpm
initscripts-4_70-1_i386.rpm
e2fsprogs-1.17-1.i386.rpm
pam-0_68-10_i386.rpm
Linux kernel 2.2.14 (linux-2 2 14 tar.gz)

Observação: O kernel do Linux é o mais importante e deve ser sempre atualizado. Veja abaixo para mais informações a construção de um kernel personalizado para o seu sistema específico.

- Você pode verificar se os softwares RPMs acima estão instalados em seu sistema, antes de fazer uma atualização, com o seguinte comando:
  [root@deep /]# **rpm -q <nome_do_software>**

Onde <nome_do_software> é o nome do software que você deseja verificar, como o groff, o sysklogd, etc.

CAPÍTULO 3

Segurança Geral do Sistema

Parte II Referência Relativa à Segurança e Otimização

Nesta Parte:

Segurança Geral do Sistema
Otimização Geral do Sistema

Capítulo 3 Segurança Geral do Sistema

Neste Capítulo:

Segurança Geral do Linux

Segurança Geral do Linux

Visão Geral

Um servidor Linux seguro depende de como o administrador o gerencia. Uma vez eliminados os riscos de segurança em potencial, removendo os serviços RPM desnecessários, podemos agora começar a tornar seguros os serviços e os softwares existentes em nosso servidor. Neste capítulo, discutiremos algumas técnicas básicas gerais para fazer a segurança do seu sistema. O que segue é uma lista de características que podem ser usadas para ajudar a evitar ataques de fontes externas e internas.

1. Segurança a nível de BIOS. Crie uma senha de boot.

É recomendado desabilitar o boot a partir de drives de discos flexíveis e criar uma senha para acessar algumas características da BIOS. Você pode consultar o manual da sua BIOS ou dar uma olhada nela, na próxima vez que fizer o boot, para saber como fazer isto. Eliminar a possibilidade de boot a partir de drives de discos flexíveis e criar uma senha para acessar a BIOS irá melhorar a segurança de seu sistema. Isto irá bloquear pessoas indesejáveis que possam tentar fazer boot em seu sistema Linux com um disco especial de boot e irá protegê-lo contra pessoas que venham tentar alterar a BIOS para habilitar o boot a partir de drives de discos flexíveis ou que venham tentar fazer boot no servidor sem o prompt de senha.

2. Política de Segurança

É importante assinalar que você não pode implementar a segurança sem ter decidido que necessidades devem ser protegidas e de quem se proteger. Você precisa de uma política de segurança, uma lista do que você considera permissível e do que você não considera permissível, para formar a base sobre a qual irá tomar quaisquer decisões relativas à segurança. A política deve também determinar as suas respostas às violações de segurança. O que você deverá considerar ao compilar uma política de segurança irá depender inteiramente da sua definição de segurança. As seguintes perguntas deverão fornecer algumas linhas gerais:

- Como você arquiva as informações confidenciais ou sensíveis ?
- O sistema contém informações confidenciais ou sensíveis ?
- Contra quem exatamente você quer se proteger ?
- Usuários remotos realmente precisam acessar o seu sistema ?
- Senhas e criptografia fornecem proteção suficiente ?
- Você precisa de acesso à Internet ?
- Quanto acesso você quer permitir ao seu sistema a partir da Internet ?
- Que ação você tomará ao descobrir uma brecha em sua segurança ?

Esta lista é curta e a sua política provavelmente englobará muito mais antes de estar completa. Qualquer política de segurança deve basear-se em algum grau de paranóia, decidindo o quanto você deve confiar nas pessoas, tanto de dentro quanto de fora de sua organização. Contudo, a política deve manter um equilíbrio entre a permissão razoável a seus usuários à informações de que precisam para executar seus trabalhos e a total negação de acesso às suas informações. O ponto onde esta linha é traçada determinará a sua política.

3. Escolha uma senha correta

O ponto de partida do nosso tour pela Segurança Geral do Linux é a senha. Muitas pessoas guardam suas informações valiosas e seus arquivos em um computador e a única coisa que impede os outros de vê-las é a string de oito caracteres chamada senha. Em oposição à crença popular, uma senha inquebrável não existe. Dados tempo e recursos, todas as senhas podem ser adivinhadas por engenharia social ou por força bruta.

Engenharia social de senhas de servidor e outros métodos de acesso ainda são a maneira mais fácil e popular de se ganhar acesso à contas e servidores. Frequentemente, algo tão simples quanto agir como um superior ou executivo em uma empresa e gritar com a pessoa certa, na hora certa do dia, produz grandes resultados.

A execução de um quebrador de senhas semanalmente em seu servidor é uma boa idéia. Isto ajuda a encontrar e substituir senhas fracas ou que são facilmente advinhadas. Também, um mecanismo de verificação de senhas deve estar presente para rejeitar uma senha fraca logo na primeira vez que se escolher uma senha ou quando da troca de uma antiga. Strings de caracteres que usam palavras de dicionário, ou que estão todas em caixa alta ou caixa baixa, ou que não contenham números ou caracteres especiais não devem ser aceitas como nova senha.

Recomendamos as seguintes regras para criar senhas efetivas:

- Elas devem ter pelo menos 6 caracteres de comprimento, de preferência 8 caracteres que incluam pelo menos um caractere numérico ou especial.

- Elas não devem ser triviais. Uma senha trivial é aquela que é fácil de ser adivinhada e que, geralmente, está baseada no nome do usuário, no seu cargo ou em outras características pessoais.

- Elas devem ter um período de validade, exigindo-se que sejam trocadas periodicamente.

- Elas devem ser revogadas e resetadas após um número concorrente de tentativas incorretas.

4. O tamanho da senha

Por default, o tamanho mínimo aceitável para uma senha quando você instala o seu sistema Linux é 5. Isto significa que, quando um usuário tem permissão para acessar o servidor, o tamanho da sua senha será no mínimo de 5 entre strings de caracteres, letras, números, caracteres especiais, etc. Isto não é o suficiente e deve ser 8. Para impedir que o administrador ou pessoas inconcientes possam entrar com a sua senha valiosa usando apenas 5 caracteres, edite o não menos importante arquivo "/etc/login.defs" e altere o valor de tamanho 5 para tamanho 8.

Edite o arquivo **login.defs** (vi /etc/login.defs) e altere a linha onde se lê:

PASS_MIN_LEN 5

Passando a ler-se:

PASS_MIN_LEN 8

O "login.defs" é o arquivo de configuração do programa login. Você deve revisar ou fazer alterações neste arquivo para atender ao seu sistema em particular. Aí é onde você configura outras políticas de segurança (como o default para expiração de senhas ou o tamanho mínimo aceitável para o tamanho de uma senha).

5. A conta root

A conta "root" é a conta que tem mais privilégios em um sistema Unix. A conta "root" não tem qualquer restrição de segurança imposta a ela. Isto significa que o sistema pressupõe que você sabe o que está fazendo, e fará exatamente o que você solicitar - sem quaisquer perguntas. Portanto, é fácil, com um comando mal digitado, apagar arquivos cruciais de sistema. Quando se está usando esta conta, é importante ser o mais cuidadoso possível. Por razões de segurança, nunca faça o login em seu servidor como root, a menos que seja absolutamente necessário para execução de tarefas que necessitem de acesso de "root". Também, se você não estiver diante de seu servidor nunca faça login, nem permita que seja feito login como "root". MUITO MUITO MUITO RUIM.

6. Configure o time out para a conta root

Apesar do aviso de nunca fazer login, nem permitir que seja feito login como root, a não ser que seja feito diretamente diante do servidor, os administradores ainda permanecem como "root" ou esquecem de fazer logout após terminar seus trabalhos e deixam seus terminais desatendidos. A solução para resolver este problema é fazer com que o shell bash faça o logout automaticamente após um certo período de inatividade. Para fazer isto, você deve configurar a variável especial do Linux chamada "TMOUT" com o tempo de inatividade em segundos antes do logout.

Edite o seu arquivo **profile** (vi /etc/profile) e adicione a seguinte linha em algum lugar após a linha onde se lê "HISTFILESIZE=" nesse arquivo:

```
TMOUT=7200
```

O valor que entramos para a variável está em segundos e representa 2 horas (60 * 60 = 3600 * 2 = 7200 segundos). É importante observar que se você decidir colocar a linha acima em seu arquivo "/etc/profile", então o logout automático após duas horas de inatividade entrará em vigor para todos os usuários do sistema. Por isso, se, ao invés disso, você quiser controlar quais usuários receberão o logout automático e quais não o receberão, você pode configurar esta variável em seu arquivos ".bashrc" individuais.

7. O arquivo "/etc/exports"

Caso você esteja exportando sistemas de arquivo usando o serviço NFS, certifique-se de configurar o arquivo "/etc/exports" com os acessos mais restritivos possíveis. Isto significa não usar caracteres coringa, nem permitir acesso de gravação ao root, e deve-se permitir montagens somente para leitura sempre que possível.

Edite o arquivo **exports** (vi /etc/exports) e adicione:

Como exemplo:
/dir/to/export host1.mydomain.com(ro,root_squash)
/dir/to/export host2.mydomain.com(ro,root_squash)

Onde "**/dir/to/export**" é o diretório que você deseja exportar, **host#.mydomain.com** é a máquina autorizada a logar nesse diretório, a opção **<ro>** significa somente montagem e a opção **<root_squash>** serve para negar o direito de gravação para o root nesse diretório.

Para que esta alteração tenha efeito, você precisará executar o seguinte comando em seu terminal:

[root@deep /]# **/usr/sbin/export -a**

Observação: Por favor, esteja ciente de que ter um serviço NFS disponível em seu sistema pode representar um risco de segurança. Pessoalmente, eu não recomendo o seu uso.

8. Desabilitando o acesso à programas de console

Em um ambiente seguro, onde temos certeza de que a console está segura devido a implementação das senhas de BIOS e do LILO e todos os botões liga-desliga e reset do sistema estão desabilitados, pode ser vantajoso desabilitar completamente todos os programas com direitos equivalente de console como shutdown, reboot e halt para usuários comuns em seu servidor.

Para fazer isto, execute o seguinte comando:

[root@deep /]# **rm -f /etc/security/console.apps/<nome_do_serviço>**

Onde **<nome_do_serviço>** é o nome do programa ao qual você quer desabilitar o acesso equivalente de console. A menos que você use o xdm, no entanto, seja cuidadoso em não remover o arquivo xserver. Do contrário, ninguém, a não ser o root, poderá iniciar o servidor X. (Se você sempre usa o xdm para iniciar o servidor X, root é o único usuário que precisa iniciar o X, e neste caso você poderá realmente desejar remover o arquivo xserver).

Como um exemplo:

[root@deep /]# **rm -f /etc/security/console.apps/halt**
[root@deep /]# **rm -f /etc/security/console.apps/poweroff**
[root@deep /]# **rm -f /etc/security/console.apps/reboot**
[root@deep /]# **rm -f /etc/security/console.apps/shutdown**
[root@deep /]# **rm -f /etc/security/console.apps/xserver** (se removido, root será o único usuário que poderá iniciar o X)

Esses comandos irão desabilitar o acesso aquivalente a console para os programas halt, poweroff, reboot e shutdown. Mais uma vez, o programa xserver só se aplica se você tiver instalado a interface X-Window em seu sistema.

Observação: Se você estiver seguindo a nossa configuração de instalação, a interface X-Window não estará instalada em seu servidor e todos os arquivos acima não aparecerão no diretório "/etc/security". Portanto, não dê atenção aos passos acima.

9. Desabilitando todo o acesso de console

A biblioteca Linux-PAM, instalada por default em seu sistema, permite ao administrador do sistema escolher como as aplicações autenticam os usuários para acesso a console, arquivos e programas. Para desabilitar todos esses acessos para os usuários, você deve descomentar todas as linhas que se referem a **pam_console.so** no diretório "/etc/pam.d/". Este passo é a continuidade do exposto acima no item "8. Desabilitando o acesso à programas de console".

O seguinte script fará isso automaticamente para você. Como "root", crie o arquivo de script **disabling.sh** (touch disabling.sh) e adicione as seguintes linhas dentro dele:

```
#! /bin/sh
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' <$i> foo && mv foo $i
done
```

Torne este script executável com o seguinte comando e execute-o:

```
[root@deep /]# chmod 700 disabling.sh
[root@deep /]# ./disabling.sh
```

Isto irá comentar todas as linhas que se referem à "pam_console.so" para todos os arquivos localizados sob o diretório "/etc/pam.d". Uma vez executado o script, você poderá removê-lo de seu sistema.

10. O arquivo "/etc/inetd.conf"

O inetd, também chamado de "super servidor", faz a carga de um programa de rede com base em uma solicitação de rede. O arquivo "inetd.conf" diz ao inetd quais portas ouvir e quais servidores iniciar para cada porta. A primeira coisa que você precisa verificar, assim que você colocar o seu servidor Linux em QUALQUER rede, é que serviços você precisa oferecer.

Serviços que você não precisa oferecer devem ser desabilitados e desinstalados para que você tenha uma coisa a menos com que se preocupar e para que atacantes tenham um lugar a menos onde procurar por uma brecha. Dê uma olhada em seu arquivo "/etc/inetd.conf" e verifique que serviços estão sendo oferecidos pelo seu programa inetd. Desabilite os que você não precisa, comentando-os (adicionando um # no início da linha) e, depois, enviando um comando SIGHUP ao processo inetd para refletir a atualização do arquivo inetd.conf.

Passo 1
Altere as permissões deste arquivo para **600**.
[root@deep /]# **chmod 600 /etc/inetd.conf**

Passo 2
CERTIFIQUE-SE de que o proprietário seja **root**.
[root@deep /]# **stat /etc/inetd.conf**

```
File: "/etc/inetd.conf"
Size: 2869          Filetype: Regular File
Mode: (0600/-rw-------)         Uid: (   0/    root)  Gid: (    0/    root)
Device: 8,6   Inode: 18219    Links: 1
Access: Wed  Sep 22  16:24:16  1999(00000.00:10:44)
Modify: Mon Sep 20  10:22:44  1999(00002.06:12:16)
Change: Mon Sep 20  10:22:44  1999(00002.06:12:16)
```


Passo 3
Edite o arquivo **inetd.conf** (vi /etc/inetd.conf) e desabilite serviços como:

ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth e outros, a menos que você planeje usá-los. Se estiverem desligados, o risco será muito menor.

```
# Para re-ler este arquivo após as alterações, simplesmente digite ‘killall -HUP inetd’
#
#echo          stream          tcp     nowait          root    internal
#echo          dgram           udp     wait            root    internal
#discard       stream          tcp     nowait          root    internal
#discard       dgram           udp     wait            root    internal
#daytime       stream          tcp     nowait          root    internal
#daytime       dgram           udp     wait            root    internal
#chargen       stream          tcp     nowait          root    internal
#chargen       dgram           udp     wait            root    internal
#time          stream          tcp     nowait          root    internal
#time          dgram           udp     wait            root    internal
#
# Estes são serviços padrão
#
#ftp           stream          tcp     nowait          root    /usr/sbin/tcpd in.ftpd -l -a
#telnet        stream          tcp     nowait          root    /usr/sbin/tcpd in.telnetd
#
# shell, login, exec, comsat e talk são protocolos BSD
#
#shell         stream          tcp     nowait          root    /usr/sbin/tcpd in.rshd
#login         stream          tcp     nowait          root    /usr/sbin/tcpd in.rlogind
#exec          stream          tcp     nowait          root    /usr/sbin/tcpd in.rexecd
#comsat        stream          tcp     nowait          root    /usr/sbin/tcpd in.comsat
#talk          dgram           udp     wait            root    /usr/sbin/tcpd in.talkd
#ntalk         dgram           udp     wait            root    /usr/sbin/tcpd in.ntalkd
#dtalk         stream          tcp     nowait          nobody /usr/sbin/tcpd in.dtalkd
#
# Serviços de correio pop e imap
#
#pop-2         stream          tcp     nowait          root    /usr/sbin/tcpd ipop2d
#pop-3         stream          tcp     nowait          root    /usr/sbin/tcpd ipop3d
#imap          stream          tcp     nowait          root    /usr/sbin/tcpd imapd
#
# O serviço Internet UUCP
#
#uucp          stream          tcp     nowait          uucp    /usr/sbin/tcpd /usr/lib/uucp/uucico -l
# O serviço tftp é fornecido primariamente para boot remoto. A maioria dos sites
# rodam isto somente em máquinas que funcionam como "servidores de boot".
# Não descomente isto, a menos que "precise".
```

```
#
#tftp          dgram          udp     wait           root    /usr/sbin/tcpd in.tftpd
#bootps        dgram          udp     wait           root    /usr/sbin/tcpd bootpd
#
# finger, systat e netstat fornecem informações de usuários que podem ser valiosas
# para "crackers de sistema" em potencial. Muitos sites preferem desabilitar alguns
# ou todos esses serviços para melhorar a segurança
#
#finger         stream         tcp     nowait         root    /usr/sbin/tcpd in.fingerd
#cfinger        stream         tcp     nowait         root    /usr/sbin/tcpd in.cfingerd
#systat         stream         tcp     nowait         guest   /usr/sbin/tcpd /bin/ps -auWwx
#netstat        stream         tcp     nowait         guest   /usr/sbin/tcpd /bin/netstat -f inet
#
# Autenticação
#
#auth           stream         tcp     nowait         nobody /usr/sbin/in.identd in.identd -l -e -
o
#
# Fim do inetd.conf
```

Observação:

Não esqueça de enviar um sinal SIGHUP ao seu processo inetd (killall -HUP inetd) após fazer as alterações em seu arquivo inetd.conf. Os serviços que você ativa em um determinado host dependem das funções que você quer que o host desempenhe. As funções poderiam suportar o serviço de rede selecionado, outros serviços hospedados neste computador, ou desenvolvimento e manutenção do sistema operacional e das aplicações.

[root@deep /]# **killall -HUP inetd**

Passo 4
Uma outra medida de segurança que você pode tomar para tornar seguro o arquivo "**inetd.conf**" é configurá-lo com atributo de imutável, usando o comando **chattr**.

- Para tornar o arquivo imutável, simplesmente execute o comando:
  [root@deep /]# **chattr +i /etc/inetd.conf**

Isto impedirá quaisquer alterações (acidentais ou não) do arquivo "inetd.conf". Um arquivo com o atributo "i" setado não pode ser modificado, deletado ou renomeado, nenhum link pode ser criado para este arquivo e nenhum dado pode ser gravado nele. A única pessoa que pode setar ou resetar este atributo é o superusuário root.

Caso, mais tarde, você queira modificar o arquivo inetd.conf, você precisará resetar o flag de imutável.

- Para resetar o flag de imutável, simplemente execute o seguinte comando:
  [root@deep /]# **chattr -i /etc/inetd.conf**

11. TCP_WRAPPERS

Por default, o Red Hat Linux permite que todos os serviços sejam solicitados. A utilização do TCP_WRAPPERS torna a segurança dos seus servidores, contra a intrusão externa, muito mais simples e menos dolorosa do que você poderia esperar. Negue todos os hosts, colocando "ALL: ALL@ALL PARANOID" em "/etc/hosts.deny" e liste explicitamente os hosts confiáveis que têm permissão para acessar sua máquina no arquivo "/etc/hosts.allow". Esta é a melhor configuração e a mais segura.

O TCP_WRAPPERS é controlado por dois arquivos e a busca encerra quando a primeira combinação for encontrada.

/etc/hosts.allow
/etc/hosts.deny

- O acesso será permitido quando um par (daemon, cliente) coincidir com uma entrada no arquivo /etc/hosts.allow.
- Do contrário, o acesso será negado quando um par (daemon cliente) coincidir com uma entrada no arquivo /etc/hosts.deny.
- Do contrário, o acesso será permitido.

Passo 1
Edite o arquivo **hosts.deny** (vi /etc/hosts.deny) e adicione a seguinte linha:

 # Por default, o acesso é negado.
 # Negar o acesso a todo mundo:
ALL: ALL@ALL, PARANOID # Coincide com qualquer host cujo nome não coincida com
o seu endereço. Veja abaixo.

Que significa que todos os serviços e todos os endereços que não sejam explicitamente permitidos, são bloqueados, a menos que o acesso seja concedido a eles através das entradas do arquivo de permissão.

Observação:

Com o parâmetro "**PARANOID**", caso você pretenda executar os serviços telnet ou ftp em seu servidor, não esqueça de adicionar o nome e o endereço IP da máquina cliente no seu arquivo "/etc/hosts". Do contrário, pode contar com uma espera de vários minutos até o tempo limite da pesquisa de DNS antes de obter um pronto de login. (login:).

Passo 2
Edite o arquivo **hosts.allow** (vi /etc/hosts.allow) e, por exemplo, adicione a seguinte linha:

sshd: 208.164.186.1 gate.openarch.com

Os hosts explicitamente autorizados são listados no arquivo de permissão.

Para a sua máquina cliente: 208.164.186.1 é o endereço IP e gate.openarch.com é o nome do host de um de seus clientes que está autorizado a usar o sshd.

