Instalação e Configuração de Serviços de Internet

Iptables

Ivo Calado
ivo.calado@ifal.edu.br

Instituto Federal de Educação, Ciência e Tecnologia de Alagoas

28 de abril de 2017

Roteiro

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

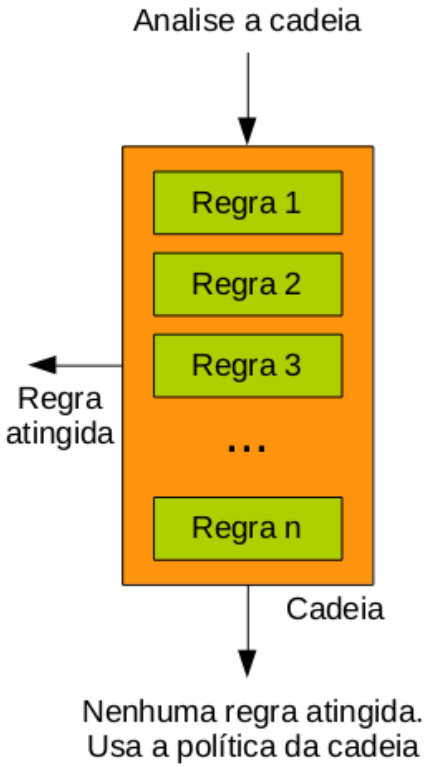
Características I

- A implementação de filtro de pacotes nos kernels 2.4, 2.6, 3.x e 4.x é realizado pelo iptables (projeto netfilter)
- O iptables é o programa capaz de gerenciar a configuração do netfilter
- Principais características:
  - Filtragem sem considerar o estado do pacote
  - Filtragem considerando o estado do pacote
  - Suporte a NAT, tanto para endereços de rede ou portas
  - Flexível, com suporte a plugins

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Conceitos básicos I

- **regras**: são instruções dados para o firewall, indicando o que ele deve fazer
- **cadeias**: locais onde as regras podem ser agrupadas. As regras são processadas em ordem pelo firewall
- Toda cadeia tem uma política padrão, definida pelo usuário
- A cadeia é percorrida até uma regra ser atingida. As seguintes são ignoradas
- Regras com erro são ignoradas
- Se nenhuma regra é atingida, usa-se a regra da política padrão



Conceitos básicos II

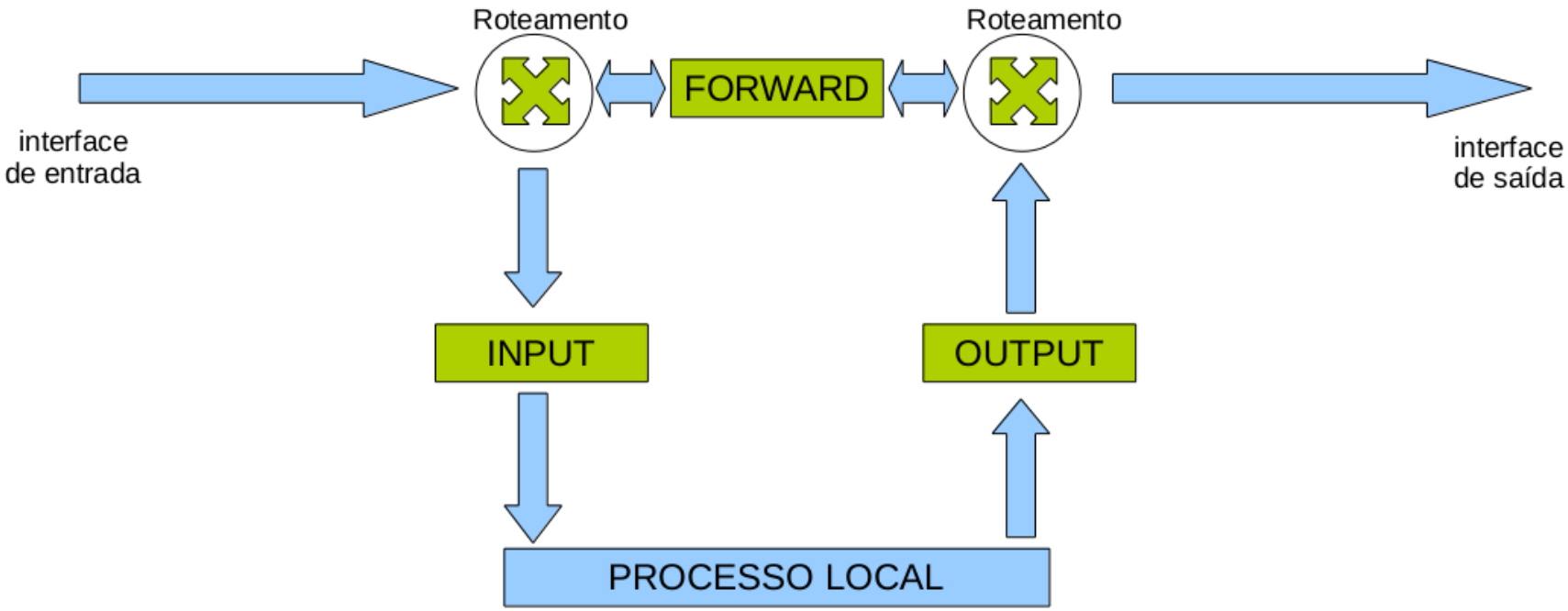
- **tabelas**: o iptables organiza o seu fluxo de pacotes em tabelas, cada uma com um conjunto de cadeias pré-definidas:
  - Tabela **filter**: é a tabela padrão, com três cadeias
    - INPUT
    - OUTPUT
    - FORWARD
  - Tabela **nat**: tabela usada para NAT (gera outras conexões)
    - PREROUTING
    - OUTPUT
    - POSTROUTING
  - Tabela **mangle**: permite alterações nos pacotes (TOS, TTL, etc)
    - PREROUTING
    - INPUT
    - FORWARD

