Marcos Laureano
Um site diferente sobre seguranÃ§a, sistemas operacionais e sobre mim tambÃ©m…

Firewall no Linux com IPTABLES

Este guia nÃ£o pretende ser definitivo, ele somente Ã© utilizado para fins de ensino. Qualquer configuraÃ§Ã£o adicional Ã© bom olhar no prÃ³prio manual que acompanha o software.

VersÃ£o original do guia: 07/11/2007

ConsideraÃ§Ãµes

- Os testes para configuraÃ§Ã£o e utilizaÃ§Ã£o foram feitos utilizando a distribuiÃ§Ã£o Suse Linux (versÃ£o 8.0) e no Red Hat Linux (versÃ£o 8.0)
- Literatura recomendada: Firewalls em Linux. Antonio Marcelo. Editora Brasport.

Conceito de Firewall

Um firewall Ã© um sistema (ou grupo de sistemas) que reforÃ§am a norma de seguranÃ§a entre uma rede interna segura e uma rede nÃ£o-confiÃ¡vel como a Internet. Os firewalls tendem a serem vistos como uma proteÃ§Ã£o entre a Internet e a rede privada. Mas em geral, um firewall deveria ser considerado como um meio de dividir o mundo em duas ou mais redes: uma ou mais redes seguras e uma ou mais redes nÃ£o-seguras.

Um firewall pode ser um PC, um roteador, um computador de tamanho intermediÃ¡rio, um mainframe, uma estaÃ§Ã£o de trabalho UNIX ou a combinaÃ§Ã£o destes que determine qual informaÃ§Ã£o ou serviÃ§os podem ser acessados de fora e a quem Ã© permitido usar a informaÃ§Ã£o e os serviÃ§os de fora. Geralmente, um firewall Ã© instalado no ponto onde a rede interne segura e a rede externa nÃ£o-confiÃ¡vel se encontram, ponto que tambÃ©m Ã© conhecido como ponto de estangulamento.

A fim de entender como um firewall funciona, considere que a rede seja um edifÃcio onde o acesso deva ser controlado. O edifÃcio tem uma sala de espera como o Ãºnico ponto de entrada. Nesta sala de espera, as recepcionistas recebem os visitantes, os guardas de seguranÃ§a observam os visitantes, as cÃ¢meras de vÃdeo gravam as aÃ§Ãµes de cada visitante e leitores de sinais autenticam os visitantes que entram no edifÃcio.

Estes procedimentos devem funcionar bem para controlar o acesso ao edifÃcio, contudo se uma pessoa nÃ£o autorizada consegue entrar, nÃ£o hÃ¡ meio de proteger o edifÃcio contra as aÃ§Ãµes do intruso. PorÃ©m, se os movimentos do intruso sÃ£o monitorados, Ã© possÃvel detectar qualquer atividade suspeita.

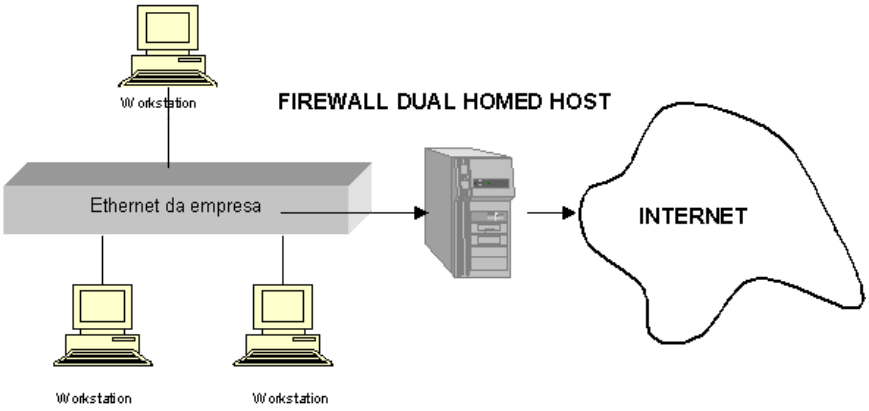
Um firewall Ã© projetado para proteger as fontes de informaÃ§Ã£o de uma organizaÃ§Ã£o, controlando o acesso entre a rede interna segura e a rede externa nÃ£o-confiÃ¡vel. Ã‰ importante notar que mesmo se o firewall tiver sido projetado para permitir que dados confiÃ¡veis passem, negar serviÃ§os vulnerÃ¡veis e proteger a rede interna contra ataques externos, um ataque recÃ©m-criado pode penetrar o firewall a qualquer hora. O administrador da rede deve examinar regularmente os registros de eventos e alarmes gerados pelo firewall.