Passo 3
O programa tcpdchk é o verificador da configuração do TCP_WRAPPERS. Ele examina a configuração do seu TCP_WRAPPERS e relata todos os problemas reais e potenciais que puder encontrar.

- Após ter feito a sua configuração, execute o programa **tcpdchk**:
  [root@deep /]# **tcpdchk**

Observação:

Mensagens de erro podem parecer-se com isto:

warning: /etc/hosts.allow, line 6: can't verify hostname:
gethostbyname(win.openarch.com) failed.

(advertência: /etc/hosts.allow, linha 6: nome de host não pôde ser verificado: gethostbyname(win.openarch.com) falhou).

Se você receber este tipo de mensagem de erro, verifique a existência deste nome de host no seu arquivo de configuração do DNS.

12. O arquivo "/etc/aliases"

A administração descuidada ou errônea do arquivo de pseudônimos (aliases) pode facilmente ser usada para se obter status privilegiado. Por exemplo, vários vendedores distribuem sistemas com um pseudônimo (alias) "**decode**" no arquivo "/etc/aliases". A intenção é oferecer uma maneira fácil para os usuários transferirem arquivos binários usando o correio. No site remetente, o usuário converte o binário para ASCII with "**uuencode**". Depois, envia o resultado por correio ao pseudônimo "**decode**" no site destinatário. Esse pseudônimo bombeia a mensagem de correio através do programa "/usr/bin/uuencode", que converte o ASCII de volta para o arquivo binário original. Você pode imaginar o furo de segurança que pode acontecer com esta característica ativada em seu arquivo "aliases".

Remova a linha do pseudônimo "**decode**" de seu arquivo "/etc/aliases". Da mesma forma, qualquer pseudônimo que execute um programa que você mesmo não colocou lá e nem verificou criteriosamente, deve ser questionado e, provavelmente, removido.

Edite o arquivo **aliases** (vi /etc/aliases) e remova ou comente as seguintes linhas:

```
# Pseudônimos (aliases) básicos do sistema - estes devem estar presentes.
MAILER-DAEMON: postmaster
postmaster:         root

# Redirecionamentos gerais para pseudo-contas.
bin:                root
daemon:             root
#games:             root ← remova ou comente
#ingres:            root ← remova ou comente
nobody:             root
#system:            root ← remova ou comente
#toor:              root ← remova ou comente
#uucp:              root ← remova ou comente

# Pseudônimos bem conhecidos.
#manager:           root ← remova ou comente
#dumper:            root ← remova ou comente
#operator:          root ← remova ou comente

# capture o decode para apanhar riscos de ataques.
#decode:            root

# Pessoa que deve receber os emails do root
#root:              marc
```

Para que esta alteração tenha efeito, você precisa executar:
[root@deep /]# **/usr/bin/newaliases**

13. Impeça o abuso do seu Sendmail por usuários não autorizados

As versões mais recentes do Sendmail (8.9.3) incluem as poderosas características Anti-Spam que podem ajudar a impedir que usuários não autorizados abusem do seu servidor de correio. Para fazer isso, edite o seu arquivo "/etc/sendmail.cf" e faça uma alteração na configuração para bloquear os "abusados".

Edite o arquivo **sendmail.cf** (vi /etc/sendmail.cf) e altere a linha:

O PrivacyOptions=authwarnings

Para que leia:

O PrivacyOptions=authwarnings**,noexpn,novrfy**

Já que indivíduos sem ética abusam com muita frequência destes comandos, esta alteração impedirá que esses abusados usem os comandos "EXPN" e "VRFY", disponíveis no Sendmail. Consulte a seção de instalação e configuração do Sendmail, neste livro, para maiores informações sobre este tópico.

Edite o arquivo **sendmail.cf** (vi /etc/sendmail.cf) e altere a linha:

O SmtpGreetingMessage=$j Sendmail $v/$Z; $b

Para que leia:

O SmtpGreetingMessage=$j Sendmail $v/$Z; $b **NO UCE C=xx L=xx**

Esta alteração não afeta coisa alguma, na verdade, mas foi recomendada por pessoas do newsgroup news.admin.net-abuse.email como uma precaução de ordem legal. Ela modifica o banner que o Sendmail mosta ao receber uma conexão. Você deve substituir o "xx" nas entradas "C= xx L=xx" com o código do seu país e o código da sua localidade. Por exemplo, no meu caso, eu usaria "C=CA L=QC" para Canadá, Quebec.

14. Impeça que seu sistema responda à solicitações de ping

Impedir que o seu sistema responda à solicitações de ping pode representar uma grande melhoria na segurança de sua rede, já que ninguém poderá pingar o seu servidor e receber uma resposta. A pilha de protocolos TCP/IP tem um número de fraquezas que permitem a um atacante usar técnicas de camuflagem para passar dados através de canais pelos quais deveriam passar pacotes benignos. Impedir que o seu servidor responda à solicitação de ping pode ajudar a minimizar o problema.

Um ...
[root@deep /]# **echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all**
... deveria cumprir a tarefa, também, e o seu sistema não responderá à ping em quaisquer interfaces. Você pode adicionar esta linha no seu arquivo "/etc/rc.d/rc.local" para que o comando seja executado automaticamente quando for feito o reboot do sistema. Não responder à pings manteria de fora pelo menos a maioria dos "crackers" porque eles nem mesmo saberiam que o host está lá.

Para ativá-lo novamente, simplesmente
[root@deep /]# **echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all**

15. Não permita que o sistema mostre o arquivo issue

Se você não quiser que o seu arquivo **issue** do sistema seja mostrado quando as pessoas fizerem login remotamente, você poderá alterar uma opção do telnet no seu arquivo "/etc/inetd.conf" para que se pareça com isto:

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h

A adição do flag "-h" no final, fará com que o daemon não mostre qualquer informação de sistema e só mostre ao usuário um pronto de login (login:). Esta saída só é necessária se você estiver usando o daemon do Telnet em seu servidor (ao invés disso, eu recomendo o uso do SSH).

16. O arquivo "/etc/host.conf"

O Linux utiliza uma biblioteca de resolução para obter o endereço IP correspondente à um nome de host. O arquivo "/etc/host.conf" especifica como os nomes são resolvidos. As entradas do arquivo "/etc/host.conf" dizem à biblioteca resolvedora que serviços utilizar, e em que ordem, para resolver os nomes.

Edite o arquivo **host.conf** (vi /etc/host.conf) e adicione as seguintes linhas:

```
# Pesquise nomes via DNS primeiramente, depois consulte o /etc/hosts.
order bind,hosts
# Temos máquinas com múltiplos endereços IP
multi on
# Faça a checagem de falsificação de endereço IP (spoofing)
nospoof on
```

A opção **order** indica a ordem dos serviços. A entrada do exemplo especifica que a biblioteca de resolução deve primeiramente consultar o servidor de nomes para resolver um nome e, depois, verificar o arquivo "/etc/hosts". É recomendado configurar a biblioteca de resolução para primeiramente verificar o servidor de nomes (bind) e, depois, o arquivo de hosts (hosts) para que se obtenha uma melhor performance e segurança em todos os seus servidores. É claro que você precisa ter o software DNS/BIND instalado, do contrário esta configuração não funcionará.

A opção **multi** determina se um host no arquivo "/etc/hosts" pode ter múltiplos endereços IP (múltiplas interfaces ethN). Hosts que tenham mais de um endereço IP são conhecidos como multihomed, porque a presença de múltiplos endereços IP implica que o host tem várias interfaces de rede. Como exemplo, um Gateway Server sempre terá múltiplos endereços IP e, portanto, deverá ter esta opção posta em ON.

A opção **nospoof** indica para se tomar o cuidado de não permitir spoof nesta máquina. O Spoof de IP é um tipo de ataque que funciona enganando-se os computadores em uma relação de confiança, onde o atacante se faz passar por quem na verdade não é. Neste tipo de ataque, uma máquina é configurada para se parecer com um servidor legítimo e, então, emitir conexões e outros tipos de atividade de rede para legitimar sistemas de destino, outros servidores ou grandes sistemas repositórios de dados. Esta opção deve ser colocada em ON para todos os tipos de servidores.

17. Protocolos de Roteamento

O roteamento e os protocolos de roteamento podem criar vários problemas. O roteamento IP na origem, onde um pacote IP contém detalhes sobre que caminho tomar para chegar ao destino pretendido, é perigoso porque, de acordo com a RFC 1122, o host de destino deve responder pelo mesmo caminho. Se um atacante foi capaz de enviar para a sua rede um pacote roteado na origem, então ele poderia interceptar as respostas e enganar o seu host, fazendo-o pensar que está se comunicando com um host confiável. Eu recomendo enfaticamente que você desative o roteamento de IP na origem para proteger o seu servidor deste furo de segurança.

Para desativar o roteamento IP na origem em seu servidor, digite o seguinte comando em seu terminal:

```
[root@deep /]# for f in /proc/sys/net/ipv4/conf/*/accept_source_route; do
> echo 0 > $f
> done
[root@deep /]#
```

Adicione os comandos acima ao arquivo de script "**/etc/rc.d/rc.local**" e você não terá que redigitá-lo novamente na próxima vez que o seu sistema fizer o reboot. Observe que o comando acima desativará os Pacotes Roteados na Origem para todas as suas interfaces (lo, ethN, pppN, etc). Se você pretende instalar as regras de Firewall do IPCHAINS, descritas neste livro (consulte o capítulo 7 Firewall de Rede), você não precisará digitar este comando, visto que ele já aparece no arquivo de script de Firewall.

18. Ativa a Proteção TCP SYN Cookie

Um "Ataque de SYN" é um ataque de negação de serviço (Denial of Service - DoS) que consome todos os recursos de sua máquina, forçando você a fazer o reboot. Ataques de negação de serviço (ataques que incapacitam um servidor devido ao alto volume de tráfego ou ataques que prendem os recursos do sistema o suficiente para que o servidor não consiga responder à uma solicitação de conexão legítima de um sistema remoto) são facilmente alcançáveis a partir de recursos internos ou conexões externas via extranets e Internet. Para ativar a proteção, você tem que fazer o seguinte:

[root@deep /]# **echo 1 > /proc/sys/net/ipv4/tcp_syncookies**

Adicione o comando acima ao arquivo de script "**/etc/rc.d/rc.local**" e você não terá que redigitá-lo novamente na próxima vez que o seu sistema fizer o reboot. Se você pretende instalar as regras de Firewall do IPCHAINS, descritas neste livro (consulte o capítulo 7 Firewall de Rede), você não precisará digitar este comando, visto que ele já aparece no arquivo de script de Firewall.

Observação:

Se você receber uma mensagem de erro durante a execução do comando acima, verifique se a opção TCP syncookie está ativada na configuração do seu kernel:

IP: TCP syncookie support (not enabled by default) (CONFIG_SYN_COOKIES) [Y/n?]

19. O arquivo "/etc/services"

Os números de portas nas quais certos serviços "padrão" são oferecidos estão definidos na RFC 1700 "Assigned Numbers" (Números Atribuídos). O arquivo "/etc/services" permite que programas servidores e clientes convertam nomes de serviços para estes números (portas). A lista é mantida em cada host e armazenada no arquivo "/etc/services". Somente ao "root" é permitido fazer alteração neste arquivo e, ainda assim, é rara a necessidade de se editar o "/etc/services" para fazer alterações, tendo em vista que ele já contém o mapeamento de nome de serviço para número de porta para os serviços mais comuns. Para melhorar a segurança, podemos imunizar este arquivo, visando impedir uma deleção ao adição não autorizada de serviços.

- Para imunizar o arquivo "/etc/services", use o comando:
  [root@deep /]# **chattr +i /etc/services**

20. O arquivo "/etc/securetty"

O arquivo "/etc/securetty" permite a você especificar por quais dispositivos **TTY** o root está autorizado a fazer login. O arquivo "/etc/securetty" é lido pelo programa login (normalmente "/bin/login"). Seu formato é uma lista de nomes de dispositivos **tty** que têm permissão de login. Para todos os outros **tty**s que estejam comentados ou que não apareçam neste arquivo, o login de root está desabilitado.

Desabilite qualquer **tty** que você não precise, comentando-o (# no início da linha).

Edite o arquivo **securetty** (vi /etc/securetty) e comente as seguintes linhas:

tty1
#tty2
#tty3
#tty4
#tty5
#tty6
#tty7
#tty8

O que significa que o root está autorizado a fazer login somente pela tty1. Esta é a minha recomendação: permitir que o "root" faça login somente por um dispositivo tty e usar o comando "su" para mudar para "root", caso você precise de mais dispositivos tty para logar como "root".

21. Contas especiais

É importante verificar e **DESABILITAR TODAS as contas default do vendedor** que você não utilize em seu sistema (algumas contas existem por default mesmo que você não tenha instalado os serviços à elas relacionados em seu servidor). Isto deve ser verificado após cada atualização ou instalação de software novo. O Linux fornece estas contas para várias atividades de sistema, as quais você pode não precisar se você não tiver os serviços instalados em seu servidor. Se você não precisa das contas, remova-as. Quanto mais contas você tem, mais fácil é acessar o seu sistema.

Pressupomos que você esteja usando senhas Shadow em seu sistema Linux. Se você não estiver, você deveria levar em consideração o seu uso, pois ajuda um pouco a estreitar a segurança. Isto já deve estar configurado se você seguiu a nossa instalação do Linux acima e selecionou, em "Authentication Configuration" (Configuração da Autenticação), a opção "Enable Shadow Passwords" (Ativar Senhas Shadow) (veja o capítulo 2, Instalação do Seu Servidor Linux" para mais informações).

- Para deletar um usuário em seu sistema, use o comando:
  [root@deep /]# **userdel username**

- Para deletar um grupo em seu sistema, use o comando:
  [root@deep /]# **groupdel groupname**

Passo 1
Digite os seguintes comandos em seu terminal para deletar os usuários abaixo:

[root@dep /]# **userdel adm**
[root@dep /]# **userdel lp**
[root@dep /]# **userdel sync**
[root@dep /]# **userdel shutdown**
[root@dep /]# **userdel halt**
[root@dep /]# **userdel news**
[root@dep /]# **userdel uucp**
[root@dep /]# **userdel operator**
[root@dep /]# **userdel games** (delete este usuário se você não usar o servidor X Window)
[root@dep /]# **userdel gopher**
[root@dep /]# **userdel ftp** (delete este usuário se você não usar o servidor ftp anônimo)

Passo 2
Digite os seguintes comandos em seu terminal para deletar os grupos de usuários abaixo:

[root@dep /]# **groupdel adm**
[root@dep /]# **groupdel lp**
[root@dep /]# **groupdel news**
[root@dep /]# **groupdel uucp**
[root@dep /]# **groupdel games** (delete este grupo se você não usar o servidor X Window)
[root@dep /]# **groupdel dip**
[root@dep /]# **groupdel pppusers**
[root@dep /]# **groupdel popusers** (delete este grupo se você não usar o servidor pop para email)
[root@dep /]# **groupdel slipusers**

Passo 3
Adicione os usuários necessários ao sistema:

- Para adicionar um novo usuário em seu sistema, use o comando:
  [root@deep /]# **useradd username**

- Para adicionar ou mudar a senha de um usuário em seu sistema, use o comando:
  [root@deep /]# **passwd username**

  Por exemplo:
  [root@deep /]# **useradd admin**
  [root@deep /]# **passwd admin**

  A saída deve parecer-se algo com isto:

  Changing password for user admin
  New UNIX password: algumasenha
  passwd: all authentication tokens updated successfully

Passo 4
O bit de imutável pode ser usado para impedir deleção ou gravação acidental sobre um arquivo que deve ser protegido. Também impede que alguém crie um link simbólico para este arquivo, que tem sido a fonte de ataques envolvendo a deleção de "/etc/passwd", "/etc/shadow", "/etc/group" ou "/etc/gshadow".

- Para ativar o bit de imutável em arquivos de senha e de grupos, use os comandos:

  [root@deep /]# **chattr +i /etc/passwd**
  [root@deep /]# **chattr +i /etc/shadow**
  [root@deep /]# **chattr +i /etc/group**
  [root@deep /]# **chattr +i /etc/gshadow**

Observação:

No futuro, caso você pretenda adicionar ou deletar usuário, grupo de usuários em seu /etc/passwd ou grupo de arquivos, você deve desativar o bit de imutável em todos esses arquivos, do contrário você não conseguirá fazer as suas alterações. Também, caso você pretenda instalar um programa RPM que insira automaticamente um novo usuário aos arquivos passwd e group imunizados, você receberá uma mensagem de erro durante a instalação enquanto você não tiver desativado o bit de imutável desses arquivos.

22. Impedindo que qualquer um faça su para root

O comando su (Substitui Usuário) permite a você se tornar um outro usuário existente no sistema. Por exemplo, você pode temporariamente tornar-se "root" e executar comandos como o superusuário "root". Se você não quer que qualquer um faça um su para root ou queira restringir o comando "su" para certos usuários, então adicione as duas linhas seguintes no início do arquivo de configuração do "su" no diretório "/etc/pam.d/". Recomendamos, enfaticamente, limitar as pessoas que farão "su" para a conta root.

Passo1
Edite o arquivo **su** (vi /etc/pam.d/su) e adicione as duas linhas seguintes no arquivo:

auth sufficient /lib/security/pam_rootok.so debug
auth required /lib/security/pam_wheel.so group=wheel

Após adicionar as duas linhas acima, o arquivo "/etc/pam.d/su" deve parecer-se com isto:

```
#%PAM-1.0
auth        sufficient  /lib/security/pam_rootok.so debug
auth        required    /lib/security/pam_wheel.so group=wheel
auth        required    /lib/security/pam_pwdb.so shadow nullok
account     required    /lib/security/pam_pwdb.so
passwd      required    /lib/security/pam_cracklib.so
passwd      required    /lib/security/pam_pwdb.so shadow use_authok nullok
session     required    /lib/security/pam_pwdb.so
session     optional    /lib/security/pam_xauth.so
```

Que significa que somente aqueles que são membros do grupo "**wheel**" podem fazer su para root.. Isto também inclui o registro em arquivo de log. Observe que o grupo "wheel" é uma conta especial em seu sistema que pode ser usada para este propósito. Você não poderá usar qualquer nome de grupo, caso queira adotar esta técnica. Esta técnica, combinada com a restrição de login de root pelos dispositivos **TTY**, melhorará em muito a segurança do seu sistema.

Passo 2
Agora que já definimos o grupo "wheel" no nosso arquivo de configuração "/etc/pam.d/su", é hora de adicionar os usuários que terão permissão de fazer "su" para a conta "root". Caso você queira tornar, como um exemplo, o usuário admin um membro do grupo "wheel" para que ele possa fazer um su para root, use o seguinte comando:

[root@deep /]# **usermod -G10 admin**

Que significa que "G" é uma lista de grupos suplementares, da qual o usuário também é membro, "10" é o valor numérico da ID do usuário "wheel" e "admin" é o usuário que queremos adicionar ao grupo "wheel". Use o mesmo comando acima para todos os usuários de seu sistema que você queira que façam su para a conta "root".

23. Limitação de recursos

O arquivo **limits.conf**, localizado sob o diretório "/etc/security", pode ser usado para controlar e limitar recursos para os usuários em seu sistema. É importante estabelecer limites de recursos para todos os usuários para que eles não possam fazer ataques do tipo denial of service (número de processos, quantidade de memória, etc). Estes limites terão que ser definidos para o usuário quando ele/ela fizer o login. Por exemplo, a limitação para todos os usuários em seu sistema poderia parecer-se com isto:

Passo 1
Edite o arquivo **limits.conf** (vi /etc/security/limits) e adicione ou troca as linhas para que leiam:

```
*       hard core       0
*       hard rss        5000
*       hard nproc      20
```

Isto diz para proibir a criação de arquivos core (core 0), restringir o número de processos para 20 (nproc 20) e restringir o uso de memória para 5M (rss 5000) para todos, exceto o superusuário "root". Tudo isto refere-se somente aos usuários que tenham entrado através do pronto de login de seu sistema. Com este tipo de cota, você tem mais controle sobre os processos, arquivos core e uso de memória que os usuários podem ter em seu sistema. O asterisco "*" significa: todos os usuários que façam login neste servidor.

Passo 2
Você também deve editar o arquivo "/etc/pam.d/login" e adicionar a seguinte linha no final do arquivo:

session required /lib/security/pam _limits.so

Após adicionar a linha acima, o arquivo "/etc/pam.d/login" deverá parecer-se com isto:

```
#%PAM-1.0
auth            sufficient      /lib/security/pam_securetty.so
auth            required        /lib/security/pam_pwdb.so shadow nullok
auth            required        /lib/security/pam_nologin.so
account         required        /lib/security/pam_pwdb.so
passwd          required        /lib/security/pam_cracklib.so
passwd          required        /lib/security/pam_pwdb.so nullok use_authtok md5 shadow
session         required        /lib/security/pam_pwdb.so
session         required        /lib/security/pam_limits.so
#session        optional        /lib/security/pam_console.so
```


24. Mais controle sobre a montagem de um sistema de arquivo

Você pode ter mais controle sobre a montagem de um sistema de arquivo, como as partições "/home" e "/tmp", com algumas opções como noexec, nodev e nosuid. Isto pode ser configurado no arquivo texto "/etc/fstab". O arquivo fstab contém informações descritivas sobre as opções de montagem dos vários sistemas de arquivo. Cada linha refere-se a um sistema de arquivo.

