

# Introdução a IPTables

Rafael Gomes

# Índice

- Requisitos básicos
- NetFilter e IPTables
- Introdução
- Tabelas
- Fluxo de pacotes e as Tabelas
- Estrutura
- Alguns exemplos
- Aplicações de IPTables
- Bibliografia

# Requisitos básicos

- Um PC com requisitos mínimos para correr uma versão de Linux actual (kernel 2.4 ou mais actual)
- Pelo menos 2 interfaces de rede

# NetFilter e IPTables

- O kernel do Linux têm um subsistema de processamento de pacotes de rede que se chama NetFilter ([www.netfilter.org](http://www.netfilter.org))
- Como se configura o NetFilter? Com o comando iptables
- IPTables (e Netfilter) funcionam (normalmente) na camada 3 do modelo OSI (Rede).
- Existem funcionalidades semelhantes para a camada 2 de OSI (Link) e chama-se ebtables ([ebtables.sourceforge.net](http://ebtables.sourceforge.net))

# Introdução

- Os pacotes recebidos podem ter 5 “estados” possíveis:

- PreRouting – Pacotes acabados de chegar à interface de rede.

- Forward – Pacotes reencaminhados entre interfaces de rede

- PostRouting – Pacotes a serem lançados na rede de seguida

- Input – Pacotes destinados ao sistema local

- Output – Pacotes originados no sistema local

# Introdução

- Estes “estados” são parte dos comandos iptables também conhecidos como regras ou “chains”
- As “chains” são em tudo semelhantes às ACL’s dadas nas aulas.
- Os pacotes vão ser comparados com cada “chain” em busca de uma que o satisfaça.

OBS: A versão anterior do IPTables chamava-se IPChains

# Tabelas e “Hook Points”

- As “chains” vão ser agrupadas em 3 tabelas: NAT, FILTER, MANGLE
- A tabela de NAT refere-se a pacotes que vão sofrer tradução de endereço de rede
- A tabela de Filter define que pacotes passam e que pacotes são descartados, têm funcionalidades muito semelhantes a uma firewall e é a tabela usada por default se nada for dito no comando iptable
- A tabela de MANGLE é a tabela que define como os pacotes serão modificados (header)

# Tabelas e “Hook Points”

- Cada tabela têm associado alguns “hook points” por defeito:

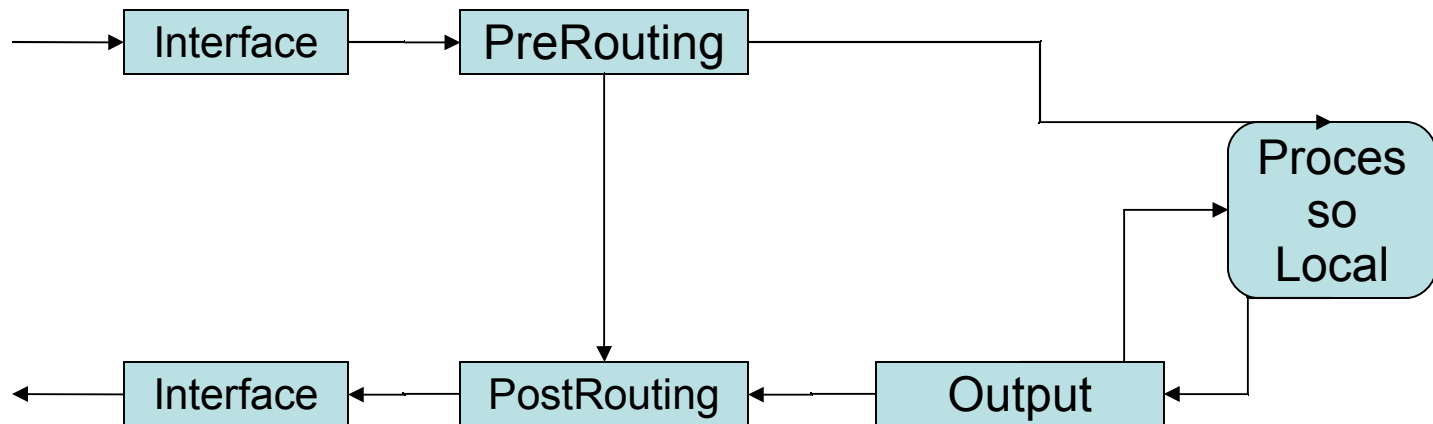
- NAT : PreRouting / Output / PostRouting

- FILTER : Forward / Input / Output

- MANGLE : PreRouting / Forward / PostRouting / Input / Output

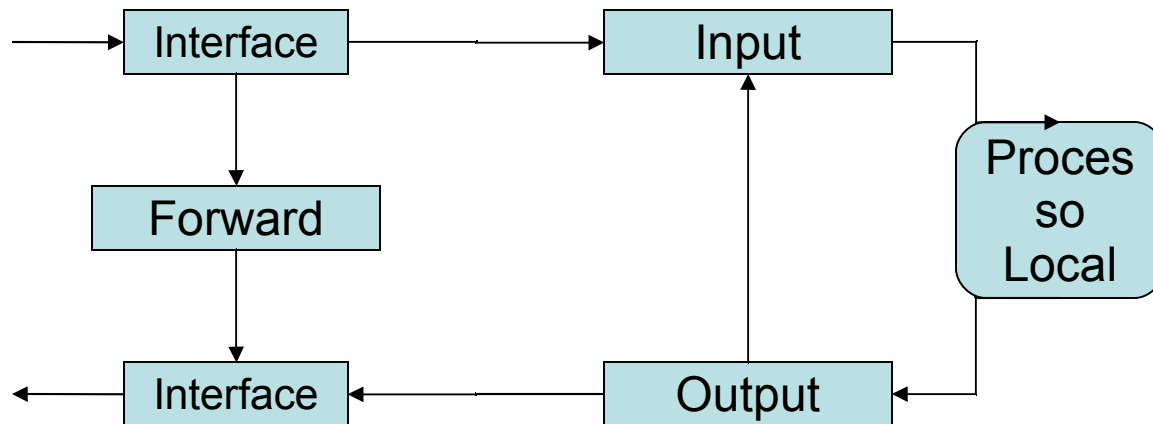
# Fluxo de pacotes e as Tabelas

- NAT:



# Fluxo de pacotes e as Tabelas

- FILTER:



# Estrutura

• iptables -t <tabela> -<opção de entrada> <chain>  
<regra> -j <ação>

## Opção de entrada para Inserção de nova regra

Opção	Descrição
-I <chain> <numero>	Insera a regra em um determinado número (padrão 1)
-A <chain>	Faz apenas um “append” após a ultima regra registrada

## Opção de entrada para modificação de regra

Opção	Descrição
-R <chain> <numero>	Faz um “replace” com a regra em um determinado número (padrão 1)
-D <chain> <numero>	Remove a linha do numero informado

# Estrutura

## Outras opções de entrada

Opção	Descrição
-L <chain> <numero>	Lista todas as regras ou apenas da chain e/ou linha informada
-F <chain>	Apaga todas as regras da chain informada, senão for informada uma chain, será apagada de todas da tabela.

# Estrutura

## Regras

Regra	Descrição
-s ou --source	Especifica a origem
-d ou --destination	Especifica o destino
-p ou --proto	Especifica o protocolo
-i ou --in-interface	Interface de entrada
-o ou --out-interface	Interface de saída

## Sub-regras do -proto [tcp|udp|icmp|...]

Regra	Descrição
--dport	Porta de destino
--sport	Porta de origem

# Matches

Matches são extensões que adicionam novas opções para as nossas regras de filtragem

Opção -m ou --match

Exemplos	Descrição
mac	Verifica o endereço mac
state	Verifica o estado do pacote
multiport	Verifica várias portas

-m mac

Exemplos	Descrição
--mac-source	Endereço mac da origem

-m multiport

Exemplos	Descrição
--source-ports	Portas de origem
--destination-ports	Portas de destino
--ports	Portas tanto de origem quanto de destino

# Matches

-m state

Exemplos	Descrição
INVALID	Pacote associados a conexão não conhecida
NEW	Pacotes associados a inicio de conexão
ESTABLISHED	Pacotes em trânsito em conexões estabelecidas.
RELATED	Pacotes que estão iniciando uma nova conexão, porém está relacionado a uma conexão já existente, como a conexão de dados do FTP ou então um erro ICMP

# Ações

-j <ações>

## **Filter**

- REJECT – Rejeita com envio de erros
- DROP – Rejeita apenas ignorando
- ACCEPT – Aceita a regra

## **Nat - POSTROUTING**

- SNAT --to-source – Traduz para origem informada
- MASQUERADE – Mascara o ip inválido para ips válidos do firewall

## **Nat - PREROUTING**

- DNAT --to-destination – Traduz para destino informado
- REDIRECT --to-ports – Redireciona trafego para porta informada

# Alguns exemplos

• Quando um pacote chega a uma interface com destino o sistema local são analisadas as chains associadas primeiro a PreRouting (tabela NAT) e de seguida Input (tabela de Filter ).

## • Alguns exemplos de match possíveis para pacotes icmp e udp:

```
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
```

```
iptables -A INPUT -p udp --sport 53 -j DROP
```

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

## • Proxy transparente

```
iptables -t nat -A PREROUTING -i <interface> -p tcp --dport 80 -j REDIRECT --to-ports 3128
```

## • Compartilhar internet ADSL

```
iptables -t nat -A POSTROUTING -o <interface> -s <sua rede> -j MASQUERADE
```

## • Compartilhar internet Ip fixo

```
iptables -t nat -A POSTROUTING -o <interface> -s <sua rede> -j SNAT --to-source <ip válido>
```

## • “Liberar” VNC pra internet

```
iptables -t nat -A PREROUTING -i <interface> -p tcp --dport 5900 -j DNAT --to-destination <ip da máquina>
```

# Aplicações de IPTables

- Filtragem de pacotes
- Monitorização de rede (Accounting)
- Controlo de conexões (Connection tracking)
- Manipulação de pacotes (Mangling)
- NAT (SNAT & DNAT)
- Masquerading ( Tipo de SNAT)
- Reencaminhamento de pacotes (Port forwarding)
- Balanciamento de carga

# Bibliografia

• **“Linux iptables – Pocket reference” por Gregor N. Purdy - O’Reilly**

• <http://iptables-tutorial.frozentux.net/iptables-tutorial.html>

• [http://upload.wikimedia.org/wikipedia/en/7/72/Iptables\\_packet\\_traversal.pdf](http://upload.wikimedia.org/wikipedia/en/7/72/Iptables_packet_traversal.pdf)

• <http://www.netfilter.org/>

• [http://en.wikipedia.org/wiki/Stateful\\_firewall](http://en.wikipedia.org/wiki/Stateful_firewall)

• [http://www.linuxhomenetworking.com/wiki/index.php/Quick\\_HOWTO::\\_Ch14::\\_Lin](http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO::_Ch14::_Lin)

• <http://www.tenablesecurity.com/>

• [http://segderedes.googlepages.com/artigo\\_iptables.html](http://segderedes.googlepages.com/artigo_iptables.html)

**Helder Ferreira – Autor Original dessa apresentação -**

[http://www.dei.isep.ipp.pt/~i020113/Introducao\\_iptables.pps](http://www.dei.isep.ipp.pt/~i020113/Introducao_iptables.pps)