Os firewalls podem ser divididos em duas grandes classes: Filtros de pacote e servidores proxy.

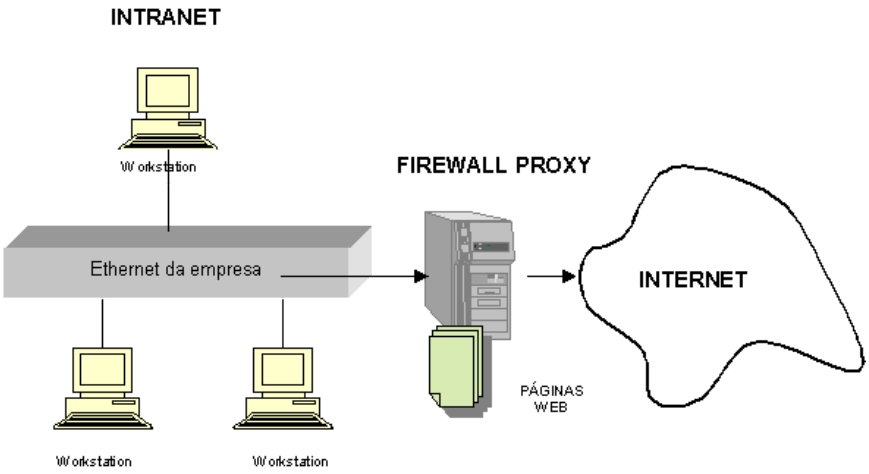
Filtros de Pacotes
A filtragem de pacotes Ã© um dos principais mecanismos que, mediante regras definidas pelo administrador em um firewall,

permite ou nÃ£o a passagem de datagramas IP em uma rede. PoderÃamos filtrar pacotes para impedir o acesso a um serviÃ§o de Telnet, um chat ou mesmo um site na Internet.

O modelo mais simples de firewall Ã© conhecido como o *dual homed system*, ou seja, um sistema que interliga duas redes distintas. Este sistema possui um servidor com duas placas de rede que faz com que os usuÃ¡rios possam falar entre si. O exemplo clÃ¡ssico Ã© um firewall entre uma Intranet e a Internet.



Servidores Proxy
Permite executar a conexÃ£o ou nÃ£o a serviÃ§os em uma rede modo indireto. Normalmente os proxies sÃ£o utilizados como caches de conexÃ£o para serviÃ§os Web. Um proxy Ã© utilizado em muitos casos como elemento de aceleraÃ§Ã£o de conexÃ£o em links lentos.



Entendendo a Necessidade do Firewall
Independente de vocÃª estar implementando um filtro de pacotes ou um servidor proxy, o firewall fornece diversos serviÃ§os. As funÃ§Ãµes firewall mais essenciais no Linux sÃ£o:

- **ConservaÃ§Ã£o de endereÃ§o IP e encaminhamento de trÃ¡fego** – Muitos firewalls agem primeiro como roteadores de modo que vÃ¡rias redes possam se comunicar entre si. Muitos administradores de rede somente utilizam esta funÃ§Ã£o para ajudar a criar subredes adicionais. Este recurso Ã© incluÃdo como um elemento de firewall somente porque ele Ã© conseguido com a utilizaÃ§Ã£o de IPCHAINS (kernel 2.2) e IPTABLES (kernel 2.4). Assim qualquer um com apenas um endereÃ§o IP pode ser capaz de criar uma rede local (LAN) ou rede remota (WAN) com acesso total Ã Internet. Entretanto um firewall nÃ£o tem necessariamente que fornecer o serviÃ§o de NAT (Network Address Translation). Mesmo assim, muitos firewalls permitem que vocÃª utilize este recurso;
- **DistinÃ§Ã£o de rede** – Um firewall Ã© o meio principal de criar uma borda entre a sua rede e quaisquer outras redes. Como ele criar uma clara distinÃ§Ã£o entre as redes, o firewall ajuda a administrar o trÃ¡fego. O firewall nÃ£o tem que

necessariamente ser instalado entre uma rede privada confiÃ¡vel e a Internet. Muitas vezes, o firewall Ã© instalado dentro de uma rede corporativa para diferenciar ainda mais certas Ã¡reas da empresa do restante da rede;

- **ProteÃ§Ã£o contra ataques denial-of-service (DoS) ou negaÃ§Ã£o de serviÃ§os, anÃ¡lises e farejadores (sniffers)** – Um firewall funciona como um ponto Ãºnico que monitora o trÃ¡fego de entrada e de saÃda. Ã‰ possÃvel para este firewall limitar qualquer tipo de trÃ¡fego que vocÃª desejar;
- **Filtragem de IP e de portas** – A capacidade de permitir ou rejeitas uma conexÃ£o baseada no endereÃ§o IP e na porta. Este tipo de filtragem Ã© provavelmente a funÃ§Ã£o mais bem entendida de um firewall. De uma forma geral, este tipo de filtragem Ã© geralmente feito por filtros de pacotes. A filtragem de pacotes pode se tornar bastante complexa, pois vocÃª deve sempre considerar que o trÃ¡fego pode ser filtrado de acordo com a origem ou o destino do pacote. Por exemplo, um filtro de pacotes pode bloquear o trÃ¡fego que chega Ã sua rede vindo de um determinado endereÃ§o IP e uma determinada porta;
- **Filtragem de conteÃºdo** – Os servidores proxy sÃ£o geralmente os Ãºnicos tipos de firewall que administram e controlam o trÃ¡fego atravÃ©s da inspeÃ§Ã£o de URL e conteÃºdo de pÃ¡gina. Se configurado corretamente, um firewall baseado em proxy Ã© capaz de identificar e bloquear todo o conteÃºdo que vocÃª considere imprÃ³prio;
- **Redirecionamento de pacotes** – Algumas vezes, Ã© preciso que um firewall envie o trÃ¡fego para outra porta ou outro servidor. Por exemplo, suponha que vocÃª tenha instalado o servidor proxy Squid em um servidor separado do seu firewall. Ã‰ possÃvel que vocÃª configure o seu firewall para encaminhar automaticamente todo o trÃ¡fego enviado Ã s portas 80 (HTTP) e 443 (HTTPS) para o seu servidor proxy.
- **AutenticaÃ§Ã£o e criptografia mais fortes** – Um firewall Ã© capaz de autenticar usuÃ¡rios e criptografar transmissÃµes entre ele mesmo e o firewall de uma outra rede.
- **Registros complementares** – Um dos benefÃcios mais importantes (mas ignorado) de um firewall Ã© que ele permite examinar todos os detalhes dos pacotes de rede que passam por ele. VocÃª pode descobrir se estÃ¡ para sofrer (ou jÃ¡ sofreu) um ataque, basta verificar se existem anÃ¡lises de portas e vÃ¡rios tipos de conexÃ£o ao seu sistema.