As informações relacionadas às opções de segurança no arquivo texto fstab, são:

defaults	Permite tudo (cota, leitura/escrita e suid) nesta partição
noquota	Não permite cotas de usuário nesta partição
nosuid	Não permite acesso SUID/SGID nesta partição
nodev	Não permite acesso de dispositivos caractere ou especiais nesta partição
noexec	Não permite a execução de quaisquer binários nesta partição
quota	Permite cotas de usuário nesta partição
ro	Permite somente leitura nesta partição
rw	Permite leitura-escrita nesta partição
suid	Permite acesso SUID/SGID nesta partição

Observação:

Para mais informações sobre o que você pode configurar nesta arquivo (fstab), consulte as páginas de manual sobre o mount (8).

Edite o arquivo **fstab** (vi /etc/fstab) e altere, conforme suas necessidades:

```
/dev/sda11    /tmp    ext2    defaults        1 2
/dev/sda6     /home   ext2    defaults        1 2
```

Para que leia:

```
/dev/sda11    /tmp    ext2    rw,nosuid,nodev,noexec    1 2
/dev/sda6     /home   ext2    rw,nosuid,nodev           1 2
```

Que significa, para <*nosuid*>, não permite que os bits seta-identificador-de-usuário e seta-identificador-de-grupo tenham efeito; para <*nodev*>, não permite a interpretação de dispositivos caraceteres ou especiais nesta partição do sistema de arquivos e; para <*noexec*>, não permite a execução de quaisquer arquivos binários no sistema de arquivo montado. Observe que adicionamos a opção "rw" nas linhas modificadas acima. Isto deve-se ao fato das opções default para estas linhas serem "defaults", o que significa permitir cotas, leitura-escrita e suid. Por isso, devemos adicionar a opção "rw" para continuar a ter acesso de leitura-escrita nestes sistemas de arquivos modificados.

Observação:

No nosso exemplo acima, o "/dev/sda11" representa a nossa partição "/tmp" no sistema e "/dev/sda6" representa a partição "/home". É claro que isto não será o mesmo para você, dependendo de como você particionou o seu disco rígido e do tipo de disco que está instalado em seu sistema: IDE (hda, hdb, etc) ou SCSI (sda, sdb, etc).

25. Mova o binário RPM para um lugar seguro ou altere as suas parmissões default

Uma vez instalado todo o software que você precisa em seu servidor Linux com o comando RPM, é uma boa idéia, para uma melhoria na segurança, movê-lo para um lugar seguro, como um disco flexível ou outro lugar de sua escolha. Com este método, caso alguém acesse o seu servidor e tenha a intenção de instalar softwares danosos com o comando RPM, não conseguirá. É claro que se no futuro você desejar atualizar ou instalar software novo via RPM, tudo o que você precisa fazer é restaurar o binário RPM para o seu diretório original novamente.

- Para mover o binário RPM para um disco flexível, use os comandos:
  [root@deep /]# **mount /dev/fd0 /mnt/floppy**
  [root@deep /]# **mv /bin/rpm /mnt/floppy**
  [root@deep /]# **umount /mnt/floppy**

Observação:

Nunca desinstale completamente o programa RPM de seu sistema. Do contrário, você não conseguirá reinstalá-lo novamente mais tarde, já que para instalar o RPM ou outro software você precisa ter disponíveis todos os comandos RPM.

Mais uma coisa que você pode fazer é alterar as permissões default do comando "rpm" de 755 para 700. Com esta modificação, nenhum usuário que não seja o root poderá usar o programa "rpm" para consultar, instalar, etc, caso você esqueça de movê-lo para um lugar seguro após a instalação de novos programas.

- Para alterar as permissões default do "/bin/rpm", use o comando:
  [root@deep /]# **chmod 700 /bin/rpm**

26. Registro em log do shell

Para tornar fácil a repetição de comandos longos, o shell bash armazena até 500 comandos antigos no arquivo "~/.bash_history" (onde "~/" é o seu diretório base). Cada usuário que tenha uma conta no sistema terá o arquivo ".bash_history" em seu diretório base. A redução do número de comandos antigos nos arquivos ".bash_history" pode proteger os usuários no servidor de entrarem, por engano, suas senhas na tela, em texto plano, e terem suas senhas armazenadas por um longo tempo nos arquivos ".bash_history".

As linhas HISTFILESIZE e HISTSIZE no arquivo "/etc/profile" determinam o tamanho do arquivo de comandos ".bash_history" para todos os usuários de seu sistema. Para todas as contas, eu recomendaria enfaticamente a configuração de HISTFILESIZE e HISTSIZE em "/etc/profile" em um valor baixo, como **20**.

Edite o arquivo **profile** (vi /etc/profile) e altere as linhas para :

HISTFILESIZE=**20**
HISTSIZE=**20**

Que significa que o arquivo ".bash_history" em cada diretório base de usuário poderá armazenar até 20 comandos antigos e nada mais. Agora, se um cracker tentar consultar o arquivo "~/.bash_history" dos usuários de seu servidor para encontrar alguma senha digitada por engano em texto plano, ele terá menos chance de encontrar uma.

27. O arquivo "/etc/lilo.conf"

O LILO é o carregador de boot mais comumente usado para Linux. Ele gerencia o processo de boot e pode fazer boot de imagens de kernel do Linux a partir de discos flexíveis, discos rígidos e até mesmo agir como um gerenciador de boot para outros sistemas operacionais. O LILO é muito importante no Sistema Linux e por esta razão devemos protegê-lo o melhor que pudermos. O arquivo mais importante de configuração do LILO é o arquivo "lilo.conf" que reside sob o diretório "/etc". É com este arquivo que podemos configurar e melhorar a segurança do nosso programa LILO e do sistema Linux. A seguir, três opções importantes que melhorarão a segurança do nosso valioso programa LILO:

- Adição: **timeout=00**
  Esta opção controla quanto tempo (em segundos) o LILO espera por uma entrada do usuário, antes de fazer o boot com a seleção default. Uma das exigências do nível de segurança C2, é que este intervalo de tempo seja 0, a menos que haja dual boot no sistema (boot de mais de um sistema operacional).

- Adição: **restricted**
  Esta opção pede uma senha somente se forem especificados parâmetros na linha de comando (por exemplo, linux single). A opção "restricted" só pode ser usada com a opção "password". Certifique-se de vê-la em cada imagem.

- Adição: **password=<senha>**
  Esta opção pede uma senha ao usuário ao tentar carregar o sistema Linux no modo monousuário (single mode). As senhas são sempre sensíveis a maiúsculas e minúsculas. Também, certifique-se de que o arquivo "/etc/lilo.conf" não mais seja legível por todo mundo. Do contrário, qualquer usuário poderá ler a senha. Aquí está um exemplo do arquivo "lilo.conf" para o nosso LILO protegido:

  Passo 1
  Edite o arquivo **lilo.conf** (vi /etc/lilo.conf) e adicione ou altere as três opções acima, conforme mostrado:

  boot=/dev/sda
  map=/boot/map
  install=/boot/boot.b
  prompt
  timeout=00 ← adicione esta linha.
  password=<senha> ← adicione esta linha e coloque a sua senha.
  image=/boot/vmlinuz-2.2.12-20
  label=linux
  initrd=/boot/initrd-2.2.12-10.img
  root=/dev/sda6
  read-only

Passo 2
Já que o arquivo de configuração "/etc/lilo.conf" agora contém senha não criptografada, ele deve ser lido somente pelo superusuário "root".

[root@deep /]# **chmod 600 /etc/lilo.conf** (não mais será lido por todos).

Passo 3
Agora, devemos atualizar nosso arquivo de configuração "lilo.conf" para que as alterações tenham efeito:

[root@deep /]# **/sbin/lilo -v** (atualiza o arquivo /etc/lilo.conf)

Passo 4
Mais uma medida de segurança que você pode tomar para proteger o arquivo "lilo.conf", é torná-lo imutável, usando o comando **chattr**.

- Para tornar o arquivo imutável, simplesmente use o comando:
  [root@deep /]# **chattr +i /etc/lilo.conf**

E isto impedirá quaisquer alterações (acidentais ou não) no arquivo "lilo.conf". Caso você deseje modificar o arquivo "lilo.conf", você precisará resetar o flag de imutável:

- Para resetar o flag de imutável, use o comando:
  [root@deep /]# **chattr -i /etc/lilo.conf**

28. Desative o comando de desligamento Ctrl-Alt-Del

O comentário (#) na linha listada abaixo no arquivo "/etc/inittab" desativará a possibilidade de se usar o comando Ctrl-Alt-Del para desligar o seu computador. Isto é muito importante, caso você não tenha a melhor segurança física para o seu sistema.

Para fazer isto, edite o arquivo **inittab** (vi /etc/inittab) e altere a linha:

ca::ctrlaltdel:/sbin/shutdown -t3 -r now

Para que leia:

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

Agora, para que a alteração tenha efeito, digite o seguinte no pronto:

[root@deep /]# **/sbin/init q**

29. Cópia física de todos os logs importantes

Uma das considerações de segurança mais importantes é a integridade dos diferentes arquivos de log sob o diretório "/var/log" de seu servidor. Se, apesar de todas as seguranças implementadas em nosso servidor, um cracker conseguir obter acesso a ele, a nossa última defesa são os arquivos de log. Por isto, é muito importante considerar um método de certificar-se da integridade dos nossos arquivos de log.

Se você tiver uma impressora instalada em seu servidor, ou em um outro de sua rede, uma boa idéia seria ter realmente cópias físicas de todos os logs importantes. Isto pode ser facilmente conseguido usando-se uma impressora de formulário contínuo e fazendo-se com que o programa syslog envie todos os logs que pareçam importantes para "/dev/lp0" (o dispositivo de impressão). O cracker poderá alterar arquivos, programas, etc, em seu servidor, porém não poderá fazer nada quando você tiver um papel real com a cópia impressa de todos os seus logs importantes.

Como exemplo:

Para registrar em log todo telnet, correio, mensagens de boot e conexões ssh de seu servidor em uma impressora conectada a este servidor, você desejará adicionar a seguinte linha no arquivo "/etc/syslog.conf":

Edite o arquivo syslog.conf (vi /etc/syslog.conf) e adicione, no final deste arquivo, a seguinte linha:

authpriv.*;mail.*;local7.*;auth.*;daemon.info /dev/lp0

- Agora, reinicialize o seu daemon syslog para que a alteração tenha efeito:
  [root@deep /]# **/etc/rc.d/init.d/syslogd restart**

Como exemplo:

Para registrar em log todo telnet, correio, mensagens de boot e conexões ssh de seu servidor em uma impressora conectada a um servidor remoto em sua rede local, você desejará adicionar a seguinte linha no arquivo "/etc/syslog.conf" do servidor remoto:

Caso você não tenha uma impressora em sua rede, você também poderá copiar todos os arquivos de log para uma outra máquina simplesmente omitindo o primeiro passo abaixo de adicionar "/dev/lp0" ao seu arquivo "syslog.conf" na máquina remota e indo diretamente para o passo da opção "-r" na máquina remota. Usar o recurso de cópia de todos os seus arquivos de log para uma outra máquina lhe dará a possibilidade de controlar todas as mensagens do syslog em um único host e diminuirá as necessidades de administração.

Edite o arquivo syslog.conf (vi /etc/syslog.conf) do servidor remoto (por exemplo, mail.openarch.com) e adicione, no final deste arquivo, a seguinte linha:

authpriv.*;mail.*;local7.*;auth.*;daemon.info /dev/lp0

Já que a configuração default do daemon do syslog é de não receber quaisquer mensagens da rede, devemos habilitar, no servidor remoto, a facilidade de receber mensagens a partir da rede. Para habilitar a facilidade de receber mensagens a partir da rede no servidor remoto, adicione a opção "-r" ao arquivo de script do daemon do syslog (somente no host remoto):

- Edite o daemon do **syslog** (vi +24 /etc/rc.d/init.d/syslogd) e altere:

  daemon syslogd -m 0

  Para que leia:

  daemon syslogd -r -m 0

- Agora, reinicialize o daemon do syslog no host remoto para que a alteração tenha efeito:

  [root@deep /]# **/etc/rc.d/init.d/syslogd restart**

Agora, se tivermos um firewall no servidor remoto (supõe-se que você o tenha), devemos adicionar ou verificar a existência das seguintes linhas:

```
ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $SYSLOG_CLIENT \
        -d $IPADDR 514 -j ACCEPT
```

Onde EXTERNAL_INTERFACE="eth0" no arquivo de firewall.
Onde IPADDR="208.164.186.2" no arquivo de firewall.
Onde SYSLOG_CLIENT="208.164.168.0/24" no arquivo de firewall.

- Agora, reinicialize o seu firewall no host remoto para que as alterações tenham efeito:

  [root@deep /]# **/etc/rc.d/init.d/firewall restart**

Esta regra de firewall permitirá que sejam aceitos pacotes UDP entrantes pela porta 514 (porta do syslog) do servidor remoto a partir do nosso cliente interno. Para mais informações sobre firewall, consulte o capítulo 7 "Firewall de Rede".

Finalmente, edite o arquivo syslog.conf (vi /etc/syslog.conf) do servidor local e adicione, no final deste arquivo, a seguinte linha:

authpriv.*;mail.*;local7.*;auth.*;daemon.info @mail

Onde "mail" é o nome de host do servidor remoto. Agora, se alguém hackear o seu sistema a apagar logs vitais do sistema, você ainda terá uma cópia de tudo. Então, deveria ser relativamente simples rastrear de onde veio o ataque e tratá-lo adequadamente.

- Agora, reinicialize o daemon do seu syslog para que as alterações tenham efeito:

  [root@deep /]# **/etc/rc.d/init.d/syslogd restart**

Da mesma forma que no host remoto, devemos adicionar ou verificar a existência das seguintes linhas em nosso arquivo de script de firewall no host local:

```
ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR 514 \
        -d $SYSLOG_SERVER 514 -j ACCEPT
```

Onde EXTERNAL_INTERFACE="eth0" no arquivo de firewall.
Onde IPADDR="208.164.186.1" no arquivo de firewall.
Onde SYSLOG_SERVER="mail.openarch.com" no arquivo de firewall.

- Agora, reinicialize o seu firewall para que as alterações tenham efeito:

  [root@deep /]# **/etc/rc.d/init.d/firewall restart**

Esta regra de firewall permitirá que sejam aceitos pacotes UDP saintes pela porta 514 (porta do syslog), do servidor local, com destino ao servidor de syslog remoto. Para mais informações sobre firewall, consulte o capítulo 7 "Firewall de Rede".

Observação:

Nunca use o seu Servidor de Gateway como um host de controle para todas as mensagens do syslog. Esta é uma idéia muito ruim. Mais opções e estratégias existem com o programa sysklogd. Consulte as páginas de manual sobre sysklogd (8), syslog (2) e syslog.conf (5) para maiores informações.

30. Conserte as permissões dos arquivos de script no diretório "/etc/rc.d/init.d"

Conserte as permissões dos arquivos de script responsáveis por iniciar e parar todos os seus processos normais que necessitam ser executados por ocasião do boot.

[root@deep /]# **chmod -R 700 /etc/rc.d/init.d/***

Que significa que somente o root tem permissão para Ler, Escrever e Executar arquivos de script deste diretório. Não acho que usuários comuns precisem saber do conteúdo desses arquivos de script.

Observação:

Se você instalar um novo programa ou atualizar um programa que utilize o script System V localizado sob o diretório "/etc/rc.d/init.d", não esqueça de alterar ou verificar as permissões deste arquivo de script novamente.

31. O arquivo "/etc/rc.d/rc.local"

Por default, quando você faz login no Linux, ele informa o nome da distribuição Linux, a versão, a versão do kernel e o nome do servidor. Isto é liberar informação demais. Nós preferimos apenas apresentar ao usuário um "Login:".

Passo 1
Para fazer isto, edite o arquivo "/etc/rc.d/rc.local" e coloque um "**#**" na frente das seguintes linhas, conforme mostrado:

--
Isto irá sobrescrever o /etc/issue a cada boot. Assim, faça quaisquer alterações que
queira fazer no /etc/issue aquí. Do contrário, você as perderá quando fizer o reboot.
#echo "" > /etc/issue
#echo "$R" >> /etc/issue
#echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue
#
#cp -f /etc/issue /etc/issue.net
#echo >> /etc/issue
--

Passo 2
Então, remova os arquivos "issue.net" e "issue" do diretório "/etc":

[root@deep /]# **rm -f /etc/issue**
[root@deep /]# **rm -f /etc/issue.net**

Observação:

O arquivo "/etc/issue.net" é o banner de login que os usuários verão quando fizerem uma conexão via rede com a sua máquina (ou seja: telnet, SSH). Você o encontrará no diretório "/etc", juntamente com um arquivo chamado "issue", que é o banner de login mostrado aos usuários locais. É um arquivo somente texto e pode ser personalizado segundo o seu gosto, porém esteja ciente de que se você alterá-lo ou removê-lo como fizemos, você também terá que modificar o shell script "/etc/rc.d/rc.local", que recria tanto o arquivo "issue" quanto o arquivo "issue.net" cada vez que o sistema é reinicializado.

32. Bits dos programas pertencentes ao root

Um usuário comum poderá executar um programa como root se este programa estiver com SUID root. Todos os programas e arquivos em seu computador com os bits "s" aparecendo, estão com os bits SUID (- rw**s** r-x r-x) ou SGID (- r-x r-**s** r-x) ativados. Já que esses programas concedem privilégios especiais ao usuário que os está executando, é importante remover os bits "s" dos programas pertencentes ao root que absolutamente não precisem de tais privilégios. Isto pode ser feito executando-se o comando **'chmod a-s'** com os nomes dos arquivos SUID/SGID como argumentos.

Tais programas incluem, mas não estão limitados a:

- Programas que você nunca usa.
- programas que você não quer que qualquer usuário não-root use.
- Programas que você usa ocasionalmente e que não se importa em fazer um su (1) para root para executá-los.

Colocamos um asterisco (*) próximo de cada programa que pessoalmente poderíamos desabilitar e considerá-los não necessários para o trabalho obrigatório de nosso servidor. Lembre-se de que o seu sistema precisa de alguns programas suid root para funcionar adequadamente. Portanto, tenha cuidado.

- Para encontrar todos os arquivos com bits "s" pertencentes ao root, use o comando:
  [root@deep /]# **find / -type f \(-perm -04000 -o -perm 02000 \) \-exec ls -lg {} \;**

***-rwsr-xr-x 1 root root 35168 Sep 22 23:35 /usr/bin/chage**
***-rwsr-xr-x 1 root root 36756 Sep 22 23:35 /usr/bin/gpasswd**
***-r-xr-sr-x 1 root tty 6788 Sep 6 18:17 /usr/bin/wall**
-rwsr-xr-x 1 root root 33152 Aug 16 16:35 /usr/bin/at
-rwxr-sr-x 1 root man 34656 Sep 13 20:26 /usr/bin/man
-r-s--x--x 1 root root 22312 Sep 25 11:52 /usr/bin/passwd
-rws--x--x 2 root root 518140 Aug 30 23:12 /usr/bin/suidperl
-rws--x--x 2 root root 518140 Aug 30 23:1 /usr/bin/sperl5.00503
-rwxr-sr-x 1 root slocate 24744 Sep 20 10:29 /usr/bin/slocate
***-rws--x--x 1 root root 14024 Sep 9 01:01 /usr/bin/chfn**
***-rws--x--x 1 root root 13768 Sep 9 01:01 /usr/bin/chsh**
***-rws--x--x 1 root root 5576 Sep 9 01:01 /usr/bin/newgrp**
***-rwxr-sr-x 1 root tty 8328 Sep 9 01:01 /usr/bin/write**
-rwsr-xr-x 1 root root 21816 Sep 10 16:03 /usr/bin/crontab
***-rwsr-xr-x 1 root root 5896 Nov 23 21:59 /usr/sbin/usernetctl**
***-rwsr-xr-x 1 root bin 16488 Jul 2 10:21 /usr/sbin/traceroute**
-rwxr-sr-x 1 root utmp 6096 Sep 13 20:11 /usr/sbin/utempter
-rwsr-xr-x 1 root root 14124 Aug 17 22:31 /bin/su

***-rwsr-xr-x 1 root root 53620 Sep 13 20:26 /bin/mount**
***-rwsr-xr-x 1 root root 26700 Sep 13 20:26 /bin/umount**
***-rwsr-xr-x 1 root root 18228 Sep 10 16:04 /bin/ping**
***-rwxr-sr-x 1 root root 3860 Nov 23 21:59 /sbin/netreport**
-r-sr-xr-x 1 root root 26309 Oct 11 20:48 /sbin/pwdb_chkpwd

- Para desativar os bits suid nos programas selecionados acima, digite os seguintes comandos:

```
[root@deep /]# chmod a-s /usr/bin/chage
[root@deep /]# chmod a-s /usr/bin/gpasswd
[root@deep /]# chmod a-s /usr/bin/wall
[root@deep /]# chmod a-s /usr/bin/chfn
[root@deep /]# chmod a-s /usr/bin/chsh
[root@deep /]# chmod a-s /usr/bin/newgrp
[root@deep /]# chmod a-s /usr/bin/write
[root@deep /]# chmod a-s /usr/sbin/usernetctl
[root@deep /]# chmod a-s /usr/sbin/traceroute
[root@deep /]# chmod a-s /bin/mount
[root@deep /]# chmod a-s /bin/umount
[root@deep /]# chmod a-s /bin/ping
[root@deep /]# chmod a-s /sbin/netreport
```

Se você quiser saber o que esses programas fazem, execute um "man <nome_do_programa> e leia.