Conceitos básicos III

  - OUTPUT
  - POSTROUTING
- Tabela **raw**: marca pacotes para rastreio posterior

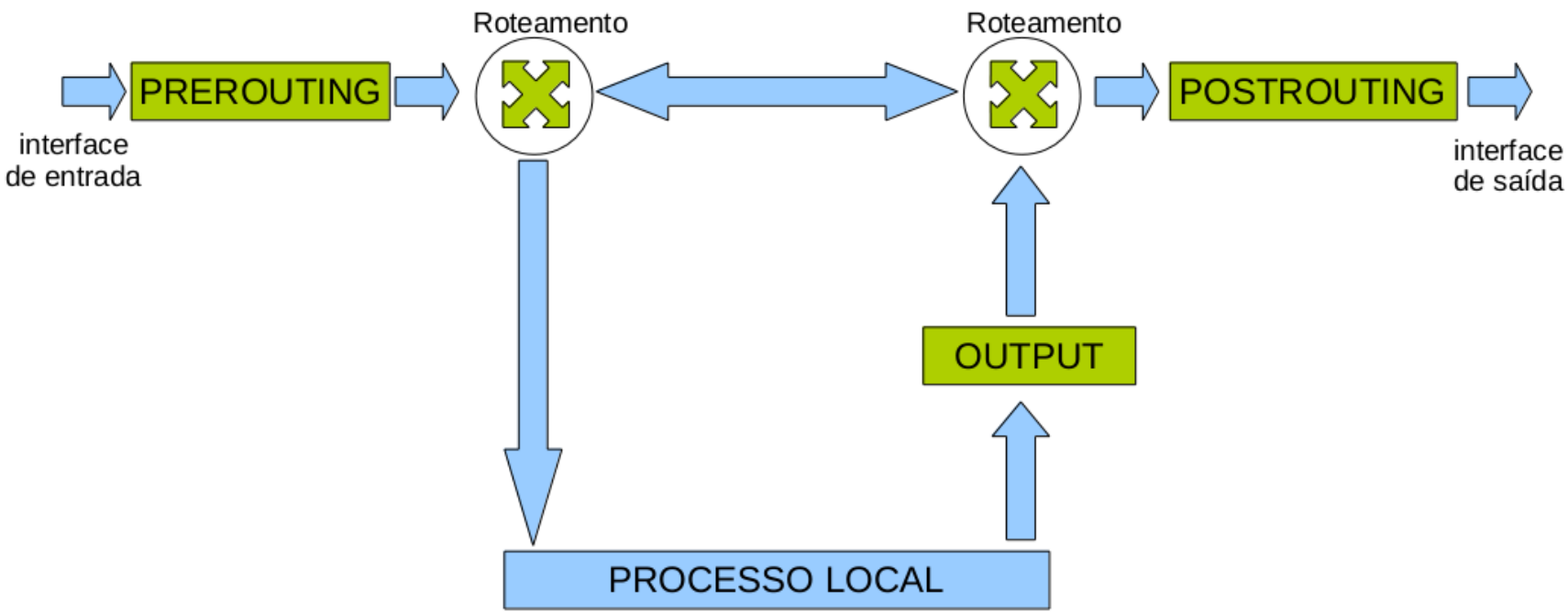
Organização das tabelas do Iptables I

- Tabela **filter** e suas cadeias



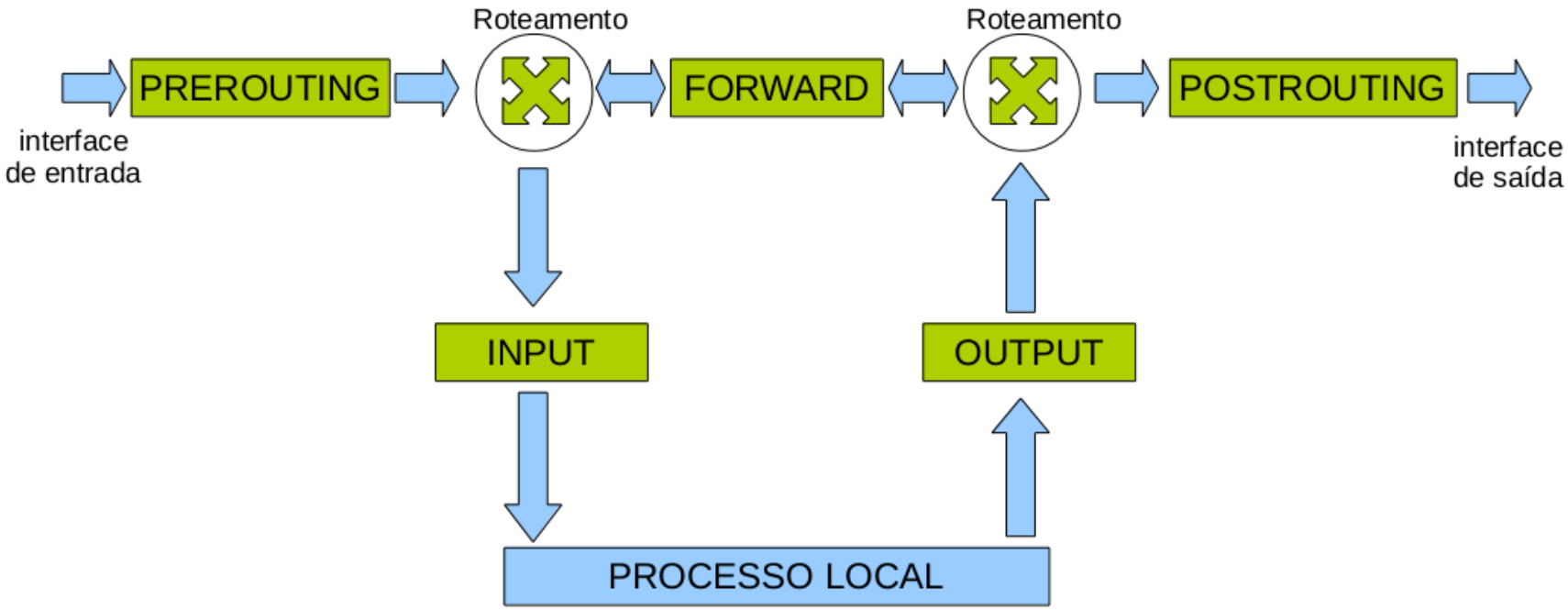