COMO PROGER O FIREWALL

Um dos benefÃcios de ter um firewall Ã© que ele proporciona um ponto Ãºnico para processar trÃ¡fego de entrada e saÃda. Contudo, considere que um firewall tambÃ©m pode fornecer um ponto central de ataque ou falhas. Ele informa ao hacker que hÃ¡ uma sÃ©rie de redes por trÃ¡s dele. Se o hacker conseguir derrotar este Ãºnico firewall, toda a rede ficarÃ¡ aberta ao ataque. AlÃ©m disso, se o hacker, de alguma maneira, for capaz de desativar o servidor, toda a rede serÃ¡ recusada por todos os serviÃ§os de Internet. Ã‰ importante que vocÃª tome medidas que protejam o seu firewall.

Algumas coisas que podem ser feitas:

1. Limite o acesso ao roteador e o firewall apenas para login interativo e proteja o sistema fisicamente. Assim, seu firewall estarÃ¡ muito menos suscetÃvel a ataques remotos. Ainda assim, Ã© possÃvel que ocorram problemas no kernel (estouros de buffer ou buffer overflow e outros problemas de programaÃ§Ã£o). Tais problemas podem levar ao comprometimento do sistema, mesmo que vocÃª nÃ£o tenha outros serviÃ§os rodando;
2. Se for necessÃ¡rio o acesso remoto, analise a possibilidade de usar o acesso somente atravÃ©s do SSH (Secure Shell). Devidamente configurado para utilizar chaves pÃºblicas na autenticaÃ§Ã£o. Embora o SSH nÃ£o seja imune Ã s ameaÃ§as de seguranÃ§a, Ã© uma das ferramentas de administraÃ§Ã£o remota mais populares e seguras para servidores;
3. Crie um servidor de seguranÃ§a – Se o seu servidor entrar em pane devido a um ataque, ou simplesmente por causa de uma falha em disco rÃgido, vocÃª deverÃ¡ ter um sistema idÃªntico disponÃvel para substituÃ-lo;
4. Monitore o servidor – Use um aplicativo IDS (Intrusion Detection System) para ouvir as conexÃµes feitas no seu roteador. Geralmente, o melhor Ã© instalar um aplicativo IDS em um servidor independente na rede. Isto se chama monitoramente passivo, porque o servidor remoto nÃ£o consome os recursos de sistema do firewall. O aplicativo IDS pode, por exemplo, enviar um ping aleatÃ³rio ao firewall para saber dele estÃ¡ ativo, e pode entÃ£o informar se o servidor estiver parado.

5. Fique atento aos relatÃ³rios e informativos sobre bugs relacionados ao firewall e ao sistema operacional. Manter-se atualizado sobre tais alteraÃ§Ãµes ajudarÃ¡ a atualar rapidamente seu sistema, caso um problema seja descoberto.

IPTABLES

O iptables Ã© o firewall padrÃ£o do Kernel 2.4.x (quando este guia estava sendo escrito, a versÃ£o do kernel era 2.4.19 – vocÃª pode baixar a novas versÃµes do Kernel do Linux no site The Linux Kernel Archives).

A sintaxe genÃ©rica usada pelo comando iptables Ã©:

```
iptables comando regras extensÃµes
```