Como exemplo:

[root@deep /]# **man netreport**

33. Arquivos ocultos ou incomuns

É importante não esquecer de dar uma olhada em todo o sistema a procura de arquivos ocultos ou incomuns (arquivos que comecem com um ponto (".") e que normalmente não são mostrados pelo comando "ls"), pois estes podem esconder ferramentas e informações (programas de quebra de senha, arquivos de senhas de outros sistemas, etc). Uma técnica comum em sistemas UNIX é colocar um diretório ou arquivo oculto na conta de um usuário com um nome incomum, algo como '...' ou '.. ' (ponto ponto espaço) ou '..^G' (ponto ponto Ctrl-G). O programa find pode ser usado para procurar arquivos ocultos.

Como exemplo:
[root@deep /]# **find / -name ".. " -print -xdev**
[root@deep /]# **find / -name ".*" -print -xdev | cat -v**

Observação:

Arquivos com nomes tais como '.xx' e '.mail' têm sido usados (ou seja, arquivos que poderiam parecer normais).

34. Encontre todos os arquivos com o bit SUID/SGID ativado

Todos os arquivos SUID e SGID que ainda existam em seu sistema, após termos removido todos aqueles que não precisam de tais privilégios, representam um risco de segurança em potencial e devem ser monitorados de perto. Já que esses programas concedem privilégios especiais aos usuários que os esteja executando, é necessário assegurar-se de que programas inseguros não sejam instalados.

Uma das artimanhas favoritas dos crackers é explorar programas SUID "root" e deixar um programa SUID como backdoor (porta dos fundos) para obter acesso na próxima vez. Encontre todos os programas SUID e SGID em seu sistema e procure saber o que cada um é para que você saiba a respeito de qualquer alteração que possa indicar um intruso em potencial.

- Use o seguinte comando para encontrar todos os programas SUID/SGID em seu sistema:
  [root@deep /]# **find / -type f \(-perm 04000 -o -perm -02000 \) \-exec ls -lg {} \;**

  Observação:

  Consulte o capítulo 10 "Softwares de segurança (Ferramentas de Monitoração)" para mais informações sobre o software sXid que fará o trabalho para você automaticamente a cada dia e reportará sobre os resultados via email.

35. Encontre grupos, arquivos e diretórios com direito de escrita para todos

Grupos, arquivos e diretórios que podem ser gravados por todos, particularmente sistemas de arquivo (partições), podem ser um furo de segurança se um cracker ganhar acesso ao seu sistema e modificá-los. Além disso, diretórios com direito de escrita para todos são perigosos, já que eles permitem a um cracker adicionar e deletar arquivos como quiserem nesses diretórios. No curso normal de operação, vários arquivos serão gravados, incluindo alguns dos diretórios "/dev", "/var/catman" e todos os links simbólicos em seu sistema.

- Para localizar todos os grupos e arquivos com direito de escrita para todos, use o comando:
  [root@deep /]# **find / -type f \(-perm -2 -o -perm -20 \) -exec ls -lg {} \;**

- Para localizar todos os grupos e diretórios com direito de escrita para todos, use o seguinte comando:
  [root@deep /]# **find / -type d \(-perm -2 -o -perm -20 \) -exec ls -ldg {} \;**

  Observação:

  Um verificador de integridade de arquivos e diretórios, como o software Tripwire, pode ser usado regularmente para varrer, gerenciar e encontrar com facilidade grupos ou arquivos e diretórios com direito de escrita para todos que tenham sido modificados. Consulte, neste livro, o capítulo 10 "Softwares de Segurança (Ferramentas de Monitoração)" para mais informações sobre o Tripwire.

36. Arquivos sem proprietários

Não permita quaisquer arquivos sem dono. Arquivos sem proprietários podem ser uma indicação de que um intruso acessou o seu sistema. Se você encontrar um arquivo ou diretório sem proprietário em seu sistema, verifique sua integridade e, se tudo parecer bem, dê-lhe um nome de proprietário. Às vezes, você pode desinstalar um programa e obter um arquivo ou diretório sem proprietário relacionado a esse software. Neste caso, você pode remover o arquivo ou diretório com segurança.

- Para localizar arquivos em seu sistema que não tenham um proprietário, use o seguinte comando:
  [root@deep /]# **find / -nouser -o nogroup**

  Observação:

  Mais uma vez, arquivos do diretório "/dev" não contam.

37. Encontrando arquivos ".rhosts"

Encontrar todos os arquivos ".rhosts" que possam existir em seu servidor deve ser parte das obrigações administrativas regulares de seu sistema, pois esses arquivos não devem ser permitidos em seu sistema. Lembre-se de que um cracker somente precisa de uma conta insegura para potencialmente ganhar acesso à sua rede inteira.

- Você pode localizar todos os arquivos ".rhosts" em seu sistema com o seguinte comando:
  [root@deep /]# **find /home -name .rhosts**

Você também pode usar uma tarefa cron para periodicamente verificar, relatar os conteúdos e deletar os arquivos $HOME/.rhosts. Também, os usuários devem estar cientes de que você regularmente executa este tipo de auditoria, conforme orientação da política de segurança.

- Para usar uma tarefa cron para periodicamente verificar e relatar via email todos os arquivos ".rhosts", faça o seguinte:

  Crie, como "root", o arquivo de script **find_rhosts_files** no diretório "/etc/cron.daily" (touch /etc/cron.daily/find_rhosts_files) e adicione as seguintes linhas a este arquivo de script:

  ```
  #! /bin/bash
  /usr/bin/find /home -name .rhosts | (cat <<EOF
  Este é um relatório automatizado dos possíveis arquivos ".rhosts" existentes no servidor deep.openarch.com, gerado pelo comando find.

  Novos arquivos ".rhosts" detectados no diretório "/home" incluem:
  EOF
  cat
  ) | /bin/mail -s "Conteúdo do relatório de auditoria de arquivos .rhosts" root
  ```

Agora torne este arquivo de script executável e faça com que o arquivo pertença ao usuário e grupo "root":

[root@deep /]# **chmod 755 /etc/cron.daily/find_hosts_files**
[root@deep /]# **chown 0.0 /etc/cron.daily/find_hosts_files**

A cada dia, um email será enviado ao "root" com o assunto "Conteúdo do relatório de auditoria de arquivos .rhosts", contendo a descoberta potencial de novos arquivos ".rhosts".

38. O sistema foi comprometido

Se você acredita que o seu sistema foi comprometido, entre em contato com o CERT ® Coordination Center ou com seu representante no FIRST (Forum of Incident Response and Security Teams - Fórum de Respostas à Incidentes e Equipes de Segurança).

Email Internet:	cert@cert.org
CERT Hotline:	(+1) 412-268-7090
Fax:	(+1) 412-268-6989

O pessoal do CERT/CC responde das 08:00 da manhã às 08:00 da noite EST (GMT -5) / EDT (GMT -4) em dias úteis. Eles aceitam chamadas durante outros horários e durante fins de semana e feriados.

CAPÍTULO 4

Firewall de Rede

Capítulo 4 Firewall de Rede

Neste Capítulo:

Linux IPCHAINS
Construa um kernel com suporte à Firewall IPCHAINS
Algumas explicações sobre regras usadas em arquivos de scripts de firewall
Os arquivos de scripts de firewall
Configuração dos arquivo de script para o Servidor Web
Configuração dos arquivo de script para o Servidor de Email

Linux IPCHAINS

Visão Geral

Alguém poderá me dizer: por quê eu iria querer algo como um produto de firewall comercial ao invés de usar o IPchains e restringir certos pacotes e outras coisas? O que eu estou perdendo por usar o IPchains? Agora, sem dúvida alguma, há espaço para debate sobre isto. O IPchains é tão bom (a maioria das vezes melhor) quanto pacotes de firewall comerciais, do ponto de vista de funcionalidade e suporte. Você, provavelmente, terá mais compreensão do que está acontecendo em sua rede usando o IPchains do que usando uma solução comercial. Tendo dito isto, uma porção de pessoas do tipo corporativo irá querer dizer aos seus acionistas, CEO/CTO, etc. que eles têm o suporte de uma respeitável Empresa de Software de segurança. O firewall poderia estar fazendo nada mais do que deixar passar todo o tráfego e ainda assim o tipo corporativo se sentiria mais confortável do que ter que confiar no cara do cubículo da esquina que fica irritado quando ligam as luzes antes do meio-dia.

No final, muitas empresas desejam poder se virar e exigir algum tipo de restituição de um vendedor se a rede ficar vulnerável, mesmo que não consigam realmente levar alguma coisa ou mesmo tentar. Tudo o que eles podem fazer tipicamente com uma solução open source (fonte aberto) é demitir o cara que a implementou. Pelo menos, alguns dos firewalls comerciais são baseados em Linux ou algo similar. É bem provável que o IPchains seja seguro o bastante para você, mas não para aqueles comprometidos com sérios valores de altas ações comerciais. Fazer uma análise custo/benefício e uma série de perguntas pertinentes é recomendado antes de gastar dinheiro sério em um firewall $$$$. Do contrário, você poderá terminar com algo inferior à sua ferramenta IPchains. Alguns firewalls NT não são, na verdade, melhores do que o IPchains e o consenso geral na bugtraq e na bugtraq NT (listas de email sobre segurança) é de que o NT é, de longe, muito inseguro para firewall sério.

O que vem a ser uma Política de Segurança por Firewall de Rede?

A política de segurança por firewall de rede define explicitamente aqueles serviços que serão permitidos ou proibidos, como esses serviços serão usados e as exceções à estas regras. Um política geral de segurança da empresa deve ser determinada de acordo com a análise de segurança e a análise das necessidades de negócios. Já que um firewall está relacionado somente à segurança de rede, um firewall tem pouco valor, a menos que uma política geral de segurança seja adequadamente definida. Cada regra da política de segurança por firewall de rede deve ser implementada em um firewall. Geralmente, um firewall usa um dos seguintes métodos:

Tudo o que não for especificamente permitido, é proibido

Esta abordagem bloqueia todo o tráfego entre duas redes, exceto para aqueles serviços e aplicações que sejam permitidos. Portanto, cada serviço e aplicação desejados devem ser implementados um a um. Nenhum serviço ou aplicação que possa ser um

potencial furo no firewall deve ser permitido. Este é o método mais seguro: negar serviços e aplicações, a menos que o administrador dê permissões explícitas. Por outro lado, do ponto de vista dos usuários, isto pode ser mais restritivo e menos conveniente. Este método é o que usaremos em nossos arquivos de configuração de Firewall, neste livro.

Tudo o que não for especificamente proibido, é permitido

Esta abordagem permite todo o tráfego entre duas redes, exceto para aqueles serviços e aplicações que sejam proibidos. Portanto, cada serviço ou aplicação potencialmente prejudicial ou não confiável deve ser proibido um a um. Embora este método seja flexível e conveniente para os usuários, ele poderia, potencialmente, causar alguns problemas sérios de segurança.

O que vem a ser Filtro de Pacotes?

Filtro de Pacotes é o tipo de firewall que vem embutido no kernel do Linux. Um filtro de pacotes funciona a nível de rede. Só é permitido aos dados deixarem o sistema se as regras do firewall assim o permitirem. Todos os pacotes que chegam são filtrados pelo seu tipo, endereço de origem, endereço de destino e informações de portas contidas em cada pacote.

Na maioria das vezes, a filtragem de pacotes é feita usando-se um roteador que possa repassar pacotes de acordo com as regras de filtragem. Quando um pacote chega em um roteador de filtragem de pacotes, o roteador extrai certas informações do cabeçalho do pacote e toma decisões, de acordo com as regras do filtro, relativas a passagem ou ao descarte do pacote.

As seguintes informações podem ser extraídas do cabeçalho do pacote:

- Endereço IP de origem
- Endereço IP de destino
- Porta TCP/UDP de origem
- Porta TCP/UDP de destino
- Tipo de mensagem ICMP
- Informação do protocolo encapsulado (TCP, UDP, ICMP ou túnel IP)

Já que poucos dados são analisados e registrados em log, firewalls tipo filtro consomem menos CPU e criam menos latência em sua rede. Há muitas maneiras de estruturar sua rede para proteger seus sistemas usando um firewall.

A Topologia

Todas as máquinas servidoras devem, pelo menos, ser configuradas para bloquear portas que não estejam em uso mesmo que não exista um servidor de firewall. Isto é necessário para maior segurança. Imagine que alguém ganhe acesso ao seu servidor gateway de firewall! Se os seus servidores vizinhos não estiverem configurados para

bloquear as portas que não estejam em uso, então vamos ter uma festa! O mesmo é verdade para uma conexão local. Empregados não autorizados podem ganhar acesso a partir da rede interna aos seus outros servidores.

Em nossa configuração, lhe daremos três exemplos diferentes que poderão ajudá-lo a configurar as regras de seu firewall, dependendo dos tipos de servidores que você quer proteger e da posição destes servidores dentro da sua arquitetura de rede. O primeiro exemplo de arquivo de regras de firewall será para um Servidor Web, o segundo para um servidor de Email e o último para um Servidor de Gateway que age como um proxy para o Wins interno, para as Estações de Trabalho e para as máquinas Servidoras. Veja o gráfico mostrado abaixo para ter uma idéia:

www.openarch.com DNS Somente de Cache 208.164.186.3	deep.openarch.com Servidor DNS Mestre 208.164.186.1	mail.openarch.com Servidor DNS Escravo 208.164.186.2
1. Tráfego ilimitado na interface loopback permitido. 2. Tráfego ICMP permitido. 3. Cache, Cliente e Servidor DNS na porta 53 permitido. 4. Servidor SSH na porta 22 permitido. 5. Servidor HTTP na porta 80 permitido. 6. Servidor HTTPS na porta 443 permitido. 7. Cliente SMTP na porta 25 permitido. 8. Servidor FTP nas portas 20 e 21 permitido. 9. Solicitação de traceroute sainte permitida.	1. Tráfego ilimitado na interface loopback permitido. 2. Tráfego ICMP permitido. 3. Cliente e Servidor DNS na porta 53 permitido. 4. Servidor e Cliente SSH na porta 22 permitidos. 5. Servidor e Cliente HTTP na porta 80 permitidos. 6. Servidor e Cliente HTTPS na porta 443 permitidos. 7. Cliente WWW-CACHE na porta 8080 permitido. 8. Cliente POP externo na porta 110 permitido. 9. Cliente NNTP NEWS externo na porta 119 permitido. 10. Cliente e Servidor SMTP na porta 25 permitidos. 11. Servidor IMAP na porta 143 permitido. 12. Cliente IRC na porta 6667 permitido. 13. Cliente ICQ na porta 4000 permitido. 14. Cliente FTP nas portas 20 e 21 permitido. 15. Cliente RealAudio / QuickTime permitido. 16. Solicitação traceroute sainte permitida.	1. Tráfego ilimitado na interface loopback permitido. 2. Tráfego ICMP permitido. 3. Cliente e Servidor DNS na porta 53 permitido. 4. Servidor SSH na porta 22 permitido. 5. Cliente e Servidor SMTP na porta 25 permitidos. 6. Servidor IMAP na porta 143 permitido. 7. Solicitação traceroute sainte permitida.

A tabela acima mostra as portas que eu habilito por default nos diferentes servidores em meu arquivo de script de firewall, neste livro. Dependendo de quais serviços devem estar disponíveis no servidor para acesso externo, você deve configurar o seu arquivo de script de firewall para permitir o tráfego nas portas especificadas.

www.openarch.com é o nosso Servidor Web, **mail.openarch.com** é o nosso Servidor Concentrador de Email para toda a rede interna e **deep.openarch.com** é o nosso Servidor de Gateway para todos os exemplos explicados neste capítulo.

Compile um kernel com suporte a Firewall IPCHAINS

A primeira coisa que você precisa fazer é assegurar-se que o seu kernel foi compilado com Firewall e com suporte a Firewall de Rede ativado. Lembre-se de que todas as máquinas servidoras devem ser configuradas para bloquear, pelo menos, portas que não estejam em uso, mesmo que não haja um servidor de firewall. No kernel versão 2.2.14, você precisa assegurar-se de que respondeu **Y** às seguintes perguntas:

Networking options (Opções de rede):

Network firewalls (CONFIG_FIREWALL) [N] **Y**
IP:Firewall (CONFIG_IP_FIREWALL) [N] **Y**
IP:TCP syncookie support (CONFIG_SYN_COOKIES) [N] **Y**

Observação:

Se você seguiu a seção Linux Kernel e compilou o seu kernel, as opções "Network firewalls, IP:Firewalling e IP:TCP syncookie support", mostradas acima, já foram configuradas.

Algumas explicações sobre as regras usadas nos arquivos de scripts de firewall

O que se segue é uma explicação de algumas regras que serão usadas nos exemplos de Firewall abaixo. Isto é apenas uma referência. Os arquivos de scripts de firewall estão bem comentados e muito fáceis de modificar.

Constantes usadas nos exemplos de arquivos de scripts de firewall

Constantes são usadas para a maioria dos valores. As constantes mais básicas são:

EXTERNAL_INTERFACE
Este é o nome da interface externa de rede com a Internet. Está definida como **eth0** nos exemplos.

LOCAL_INTERFACE_1
Este é o nome da interface interna de rede com a LAN, caso haja. Está definida como **eth1** nos exemplos.

LOOPBACK_INTERFACE
Este é o nome da interface de loopback. Está definida como **lo** nos exemplos.

IPADDR

Este é o endereço IP da sua interface externa. Pode ser ou um endereço IP estático registrado no InterNIC ou pode ser um endereço atribuído dinamicamente pelo seu provedor de serviços Internet (normalmente via DHCP).

LOCALNET_1

Este é o endereço de sua LAN, caso haja - toda a faixa de endereços IP usada pelas máquinas de sua LAN. Os endereços podem ser atribuídos estaticamente ou você poderia rodar um servidor DHCP local para atribuí-los. Nestes exemplos, a faixa é 192.168.1.0/24: parte da faixa de endereços privados Classe C.

ANYWHERE

Anywhere é um rótulo para um endereço usado pelo IPchains para coincidir com qualquer endereço (não-broadcast). Ambos os programas fornecem **any/0** como um rótulo para este endereço, que é 0.0.0.0/0.

NAMESERVER_1

Este é o endereço IP do seu Servidor DNS Primário de sua rede ou de seu provedor.

NAMESERVER_2

Este é o endereço IP de seu Servidor DNS Secundário de sua rede ou de seu provedor.

LOOPBACK

A faixa de endereços de loopback é 127.0.0.0/8. A interface propriamente dita é endereçada como 127.0.0.1 (em /etc/hosts).

PRIVPORTS

As portas privilegiadas, de 0 à 1023, normalmente são referenciadas pelo total.

UNPRIVPORTS

As portas não privilegiadas, de 1024 à 65535, normalmente são referenciadas pelo total. Elas são endereços atribuídos dinamicamente ao lado cliente de uma conexão.

Default Policy

Um firewall tem uma política default e uma série de ações a tomar em resposta a tipos de mensagens específicas. Isto significa que se um dado pacote não foi selecionado por nenhuma outra regra, então a regra da política default será aplicada.

Habilitando o Tráfego Local

Já que as políticas default para todos os exemplos de arquivos de scripts de regra de firewall é negar tudo, algumas dessas regras podem ser desfeitas. Serviços de rede local não passam para a interface externa de rede. Nenhum de seus programas de rede local funcionarão até que o tráfego de loopback seja permitido.


```
# Tráfego ilimitado na interface de loopback
ipchains -A input -i $LOOPBACK_INTERFACE -j ACCEPT
ipchains -A output -i $LOOPBACK_INTERFACE -j ACCEPT
```

Filtragem de Endereço de Origem

Todos os cabeçalhos de pacotes IP contêm os endereços de origem e de destino e o tipo da mensagem do protocolo IP (ICMP, UDP ou TCP) que este pacote contém. No Protocolo Internet (IP), a única forma de identificação é o endereço de origem no cabeçalho do pacote. Este é um problema que abre a porta para o spoof (imitação) de endereço de origem, onde o remetente pode substituir o seu endereço por um endereço não existente ou pelo endereço de algum outro site.

```
# Recusar pacotes forjados que finjam ser de um endereço externo
ipchains -A input -i $EXTERNAL_INTERFACE -s $IPADDR -l -j DENY
```

Também, há, pelo menos, sete conjuntos de endereços de origem que você deve recusar em sua interface externa em todos os casos.