Organização das tabelas do Iptables II

- Tabela **nat** e suas cadeias



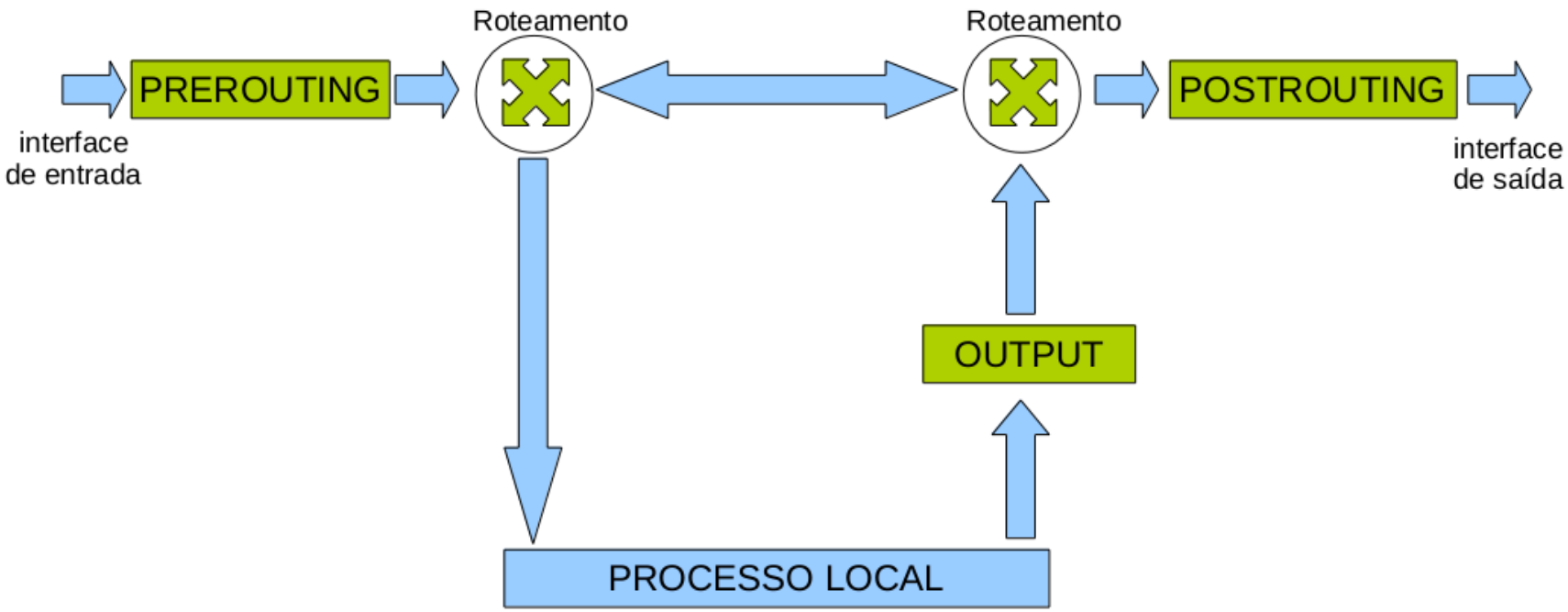
Organização das tabelas do Iptables III

- Tabela **mangle** e suas cadeias



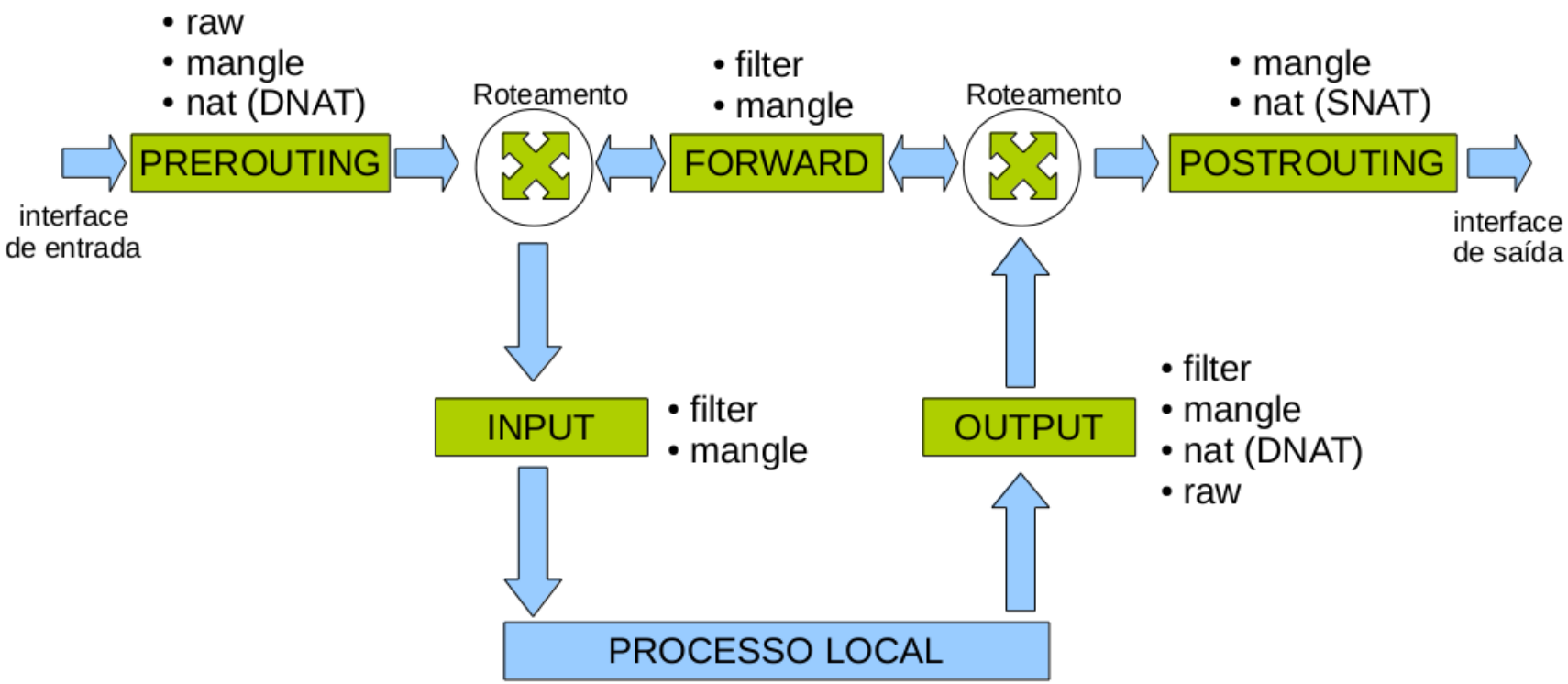
Organização das tabelas do Iptables IV

