IPTABLES

Iptables

Roteiro

- **Introdução**
- **Tabela Filter**
- **Tabela Nat**
- **Tabela Mangle**
- **Tabela Raw**
- **Perguntas e Dúvidas**

Iptables

Introdução

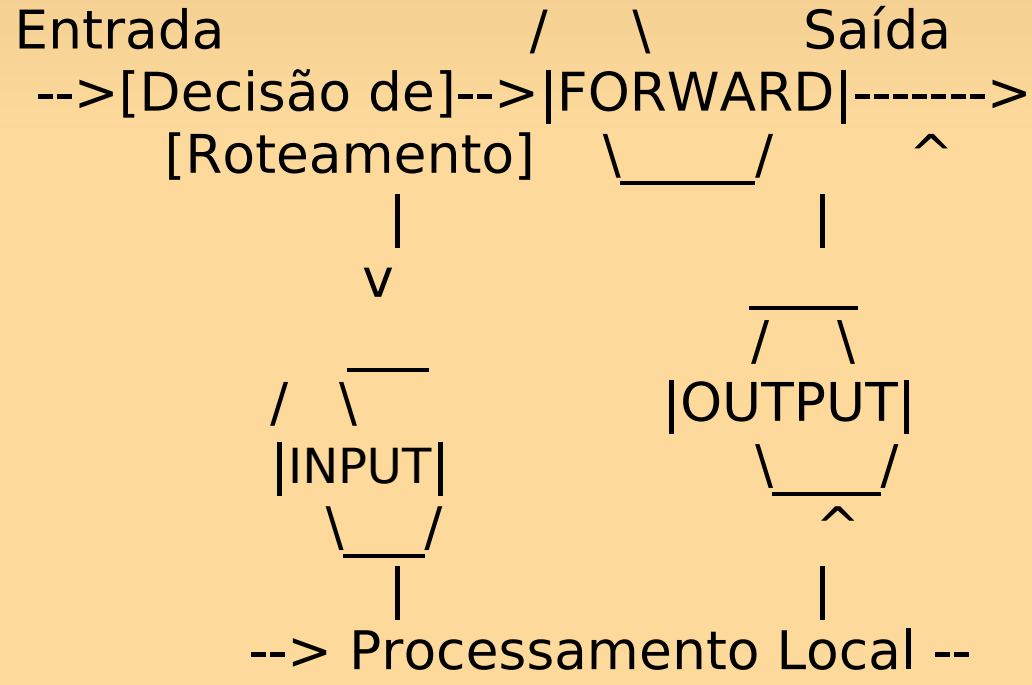
O subsistema de processamento de pacote de rede do kernel do Linux é denominado Netfilter, e **iptables** é o comando utilizado para sua configuração. Netfilter e **iptables** estão estreitamente relacionados e, por tal motivo, usarei "**iptables**" ao fazer referência a um ou ambos do início ao fim da palestra.

A arquitetura **iptables** agrupa regras de processamento de pacotes de rede dentro de de tabelas por função(filtragem de pacotes, tradução de endereços de rede e outros pacotes "mangling"), cada um dos recursos tem "chains"(sequências) de regras de processamento. As regras consistem em "matches", (utilizados para determinar a quais pacotes a regra será aplicada) e alvos(que determinam o que será feito aos pacotes coincidentes).

Iptables

Tabela Filter

O kernel começa com três listas de regras na tabela `filter'; tais listas são denominadas **firewall chains** ou apenas **chains**. As três chains chamam-se **INPUT**, **OUTPUT** e **FORWARD**.



Iptables

Tabela Nat

É a modificação de endereços e/ou portas de pacotes de rede quando eles percorrem o computador. O computador executando uma NAT em pacotes pode ser a origem ou destino desses pacotes, ou pode ser um dos computadores presentes na rota entre a origem e o destino.

Iptables

Tabela Mangle

Esta serve para especificar ações especiais para o tratamento do tráfego que atravessa os chains. Nesta tabela existem cincos chains: ***PREROUTING***, ***POSTROUTING***, ***INPUT***, ***OUTPUT*** e ***FORWARD*** .