Estes são pacotes entrantes afirmando serem de:

- Seu endereço IP externo
- Endereços IP privados Classe A
- Endereços IP privados Classe B
- Endereços IP privados Classe C
- Endereços de multicast Classe D
- Endereços reservados Classe E
- A interface de loopback

Com exceção do seu próprio endereço IP, bloquear pacotes saintes contendo estes endereços de origem lhe protege de possíveis erros de configuração de sua parte.

Observação:

Não esqueça de excluir o seu próprio endereço IP dentre os pacotes saintes bloqueados.

O restante das regras

Outras regras usadas nos arquivos de scripts de firewall são:

- O acesso a um serviço do Mundo Externo
- A oferta de um serviço ao Mundo Externo
- O mascaramento das máquinas internas

Os arquivos de scripts de firewall

A ferramenta IPchains lhe permite configurar firewalls, mascaramentos de IP, etc. O IPchains conversa com o kernel e lhe diz quais pacotes filtrar. Portanto, todas as suas configurações de firewall são armazenadas no kernel e, por isso, serão perdidas no reboot. Para evitar isto, crie um arquivo de script, conforme mostrado abaixo, em seu diretório "/etc/rc.d/init.d/" para cada servidor que você tenha. É claro que cada servidor tem serviços diferentes a oferecer e precisam de diferentes configurações de firewall. Por esta razão, fornecemos a você três configurações diferentes de firewall, as quais você poderá manipular, examinar e adequar às suas necessidades. Também, eu assumo que você tem um mínimo de conhecimento sobre como funcionam um firewall tipo filtro e regras de firewall.

Configuração do arquivo de script "/etc/rc.d/init.d/firewall" para o Servidor Web

Este é o arquivo de script de configuração para a nossa máquina do Servidor Web. Esta configuração permite tráfego ilimitado na interface de loopback, solicitações ICMP, Cache/Cliente/Servidor DNS (53), Servidor SSH (22), Servidor HTTP (80), Servidor HTTPS (443), Cliente SMTP (25), Servidor FTP (20, 21) e solicitações TRACEROUTE SAINTES, por default.

Caso você não queira alguns serviços listados nos arquivos de regras de firewall para o Servidor Web, os quais eu torno ATIVOS por default, comente-os com um "#" no início da linha. Caso você queira alguns outros serviços que eu comentei com um "#", então remova o "#" do início de suas linhas.

Crie o arquivo de script **firewall** (touch /etc/rc.d/init.d/firewall) no seu Servidor Web e adicione:

```
#! /bin/bash
#
# ----------------------------------------------------------------------------
# Modificado pela última vez por Garhard Mourani: 01-02-2000
# ----------------------------------------------------------------------------
# Copyright (C) 1997, 1998, 1999 Robert L. Ziegler
#
# Pela presente, é concedida a permissão para copiar, modificar e distribuir este
# software e sua documentação para propósitos educacionais, de pesquisa,
# privados e não lucrativos, sem taxa e sem um acordo escrito.
# Este software é fornecido como um exemplo e como base para o
# desenvolvimento de firewall individual. Este software é fornecido
# sem garantias.
#
# Qualquer material fornecido por Robert L. Ziegler é fornecido numa
# base "do jeito que está". Ele não dá nenhuma garantia de qualquer espécie,
# seja expressa ou implícita, relativa a qualquer material incluindo, porém não
# limitado à, garantia de adaptação à um propósito em particular, exclusividade
# ou resultados obtidos do uso do material.
# ----------------------------------------------------------------------------
#
# Chamado a partir de /etc/rc.d/init.d/firewall.
# chkconfig: - 60 95
# Descrição: Inicia e pára o Firewall IPCHAINS \
#            usado para fornecer serviços de Firewall de rede.
#
# Biblioteca de funções.
. /etc/rc.d/init.d/functions

# Configuração de rede.
. /etc/sysconfig/network
```

```
# Verifique se a rede está ativa.
if [ ${NETWORKING} = "no" ]
then
        exit 0
fi

[ -f /sbin/ipchains ] || exit 0

# Verifique como fomos chamados.
case "$1" in
        start)
                echo -n "Iniciando Serviços de Firewall: "

# Algumas definições para facilitar a manutenção.

# ------------------------------------------------------------------------
# EDITE ESTAS DE CONFORMIDADE COM O SEU SISTEMA
# E SEU PROVEDOR.
# ------------------------------------------------------------------------

EXTERNAL_INTERFACE="eth0"          # ou o que você usar
LOOPBACK_INTERFACE="lo"
IPADDR="208.164.186.3"
ANYWHERE="any/0"
NAMESERVER_1="208.164.186.1"       # O seu servidor de nomes primário
NAMESERVER_2="208.164.186.2"       # O seu servidor de nomes secundário

SMTP_SERVER="mail.openarch.com"    # O seu servidor de Email
SYSLOG_SERVER="mail.openarch.com"  # O seu servidor interno de syslog
SYSLOG_CLIENT="208.164.168.0/24"   # O seu cliente interno de syslog

LOOPBACK="127.0.0.0/8"
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
BROADCAST_SRC="0.0.0.0"
BROADCAST_DEST="255.255.255.255"
PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"
```

```
# ------------------------------------------------------------------------

# O SSH começa em 1023 e vai até 513 para cada conexão
# entrante simultânea adicional.
SSH_PORTS="1022:1023"           # faixa das portas SSH privilegiadas

# O traceroute normalmente utiliza -S 32769:65535 -D 33434:33523
TRACEROUTE_SRC_PORTS="32769:65535"
TRACEROUTE_DEST_PORTS="33434:33523"

# ------------------------------------------------------------------------
# A política default é negar (DENY)
# Aceita explicitamente conexões ENTRANTES & SAINTES desejadas

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Configura a política default do filtro para negar.
ipchains -P input DENY
ipchains -P output REJECT
ipchains -P forward REJECT

# ------------------------------------------------------------------------

# Ativa a proteção contra TCP SYN Cookie
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

# Ativa a proteção contra spoof de IP
# Ativa a Verificação de Endereço de Origem
for f in /proc/sys/net/ipv4/conf/*/rp_filter;
do
        echo 1 > $1
done

# Desativa a Aceitação de Redirecionamento ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 0 > $f
done

# Desativa Pacotes Roteados na Origem
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 0 > $f
done
```

```
# ------------------------------------------------------------------------
# LOOPBACK
# ------------------------------------------------------------------------

# Tráfego ilimitado na interface de loopback
ipchains -A input -i $LOOPBACK_INTERFACE -j ACCEPT
ipchains -A output -i $LOOPBACK_INTERFACE -j ACCEPT

# ------------------------------------------------------------------------
# Demônios de Rede
# Negar acesso a tolos

# /etc/rc.d/rc.firewall.blocked contém uma lista de
# regras de bloqueio a partir de qualquer acesso
# ipchains -A input -i $EXTERNAL_INTERFACE -s address -j DENY

# Recusa qualquer conexão de sites problemáticos
# if [ -f /etc/rc.d/rc.firewall.blocked ]; then
#         ./etc/rc.d/rc.firewall.blocked
# fi

# ------------------------------------------------------------------------
# ENDEREÇOS RUINS & ATAQUES DE  SPOOF
# ------------------------------------------------------------------------

# Recusa pacotes forjados.
# Ignora ostensivamente endereços de origem ilegais.
# Proteja a sí próprio de enviar para endereços ruins.

# Recusar pacotes forjados finjindo serem do endereço externo.
ipchains -A input -i $EXTERNAL_INTERFACE -s $IPADDR -j DENY -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe A
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_A -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_A -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_A -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_A -j REJECT -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe B
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_B -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_B -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_B -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_B -j REJECT -l
```

 # Recusar pacotes que afirmem ser para ou de uma rede privada Classe C
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_C -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_C -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_C -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_C -j REJECT -l

 # Recusar pacotes que afirmem ser da interface de loopback
ipchains -A input -i $EXTERNAL_INTERFACE -s $LOOPBACK -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $LOOPBACK -j REJECT -l

 # Recusar pacotes de ORIGEM do endereço de broadcast
ipchains -A input -i $EXTERNAL_INTERFACE -s $BROADCAST_DEST -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $BROADCAST_SRC -j DENY -l

 # Recusar endereços multicast Classe D (in.h) (NET-3-HOWTO)
Multicast é ilegal como endereço de origem.
Multicast utiliza UDP.
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_D_MULTICAST -j DENY -l

 # Recusar endereços IP reservados Classe E.
ipchains -A input -i $EXTERNAL_INTERFACE -s -$CLASS_E_RESERVED_NET -j DENY -l

 # Recusar endereços definidos como reservados pela IANA
0.*.*.*, 1.*.*.*, 2.*.*.*, 5.*.*.*, 7.*,*,*, 23.*.*.*, 27.*.*.*
31.*.*.*, 37.*.*.*, 39.*.*.*, 41.*.*.*, 42.*.*.*, 58-60.*.*.*
65-95.*.*.*, 96-126.*.*.*, 197.*.*.*, 201.*.*.* (?), 217-223.*.*.*
ipchains -A input -i $EXTERNAL_INTERFACE -s 1.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 2.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 5.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 7.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 23.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 27.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 31.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 37.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 39.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 41.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 42.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 58.0.0.0/7 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 60.0.0.0/8 -j DENY -l


```
#65: 01000001    - /3 inclui 64 - precisa 65-79 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 65.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 66.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 67.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 68.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 69.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 70.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 71.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 72.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 73.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 74.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 75.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 76.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 77.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 78.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 79.0.0.0/8 -j DENY -l

# 80: 01010000   - /4 mascara 80-95
ipchains -A input -i $EXTERNAL_INTERFACE -s 80.0.0.0/4 -j DENY -l

# 96: 01100000   -/4 mascara 96-111
ipchains -A input -i $EXTERNAL_INTERFACE -s 96.0.0.0/4 -j DENY -l

# 126: 01111110 -/3 inclui 127 - precisa 112-126 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 112.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 113.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 114.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 115.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 116.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 117.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 118.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 119.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 120.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 121.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 122.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 123.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 124.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 125.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 126.0.0.0/8 -j DENY -l

# 217: 11011001 -/5 inclui 216 - precisa 217-219 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 217.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 218.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 219.0.0.0/8 -j DENY -l
```

```
# 223: 11011111 - /6 mascara 220-223
ipchains -A input -i $EXTERNAL_INTERFACE -s 220.0.0.0/6 -j DENY -l

# ------------------------------------------------------------------------
# ICMP
# ------------------------------------------------------------------------

# Para evitar ataques de negação de serviço baseados em bombas ICMP,
# filtrar Redirect (5) entrante e Destination Unreachable (3) sainte.
# Observe, contudo, que desativar Destination Unreachable (3) não é
# aconselhável, pois o mesmo é usado para negociar o tamanho dos
# fragmentos de pacote.

# Para ping bi-direcional.
#       Tipos de Mensagem: Echo Reply (0), Echo Request (8)
#       Para impedir ataques, limite os endereços de origem à faixa de seu provedor.
#
# Para traceroute sainte.
#       Tipos de Mensagem: INCOMING Dest Unreachable (3), Time Exceeded (11)
#       Base UDP default: 33434 à base+nr_saltos-1
#
# Para traceroute entrante.
#       Tipos de Mensagem: OUTGOING Dest Unreachable (3), Time Exceeded (11)
#       Para bloquear isto, negue OUTGOING 3 e 11

# 0: echo-reply (pong)
# 3: destination-unreachable, port-unreachable, fragmentation-needed, etc.
# 4: source-quench
# 5: redirect
# 8: echo-request (ping)
# 11: time-exceeded
# 12: parameter-problem

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 0 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 3 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 4 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 11 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 12 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s 208.164.186.0/24 8 -d $IPADDR -j ACCEPT
```

```
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 0 -d 208.164.186.0/24 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 3 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 4 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 8 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 12 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 11 -d 208.164.186.0/24 -j ACCEPT

# ------------------------------------------------------------------------
# UDP TRACEROUTE ENTRANTE
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s 208.164.186.0/24 $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j ACCEPT -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j DENY -l

# ------------------------------------------------------------------------
# Servidor DNS
# ------------------------------------------------------------------------

# ------------------------------------------------------------------------
# Repasse de DNS, servidor de nomes somente de cache (53)
# ------------------------------------------------------------------------

# Consulta ou resposta de servidor para servidor
# Servidor de nomes somente de cache só precisa de UDP e não de TCP

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_1 53 \
        -d $IPADDR 53 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR 53 \
        -d $NAMESERVER_1 53 -j ACCEPT
```

```
ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_2 53 \
        -d $IPADDR 53 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR 53 \
        -d $NAMESERVER_2 53 -j ACCEPT

# ------------------------------------------------------------------------------
#Cliente DNS (53)
# ------------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_2 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_2 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $NAMESERVER_2 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_2 53 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Aceitar TCP somente nas portas selecionadas
# ------------------------------------------------------------------------

# ------------------------------------------------------------------------
# Servidor SSH (22)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $SSH_PORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $SSH_PORTS -j ACCEPT

# ------------------------------------------------------------------------
# Cliente SSH (22)
# ------------------------------------------------------------------------

# ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#        -s $ANYWHERE 22 \
#        -d $IPADDR $UNPRIVPORTS -j ACCEPT

# ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#        -s $IPADDR $UNPRIVPORTS \
#        -d $ANYWHERE 22 -j ACCEPT

# ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#        -s $ANYWHERE 22 \
#        -d $IPADDR $SSH_PORTS -j ACCEPT

# ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#        -s $IPADDR $SSH_PORTS \
#        -d $ANYWHERE 22 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Servidor HTTP (80)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 80 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 80 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# ------------------------------------------------------------------------
# Servidor HTTPS (443)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 443 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 443 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# ------------------------------------------------------------------------
# Servidor SYSLOG (514)
# ------------------------------------------------------------------------

# Fornece registro de log remoto completo. Usando este recurso, você
# pode controlar todas as mensagens do syslog por um único host.

# ipchains -A input  -i $EXTERNAL_INTERFACE -p udp \
#        -s $SYSLOG_CLIENT \
#        -d $IPADDR 514 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente SYSLOG (514)
# ------------------------------------------------------------------------

# ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
#        -s $IPADDR 514 \
#        -d $SYSLOG_SERVER 514 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Servidor AUTH (113)
# ------------------------------------------------------------------------

# Rejeitar, ao invés de negar, a porta auth entrante . (NET-3-HOWTO)

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE \
        -d $IPADDR 113 -j REJECT

# ------------------------------------------------------------------------
# Cliente SMTP (25)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $SMTP_SERVER 25 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFAC E -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $SMTP_SERVER 25 -j ACCEPT

# ------------------------------------------------------------------------
# Servidor FTP (20, 21)
# ------------------------------------------------------------------------

# Solicitação entrante

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 21 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 21 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# respostas do canal de dados PORT MODE

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 20 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR 20 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

```
# respostas do canal de dados PASSIVE MODE

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# ------------------------------------------------------------------------
# TRACEROUTE SAINTE
# ------------------------------------------------------------------------

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $TRACEROUTE_SRC_PORTS \
        -d $ANYWHERE $TRACEROUTE_DEST_PORTS -j ACCEPT

# ------------------------------------------------------------------------
# Ativa o registro em log dos pacotes negados selecionados
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $PRIVPORTS -j DENY -l

ipchains -A input -j $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $UNPRIVPORTS -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 5 -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 13:255 -d $IPADDR -j DENY -l

# ------------------------------------------------------------------------
```

```
;;

stop)
        echo -n "Desativando Serviços de Firewall: "

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Deleta todas as cadeias definidas pelo usuário para este filtro
ipchains -X

# Reseta a política default do filtro para ACEITAR.
ipchains -P input ACCEPT
ipchains -P output ACCEPT
ipchains -P forward ACCEPT

# Desativa a Proteção TCP SYN Cookie.
echo 0 > /proc/sys/net/ipv4/tcp_syncookies

# Desativa a proteção contra spoof de IP.
# Ativa a Verificação de Endereço de Origem.
for f in /proc/sys/net/ipv4/conf*/rp_filter;
do
        echo 0 > $f
done

# Ativa a Aceitação de Redirecionamento de ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 1 > $f
done

# Ativa o Roteamento de Pacotes na Origem
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 1 > $f
done
```

```
;;

status)
        status firewall

;;

restart|reload)
        $0 stop
        $0 start

;;

*)
        echo "Sintaxe: firewall (start|stop|status|restart|reload)"
        exit 1

esac

exit 0
```

Agora, torne este script executável e altere suas permissões default:

[root@deep /]# **chmod 700 /etc/rc.d/init.d/firewall**
[root@deep /]# **chown 0.0 /etc/rc.d/init.d/firewall**

Crie os links simbólicos rc.d para o seu Firewall, com o seguintes comandos:

[root@deep /]# **chkconfig --add firewall**
[root@deep /]# **chkconfig --level 345 firewall on**

Agora, as suas regras de firewall estão configuradas para usar o System V init (o System V init é o engarregado de inicializar todos os processos normais que precisam ser executados por ocasião do boot) e o serviço será automaticamente inicializado cada vez que seu servidor fizer reboot.

- Para parar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall stop**
  Desativando o Serviço de Firewall: [OK]

- Para inicializar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall start**
  Iniciando Serviços de Firewall: [OK]

Configuração do arquivo de script "/etc/rc.d/init.d/firewall" para o Servidor de Email

Este é o arquivo de script de configuração para a nossa máquina Servidora de Email. Esta configuração permite tráfego ilimitado na interface de Loopback, solicitações ICMP, Cliente e Servidor DNS (53), Servidor SSH (22), Cliente e Servidor SMTP (25), Servidor IMAP (143) e solicitações TRACEROUTE SAINTES, por default.

Caso você não queira alguns serviços listados nos arquivos de regras de firewall para o Servidor de Email, os quais eu torno ATIVOS por default, comente-os com um "#" no início da linha. Caso você queira alguns outros serviços que eu comentei com um "#", então remova o "#" do início de suas linhas.

Crie o arquivo de script **firewall** (touch /etc/rc.d/init.d/firewall) no seu Servidor de Email e adicione:

```
#! /bin/bash
#
# --------------------------------------------------------------------------
# Modificado pela última vez por Garhard Mourani: 01-02-2000
# --------------------------------------------------------------------------
# Copyright (C) 1997, 1998, 1999 Robert L. Ziegler
#
# Pela presente, é concedida a permissão para copiar, modificar e distribuir este
# software e sua documentação para propósitos educacionais, de pesquisa,
# privados e não lucrativos, sem taxa e sem um acordo escrito.
# Este software é fornecido como um exemplo e como base para o
# desenvolvimento de firewall individual. Este software é fornecido
# sem garantias.
#
# Qualquer material fornecido por Robert L. Ziegler é fornecido numa
# base "do jeito que está". Ele não dá nenhuma garantia de qualquer espécie,
# seja expressa ou implícita, relativa a qualquer material incluindo, porém não
# limitado à, garantia de adaptação à um propósito em particular, exclusividade
# ou resultados obtidos do uso do material.
# --------------------------------------------------------------------------
#
# Chamado a partir de /etc/rc.d/init.d/firewall.
# chkconfig: - 60 95
# Descrição: Inicia e pára o Firewall IPCHAINS \
#            usado para fornecer serviços de Firewall de rede.
#
# Biblioteca de funções.
./etc/rc.d/init.d/functions

# Configuração de rede.
./etc/sysconfig/network
```

```
# Verifique se a rede está ativa.
if [ ${NETWORKING} = "no" ]
then
        exit 0
fi

[ -f /sbin/ipchains ] || exit 0

# Verifique como fomos chamados.
case "$1" in
        start)
                echo -n "Iniciando Serviços de Firewall: "

# Algumas definições para facilitar a manutenção.

# ------------------------------------------------------------------------
# EDITE ESTAS DE CONFORMIDADE COM O SEU SISTEMA
# E SEU PROVEDOR.
# ------------------------------------------------------------------------

EXTERNAL_INTERFACE="eth0"           # ou o que você usar
LOOPBACK_INTERFACE="lo"
IPADDR="208.164.186.2"
ANYWHERE="any/0"
NAMESERVER_1="208.164.186.1"        # O seu servidor de nomes primário
NAMESERVER_2="208.164.186.2"        # O seu servidor de nomes secundário

SYSLOG_SERVER="mail.openarch.com"  # O seu servidor interno de syslog
SYSLOG_CLIENT="208.164.168.0/24"    # O seu cliente interno de syslog

LOOPBACK="127.0.0.0/8"
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
BROADCAST_SRC="0.0.0.0"
BROADCAST_DEST="255.255.255.255"
PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"
```

```
# ------------------------------------------------------------------------

# O SSH começa em 1023 e vai até 513 para cada conexão
# entrante simultânea adicional.
SSH_PORTS="1022:1023"           # faixa das portas SSH privilegiadas

# O traceroute normalmente utiliza -S 32769:65535 -D 33434:33523
TRACEROUTE_SRC_PORTS="32769:65535"
TRACEROUTE_DEST_PORTS="33434:33523"

# ------------------------------------------------------------------------
# A política default é negar (DENY)
# Aceita explicitamente conexões ENTRANTES & SAINTES desejadas

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Configura a política default do filtro para negar.
ipchains -P input DENY
ipchains -P output REJECT
ipchains -P forward REJECT

# ------------------------------------------------------------------------

# Ativa a proteção contra TCP SYN Cookie
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

# Ativa a proteção contra spoof de IP
# Ativa a Verificação de Endereço de Origem
for f in /proc/sys/net/ipv4/conf/*/rp_filter;
do
        echo 1 > $1
done

# Desativa a Aceitação de Redirecionamento ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 0 > $f
done

# Desativa Pacotes Roteados na Origem
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 0 > $f
done
```

```
# ------------------------------------------------------------------------
# LOOPBACK
# ------------------------------------------------------------------------

# Tráfego ilimitado na interface de loopback
ipchains -A input -i $LOOPBACK_INTERFACE -j ACCEPT
ipchains -A output -i $LOOPBACK_INTERFACE -j ACCEPT

# ------------------------------------------------------------------------
# Demônios de Rede
# Negar acesso a tolos

# /etc/rc.d/rc.firewall.blocked contém uma lista de
# regras de bloqueio a partir de qualquer acesso
# ipchains -A input -i $EXTERNAL_INTERFACE -s address -j DENY

# Recusa qualquer conexão de sites problemáticos
# if [ -f /etc/rc.d/rc.firewall.blocked ]; then
#         ./etc/rc.d/rc.firewall.blocked
# fi

# ------------------------------------------------------------------------
# ENDEREÇOS RUINS & ATAQUES DE SPOOF
# ------------------------------------------------------------------------

# Recusa pacotes forjados.
# Ignora ostensivamente endereços de origem ilegais.
# Proteja a sí próprio de enviar para endereços ruins.