- Tabelas raw e suas cadeias



Organização das tabelas do Iptables V

- Tabelas filter, nat, mangle e raw e suas cadeias



Salvando e restaurando regras no iptables

- Pode ser feito com um arquivo de script ou usando os comandos *iptables-save* e *iptables-restore*
- *iptables-[save|restore]* executam a operação em um só passo, de maneira mais segura (sem brechas temporárias) e rápida.
- Salvando:

```
sudo iptables-save > arquivo_de_regras
```

- Restaurando:

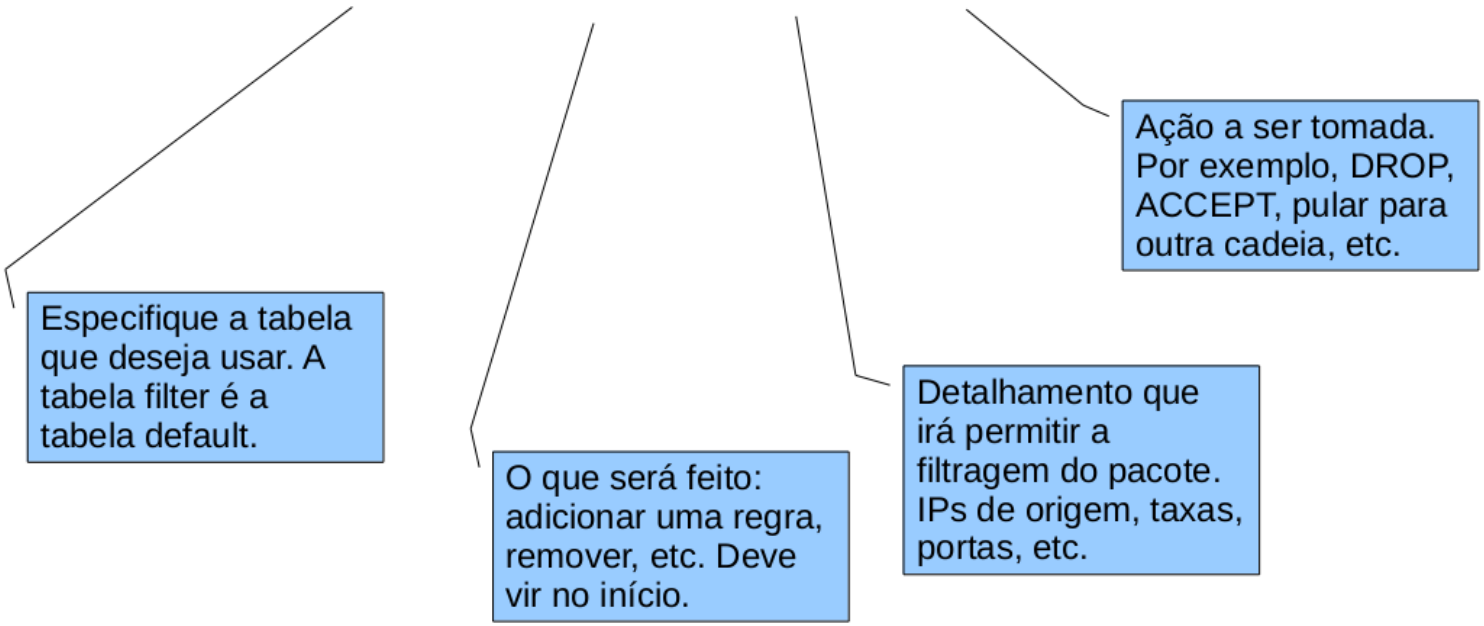
```
sudo iptables-restore < arquivo_de_regras
```