- **-A cadeia** – Anexa regras ao final de uma cadeia. Se um nome de host Ã© fornecido, como fonte ou como destino, uma regra Ã© adicionada para cada IP relacionado a este host.
- **-D cadeia** – Apaga uma ou mais regras da cadeia especificada
- **-D cadeia regra_num** – Apaga a regra residente na posiÃ§Ã£o indicada por regra_num da cadeia especificada. A primeira regra na cadeia Ã© a de nÃºmero 1.
- **-R cadeia regra_num** – SubstituÃ a regra regra_num da cadeia especificada pela regra dada
- **-I cadeia regra_num** – Insere uma ou mais regras no comeÃ§o da cadeia. Se um nome de host Ã© fornecido, como fonte ou como destino, uma regra Ã© adicionada para cada IP relacionado a este host.
- **-L [cadeia]** – Lista todas as regras em uma cadeia. Caso nÃ£o haja nenhuma cadeia especificada, todas as regras em todas as cadeias sÃ£o listadas.
- **-F [cadeia]** – Remove todas as regras de uma cadeia. Se nenhuma cadeia for especificada, remove as regras de todas as cadeias existentes, inclusive as do usuÃ¡rio.
- **-Z [cadeia]** – Restaura os contadores de datagramas e de bytes em todas as regras das cadeias especificadas para zero, ou para todas as cadeias se nenhuma for especificada.
- **-N cadeia** – Cria uma cadeia definida pelo usuÃ¡rio com o nome especificado.
- **-X [cadeia]** – Apaga a cadeia definida pelo usuÃ¡rio ou todas se nÃ£o for especificada uma.
- **-C cadeia** – Verifica o datagrama descrito pela regra especificada contra a cadeia especificada. Este comando retorna uma mensagem descrevendo como a cadeia processou o datagrama. Isto Ã© muito Ãºtil para testar a configuracÃ£o do firewall, e para uma anÃ¡lise posterior.
- **-P cadeia polÃtica** – Define a polÃtica padrÃ£o para uma cadeia dentro de uma polÃtica especificada. As polÃticas vÃ¡lidas: ACCEPT, DROP, QUEUE e RETURN. ACCEPT permite a passagem do datagrama. DROP descarta o datagrama. QUEUE passa o datagrama para Ã¡rea do usuÃ¡rio para posterior processamento. RETURN forÃ§a o cÃ³digo do firewall a retornar para a cadeia anterior e continua o processamento na regra seguinte Ã que retornou.

Regras

As seguintes regras podem ser usadas:

- **-p[!] Protocol** – Define o protocolo ao qual a regra se aplica. O parÃ¢metro protocol pode ser qualquer valor numÃ©rico do arquivo `/etc/protocol` ou uma das palavras chave: tcp,udp ou icmp
- **-s [!] addres[/mask]** – Define a origem do pacote ao qual a regra se aplica. O parÃ¢metro *address* pode ser um nome de host, um nome de rede ou um endereÃ§o IP com uma mÃ¡scara de rede opcional.
- **-d [!] address[/mask]** – Define o destino do pacote ao qual a regra se aplica. O endereÃ§o e a porta sÃ£o definidos usando-se as mesmas regras utilizadas para definir esses valores para a origem do pacote.
- **-j alvo** – Define um alvo para o pacote caso ele se encaixe nesta regra. Os alvos possÃveis sÃ£o ACCEPT, DROP, QUEUE ou RETURN. Ã‰ possÃvel especificar uma cadeia do usuÃ¡rio. TambÃ©m Ã© possÃvel especificar uma

extensÃ£o.

- **-i [!] interface_name** – Define o nome da interface por onde o datagrama foi recebido. Um nome de interface parcial pode ser usado encerrando-o com um sinal de â€œ+â€ ; por exemplo, eth+ corresponderia a todas as interfaces Ethernet iniciadas com eth.
- **-o [!] interface_name** – Define o nome da interface por onde o datagrama serÃ¡ transmitido.
- **[!] -f** – Indica que a regra somente se refere ao segundo fragmento e aos subseqÃ¼entes de pacotes fragamentados.

ObservaÃ§Ã£o: O sÃmbolo â€œ!â€ Ã© usado na regras como uma negaÃ§Ã£o da expressÃ£o. Exemplo: `-s 192.168.0.10/32` equivale ao endereÃ§o de origem 192.168.0.10, `-s !192.168.0.10/32` equivale a todos os endereÃ§os exceto o 192.168.0.10.

OpÃ§Ãµes

- **-v** – SaÃda em modo verbose. Mais rico em termos de detalhes sobre o que estÃ¡ acontecendo ou sendo feito.
- **-n** – SaÃda em modo numÃ©rico e nÃ£o por nome de host, rede ou porta.
- **-x** – Exibe o valor exato do pacote e dos contadores de bytes em vez de arrendondÃ¡-los para o milhar, milhÃ£o ou bilhÃ£o mais prÃ³ximo.
- **–line-numbers** – Quando lista as regras, adiciona um nÃºmero de linha ao comeÃ§o de cada regra, correspondendo Ã posiÃ§Ã£o da regra dentro da cadeia.