# Recusar pacotes forjados finjindo serem do endereço externo.
ipchains -A input -i $EXTERNAL_INTERFACE -s $IPADDR -j DENY -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe A
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_A -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_A -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_A -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_A -j REJECT -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe B
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_B -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_B -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_B -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_B -j REJECT -l
```

 # Recusar pacotes que afirmem ser para ou de uma rede privada Classe C
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_C -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_C -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_C -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_C -j REJECT -l

 # Recusar pacotes que afirmem ser da interface de loopback
ipchains -A input -i $EXTERNAL_INTERFACE -s $LOOPBACK -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $LOOPBACK -j REJECT -l

 # Recusar pacotes de ORIGEM do endereço de broadcast
ipchains -A input -i $EXTERNAL_INTERFACE -s $BROADCAST_DEST -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $BROADCAST_SRC -j DENY -l

 # Recusar endereços multicast Classe D (in.h) (NET-3-HOWTO)
Multicast é ilegal como endereço de origem.
Multicast utiliza UDP.
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_D_MULTICAST -j DENY -l

 # Recusar endereços IP reservados Classe E.
ipchains -A input -i $EXTERNAL_INTERFACE -s -$CLASS_E_RESERVED_NET -j DENY -l

 # Recusar endereços definidos como reservados pela IANA
0.*.*.*, 1.*.*.*, 2.*.*.*, 5.*.*.*, 7.*,*,*, 23.*.*.*, 27.*.*.*
31.*.*.*, 37.*.*.*, 39.*.*.*, 41.*.*.*, 42.*.*.*, 58-60.*.*.*
65-95.*.*.*, 96-126.*.*.*, 197.*.*.*, 201.*.*.* (?), 217-223.*.*.*
ipchains -A input -i $EXTERNAL_INTERFACE -s 1.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 2.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 5.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 7.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 23.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 27.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 31.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 37.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 39.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 41.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 42.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 58.0.0.0/7 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 60.0.0.0/8 -j DENY -l


```
#65: 01000001    - /3 inclui 64 - precisa 65-79 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 65.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 66.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 67.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 68.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 69.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 70.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 71.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 72.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 73.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 74.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 75.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 76.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 77.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 78.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 79.0.0.0/8 -j DENY -l

# 80: 01010000   - /4 mascara 80-95
ipchains -A input -i $EXTERNAL_INTERFACE -s 80.0.0.0/4 -j DENY -l

# 96: 01100000   -/4 mascara 96-111
ipchains -A input -i $EXTERNAL_INTERFACE -s 96.0.0.0/4 -j DENY -l

# 126: 01111110 -/3 inclui 127 - precisa 112-126 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 112.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 113.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 114.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 115.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 116.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 117.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 118.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 119.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 120.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 121.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 122.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 123.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 124.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 125.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 126.0.0.0/8 -j DENY -l

# 217: 11011001 -/5 inclui 216 - precisa 217-219 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 217.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 218.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 219.0.0.0/8 -j DENY -l
```

```
# 223: 11011111 - /6 mascara 220-223
ipchains -A input -i $EXTERNAL_INTERFACE -s 220.0.0.0/6 -j DENY -l

# ------------------------------------------------------------------------
# ICMP
# ------------------------------------------------------------------------

# Para evitar ataques de negação de serviço baseados em bombas ICMP,
# filtrar Redirect (5) entrante e Destination Unreachable (3) sainte.
# Observe, contudo, que desativar Destination Unreachable (3) não é
# aconselhável, pois o mesmo é usado para negociar o tamanho dos
# fragmentos de pacote.

# Para ping bi-direcional.
#       Tipos de Mensagem: Echo Reply (0), Echo Request (8)
#       Para impedir ataques, limite os endereços de origem à faixa de seu provedor.
#
# Para traceroute sainte.
#       Tipos de Mensagem: INCOMING Dest Unreachable (3), Time Exceeded (11)
#       Base UDP default: 33434 à base+nr_saltos-1
#
# Para traceroute entrante.
#       Tipos de Mensagem: OUTGOING Dest Unreachable (3), Time Exceeded (11)
#       Para bloquear isto, negue OUTGOING 3 e 11

# 0: echo-reply (pong)
# 3: destination-unreachable, port-unreachable, fragmentation-needed, etc.
# 4: source-quench
# 5: redirect
# 8: echo-request (ping)
# 11: time-exceeded
# 12: parameter-problem

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 0 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 3 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 4 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 11 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 12 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s 208.164.186.0/24 8 -d $IPADDR -j ACCEPT
```

```
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 0 -d 208.164.186.0/24 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 3 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 4 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 8 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 12 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 11 -d 208.164.186.0/24 -j ACCEPT

# ------------------------------------------------------------------------------
# UDP TRACEROUTE ENTRANTE
# ------------------------------------------------------------------------------

# Geralmente, o traceroute usa -S 32769:65535 -D 33434:33523

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s 208.164.186.0/24 $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j ACCEPT -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j DENY -l

# ------------------------------------------------------------------------------
# Servidor DNS
# ------------------------------------------------------------------------------

# DNS: servidor completo
# Consulta ou resposta de cliente/servidor para servidor

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 53 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR 53 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

```
# ------------------------------------------------------------------------
#Cliente DNS (53)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

# ------------------------------------------------------------------------
# Aceitar TCP somente nas portas selecionadas
# ------------------------------------------------------------------------

# ------------------------------------------------------------------------
# Servidor SSH (22)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $SSH_PORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $SSH_PORTS -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Cliente SSH (22)
# ------------------------------------------------------------------------

# ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#        -s $ANYWHERE 22 \
#        -d $IPADDR $UNPRIVPORTS -j ACCEPT

# ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#        -s $IPADDR $UNPRIVPORTS \
#        -d $ANYWHERE 22 -j ACCEPT

# ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#        -s $ANYWHERE 22 \
#        -d $IPADDR $SSH_PORTS -j ACCEPT

# ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#        -s $IPADDR $SSH_PORTS \
#        -d $ANYWHERE 22 -j ACCEPT

# ------------------------------------------------------------------------
# Servidor AUTH (113)
# ------------------------------------------------------------------------

# Rejeitar, ao invés de negar, a porta auth entrante . (NET-3-HOWTO)

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE \
        -d $IPADDR 113 -j REJECT

# ------------------------------------------------------------------------
# Servidor SYSLOG (514)
# ------------------------------------------------------------------------

# Fornece registro de log remoto completo. Usando este recurso, você
# pode controlar todas as mensagens do syslog por um único host.

# ipchains -A input  -i $EXTERNAL_INTERFACE -p udp \
#        -s $SYSLOG_CLIENT \
#        -d $IPADDR 514 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Cliente SYSLOG (514)
# ------------------------------------------------------------------------

# ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
#         -s $IPADDR 514 \
#         -d $SYSLOG_SERVER 514 -j ACCEPT

# ------------------------------------------------------------------------
# Servidor SMTP (25)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 25 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 25 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# ------------------------------------------------------------------------
# Cliente SMTP (25)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 25 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFAC E -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 25 -j ACCEPT

# ------------------------------------------------------------------------
# Servidor IMAP (143)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 143 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 143 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

```
# ------------------------------------------------------------------------
# TRACEROUTE SAINTE
# ------------------------------------------------------------------------

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $TRACEROUTE_SRC_PORTS \
        -d $ANYWHERE $TRACEROUTE_DEST_PORTS -j ACCEPT

# ------------------------------------------------------------------------
# Ativa o registro em log dos pacotes negados selecionados
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $PRIVPORTS -j DENY -l

ipchains -A input -j $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $UNPRIVPORTS -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 5 -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 13:255 -d $IPADDR -j DENY -l

# ------------------------------------------------------------------------
```

```
;;

stop)
        echo -n "Desativando Serviços de Firewall: "

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Deleta todas as cadeias definidas pelo usuário para este filtro
ipchains -X

# Reseta a política default do filtro para ACEITAR.
ipchains -P input ACCEPT
ipchains -P output ACCEPT
ipchains -P forward ACCEPT

# Desativa a Proteção TCP SYN Cookie.
echo 0 > /proc/sys/net/ipv4/tcp_syncookies

# Desativa a proteção contra spoof de IP.
# Ativa a Verificação de Endereço de Origem.
for f in /proc/sys/net/ipv4/conf*/rp_filter;
do
        echo 0 > $f
done

# Ativa a Aceitação de Redirecionamento de ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 1 > $f
done

# Ativa o Roteamento de Pacotes na Origem
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 1 > $f
done
```

```
;;

status)
        status firewall

;;

restart|reload)
        $0 stop
        $0 start

;;

*)
        echo "Sintaxe: firewall (start|stop|status|restart|reload)"
        exit 1

esac

exit 0
```

Agora, torne este script executável e altere suas permissões default:

[root@deep /]# **chmod 700 /etc/rc.d/init.d/firewall**
[root@deep /]# **chown 0.0 /etc/rc.d/init.d/firewall**

Crie os links simbólicos rc.d para o seu Firewall, com o seguintes comandos:

[root@deep /]# **chkconfig --add firewall**
[root@deep /]# **chkconfig --level 345 firewall on**

Agora, as suas regras de firewall estão configuradas para usar o System V init (o System V init é o engarregado de inicializar todos os processos normais que precisam ser executados por ocasião do boot) e o serviço será automaticamente inicializado cada vez que seu servidor fizer reboot.

- Para parar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall stop**
  Desativando o Serviço de Firewall: [OK]

- Para inicializar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall start**
  Iniciando Serviços de Firewall: [OK]

CAPÍTULO 5

Gerenciamento da Rede TCP/IP

Capítulo 5 Gerenciamento da Rede TCP/IP

Neste Capítulo:

Instale mais de uma placa Ethernet por máquina
Arquivos relacionados à funcionalidade de rede
Configurando a rede TCP/IP manualmente com linha de comando

Gerenciamento da Rede TCP/IP do Linux

Visão Geral

Até agora, não manipulamos com as capacidades de rede do Linux. O Linux é um dos melhores sistemas operacionais deste mundo pelas suas características de rede. A maioria dos sites Internet por todo o mundo já sabe disto e usam-no desde muito tempo. A compreensão do seu hardware de rede e todos os arquivos relacionados a ele é muito importante se você quer ter controle total sobre o que acontece em seu servidor. Um bom conhecimento sobre comandos primários de rede é vital. O gerenciamento de rede cobre uma ampla variedade de tópicos. No geral, inclui a reunião de dados estatísticos e informações de status sobre partes de sua rede e a tomada de ações conforme necessário para lidar com falhas e outras alterações. A técnica mais primitiva de monitoramento de rede é "pingar" periodicamente os hosts críticos. Monitoramento de rede mais sofisticado exige a habilidade de se obter status específicos e informações estatísticas de vários dispositivos na rede. Isto deve incluir vários tipos de contadores de datagrama, bem como, contadores de erros de vários tipos. Por estas razões, neste capítulo, tentaremos responder perguntas fundamentais sobre dispositivos de rede, arquivos relacionados à funcionalidade de rede e comandos essenciais de rede.

Instale mais de uma placa Ethernet por máquina

Você poderia usar o Linux como um gateway entre duas redes Ethernet. Nesse caso, você poderia ter duas placas Ethernet em seu servidor. Para eliminar problemas por ocasião do boot, o kernel do Linux não detecta automaticamente múltiplas placas. Se ocorrer de você ter duas ou mais placas, você deverá especificar os parâmetros das placas no arquivo "**lilo.conf**" para um kernel monolítico ou no arquivo "**conf.modules**" para um kernel modular. O que segue são problemas que você poderá encontrar com suas placas de rede.

Problema 1

Caso os drivers das placas estejam sendo usados como módulos carregáveis (kernel modular), no caso de drivers PCI, o módulo tipicamente detectará automaticamente todas as placas instaladas. Para placas ISA, você precisará fornecer o endereço base de I/O da placa para que o módulo saiba onde procurar. Esta informação é armazenada no arquivo "/etc/conf.modules".

Como exemplo, considere que temos duas placas ISA 3c509: uma no endereço de I/O 0x300 e outra em 0x320.

Para placas ISA, edite o arquivo **conf.modules** (vi /etc/conf.modules) e adicione:

```
alias eth0 3c509
alias eth1 3c509
options 3c509 io=0x300,0x320
```

Isto diz que o driver da 3c509 deve ser carregado tanto para eth0 quanto para eth1 (alias eth0, eth1) e que deve ser carregado com as opções io=0x300,0x320 para que o driver saiba onde procurar pelas placas. Observe que o **0x** é importante - coisas como 300h, geralmente usadas no mundo DOS, não funcionarão.

Para placas PCI, normalmente você só precisa das linhas de alias para relacionar as interfaces ethN com o nome do driver apropriado, já que o endereço base de I/O de uma placa PCI pode ser detectado com segurança.

Para placas PCI, edite o arquivo **conf.modules** (vi /etc/conf.modules) e adicione:

```
alias eth0 3c509
alias eth1 3c509
```


Problema 2

Caso os drivers das placas estejam compilados no kernel (kernel monolítico), o sistema PCI fará uma varredura e detectará automaticamente todas as placas relacionadas. Placas ISA também serão todas detectadas automaticamente. Porém, em algumas circunstâncias, as placas ISA ainda precisarão do que segue abaixo. Esta informação é armazenada no arquivo "/etc/lilo.conf". O método é passar argumentos ao kernel por ocasião do boot, o que, geralmente, é feito pelo LILO.

Para placas ISA, edite o arquivo **lilo.conf** (vi /etc/lilo.conf) e adicione:

append="ether=0,0,eth1"

Observação:

Primeiramente, teste a sua placa ISA sem os argumentos de boot no arquivo "lilo.conf" e, caso isto falhe, então use os argumentos de boot.

Neste caso, eth0 e eth1 serão atribuídas para que as placas sejam encontradas no momento do boot. Já que recompilamos o kernel, devemos usar o segundo método (caso os drivers estejam compilados no kernel) para instalar a nossa segunda placa Ethernet no sistema. Lembre-se de que isto é necessário somente em algumas circunstâncias para placas ISA. Placas PCI serão encontradas automaticamente.

Arquivos relacionados à funcionalidade de rede

No Linux, a rede TCP/IP é configurada através de vários arquivos texto, os quais você poderá ter de editá-los para fazer com que a rede funcione. É muito importante conhecer os arquivos de configuração relacionados à rede TCP/IP para que você possa editá-los e configurá-los, caso seja necessário. Lembre-se de que nosso servidor não tem uma interface Xwindow para configurar os arquivos através de uma interface gráfica. Mesmo que você use uma GUI em suas atividades diárias, é importante saber como configurar a rede em modo texto. As seguintes seções descrevem os arquivos básicos de configuração da rede TCP/IP.

O arquivo "/etc/HOSTNAME"

Este arquivo armazena o seu nome de host de sistema - o seu nome de domínio de sistema totalmente qualificado (FQDN), tal como: deep.openarch.com.

O que se segue é um exemplo do arquivo "/etc/HOSTNAME":

deep.openarch.com

Os arquivos "/etc/sysconfig/network-scripts/ifcfg-ethN"

Arquivos de configuração para cada dispositivo de rede que você possa ter ou queira adicionar ao seu sistema são localizados no diretório "/etc/sysconfig/network-scripts/" com o Red Hat 6.1 e são nomeados **ifcfg-eth0** para a primeira interface, **ifcfg-eth1** para a segunda, etc.

O que se segue é um exemplo do arquivo "/etc/sysconfig/network-scripts/ifcfg-eth0:

```
DEVICE=eth0
IPADDR=208.164.186.1
NETMASK=255.255.255.0
NETWORK=208.164.186.0
BROADCAST=208.164.186.255
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
```

Caso você queira modificar o seu endereço de rede manualmente ou adicionar uma nova rede em uma nova interface, edite este arquivo (ifcfg-ethN) ou crie um novo e faça as alterações adequadas.

DEVICE=**devicename**, onde **devicename** é o nome do dispositivo físico de rede.

IPADDR=**ipaddr**, onde **ipaddr** é o endereço IP.

NETMASK=**netmask**, onde **netmask** é o valor do netmask.

NETWORK=**network**, onde **network** é o endereço IP da rede.

BROADCAST=**broadcast**, onde **broadcast** é o endereço IP de broadcast.

ONBOOT=**resposta**, onde **resposta** é yes ou no (a interface será ativada ou desativada no momento do boot?)

BOOTPROTO=**proto**, onde **proto** é um dos seguintes:

- none - Nenhum protocolo de boot deverá ser usado.
- bootp - O protocolo bootp (agora pump) deverá ser usado.
- dhcp - O protocolo dhcp deverá ser usado.

USERCTL=**resposta**, onde **resposta** é uma das seguintes:

- yes - Usuário não-root tem permissão para controlar este dispositivo.
- no - Somente o superusuário root tem permissão para controlar este dispositivo.

O arquivo "/etc/resolv.conf"

Este arquivo é um outro arquivo texto utilizado pelo resolvedor - uma biblioteca que determina o endereço IP para um nome de host.

O que se segue é um exemplo de arquivo "/etc/resolv.conf":

```
search openarch.com
nameserver 208.164.186.1
nameserver 208.164.186.2
```

Observação:

Os servidores de nomes são consultados na ordem em que aparecem neste arquivo (primário, secundário).

O arquivo "/etc/host.conf"

Este arquivo especifica como os nomes são resolvidos. O Linux utiliza uma biblioteca resolvedora para obter o endereço IP correspondente à um nome de host.

O que se segue é um exemplo de arquivo "/etc/host.conf":

```
# Pesquisar nomes primeiramente via DNS, depois pelo arquivo /etc/hosts
order bind,hosts
# Temos máquinas com múltiplos endereços
multi on
# Verificar ataques de spoof de endereço IP
nospoof on
```

A opção **order** indica a ordem dos serviços. A entrada do exemplo especifica que a biblioteca do resolvedor deve primeiramente consultar o servidor de nomes (DNS) para resolver um nome e, só então, verificar o arquivo "/etc/hosts".

A opção **multi** determina se um host no arquivo "/etc/hosts" pode ter múltiplos endereços IP (múltiplas interfaces ethN). Hosts que têm mais de um endereço IP são conhecidos como *multihomed*, porque a presença de múltiplos endereços IP implica que o host tem várias interfaces de rede.

A opção **nospoof** indica para tomar o cuidado de não permitir spoof nesta máquina. O Spoof de IP é um furo de segurança que funciona enganando computadores em uma relação de confiança, afirmando que você é alguém que na verdade não é.

O arquivo "/etc/sysconfig/network"

O arquivo "/etc/sysconfig/network" é usado para especificar informações sobre a configuração de rede desejada em seu servidor.

O que se segue é um exemplo de arquivo "/etc/sysconfig/network":