- É possível salvar os contadores com -c

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Formato geral das regras do Iptables I

- *iptables [-t table] comando [filtro] [-j ação]*



Principais comandos de manipulação de cadeias I

- Sempre maiúsculo seguido do nome da cadeia:
  - -**P**: configura a política padrão da cadeia (**DROP** ou **ACCEPT**)

```
iptables -P OUTPUT ACCEPT
```

  - -**N**: cria uma nova cadeia

```
iptables -N internet
```

  - -**F**: apaga as regras da cadeia

```
iptables -F INPUT
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Principais comandos de manipulação de cadeias II

- -**X**: apaga uma cadeia vazia

```
iptables -F internet; iptables -X internet
```

- -**Z**: zera todos os contadores da cadeia

```
iptables -Z INPUT
```

- -**A**: adicionar uma regra no final da cadeia

```
iptables -A INPUT - -dport 80 -j DROP
```

- -**L**: listar regras da cadeia (adicione -**n** para não resolver nomes e - -**line-numbers** para ver o número das regras)

```
iptables -L -n - - line-number
```

Principais comandos de manipulação de cadeias III

- -**D**: apagar uma regra da cadeia. Pode usar também a linha

```
iptables -D INPUT - -dport 80 -j DROP
iptables -D INPUT 5
```

- -**R**: trocar uma regra por outra

```
iptables -R INPUT 2 -s 10.0.1.2 -j DROP
```

- -**I**: insere uma regra em um ponto específico da cadeia

```
iptables -I INPUT 1 - -dport 80 -j DROP
```

Principais filtros no iptables I

- **-p** <protocolo>: especifica o protocolo. Por exemplo, udp, tcp ou icmp. Pode ser negado também. Para tudo menos tcp, faça: com "! -p tcp"

```
iptables -A INPUT -p icmp -j DROP
iptables -A INPUT ! -p tcp -j DROP
```

- **-s** <endereço>: especifica o endereço de origem. Aceita IPs, redes, IP/máscara, IP/nn (notação CIDR) e também a negação com "!"

```
iptables -A INPUT -s 10.1.1.1 -j ACCEPT
iptables -A INPUT ! -s 10.1.1.0/24 -j DROP
```

Principais filtros no iptables II

- **-d** <endereço>: especifica o endereço de destino (mesmas regras do **-s**)

```
iptables -A OUTPUT -d uol.com.br -j ACCEPT
```

- **-i** <interface>: especifica a interface de entrada do pacote. Use "!" para negar e "+" como curinga. "-i eth+" significa todas as interfaces eth. Válida em INPUT, PREROUTING e FORWARD

```
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i ppp+ -j DROP
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Principais filtros no iptables III

- **-o** <interfaces>: especifica a interface de saída. Válida em OUTPUT, POSTROUTING e FORWARD. Usa as mesmas regras de -i

```
iptables -A OUTPUT -o ppp+ -j ACCEPT
```