ExtensÃµes

O utilitÃ¡rio iptables Ã© extensÃvel atravÃ©s de uma biblioteca de mÃ³dulos compartilhados opcionais. Para fazer uso das extensÃµes Ã© preciso especificar o seu nome usando o parÃ¢metro -m [argumento] para o que o iptables carregue este mÃ³dulo.

Em alguns casos Ã© usuado o parÃ¢metro -p para determinar o protocolo (em certos casos nÃ£o Ã© necessÃ¡rio o parÃ¢metro -m pois ele Ã© carregado automaticamente, por exemplo quando se usa tcp, udp ou icmp).

ExtensÃ£o TCP: usada com -m tcp -p tcp

- **–sport [!] [port[:port]]** – Especifica a porta que a origem do datagrama usa. Portas podem ser especificadas com um conjunto especificando-se o seu limite superior e inferior separados por dois pontos (:). Por exemplo, 20:25 descreve todas as portas numeradas de 20 atÃ© 25 inclusive. TambÃ©m Ã© possÃvel usar o caracter â€œ!â€ para inverter a expressÃ£o.
- **–dport [!] [port[:port]]** – Especifica a porta que o destino do datagrama usa.
- **–tcp-flags [!] mask comp** – Especifica que esta regra somente serÃ¡ validada quando os flags do datagrama TCP coincidirem com o especificado em mask e comp. Mask Ã© uma lista separada por vÃrgulas dos flags que devem ser examinados quando for feito o teste. Comp Ã© uma lista separada por vÃrgulas dos flas que devem ser configurados. Os flags vÃ¡lidos sÃ£o: SYN, ACK, FIN, RST, URG, PSH, ALL ou NONE.
- **–syn** – Especifica que a regre deve encontrar somente datagramas com o bit SYN ligado e os bits ACK e FIN desligados. Datagramas com essas opÃ§Ãµes sÃ£o usados para requisitar inÃcio de conexÃ£o TCP.

ExtensÃ£o UDP: usada com -m udp -p udp

- **–sport[!][port[:port]]** – Este parÃ¢metro tem funcionamento idÃªntico ao da extensÃ£o TCP.
- **–dport[!][port[:port]]** – Este parÃ¢metro tem funcionamento idÃªntico ao da extensÃ£o TCP.

ExtensÃ£o ICMP: usada com -m icmp -p icmp

–icmp-type [!] typername – Especifica o tipo de mensagem ICMP que a regra deve satisfazer. O tipo pode ser determinado por um nÃºmero ou nome. Alguns nomes vÃ¡lidos sÃ£o: echo-request, echo-reply, source-quench, time-exceeded, destionation-unreachable, network-unreachable, host-unreanchable, protocol-unreachable e port-unreachable.

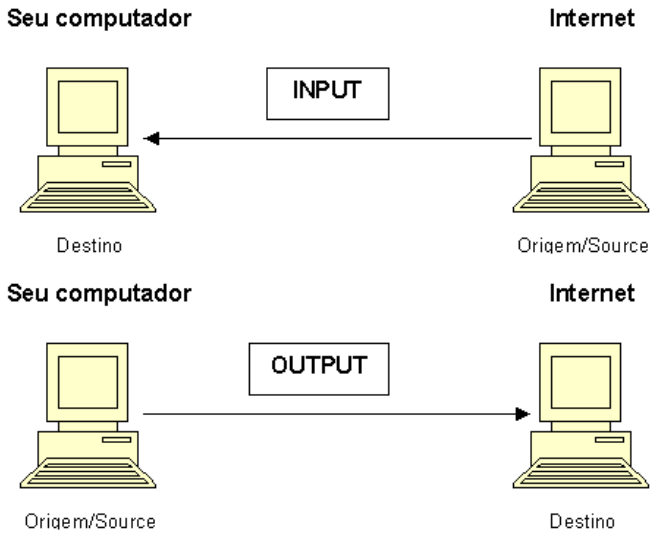
ExtensÃ£o MAC: usada com -m mac
–mac-source [!] address – Especifica o endereÃ§o Ethernet do host que transmitiu o datagrama que esta regra deve encontrar.

