



Linux para Infraestrutura

Prof. André Nasserála
nasserála@gmail.com

Classificação dos Firewalls

- Na computação, um Stateful firewall é um firewall de rede que rastreia o estado operacional e as características das conexões de rede que o atravessam.
- O firewall está configurado para distinguir pacotes legítimos para diferentes tipos de conexões.



Classificação dos Firewalls

- O iptables é um firewall com estado, ou seja, um firewall stateful.
- Os anteriores eram stateless (ipchains e ipfwadm).
-
- O modo de filtragem 'Stateless' tende a tratar cada pacote roteado pelo firewall como pacotes individuais, sendo mais simples de implementar e por terem uma resolução mais rápida que um do tipo stateful, podem ser usados para obterem um desempenho melhor em determinadas situações onde existem regras de nível de rede bem simples.

Classificação dos Firewalls

- Stateful filtering (TCP):
- Estados reconhecidos pelo iptables:
- NEW
 - Novo
- ESTABLISHED
 - Estabelecida
- RELATED
 - Relatada

Classificação dos Firewalls

- Stateful filtering (TCP):
- Exemplo de Regra:
- 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

- Excluindo uma regra:
- iptables -D FORWARD -mstate --state ESTABLISHED,RELATED -j ACCEPT

Funcionamento das Tabelas

- Uma tabela contém cadeias, e as cadeias contém regras, como podemos ver na figura a seguir:

Tabela 1

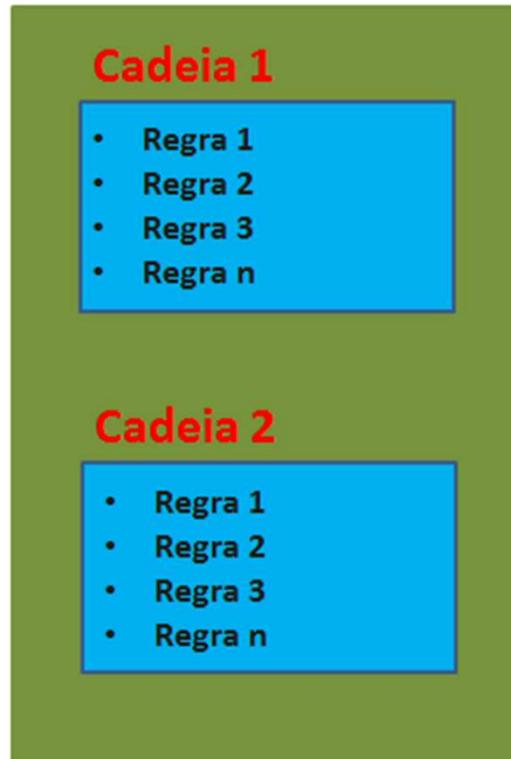
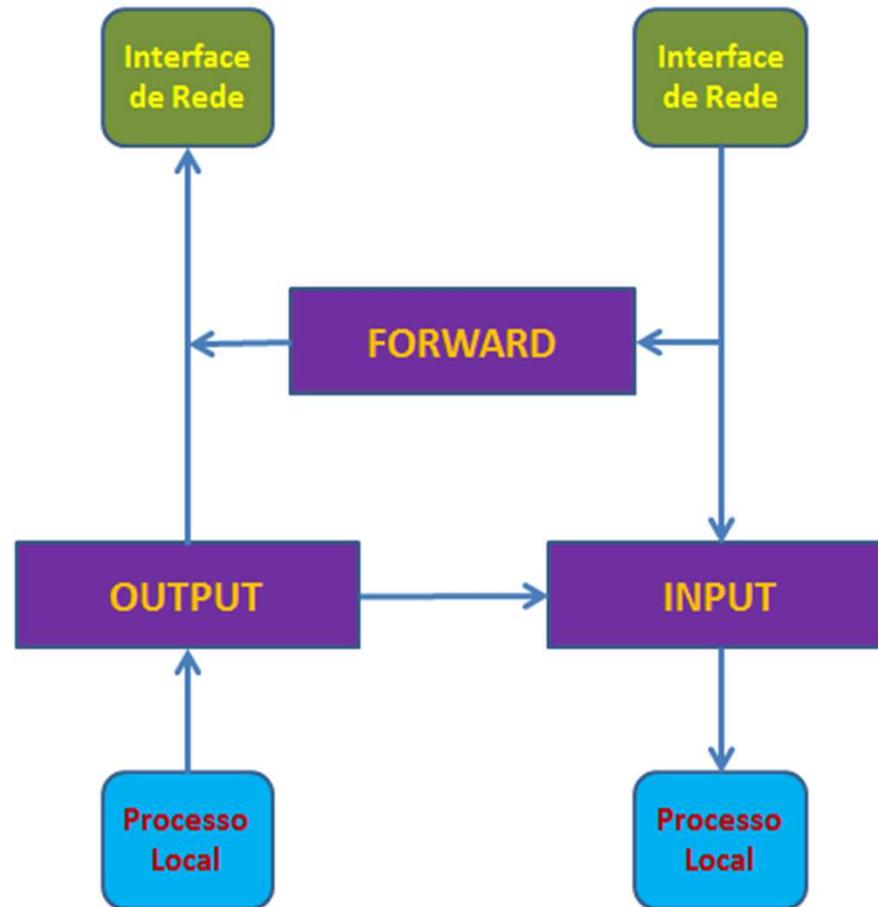