```
NETWORKING=yes
FORWARD_IPV4=yes
HOSTNAME=deep.openarch.com
GATEWAY=0.0.0.0
GATEWAYDEV=
```

Os seguintes valores podem ser usados:

NETWORKING=**resposta**, onde **resposta** é yes ou no (configurar ou não a rede).

FORWARD_IPV4=**resposta**,onde **resposta** é yes ou no (ativa ou não o repasse IP).

HOSTNAME=**hostname**, onde **hostname** é o nome de host de seu servidor.

GATEWAY=**gwip**, onde **gwip** é o endereço IP do gateway para redes remotas (caso haja).

GATEWAYDEV=**gwdev**, onde **gwdev** é o nome do dispositivo (eth#) que você usa para acessar o gateway remoto.

Observação:

Para compatibilidade com software mais antigo, o arquivo /etc/HOSTNAME deve conter o mesmo valor de HOSTNAME=**hostname** acima.

O arquivo "/etc/hosts"

Quando a sua máquina for inicializada, ela precisará conhecer o mapeamento de alguns nomes de host para endereços IP antes que o DNS possa ser consultado. Este mapeamento é mantido no arquivo "/etc/hosts". Na ausência de um servidor de nomes, qualquer programa de rede em seu sistema consulta este arquivo para determinar o endereço IP que corresponda a um nome de host.

O que se segue é um exemplo de arquivo "/etc/hosts":

Endereço IP	Nome de host	Apelido
127.0.0.1	localhost	deep.openarch.com
208.164.186.1	deep.openarch.com	deep
208.164.186.2	mail.openarch.com	mail
208.164.186.3	web.openarch.com	web

A coluna mais à esquerda é o endereço IP a ser resolvido. A próxima coluna é o nome daquele host. Quaisquer colunas subsequentes são apelidos para aquele host. Na segunda linha do arquivo, por exemplo, o endereço IP 208.164.186.1 é do host deep.openarch.com. Um nome alternativo para deep.openarch.com é deep.

Após ter finalizado a configuração de seus arquivos de rede, não esqueça de reinicializar a sua rede para que as alterações tenham efeito.

- Para reinicializar a sua rede, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/network restart**

OBSERVAÇÃO IMPORTANTE:

Problemas de temporização em conexões telnet ou ftp são, geralmente, causadas pelo servidor que está tentando resolver um endereço IP do cliente para um nome DNS. Ou o DNS não está configurado adequadamente em seu servidor ou as máquinas clientes não conhecem o DNS. Se você pretende executar os serviços telnet e ftp em seu servidor e não esteja usando DNS, não esqueça de adicionar o nome da máquina cliente e o IP no seu arquivo "/etc/hosts" no servidor. Do contrário, você pode contar com uma espera de vários minutos para que a consulta DNS expire o seu tempo antes de conseguir um prompt "login: ".

Configurando a rede TCP/IP manualmente com linha de comando

O utilitário ifconfig é a ferramenta usada para configurar a sua placa de rede. Você precisa entender este comando para o case de você precisar configurar a rede na mão. Algo importante para se tomar cuidado é que , ao se utilizar o ifconfig para configurar seus dispositivos de rede, as configurações não sobreviverão a um reboot.

- Para atribuir à interface eth0 o endereço IP 208.164.186.2, use o comando:

  [root@deep /]# **ifconfig eth0 208.164.186.2 netmask 255.255.255.0**

- Para mostrar todas as interfaces que você possa ter em seu servidor, use o comando:

  [root@deep /]# **ifconfig**

A saída deve se parecer algo com isto:

```
eth0    Link encap:Ethernet HWaddr 00:E0:18:90:1B:56
        inetd addr:208.164.186.2 Bcast:208.186.164.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1295 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1163 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        interrupt:11 Base address:0xa800

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:139 errors:0 dropped:0 overruns:0 frame:0
        TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
```


Se o ifconfig for chamado sem parâmetros, ele mostra todas as interfaces que você configurou. A opção "-a" mostra as inativas, também.

- Para mostrar todas as interfaces, bem como as interfaces inativas que você possa ter, use o comando:

  [root@deep /]# **ifconfig -a**

A saída deve se parecer algo com isto:

```
eth0    Link encap:Ethernet HWaddr 00:E0:18:90:1B:56
        inetd addr:208.164.186.2 Bcast:208.186.164.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1295 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1163 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        interrupt:11 Base address:0xa800

eth1    Link encap:Ethernet HWaddr 00:E0:18:90:44:34
        inetd 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:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        interrupt:5 Base address:0xa320

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:139 errors:0 dropped:0 overruns:0 frame:0
        TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
```

Observação:

É importante notar que a configuração feita com a ferramenta ifconfig para os seus dispositivos de rede, não sobreviverá a um reboot.

- Para atribuir o gateway default como sendo 208.186.164.1, use o comando:

  [root@deep /]# **route add default gw 208.164.186.1**

Neste exemplo, a rota default é configurada para 208.186.164.1: o seu roteador.

Verifique se você pode enxergar os seus hosts. Escolha um host de sua rede: o 208.164.186.1, por exemplo.

- Para verificar se você pode alcançar os seus hosts, use o comando:

  [root@deep /]# **ping 208.164.186.1**

A saída deve se parecer algo com isto:

```
[root@deep /]# ping 208.164.186.1
PING 208.164.186.1 (208.164.186.1) from 208.164.186.2: 56 data bytes
64 bytes from 208.164.186.2: icmp_seq=0 ttl=128 time=1.0 ms
64 bytes from 208.164.186.2: icmp_seq=1 ttl=128 time=1.0 ms
64 bytes from 208.164.186.2: icmp_seq=2 ttl=128 time=1.0 ms
64 bytes from 208.164.186.2: icmp_seq=3 ttl=128 time=1.0 ms

--- 208.164.186.1 ping statistics ---
4 packets transmitted, 4 packets received, 0 % packet loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
```


Você agora deveria mostrar as informações de roteamento com o comando **route** para ver se ambos os hosts estão com as entradas de roteamento corretas:

- Para mostrar informações de roteamento, use o comando:

  [root@deep /]# **route -n**

A saída deve se parecer algo com isto:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
208.164.186.2	0.0.0.0	255.255.255.255	UH	0	0	0	eth0
208.164.186.0	208.164.186.2	255.255.255.0	UG	0	0	0	eth0
208.164.186.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo

- Para verificar rapidamente o status das interfaces, use o comando netstat -i, conforme segue:

  [root@deep /]# **netstat -i**

A saída deve se parecer algo com isto:

Kernel interface table

Iface	MTU	Met	RX-OK	RX-ERR	RX-DRP	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
eth0	1500	0	4236	0	0	3700	0	0	0	BRU
lo	3924	0	13300	0	0	13300	0	0	0	LRU
ppp0	1500	0	14	1	0	16	0	0	0	PRU

Uma outra opção netstat útil é -t, que mostra todas as conexões TCP ativas. O seguinte é um resultado típico de netstat -t:

- Para mostrar todas as conexões TCP ativas, use o comando:

  [root@deep /]# **netstat -t**

A saída deve se parecer algo com isto:

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	deep.openar:netbios-ssn	gate.openarch.com:1045	ESTABLISHED
tcp	0	0	localhost:1032	localhost:1033	ESTABLISHED
tcp	0	0	localhost:1033	localhost:1032	ESTABLISHED
tcp	0	0	localhost:1030	localhost:1034	ESTABLISHED
tcp	0	0	localhost:1031	localhost:1030	ESTABLISHED
tcp	0	0	localhost:1028	localhost:1029	ESTABLISHED
tcp	0	0	localhost:1029	localhost:1028	ESTABLISHED
tcp	0	0	localhost:1026	localhost:1027	ESTABLISHED
tcp	0	0	localhost:1027	localhost:1026	ESTABLISHED
tcp	0	0	localhost:1024	localhost:1025	ESTABLISHED
tcp	0	0	localhost:1025	localhost:1024	ESTABLISHED

- Para mostrar todas as conexões TCP ativas e que estejam ouvindo, use o comando:

  [root@deep /]# **netstat -vat**

A saída deve se parecer algo com isto:

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	deep.openarch.co:domain	*.*	LISTEN
tcp	0	0	localhost:domain	*.*	LISTEN
tcp	0	0	deep.openarch:ssh	gate.openarch.com:1645	ESTABLISHED
tcp	0	0	*:webcache	*.*	LISTEN
tcp	0	0	deep.openar:netbios-ssn	*.*	LISTEN
tcp	0	0	localhost:netbios-ssn	*.*	LISTEN
tcp	0	0	deep.openar:netbios-ssn	gate.openarch.com:1045	ESTABLISHED
tcp	0	0	localhost:1032	localhost:1033	ESTABLISHED
tcp	0	0	localhost:1033	localhost:1032	ESTABLISHED
tcp	0	0	localhost:1030	localhost:1034	ESTABLISHED
tcp	0	0	localhost:1031	localhost:1030	ESTABLISHED
tcp	0	0	localhost:1028	localhost:1029	ESTABLISHED
tcp	0	0	localhost:1029	localhost:1028	ESTABLISHED
tcp	0	0	localhost:1026	localhost:1027	ESTABLISHED
tcp	0	0	localhost:1027	localhost:1026	ESTABLISHED
tcp	0	0	localhost:1024	localhost:1025	ESTABLISHED
tcp	0	0	localhost:1025	localhost:1024	ESTABLISHED
tcp	0	0	deep.openarch:www	*.*	LISTEN
tcp	0	0	deep.openarch:https	*.*	LISTEN
tcp	0	0	*:389	*.*	LISTEN
tcp	0	0	*:ssh	*.*	LISTEN

- Para parar todos os dispositivos de rede manualmente em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/network stop**

  Shutting down interface eth0 [OK]
  Disabling IPv4 packet forwarding [OK]

- Para iniciar todos os dispositivos de rede manualmente em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/network start**

  Enabling IPv4 packet forwarding [OK]
  Bringing up interface lo [OK]
  Bringing up interface eth0 [OK]

CAPÍTULO 6

Firewall de Rede com Suporte a Mascaramento e Repasse

Capítulo 6 Firewall de Rede

Neste Capítulo:

Compile um kernel com suporte a Firewall com Mascaramento e Repasse
Configuração do arquivo de script para o Servidor de Gateway
Negar acesso a alguns endereços
Ferramentas Administrativas do IPCHAINS

Mascaramento e Repasse do Linux

Visão Geral

Contrariamente aos exemplos do capítulo 4, a configuração de um Servidor Linux para mascarar e repassar o tráfego geralmente do lado interno da rede privada que tem endereços IP não registrados (ou seja, 192.158.1.0/24) para o lado externo da rede (ou seja, a Internet) exige uma configuração especial de seu kernel e de seu arquivo de script de configuração de firewall. Este tipo de configuração também é conhecida como **Servidor de Gateway** (uma máquina que serve como um gateway entre os tráfegos interno e externo). Esta configuração só deve ser feita se você tiver intenções ou necessidades deste tipo de serviço e é por esta razão que a configuração do arquivo de script para o Servidor de Gateway está em seu próprio capítulo.

Compile um kernel com suporte a Firewall com Mascaramento e Repasse

Mais uma vez, a primeira coisa que você precisa fazer é assegurar-se de que o seu kernel foi compilado com suporte a firewall de rede ativado. Na versão 2.2.14 do kernel, você precisa assegurar-se de que respondeu **Y** às seguintes perguntas:

Networking options:
Network firewalls (CONFIG_FIREWALL) [N] **Y**
IP:Firewalling (CONFIG_IP_FIREWALL) [N] **Y**
IP:TCP syncookie support (CONFIG_SYN_COOKIES) [N] **Y**

Observação:

Se você acompanhou a seção Linux Kernel e recompilou o seu kernel, as opções "Network firewalls, IP:Firewalling e IP:TCP syncookie support", mostradas abaixo, já foram configuradas.

IP:Masquerading and IP ICMP Masquerading are required only for a Gateway Server.
IP:Masquerading (CONFIG_IP_MASQUERADE) [N] **Y**
IP:ICMP Masquerading (CONFIG_IP_MASQUERADE_ICMP) [N] **Y**

Observação:

Somente o seu **Servidor de Gateway** precisa ter as opções "IP:Masquerading" e "IP:ICMP Masquerading" do kernel ativadas. Isto é necessário para mascarar a sua rede interna para o exterior.

Mascaramento significa que se um dos seus computadores de sua rede local, para a qual a sua máquina Linux (ou gateway) age como um firewall, quer enviar alguma coisa para o lado externo, o seu Linux pode se "mascarar" como se fosse aquele computador. Em outras palavras, ele repassa o tráfego para o destinatário externo pretendido, porém faz parecer como se tivesse partido do próprio firewall. Isto funciona em ambas as direções: Se o host externo reponder, o firewall Linux silenciosamente repassará o tráfego para o computador local correspondente. Desta forma, os computadores de sua rede local são completamente invisíveis para o mundo externo, mesmo que eles possam alcançar o lado externo e receber respostas. Isto torna possível ter computadores na rede local participando da Internet, mesmo que eles não tenham endereços IP oficialmente registrados.

O código de mascaramento de IP somente funcionará se o repasse de IP estiver ativado em seu sistema. Esta característica, por default, é desativada e você pode ativá-la com o seguinte comando:

- Para ativar a característica de repasse de IP em seu servidor, execute o seguinte comando:

  [root@deep /]# **echo "1" > /proc/sys/net/ipv4/ip_forward**

Você pode adicionar a linha acima ao seu arquivo de script "/etc/rc.d/rc.local" para que o repasse de IP seja ativado automaticamente para você, mesmo que seu servidor seja reinicializado. No Red Hat Linux, isto também pode ser feito alterando-se a linha no arquivo "/etc/sysconfig/network" de:

FORWARD_IPV4="false"

Para que leia:

FORWARD_IPV4="yes"

Você deve reinicializar a sua rede para que a alteração tenha efeito:

[root@deep /]# **/etc/rc.d/init.d/network restart**

Portando, você pode adicionar a linha de comando "echo "1" > /proc/sys/net/ipv4/ip_forward" ao seu arquivo de script "rc.local" ou você pode alterar o valor da linha "FORWARD_IPV4=false" para "yes" no arquivo "network" para ativar este recurso. Pessoalmente, eu prefiro a segunda opção.

Observação:

A linha de repasse de IP acima, somente é necessária quando você responde "Yes" à opção "IP:Masquerading (CONFIG_IP_MASQUERADE)" do kernel e escolhe ter um servidor agindo como um Gateway e Mascarador para a sua rede interna.

Se você ativar o mascaramento de IP, então os módulos ip_masq_ftp.o (para transferência de arquivos via ftp), ip_masq_irc.o (para bate-papo irc), ip_masq_quake.o (você já adivinhou), ip_masq_vdolive.o (para conexões de vídeo VDOLive), ip_masq_cuseeme.o (para broadcasts CU-SeeMe) e ip_masq_raudio.o (para downloads RealAudio) serão automaticamente compilados. Eles são necessários para fazer o mascaramento, permitindo que estes protocolos funcionem. Também, você precisa compilar um kernel modular e responder "Yes" à opção "Enable loadable module support (CONFIG_MODULES)" , ao invés de um kernel monolítico, para poder usar as funções de mascaramento e módulos como ip_masq_ftp.o em seu Servidor de Gateway (Consulte a seção Linux Kernel acima para mais informações).

O código básico de mascaramento descrito para o "IP:Masquerading" acima somente manipula pacotes TCP ou UDP (e erros ICMP para conexões existentes). A opção IP:ICMP Masquerading implementa suporte adicional para o mascaramento de pacotes ICMP, tais como ping e as explorações usadas pelo programa rastreador do Windows 95.

Observação:

Lembre-se: outros servidores, como Servidor Web e Servidor de Email, não precisam ter estas opções ativadas já que eles possuem um endereço IP real a eles atribuído ou não agem como um Gateway para a rede interna.

Alguns Pontos a Considerar

Você pode seguramente assumir que está potencialmente em risco se você conectar o seu sistema à Internet. O seu gateway para a Internet é a sua maior exposição. Por isso, recomendamos o seguinte:

- O gateway não deve executar nenhuma aplicação a mais, além daquelas absolutamente necessárias.

- O gateway deve limitar estritamente os tipos e números de protocolos com permissão para fluirem através dele (protocolos representam furos de segurança em potencial, tais como FTP e Telnet).

- Qualquer sistema que contenha informações confidenciais ou sensíveis não devem ser acessíveis diretamente a partir da Internet.

Configuração do arquivo de script "/etc/rc.d/init.d/firewall" para o Servidor de Gateway

Este é o arquivo de script de configuração para a nossa máquina Servidora de Gateway. Esta configuração permite tráfego ilimitado na interface de Loopback, solicitações ICMP, Cliente e Servidor DNS (53), Cliente e Servidor SSH (22), Cliente e Servidor HTTP (80), Cliente e Servidor HTTPS (443), Cliente POP (110), Cliente NNTP NEWS (119), Cliente e Servidor SMTP (25), Servidor IMAP (143), Cliente IRC (6667), Cliente ICQ (4000), Cliente FTP (20, 21), Cliente RealAudio / QuickTime e solicitações TRACEROUTE SAINTES, por default.

Caso você não queira alguns serviços listados nos arquivos de regras de firewall para o Servidor de Gateway, os quais eu torno ATIVOS por default, comente-os com um "#" no início da linha. Caso você queira alguns outros serviços que eu comentei com um "#", então remova o "#" do início de suas linhas.

Se você já configurou o Mascaramento em seu servidor, descomente os módulos necessários para mascarar os respectivos serviços que você precisa, como ip_masq_irc.o. ip_masq_raudio.o, etc.

Crie o arquivo de script **firewall** (touch /etc/rc.d/init.d/firewall) no seu Servidor de Email e adicione:

```
#! /bin/bash
#
# ------------------------------------------------------------------------
# Modificado pela última vez por Garhard Mourani: 01-02-2000
# ------------------------------------------------------------------------
# Copyright (C) 1997, 1998, 1999 Robert L. Ziegler
#
# Pela presente, é concedida a permissão para copiar, modificar e distribuir este
# software e sua documentação para propósitos educacionais, de pesquisa,
# privados e não lucrativos, sem taxa e sem um acordo escrito.
# Este software é fornecido como um exemplo e como base para o
# desenvolvimento de firewall individual. Este software é fornecido
# sem garantias.
#
# Qualquer material fornecido por Robert L. Ziegler é fornecido numa
# base "do jeito que está". Ele não dá nenhuma garantia de qualquer espécie,
# seja expressa ou implícita, relativa a qualquer material incluindo, porém não
# limitado à, garantia de adaptação à um propósito em particular, exclusividade
# ou resultados obtidos do uso do material.
# ------------------------------------------------------------------------
#
# Chamado a partir de /etc/rc.d/init.d/firewall.
# chkconfig: - 60 95
# Descrição: Inicia e pára o Firewall IPCHAINS \
#            usado para fornecer serviços de Firewall de rede.
#
# Biblioteca de funções.
. /etc/rc.d/init.d/functions

# Configuração de rede.
. /etc/sysconfig/network
```

```
# Verifique se a rede está ativa.
if [ ${NETWORKING} = "no" ]
then
        exit 0
fi

[ -f /sbin/ipchains ] || exit 0

# Verifique como fomos chamados.
case "$1" in
        start)
                echo -n "Iniciando Serviços de Firewall: "

# Algumas definições para facilitar a manutenção.

# ------------------------------------------------------------------------
# EDITE ESTAS DE CONFORMIDADE COM O SEU SISTEMA
# E SEU PROVEDOR.
# ------------------------------------------------------------------------

EXTERNAL_INTERFACE="eth0"            # ou o que você usar
LOCAL_INTERFACE_1="eth1"
LOOPBACK_INTERFACE="lo"
IPADDR="208.164.186.1"
LOCALNET_1="192.168.1.0/24"          # faixa que você usa como rede privada
IPSECSG="208.164.186.2"   # lista separada por espaço dos gateways VPN remotos
FREESWANVI="ipsec0"       # lista separada por espaço de interfaces virtuais
ANYWHERE="any/0"
NAMESERVER_1="208.164.186.1"         # O seu servidor de nomes primário
NAMESERVER_2="208.164.186.2"         # O seu servidor de nomes secundário

POP_SERVER="pop.videotron.ca"        # O seu servidor POP externo
NEWS_SERVER="news.videotron.ca"      # O seu servidor de news externo
SYSLOG_SERVER="mail.openarch.com"  # O seu servidor interno de syslog

LOOPBACK="127.0.0.0/8"
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
BROADCAST_SRC="0.0.0.0"
BROADCAST_DEST="255.255.255.255"
PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"
```

```
# ------------------------------------------------------------------------

# O SSH começa em 1023 e vai até 513 para cada conexão
# entrante simultânea adicional.
SSH_PORTS="1022:1023"           # faixa das portas SSH privilegiadas

# O traceroute normalmente utiliza -S 32769:65535 -D 33434:33523
TRACEROUTE_SRC_PORTS="32769:65535"
TRACEROUTE_DEST_PORTS="33434:33523"

# ------------------------------------------------------------------------
# A política default é negar (DENY)
# Aceita explicitamente conexões ENTRANTES & SAINTES desejadas

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Configura a política default do filtro para negar.
ipchains -P input DENY
ipchains -P output REJECT
ipchains -P forward REJECT

# Configura o timeout de mascaramento para 10 horas para conexões TCP
ipchains -M -S 36000 0 0

# Não repassar fragmentos. Montar antes de repassar.
ipchains -A input -f -i $LOCAL_INTERFACE_1 -j DENY

# ------------------------------------------------------------------------

# Ativa a proteção contra TCP SYN Cookie
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

# Ativa a proteção contra spoof de IP
# Ativa a Verificação de Endereço de Origem
for f in /proc/sys/net/ipv4/conf/*/rp_filter;
do
        echo 1 > $1
done

# Desativa a Aceitação de Redirecionamento ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 0 > $f
done

# Desativa Pacotes Roteados na Origem
```

```
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 0 > $f
done

# Estes módulos são necessários para mascarar seus respectivos serviços
/sbin/modprobe ip_masq_ftp.o
/sbin/modprobe ip_masq_raudio.o ports=554,7070,7071,6970,6971
/sbin/modprobe ip_masq_irc.o
# /sbin/modprobe ip_masq_vdolive.o
# /sbin/modprobe ip_masq_cuseeme.o
# /sbin/modprobe ip_masq_quake.o

# ------------------------------------------------------------------------
# LOOPBACK
# ------------------------------------------------------------------------

# Tráfego ilimitado na interface de loopback
ipchains -A input -i $LOOPBACK_INTERFACE -j ACCEPT
ipchains -A output -i $LOOPBACK_INTERFACE -j ACCEPT

# ------------------------------------------------------------------------
# Demônios de Rede
# Negar acesso a tolos

# /etc/rc.d/rc.firewall.blocked contém uma lista de
# regras de bloqueio a partir de qualquer acesso
# ipchains -A input -i $EXTERNAL_INTERFACE -s address -j DENY

# Recusa qualquer conexão de sites problemáticos
# if [ -f /etc/rc.d/rc.firewall.blocked ]; then
#         ./etc/rc.d/rc.firewall.blocked
# fi

# ------------------------------------------------------------------------
# ENDEREÇOS RUINS & ATAQUES DE SPOOF
# ------------------------------------------------------------------------

# Recusa pacotes forjados.
# Ignora ostensivamente endereços de origem ilegais.
# Proteja a si próprio de enviar para endereços ruins.