Iptables

Tabela Raw

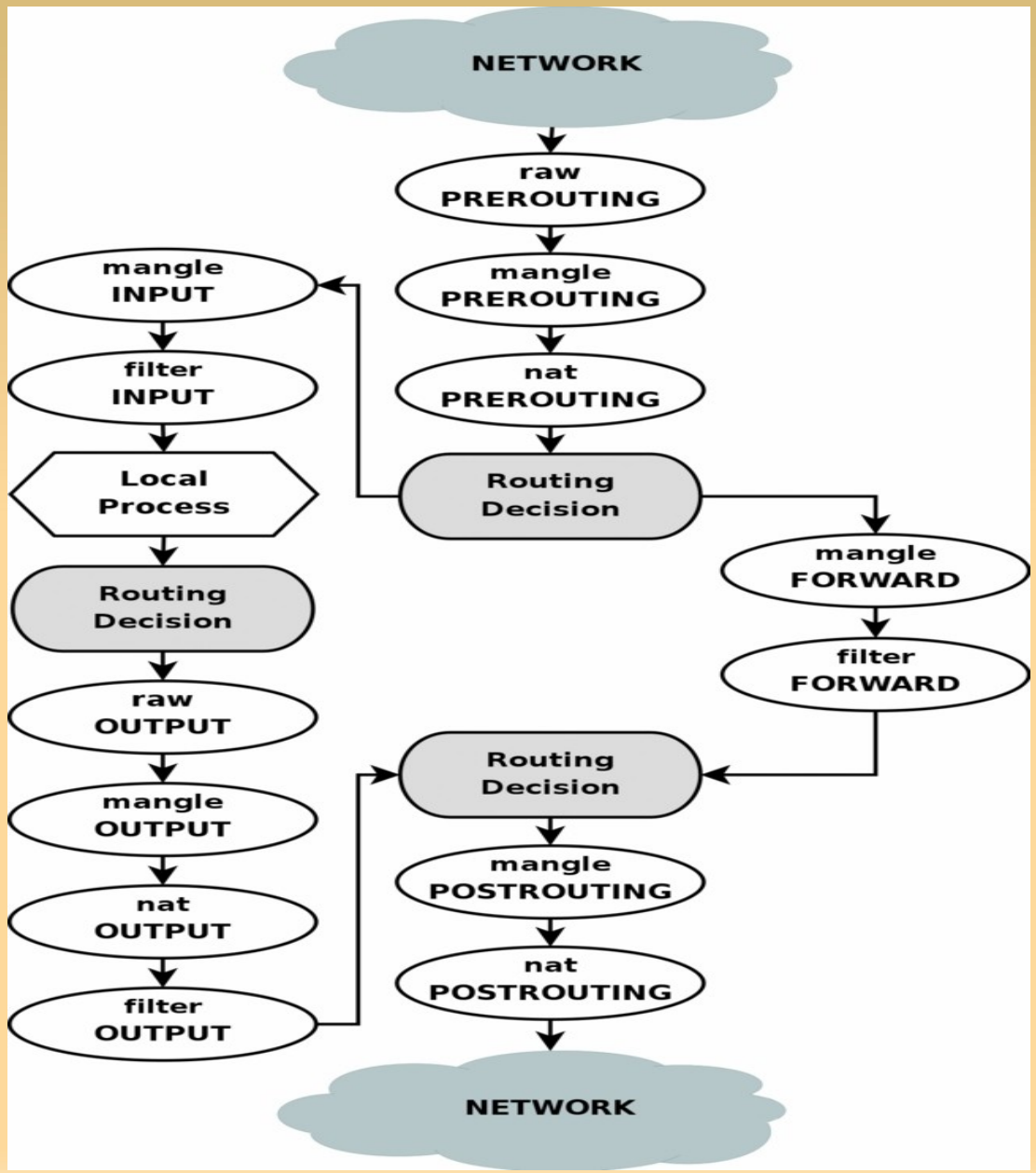
A tabela raw consegue manipular pacotes antes que eles cheguem ao conntrack (mecanismo dentro do netfilter que acompanha as conxões) logo você poderá criar regras dizendo que certas conexões não deverão ser acompanhadas.

O beneficio disto é que recursos da maquina de firewall ficarão livres. Digamos que eu não queira acompanhar pacotes com destino ao meu firewall na porta 80.

A regra seria:

```
[root]# iptables -t raw -A PREROUTING -p tcp --dport 80 -j NOTRACK
```

Iptables


NETWORK
raw
PREROUTING
mangle
PREROUTING
nat
PREROUTING
Routing
Decision
mangle
INPUT
filter
INPUT
Local
Process
Routing
Decision
raw
OUTPUT
mangle
OUTPUT
nat
OUTPUT
filter
OUTPUT
mangle
FORWARD
filter
FORWARD
Routing
Decision
mangle
POSTROUTING
nat
POSTROUTING
NETWORK

Iptables

Perguntas e Dúvidas ??