- - **-sport** <porta>: especifica a porta de origem. Pode ser dado em forma de faixa também, como em "- -sport 80:123" ou mesmo "- -sport 1023:" (todas acima de 1023). Precisa ter tcp ou udp especificado como protocolo

```
iptables -A INPUT -p udp - -dport 53 -j ACCEPT
iptables -A INPUT -p tcp - -sport 1:1023 -j REJECT
iptables -A INPUT -p tcp - -sport 1024: -j ACCEPT
```

Principais filtros no iptables IV

- - -dport <porta>: especifica a porta de destino. Mesmas regras do - -sport.

```
iptables -A OUTPUT -p tcp - -dport 23 -j DROP
```

- - -icmp-type <tipo>: filtra por tipo de pacotes ICMP. Por exemplo, 8 é o ping, mas "echo-request" poderia ser usado

```
iptables -A INPUT -p icmp - -icmp-type echo-request -j ACCEPT
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Principais ações no iptables I

```
iptables -A INPUT -p tcp - -dport 22 -j ACCEPT
```

- DROP: descarta o pacote

```
iptables -A INPUT -p tcp - -dport 23 -j DROP
```

- REJECT: rejeita o pacote, informando ao host de origem. Válida em INPUT, OUTPUT e FORWARD

```
iptables -A INPUT -p tcp –dport 23 -j REJECT
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

Principais ações no iptables II

- LOG: coloca no log informações sobre o pacote. Uma opção interessante é o –log-prefix “mensagem”, que permite a adição de um prefixo. O log não interrompe o processamento, fique atento.

```
iptables -A INPUT -p tcp - -dport 23 -j LOG - -log-prefix
“Tentativa de telnet”
iptables -A INPUT -p tcp - -dport 23 -j DROP
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

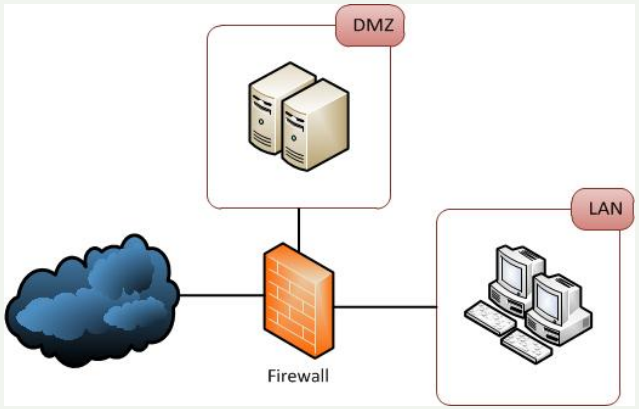
SNAT x DNAT I

- SNAT tem como origem uma máquina da rede local destinada a um *host* da rede externa
  - Trata-se da forma mais comum de NAT
  - Modifica-se o IP de origem do pacote para o IP externo da máquina do servidor
- DNAT tem como origem uma máquina da rede externa e destinada a um *host* da rede local
  - Serve como uma forma de possibilitar o acesso a servidores locais. Basicamente, configura-se o fluxo com dadas características para uma máquina específica (ex.: redireciona todos os fluxos tcp destinados a porta 80 para o servidor Web)

SNAT x DNAT II

DMZ: zona desmilitarizada (demilitarized zone)

- Também conhecida como rede de perímetro
- Trata-se de uma estratégia para isolar as máquinas internas dos eventuais servidores acessíveis externamente
- O objetivo é isolar as máquinas internas de eventuais comprometimentos da DMZ



SNAT I

- SNAT: realiza o NAT, alterando o endereço de origem do pacote. Válido em POSTROUTING, da tabela nat
- Source NAT é especificado com '-j SNAT', e a opção '–to-source' demonstra um endereço IP, um range de endereços IP, e uma porta opcional ou um range de portas (apenas para os protocolos TCP e UDP).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

SNAT II

```
## Mudando o endereço de origem para 1.2.3.4.
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --
    to 1.2.3.4

## Mudando o endereço de origem para 1.2.3.4,
    1.2.3.5 ou 1.2.3.6
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --
    to 1.2.3.4-1.2.3.6

## Mudando o endereço de origem para 1.2.3.4,
    portas 1-1023
# iptables -t nat -A POSTROUTING -p tcp -o eth0 -j
    SNAT --to 1.2.3.4:1-1023
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