# Recusar pacotes forjados finjindo serem do endereço externo.
ipchains -A input -i $EXTERNAL_INTERFACE -s $IPADDR -j DENY -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe A
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_A -j DENY -l
```

```
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_A -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_A -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_A -j REJECT -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe B
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_B -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_B -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_B -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_B -j REJECT -l

# Recusar pacotes que afirmem ser para ou de uma rede privada Classe C
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_C -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $CLASS_C -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $CLASS_C -j REJECT -l
ipchains -A output -i $EXTERNAL_INTERFACE -d $CLASS_C -j REJECT -l

# Recusar pacotes que afirmem ser da interface de loopback
ipchains -A input -i $EXTERNAL_INTERFACE -s $LOOPBACK -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -s $LOOPBACK -j REJECT -l

# Recusar pacotes de ORIGEM do endereço de broadcast
ipchains -A input -i $EXTERNAL_INTERFACE -s $BROADCAST_DEST -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -d $BROADCAST_SRC -j DENY -l

# Recusar endereços multicast Classe D (in.h) (NET-3-HOWTO)
# Multicast é ilegal como endereço de origem.
# Multicast utiliza UDP.
ipchains -A input -i $EXTERNAL_INTERFACE -s $CLASS_D_MULTICAST -j DENY -l

# Recusar endereços IP reservados Classe E.
ipchains -A input -i $EXTERNAL_INTERFACE -s -$CLASS_E_RESERVED_NET -j DENY -l

# Recusar endereços definidos como reservados pela IANA
# 0.*.*.*, 1.*.*.*, 2.*.*.*, 5.*.*.*, 7.*,*,*, 23.*.*.*, 27.*.*.*
# 31.*.*.*, 37.*.*.*, 39.*.*.*, 41.*.*.*, 42.*.*.*, 58-60.*.*.*
# 65-95.*.*.*, 96-126.*.*.*, 197.*.*.*, 201.*.*.* (?), 217-223.*.*.*
ipchains -A input -i $EXTERNAL_INTERFACE -s 1.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 2.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 5.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 7.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 23.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 27.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 31.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 37.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 39.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 41.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 42.0.0.0/8 -j DENY -l
```

```
ipchains -A input -i $EXTERNAL_INTERFACE -s 58.0.0.0/7 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 60.0.0.0/8 -j DENY -l

#65: 01000001    - /3 inclui 64 - precisa 65-79 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 65.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 66.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 67.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 68.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 69.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 70.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 71.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 72.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 73.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 74.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 75.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 76.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 77.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 78.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 79.0.0.0/8 -j DENY -l

# 80: 01010000   - /4 mascara 80-95
ipchains -A input -i $EXTERNAL_INTERFACE -s 80.0.0.0/4 -j DENY -l

# 96: 01100000   -/4 mascara 96-111
ipchains -A input -i $EXTERNAL_INTERFACE -s 96.0.0.0/4 -j DENY -l

# 126: 01111110 -/3 inclui 127 - precisa 112-126 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 112.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 113.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 114.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 115.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 116.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 117.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 118.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 119.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 120.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 121.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 122.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 123.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 124.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 125.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 126.0.0.0/8 -j DENY -l

# 217: 11011001 -/5 inclui 216 - precisa 217-219 de fora
ipchains -A input -i $EXTERNAL_INTERFACE -s 217.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 218.0.0.0/8 -j DENY -l
ipchains -A input -i $EXTERNAL_INTERFACE -s 219.0.0.0/8 -j DENY -l
```

```
# 223: 11011111 - /6 mascara 220-223
ipchains -A input -i $EXTERNAL_INTERFACE -s 220.0.0.0/6 -j DENY -l

# ------------------------------------------------------------------------------
# ICMP
# ------------------------------------------------------------------------------

# Para evitar ataques de negação de serviço baseados em bombas ICMP,
# filtrar Redirect (5) entrante e Destination Unreachable (3) sainte.
# Observe, contudo, que desativar Destination Unreachable (3) não é
# aconselhável, pois o mesmo é usado para negociar o tamanho dos
# fragmentos de pacote.

# Para ping bi-direcional.
#       Tipos de Mensagem: Echo Reply (0), Echo Request (8)
#       Para impedir ataques, limite os endereços de origem à faixa de seu provedor.
#
# Para traceroute sainte.
#       Tipos de Mensagem: INCOMING Dest Unreachable (3), Time Exceeded (11)
#       Base UDP default: 33434 à base+nr_saltos-1
#
# Para traceroute entrante.
#       Tipos de Mensagem: OUTGOING Dest Unreachable (3), Time Exceeded (11)
#       Para bloquear isto, negue OUTGOING 3 e 11

# 0: echo-reply (pong)
# 3: destination-unreachable, port-unreachable, fragmentation-needed, etc.
# 4: source-quench
# 5: redirect
# 8: echo-request (ping)
# 11: time-exceeded
# 12: parameter-problem

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 0 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 3 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 4 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 11 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 12 -d $IPADDR -j ACCEPT
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s 208.164.186.0/24 8 -d $IPADDR -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
```

```
        -s $IPADDR 0 -d 208.164.186.0/24 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 3 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 4 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 8 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 12 -d $ANYWHERE -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp \
        -s $IPADDR 11 -d 208.164.186.0/24 -j ACCEPT

# ------------------------------------------------------------------------
# UDP TRACEROUTE ENTRANTE
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s 208.164.186.0/24 $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j ACCEPT -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $TRACEROUTE_SRC_PORTS \
        -d $IPADDR $TRACEROUTE_DEST_PORTS -j DENY -l

# ------------------------------------------------------------------------
# Servidor DNS
# ------------------------------------------------------------------------

# DNS: servidor completo
# Consulta ou resposta de cliente/servidor para servidor

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 53 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR 53 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

```
# ------------------------------------------------------------------------
#Cliente DNS (53)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $NAMESERVER_1 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_1 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $NAMESERVER_2 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_2 53 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $NAMESERVER_2 53 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NAMESERVER_2 53 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Aceitar TCP somente nas portas selecionadas
# ------------------------------------------------------------------------

# ------------------------------------------------------------------------
# Servidor SSH (22)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $SSH_PORTS \
        -d $IPADDR 22 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR 22 \
        -d $ANYWHERE $SSH_PORTS -j ACCEPT
```



```
# ------------------------------------------------------------------------
# Cliente SSH (22)
# ------------------------------------------------------------------------

 ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 22 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

 ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 22 -j ACCEPT

 ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 22 \
        -d $IPADDR $SSH_PORTS -j ACCEPT

 ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $SSH_PORTS \
        -d $ANYWHERE 22 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente HTTP (80)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 80 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 80 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente HTTPS (443)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE 443 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 443 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Cliente POP (110)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $POP_SERVER 110 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $POP_SERVER 110 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente NNTP NEWS (119)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE  -p tcp ! -y \
        -s $NEWS_SERVER 119 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $NEWS_SERVER 119 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente FINGER (79)
# ------------------------------------------------------------------------

#ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#       -s $ANYWHERE 79 \
#       -d $IPADDR $UNPRIVPORTS -j ACCEPT

#ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#       -s $IPADDR $UNPRIVPORTS \
#       -d $ANYWHERE 79 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente SYSLOG (514)
# ------------------------------------------------------------------------

# ipchains -A output -i $LOCAL_INTERFACE_1 -p udp \
#       -s $IPADDR 514 \
#       -d $SYSLOG_SERVER 514 -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Servidor AUTH (113)
# ------------------------------------------------------------------------

# Rejeitar, ao invés de negar, a porta auth entrante . (NET-3-HOWTO)

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE \
        -d $IPADDR 113 -j REJECT

# ------------------------------------------------------------------------
# Cliente AUTH (113)
# ------------------------------------------------------------------------

#ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#       -s $ANYWHERE 113 \
#       -d $ipaddr $unprivports -J accept

#ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#       -s $IPADDR $UNPRIVPORTS \
#       -d $ANYWHERE 113 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente SMTP (25)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 25 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFAC E -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 25 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente IRC (6667)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 6667 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 6667 -j ACCEPT

# ------------------------------------------------------------------------
```

```
# Cliente ICQ (4000)
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 2000:4000 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 2000:4000 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE 4000 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 4000 -j ACCEPT

# ------------------------------------------------------------------------
# Cliente FTP (20, 21)
# ------------------------------------------------------------------------

# Solicitação sainte

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 21 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 21 -j ACCEPT

# Canal de dados em modo NORMAL

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYQUERE 20 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

# Respostas do canal de dados em modo NORMAL

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 20 -j ACCEPT
```

```
# Criação de canal de dados em modo PASSIVO

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT

# Respostas do canal de dados em modo PASSIVO

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT
# ------------------------------------------------------------------------
# Cliente RealAudio / QuickTime
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 554 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 554 -j ACCEPT

# TCP é um modo mais seguro: 7070:7071

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
        -s $ANYWHERE 7070:7071 \
        -d $IPADDR $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE 7070:7071 -j ACCEPT

# UDP é o método preferido: 6970:6999
# Para máquinas da LAN, o UDP exige o módulo de mascaramento RealAudio
# e o software de terceiros ipmasqadm.

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -s $ANYWHERE $UNPRIVPORTS \
        -d $IPADDR 6970:6999 -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $UNPRIVPORTS \
        -d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

```
# ------------------------------------------------------------------------
# Cliente WHOIS (43)
# ------------------------------------------------------------------------

#ipchains -A input -i $EXTERNAL_INTERFACE -p tcp ! -y \
#        -s $ANYWHERE 43 \
#        -d $IPADDR $UNPRIVPORTS -j ACCEPT

#ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
#        -s $IPADDR $UNPRIVPORTS \
#        -d $ANYWHERE 43 -j ACCEPT

# ------------------------------------------------------------------------
# TRACEROUTE SAINTE
# ------------------------------------------------------------------------

ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
        -s $IPADDR $TRACEROUTE_SRC_PORTS \
        -d $ANYWHERE $TRACEROUTE_DEST_PORTS -j ACCEPT

# ------------------------------------------------------------------------
# Tráfego ilimitado dentro da rede local
# ------------------------------------------------------------------------

# Todas as máquinas internas têm acesso à máquina firewall.

ipchains -A input   -i $LOCAL_INTERFACE_1 -s $LOCALNET_1 -j ACCEPT
ipchains -A output -i $LOCAL_INTERFACE_1 -d $LOCALNET_1 -j ACCEPT
```

```
# ------------------------------------------------------------------------------
# VPN IPSec FreeS/WAN
# ------------------------------------------------------------------------------

# Se você estiver usando a VPN IPSEC FreeSWAN, você precisará preencher os
# endereços dos gateways em IPSECSG e nas interfaces virtuais para o
# IPSec FreeS/Wan nos parâmetros FREESWANVI.

# IPSECSG é uma lista de gateways remotos separados por espaço.
# FREESWANVI é uma lista de interfaces virtuais, separadas por espaço,
# para a implementação do IPSEC FreeS/Wan.
# Somente inclua aqueles que realmente forem utilizados.

# Permite o protocolo IPSEC a partir de gateways remotos na interface externa.
#
# O IPSEC usa três tipos principais de pacotes:
#
#       IKE utiliza o protocolo UDP e a porta 500,
#       ESP utiliza o protocolo número 50, e
#       AH  utiliza o protocolo número 51

#ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
#       -s $IPSECSG -j ACCEPT

#ipchains -A output -i $EXTERNAL_INTERFACE -p udp \
#       -s $IPSECSG -j ACCEPT

#ipchains -A input -i $EXTERNAL_INTERFACE -p 50 \
#       -s $IPSECSG -j ACCEPT

#ipchains -A output -i $EXTERNAL_INTERFACE -p 50 \
#       -s $IPSECSG -j ACCEPT

#ipchains -A input -i $EXTERNAL_INTERFACE -p 51 \
#       -s $IPSECSG -j ACCEPT

#ipchains -A output -i $EXTERNAL_INTERFACE -p 51 \
#       -s $IPSECSG -j ACCEPT
```

 # Permite todo o tráfego para a interface virtual FreeS/WAN

```
#ipchains -A input -i $FREESWANVI \
#       -s $ANYWHERE \
#       -d $ANYWHERE -j ACCEPT

#ipchains -A output -i $FREESWANVI \
#       -s $ANYWHERE \
#       -d $ANYWHERE -j ACCEPT
```

 # Repassar qualquer coisa do túnel IPSEC da interface virtual FreeS/WAN

```
#ipchains -A forward -i $FREESWANVI \
#       -s $ANYWHERE \
#       -d $ANYWHERE -j ACCEPT
```

 # Desativar proteção contra ataque de spoof de IP para que o IPSEC
 # funcione adaquadamente

```
# echo 0 > /proc/sys/net/ipv4/conf/ipsec0/rp_filter
# echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter

# ------------------------------------------------------------------------
```
 # Mascarar tráfego interno
```
# ------------------------------------------------------------------------

# Todo o tráfego interno é mascarado externamente

ipchains -A forward -i $EXTERNAL_INTERFACE -s $LOCALNET_1 -j MASQ
```

```
# ------------------------------------------------------------------------
# Ativa o registro em log dos pacotes negados selecionados
# ------------------------------------------------------------------------

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
        -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $PRIVPORTS -j DENY -l

ipchains -A input -j $EXTERNAL_INTERFACE -p udp \
        -d $IPADDR $UNPRIVPORTS -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 5 -d $IPADDR -j DENY -l

ipchains -A input -i $EXTERNAL_INTERFACE -p icmp \
        -s $ANYWHERE 13:255 -d $IPADDR -j DENY -l

# ------------------------------------------------------------------------
```

```
;;

stop)
        echo -n "Desativando Serviços de Firewall: "

# Remover todas as regras existentes pentencentes a este filtro
ipchains -F

# Deleta todas as cadeias definidas pelo usuário para este filtro
ipchains -X

# Reseta a política default do filtro para ACEITAR.
ipchains -P input ACCEPT
ipchains -P output ACCEPT
ipchains -P forward ACCEPT

# Desativa a Proteção TCP SYN Cookie.
echo 0 > /proc/sys/net/ipv4/tcp_syncookies

# Desativa a proteção contra spoof de IP.
# Ativa a Verificação de Endereço de Origem.
for f in /proc/sys/net/ipv4/conf*/rp_filter;
do
        echo 0 > $f
done

# Ativa a Aceitação de Redirecionamento de ICMP
for f in /proc/sys/net/ipv4/conf/*/accept_redirects;
do
        echo 1 > $f
done

# Ativa o Roteamento de Pacotes na Origem
for f in /proc/sys/net/ipv4/conf/*/accept_source_route;
do
        echo 1 > $f
done
```

```
;;

status)
        status firewall

;;

restart|reload)
        $0 stop
        $0 start

;;

*)
        echo "Sintaxe: firewall (start|stop|status|restart|reload)"
        exit 1

esac

exit 0
```

Agora, torne este script executável e altere suas permissões default:

[root@deep /]# **chmod 700 /etc/rc.d/init.d/firewall**
[root@deep /]# **chown 0.0 /etc/rc.d/init.d/firewall**

Crie os links simbólicos rc.d para o seu Firewall, com o seguintes comandos:

[root@deep /]# **chkconfig --add firewall**
[root@deep /]# **chkconfig --level 345 firewall on**

Agora, as suas regras de firewall estão configuradas para usar o System V init (o System V init é o engarregado de inicializar todos os processos normais que precisam ser executados por ocasião do boot) e o serviço será automaticamente inicializado cada vez que seu servidor fizer reboot.

- Para parar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall stop**
  Desativando o Serviço de Firewall: [OK]

- Para inicializar manualmente o firewall em seu sistema, use o seguinte comando:

  [root@deep /]# **/etc/rc.d/init.d/firewall start**
  Iniciando Serviços de Firewall: [OK]

Negar acesso a alguns endereços

Algumas vezes, você conhece um endereço para o qual você gostaria de bloquear qualquer acesso em seu servidor. Você pode fazer isso criando o arquivo **rc.firewall.blocked** sob o diretório "/etc/rc.d" e descomentando as seguintes linhas em seu arquivo de script de regras de firewall:

Edite o seu arquivo de script de **firewall** (vi /etc/rc.d/init.d/firewall) e descomente as seguintes linhas:

```
if [ -f /etc/rc.d/rc.firewall.blocked ]; then
        . /etc/rc.d/rc.firewall.blocked
fi
```

Crie o arquivo **rc.firewall.blocked** (touch /etc/rc.d/rc.firewall.blocked) e adicione dentro deste arquivo todos os endereços IP para os quais você deseja bloquear qualquer acesso em seu servidor:

Por exemplo, Eu coloquei os seguintes endereços IP neste arquivo:

204.254.45.9
187.231.11.5

Documentação adicional

Para mais detalhes, existem várias páginas de manual que você pode ler:

$ ipchains (8)	- Administração do firewall de IP
$ ipchains-restore (8)	- Restaura as cadeias do firewall de IP de stdin
$ ipchains-save (8)	- Salva as cadeias do firewall de IP em stdout

Ferramentas Administrativas do IPCHAINS

Os comandos listados abaixo são alguns que frequentemente aplicamos em nosso uso diário, porém existem muitos mais e você deve verificar as páginas de manual e a documentação para mais detalhes e informações:

ipchains

A ferramenta ipchains é usada na administração do firewall do Sistema Operacional Linux. Podemos usá-la para configurar um arquivo de regras de firewall como estamos fazendo neste livro. Uma vez criado o arquivo de regras de firewall, podemos manipulá-lo com vários comandos para fazermos manutenção e inspeção das regras no kernel do Linux.

- Para listar as regras na cadeia selecionada, use o seguinte comando:

  [root@deep /]# **ipchains -L**

Este comando listará todas as regras da cadeia selecionada. Se nenhuma cadeia for selecionada, todas as cadeias serão listadas.

- Para listar todas as regras de entrada na cadeia selecionada, use o comando:

  [root@deep /]# **ipchains -L input**

Este comando listará todas as regras de entrada que configuramos na cadeia selecionada.

- Para listar todas as regras de saída na cadeia selecionada, use o comando:

  [root@deep /]# **ipchains -L output**

Este comando listará todas as regras de saída que configuramos na cadeia selecionada.

- Para listar todas as regras de repasse na cadeia selecionada, use o comando:

[root@deep /]# **ipchains -L forward**

Este comando listará todas as regras de repasse na cadeia selecionada. É claro que isto só funciona se você tiver configurado o Mascaramento em seu servidor (para servidores de gateway em geral).

- Para listar todas as regras de mascaramento na cadeia selecionada, use o comando:

[root@deep /]# **ipchains -ML**

Esta opção permite visualizar as conexões atualmente mascaradas. Você precisa ter configurado o Mascaramento em seu servidor para que este comando funcione (mais uma vez: somente para servidor de gateway).

- Para listar todas as regras em formato numérico na cadeia selecionada, use o comando:

  [root@deep /]# **ipchains -nL**

Este comando listará todas as regras em formato numérico. Todos os endereços IP e números de porta serão impressos em formato numérico.

