INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança de Redes

Iptables

Filipe Raulino
filipe.raulino@ifrn.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Comandos básicos

- Inserir uma regra no início de uma chain
  - iptables [-t <tabela>] -I <chain> <regra> -j <acao>
- Inserir uma regra no final de uma chain
  - iptables [-t <tabela>] -A <chain> <regra> -j <acao>
- Remover uma regra de uma chain
  - iptables [-t <tabela>] -D <chain> <regra> -j <acao>

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Comandos básicos

- Alterar a política de uma chain
  - iptables -P <chain> <politica>
- Listar as regras de uma chain
  - iptables [-t <tabela>] -L [-n] <chain>
- Remover todas as regras de uma chain
  - iptables -F <chain>

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Regras do Iptables

- Regras
  - Implementam, na prática, as ACL´s

    iptables [-t <tabela>] -I <chain> <regra> -j <acao>
  - Opções
    - **-j** Especifica uma ação (--jump)
      -i Specify the input interface (--in-interface)
      -o Specify the output interface (--out-interface)
      -p Specify the protocol (--proto)
      -s Specify the source (--source)
      -d Specify the destination (--destination)
      ! Specifies an inversion (match addresses NOT equal to)

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

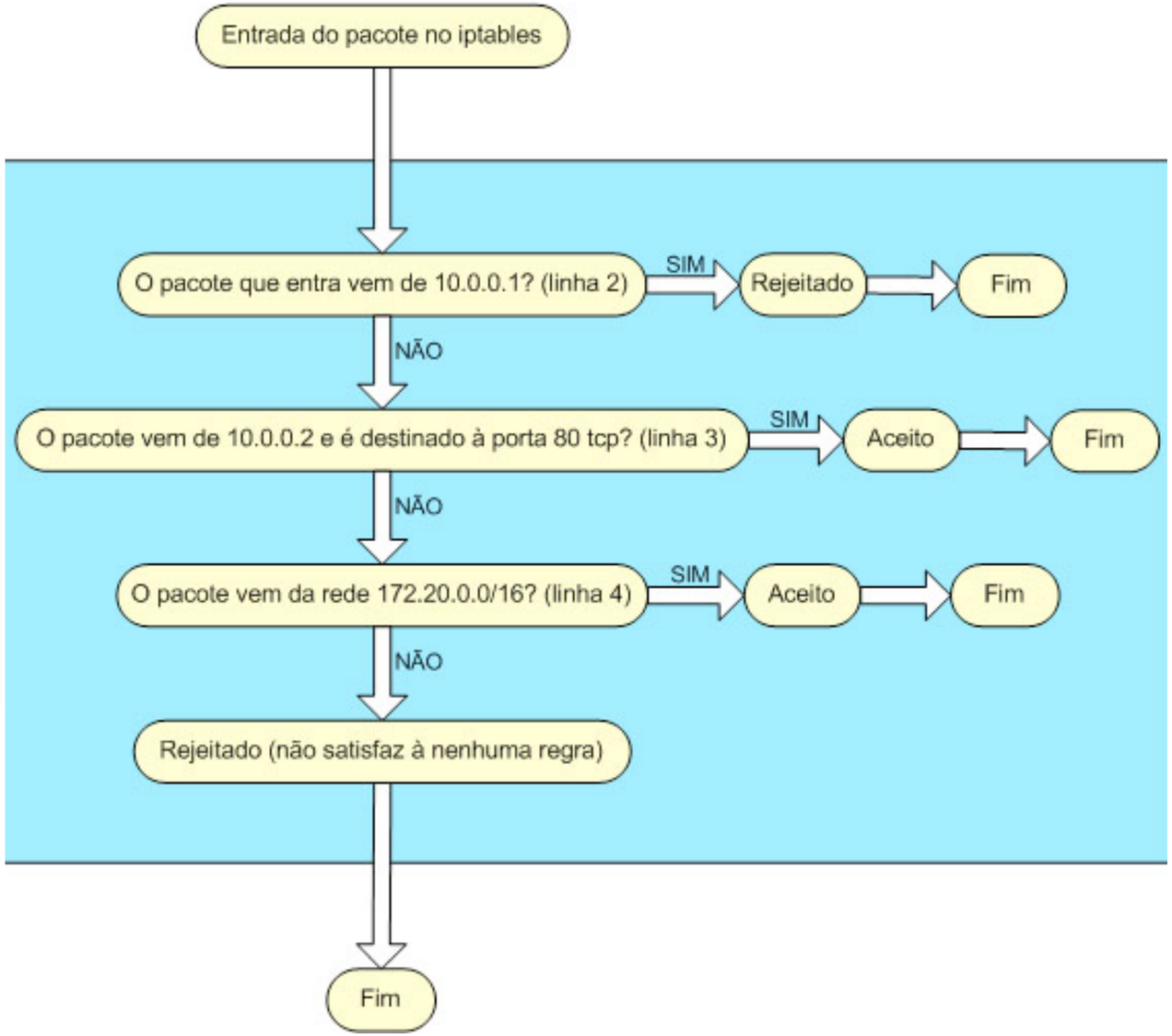
Exemplos

```
iptables -P INPUT DROP

iptables -A INPUT -s 10.0.0.1 -j DROP

iptables -A INPUT -s 10.0.0.2 -p tcp
--dport 80 -j ACCEPT

iptables -A INPUT -s 172.20.0.0/16 -j
ACCEPT
```