Dispositivos de Rede Importantes no Linux

- **ethX** – Dispositivo de rede utilizado para as placas padrÃ£o ethernet. Normalmente a primeira placa conectada no host Ã© eth0, a segunda eth1 e assim sucessivamente.
- **lo** – Dispositivo de loopback, utilizando para testes do TCP/IP. Normalmente quando aparece somente este dispositivo, significa que a parte fÃsica da rede nÃ£o estÃ¡ ativa.
- **pppX** – A interface ppp, normalmente Ã© ativa no momento de uma conexÃ£o PPP (point-to-point protocol) via modem no sistema recebe o dispositivo ppp0, a segunda ppp1, e assim sucessivamente. Para verificar sua existÃªncia Ã© necessÃ¡rio que uma conexÃ£o PPP esteja estabelecida.

Alguns Exemplos de UtilizaÃ§Ã£o

Para facilitar na criaÃ§Ã£o das regras (principalmente para saber quando utilizamos -s ou -d), podemos utilizar as seguintes dicas:



ProteÃ§Ã£o contra IP Spoofing – O IP Spoofing Ã© uma tÃ©cnica de forjar endereÃ§os IP falsos para executar ataques a uma mÃ¡quina na web. Geralmente utilizam-se IP falsos nas redes 10.0.0.0, 172.16.0.0 e 192.168.0.0. Para bloquear estes endereÃ§os:

Para mÃ¡quinas com interface de rede:

```
# iptables -A INPUT -s 10.0.0.0/8 -i eth0 -j DROP
# iptables -A INPUT -s 172.16.0.0/8 -i eth0 -j DROP
# iptables -A INPUT -s 192.168.0.0/8 -i eth0 -j DROP
```

Para mÃ¡quinas com interface com modens ADSL:

```
# iptables -A INPUT -s 10.0.0.0/8 -i ppp0 -j DROP
# iptables -A INPUT -s 172.16.0.0/8 -i ppp0 -j DROP
# iptables -A INPUT -s 192.168.0.0/8 -i ppp0 -j DROP
```

Para garantir a navegaÃ§Ã£o do nosso equipamento:

```
# iptables -A INPUT -m state -state RELATED, ESTABLISHED -j ACCEPT
```

Sem este comando, a estaÃ§Ã£o nÃ£o navegaria. O mÃ³dulo ip_conntrack permite especificar regras de acordo com o estado da conexÃ£o do pacote. Isto Ã© feito atravÃ©s do parÃ¢metro -state.

- **NEW** – Confere os pacotes que estabelecem novas conexÃµes.
- **ESTABLISHED** – Confere os pacotes com conexÃµes jÃ¡ estabelecidas.
- **RELATED** – Confere com pacotes relacionados indiretamente a uma conexÃ£o, como mensagens de erro.
- **INVALID** – Confere com pacotes que nÃ£o puderem ser identificados por algum motivo. Como respostas de conexÃ£o desconhecidas.

Registrar conexÃµes a portas nÃ£o autorizadas – Ã‰ importante sabermos quando estamos sendo monitorados, a fim de prever e se defender de possÃveis ataques. Para isso podemos fazer com que o iptables registre no messages do Linux tentativas de conexÃ£o a portas bloqueadas no sistemas.

```
# iptables -A INPUT -s 0.0.0.0/0 -i eth0 -j LOG -log-prefix â€œConexÃ£o proibidaâ€
```

Se quisermos fechar algumas portas especificamente:

```
# iptables -A INPUT -p tcp -dport 21 -j LOG -log-prefix â€œServiÃ§o: ftpâ€
# iptables -A INPUT -p tcp -dport 23 -j LOG -log-prefix â€œServiÃ§o:telnetâ€
```

O tamanho da mensagem para o parÃ¢metro -log-prefix Ã© de 64 caracteres.

