[**Tutorial básico de netfilter/iptables**](http://pratesdicas.wordpress.com/2009/11/12/tutorial-basico-de-iptables/)

O **iptables** é uma interface de configuração do **netfilter** (o Kernel pode controlar seu próprio fluxo interno, através de um firewall que funciona como um filtro de pacotes em sistemas Linux).

Sua principal função é proteger a rede de ataques externos.

O **netfilter** começou a ser implementado no kernel Línux a partir da versão 2.4.

O **iptables** trabalha com a seguinte configuração:

#**iptables [-t tabela] [opções] [chain] [dados] -j [ação]**

Tabelas: filter, NAT (SNAT e DNAT) e Mangle.

Se a tabela é NAT pode-se ter os chains POSTROUTING ou PREROUTING.

Se a tabela é Mangle, o objetivo é tratar pacotes com TOS (Type of Service) dado no cabeçalho dos pacotes IPv4.

A tabela default é a tabela **filter** e contém as seguintes “chains=situações de fluxo”:

INPUT – todos os pacotes que chegam no computador, o firewall deixa passar.  
OUTPUT – todos os pacotes saindo do computador, o firewall envia pela rede.  
FORWARD – pacotes são encaminhados para outros computadores da rede.

Na figura abaixo é descrito o funcionamento do filtro do iptable:

Diagrama de funcionamento do iptables:

**Principais opções (comandos) da tabela filter**

-P –> Policy (política). É a política do firewall, que inicialmente está configurada como ACCEPT para INPUT, OUTPUT e FOWARD, ou seja, o firewall aceita qualquer pacote. Para negar o tráfego de qual pacote deve usar a opções DROP.

-A –> Append (anexar). Acrescenta uma nova regra a tabela atual. A opção -A tem prioridade sobre a opção -p, por isso é normal negar todas entradas e saídas de pacotes da rede com DROP, e depois usar o -A para liberar pacotes específicos.

-L –> lista as regras atuais.

-D –> (Delete). Apaga uma regra. Pode usado apos ***tabela número da linha***

-F –> (Flush) – Apaga todas as regras, mas não altera a politica.

**Dados:**

-s –> source . Especifica a origem dos dados. pode ser um endereço IP.

-d –> (Destination) . Especifica o destino do pacote.

-p –> (Protocol) – Especifica o protocolo a ser filtrado.

-i –> In interface (interface de entrada) – Especifica a interface de saída.

-o –> Out-Interface (interface de saída). Especifica a interface de saída. Similar a -i, inclusive nas flexibilidades. O -o não pode ser utilizado com a chain INPUT.

-! –> Exclusão. Utilizado com -s, -d, -p, -i, -o e outros, para excluir o argumento.

–sport –> Source Port. Porta de origem. Só funciona com as opções -p udp e -p tcp.

–dport –> Destination Port. Porta de destino. Só funciona com as opções -p udp e -p tcp.

**Ações**  
As principais **ações** são:

ACCEPT –> Aceitar. Permite a passagem do pacote.

DROP –> Abandonar. Não permite a passagem do pacote, descartando-o. Não avisa a origem sobre o ocorrido.

REJECT –> Igual ao DROP, mas avisa a origem sobre o ocorrido (envia pacote icmp unreachable).

LOG –> Cria um log referente à regra, em /var/log/messages. Usar antes de outras ações.

SNAT – Altera o endereço de origem dos pacotes (ip/porta) das máquinas clientes, antes dos pacotes serem roteados ao seu destino final. (chain POSTROUTING)

DNAT – Altera o endereço de destino das máquinas clientes (ip/porta), antes que os mesmos sejam roteados ao seu destino final. (chain PREROUTING)

REDIRECT – realiza redirecionamento de portas.

TOS – Prioriza a entrada e saída de pacotes, baseada em seu “tipo de serviço”, cuja informação está no cabeçalho do pacote IPv4.