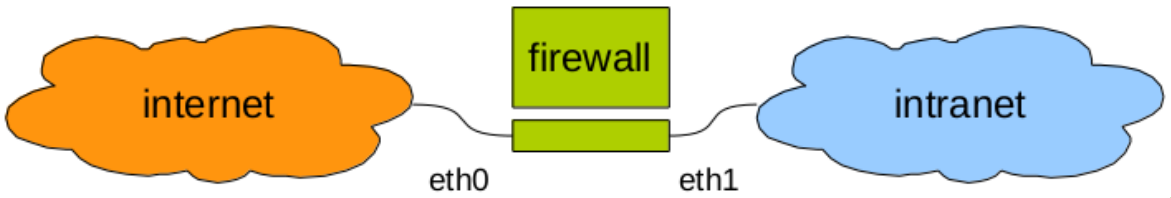
SNAT III

- Não esqueça de habilitar o forwarding, colocando 1 em */proc/sys/net/ipv4/ip_forward*, usando uma das formas abaixo:

```
$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Masquerade I

- Representa um caso especial de SNAT, denominado Masquerade, a ser utilizado como a interface de saída possuí endereço dinâmico
- MASQUERADE: realiza o NAT, alterando o endereço de origem. Similar ao SNAT, mas sem opções de endereço de saída. Válido em POSTROUTING somente, tabela nat. Muito usado para implementar as regras de NAT do firewall



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

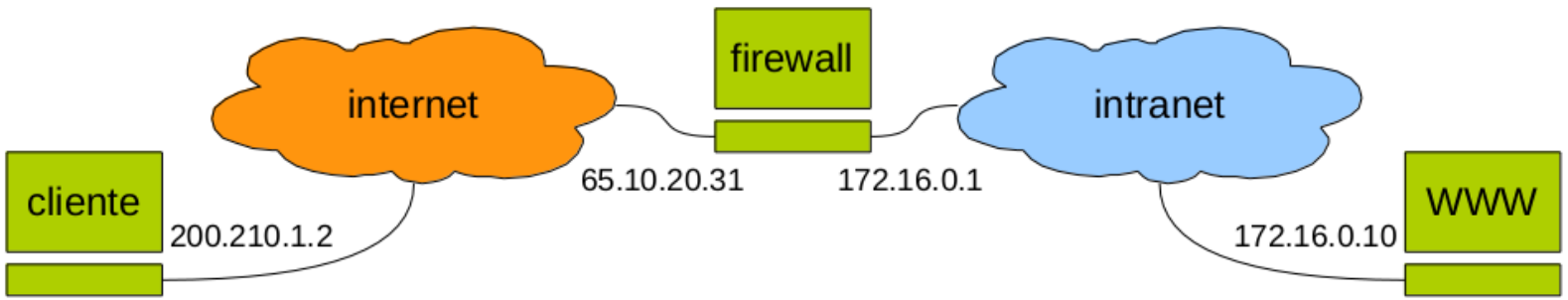
Masquerade II

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -o ppp+ -j MASQUERADE
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA ALAGOAS

DNAT I

- DNAT: realiza o NAT, alterando o endereço de destino do pacote. Pode usar a opção –to-destination ¡IPa-IPb¿ para especificar uma faixa de IPs (load balancing). Válido somente em PREROUTE e OUTPUT, tabela nat
- Caso de uso típico para criação de virtual servers, onde é preciso regras para quem vem de fora, para máquina na intranet e para o próprio firewall



DNAT II

```
iptables -t nat -A PREROUTING -p tcp -d 65.10.20.31 - -dport 80
-j DNAT - -to-destination 172.16.0.10
iptables -t nat -A POSTROUTING -p tcp -d 172.16.0.10 - -dport
80 -j SNAT - -to-source 172.16.0.1
iptables -t nat -A OUTPUT -p tcp -d 65.10.20.31 - -dport 80 -j
DNAT - -to-destination 172.16.0.10
```

Redirecionamento de cadeias

- Caso você tenha criado uma cadeia, pode usar o -j para redirecionar a filtragem para ela
- Ao terminar, caso nenhuma regra tenha sido acionada, o fluxo volta para quem redirecionou e o processamento continua. Caso contrário, é interrompido

```
iptables -N internet
iptables -A INPUT -p tcp - -dport 80 -j internet
```