

Composição do comando

```
iptables [-t tabela] [opção] [chain] [dados] -j
[ação]
Sendo
    [-t tabela] -> a tabela a ser criada, filter é a
    default
    [opção] -> Opções como criar ou deletar regras
    [chain] -> Chain a ser usada
    [dados] -> Destinos e origens
    -j [ação] -> Ação a fazer com o pacote
Ex.: iptables -t filter -A FORWARD -d 192.168.1.1 -
j DROP
#Dropa todos os pacotes que devem ser encaminhados
para o 192.168.1.1
```

Tabelas

filter	Tabela default, faz filtragem dos pacotes simples
nat	Efetua as operações com nat
mangle	para alterações avançadas nos pacotes

Na ausencia do parametro de tabela, a tabela filter é selecionada

As tabelas são sempre escritas no comando na forma minuscula

Ex.:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUE-
RADE
regra para abilitar o nat na porta eth0
```

Chains

INPUT	Regras que atuarão na entrada de pacotes no FW Tabelas Filter e Mangle
FORWARD	Regras que atuarão no redirecionamento de pacotes no FW Tabelas Filter e Mangle
OUTPUT	Regras que atuarão na saída de pacotes no FW Tabelas Filter, Mangle e NAT
PREROUTING	Regras que atuarão no pacote antes do processo de roteamento Tabelas NAT e Mangle

Chains (cont)

POSTROUTING	Regras que atuarão no pacote depois do processo de roteamento Tabelas NAT e Mangle
-------------	--

**INPUT e OUTPUT a origem é o próprio FW
FORWARD o pacote passa através do FW
Chains são sempre escrita em MAIÚSCULO**

Comandos Basicos - Visualizar Regras

iptables -L	Lista as regras da tabela FILTER
iptables -t nat -L	Lista as regras da tabela NAT
iptables -L -n	Lista as regras da tabela FILTER sem resolver os nomes e numeros de portas

Ao não definir uma tabela a filter é a **padrão**
Atenção para letras maiúsculas e minúsculas

Comandos Basicos - Criar Regras

-A <i>chain</i>	Cria a regra na CHAIN informada
-I <i>chain</i> <i>num</i>	Cria a regra na <i>chain</i> informada e coloca na posição <i>num</i>
-d <i>IP</i>	IP de destino
-s <i>IP</i>	IP de origem
-p <i>proto- colo</i>	protocolo (TCP, UDP, ICMP)
--sport <i>porta</i>	Porta de origem (necessario usar junto do -p)
--dport <i>porta</i>	Porta de destino (necessario usar junto do -p)
-i <i>int</i>	Interface de entrada de dados(ex.: ETH0)
-o <i>int</i>	Interface de saída de dados(ex.: ETH0)
-j <i>ação</i>	ação a ser tomada (ACCEPT, REJECT, DROP)
-D <i>num</i>	Deleta a regra de numero <i>num</i>
-F	apaga todas as regras

Substituir o que este em *itálico* pela opção informada
ex.: -A *chain* na INPUT ficaria:

iptables -A INPUT



By apavanello

Published 7th July, 2021.

Last updated 7th July, 2021.

Page 1 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>

AÇÕES

ACCEPT	Aceita os pacotes
DROP	Descarta o pacote
REJECT	Rejeita o pacote
MASQUERADE	Usado na tabela NAT para aplicar a mascara NAT
DNAT	efetua o nat reverso, é necessario usar junto do comando --to-destination <i>IP:port</i>



By **apavanello**

Published 7th July, 2021.

Last updated 7th July, 2021.

Page 2 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>