Tabela 2



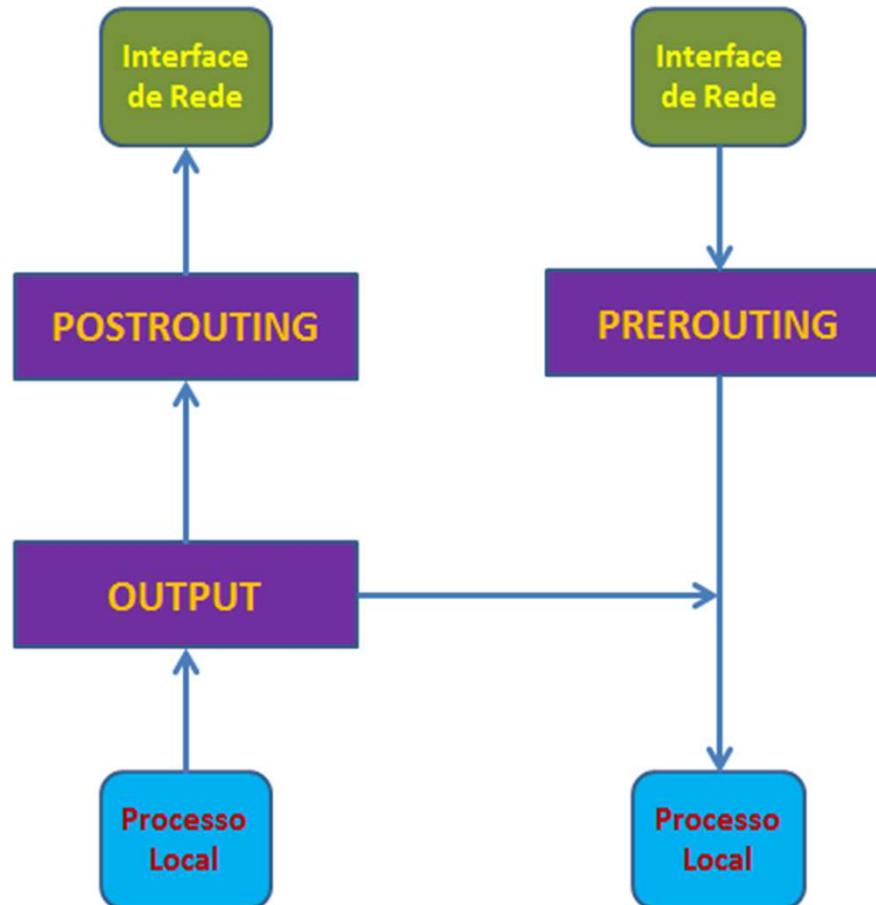
Funcionamento das Tabelas

- Filter:



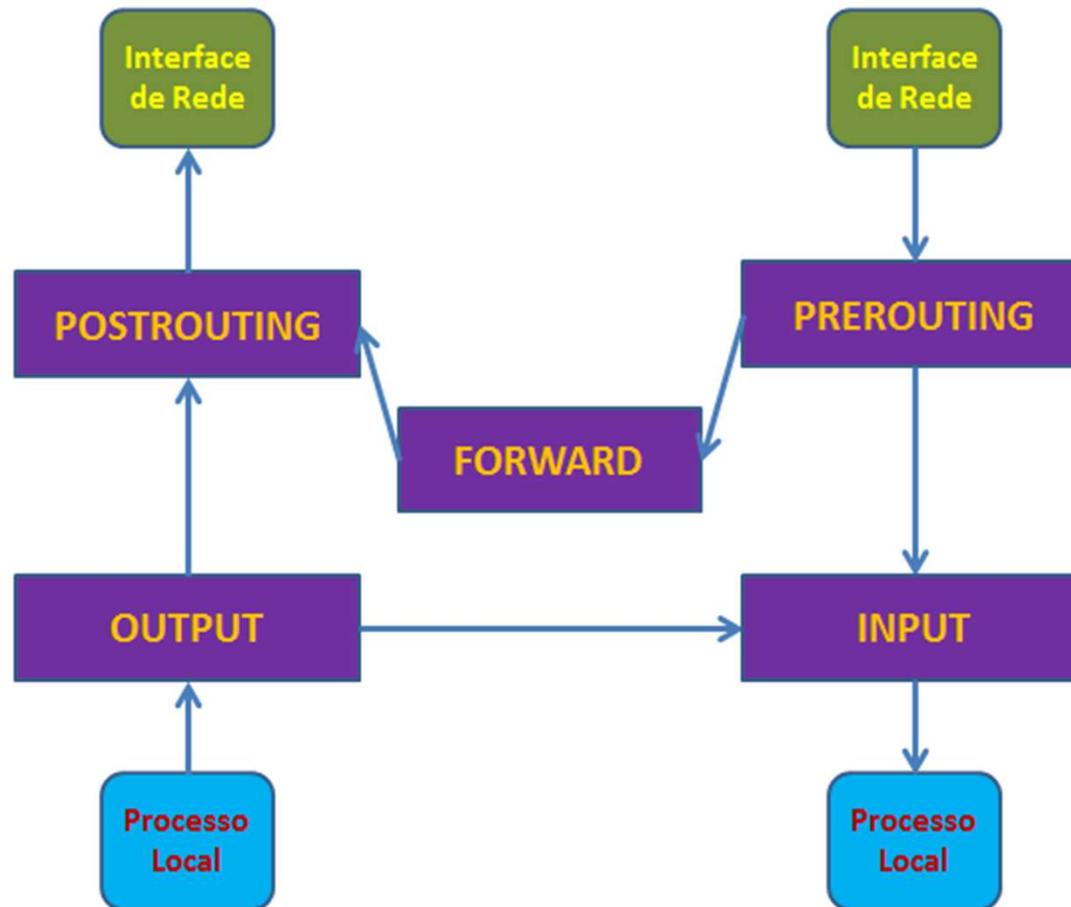
Funcionamento das Tabelas

- Nat:



Funcionamento das Tabelas

- Mangle:



Exemplos de Regras

- 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

Iniciando Junto com a Máquina

- `yum install rsyslog -y` (Syslog)
- Dando as Permissões:
 - `# chmod u+x /etc/rc.d/rc.local`
 - `# systemctl start rc-local`
- Ativando o Serviço
 - `# systemctl enable rc-local`
 - `# vi /etc/rc.local`

ATIVIDADE

- Implementar um firewall para:
 - Proteger o próprio Firewall;
 - Proteger máquinas da uma rede interna (192.168.10.0/24); e
 - Possibilitar o acesso das máquinas da rede a rede externa via NAT.
-
- Regras mínimas:
 - Política padrão DROP para as chains INPUT, FORWARD e OUTPUT;
 - O firewall deve ser stateful;
 - A rede interna deve ter acesso a servidores HTTP, FTP, SMTP e IMAP externos;
 - O firewall deve aceitar conexões ssh da rede interna e da máquina do professor;
 - Aceitar pacotes ICMP originados da da rede interna;
 - Logar todas as tentativas de conexão vindas da rede externa.
-
- Obs.: Todas as regras deverão ser aplicadas através de um script, que deve limpar as regras antigas antes de aplicar as novas.