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Exemplos

- Bloquear porta tcp
  - iptables -I INPUT -p tcp --dport 22 -j DROP
- Bloquear porta para um destino específico
  - iptables -I INPUT -p tcp -s 10.0.0.0/8 --dport 22 -j DROP
- Bloquear porta e logar tentativas de conexão
  - iptables -I INPUT -p tcp --dport 22 -j LOG
  - iptables -A INPUT -p tcp --dport 22 -j DROP

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Exemplos

- Especificando mais de uma porta ao mesmo tempo
  - iptables -I INPUT -p tcp -m multiport --dports 22,80 -j DROP
  - iptables -I INPUT -p tcp -m multiport --dports 1:2024 -j DROP
- Especificando interfaces de rede
  - iptables -I INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
  - iptables -I INPUT -i wlan0 -p tcp --dport 80 -j DROP

Exemplos

- Bloqueando o tráfego de saída para um local específico
  - iptables -I OUTPUT -o wlan0 -p tcp --dport 80 -j DROP
  - iptables -I OUTPUT -o wlan0 -p tcp -d 10.1.2.3 --dport 80 -j DROP
  - iptables -I OUTPUT -o wlan0 -p tcp -d 10.1.2.3 -m multiport \ --dports 22,80 -j DROP

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtragem Stateful

- Stateful filtering (TCP)
  - Estados reconhecidos pelo iptables
    - NEW
    - ESTABLISHED
    - RELATED

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Exemplos

- Firewall statefull
  - iptables -I INPUT -mstate --state ESTABLISHED,RELATED -j ACCEPT
  - iptables -I OUTPUT -mstate --state ESTABLISHED,RELATED -j ACCEPT
  - iptables -I FORWARD -mstate --state ESTABLISHED,RELATED -j ACCEPT

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Exemplo - NAT

- Regra de NAT N:1 (Mascaramento)
  - iptables -t nat -I POSTROUTING -o eth0 -s 10.1.2.0/24 -j MASQUERADE
- Regra de NAT 1:1
  - iptables -t nat -A POSTROUTING -s 10.1.2.4 -j SNAT --to 200.1.2.4
  - iptables -t nat -A PREROUTING -d 200.1.2.4 -j DNAT --to 10.1.2.4
- Redirecionamento
  - iptables -t nat -A PREROUTING -s 10.0.0.0/8 -p tcp --dport 80 -j REDIRECT --to-port 3128

Ativar redirecionamento de Pacotes:

```
echo "1" >/proc/sys/net/ipv4/ip_forward
```