Filtrar mensagem echo-request do ping ou traceroute – AtravÃ©s do comando ping, podemos descobrir qual o sistema operacional estÃ¡ executando num servidor. De posse desta informaÃ§Ã£o, Ã© possÃvel programas ataques e exploraÃ§Ãµes direcionados para este sistema. Caso nÃ£o queiramos que alguÃ©m execute um ping na nossa mÃ¡quina.

```
# iptables -A INPUT -p icmp -icmp-type echo-request -j DROP
```

ConsideraÃ§Ãµes Finais

A utilizaÃ§Ã£o de um firewall Ã© muito importante, mesmo em mÃ¡quinas para acessos domÃ©stico. Crie a sua seqÃ¼Ãªncia de regras e salve em arquivo para ser inicializado sempre que vocÃª for acessar a internet. Coloque no processo de boot da mÃ¡quina, dentro do arquivo `/etc/rc.d/rc.local` e nÃ£o se esqueÃ§a de liberar o acesso de execuÃ§Ã£o do arquivo (`chmod 755 nomedoscript`).

7 respostas a *Firewall no Linux com IPTABLES*

Roberto Neigenfind *disse:*
fevereiro 9, 2015 às 4:55 pm

OlÃ¡.
Gostaria de comentar que o firewall baseado em IPtables nÃ£o Ã© uma proteÃ§Ã£o suficiente. Imagine o seguinte caso: uma recepcionista em uma empresa recebe um e-mail comentando que o CPF dela vai ser cancelado. Para evitar isto ela tem que clicar em um link. Todos nos sabemos que a possibilidade dela fazer isto Ã© grande e sabemos no que vai dar, certo?

O firewall baseado em IP tables irÃ¡ bloquear as conexÃµes de fora para dentro, por exemplo. Mas Ã© quase impossÃvel gerenciar todas as conexÃµes indesejadas de dentro para fora como esta da recepcionista.

Com um Next Generation Firewall hÃ¡ diversas anÃ¡lises e bloqueios adicionais que podem evitar isto. Por exemplo, quando o e-mail passar pelo Next Generation Firewall este o analisarÃ¡ e identificarÃ¡ um link que aponta para um site jÃ¡ catalogado como spyware. Neste caso o link Ã© removido do e-mail e o ataque nÃ£o consegue prosseguir.

Este Ã© sÃ³ um exemplo. Se vocÃª quer saber mais recomendo acessar para saber mais

---

Samara *disse:*
setembro 24, 2014 às 2:47 pm

Ã“timo.

Isadora Riul *disse:*
maio 3, 2014 às 3:58 pm

IncÅ•ivel.. Muito bom o conteÃºdo desse post. Vai me ajudar bastante, obrigadaa =3

Marcos Laureano *disse:*
março 16, 2013 às 10:25 am

Obrigado!

Tiago Guimaraes *disse:*
fevereiro 7, 2013 às 12:24 pm

PARABÃ‰NS pelo material que nos disponibilizou fico muito agradecido, Ã³timo conteÃºdo.

Eduardo Uda *disse:*
março 29, 2008 às 2:47 pm

Oi! Muito bom o teu artigo! Olha sÃ³, fiquei com uma dÃºvida. Tem como eu mascarar um ip fixo que entra no firewall e mudÃ¡-lo de forma que a conexÃ£o pptp identifique coneÃ§Ãµes diferentes?

Eduardo Seixas *disse:*
outubro 4, 2007 às 3:11 pm

Realmente algo muito bom nesse manual. Qualquer um aprende com os exemplos. ParabÃ©ns

---