

# Firewall com iptables

- Intercepta e analisa os Pacotes TCP/IP
- Redireciona, aceita ou rejeita os pacotes
- Faz mascaramento de IP (NAT)


iptables TABELA opção CHAIN dados -j AÇÃO

iptables TABELA opção CHAIN dados -j AÇÃO



- filter (padrão, assumida se omitida. Como o próprio nome diz, faz filtro de pacotes)
- nat (usado para ações de Network Address Translation – ou simplesmente NAT)

# iptables TABELA opção CHAIN dados -j AÇÃO

- 
- -P (definir uma regra Padrão)
  - -A (Acrecentar regra (mais usado, com prioridade sobre -P))
  - -D (Apagar regra)
  - -L (lista as regras existentes)
  - -F ((flush) limpa todas as regras)
  - -I (Inserir uma regra)
  - -h (Help)
  - -R (substitui uma regra)
  - -Z (zera uma regra específica)

iptables TABELA opção CHAIN dados -j AÇÃO



Na tabela filter:

- INPUT (pacotes em que o destino final é o próprio host firewall)
- OUTPUT (pacotes que saem (origem) do host firewall)
- FORWARD (pacotes que vão atravessar o firewall, cujo o destino seja outro host)


iptables TABELA opção CHAIN dados -j AÇÃO



Na tabela nat:

- PREROUTING (pacotes que entram para sofrer NAT)
- POSTROUTING (pacotes saem após sofrer NAT)
- OUTPUT (pacotes gerados no próprio host para sofrer NAT)

# iptables TABELA opção CHAIN dados -j AÇÃO

- 
- -s ((source) Origem do pacote)
  - -d ((destination) destino do pacote)
  - -p (Protocolo (pode ser tcp udp ou icmp))
    - --dport Porta de destina
    - --sport Porta de Origem
  - -i ((input) interface que está recebendo o pacote)
  - -o ((output) interface que despachará o pacote)
  - -m mac (trabalhar com mac address)
    - --mac-source xx.xx.xx.xx.xx mac address de origem

# iptables TABELA opção CHAIN dados -j AÇÃO



- ACCEPT (aceita o pacote)
- REJECT (rejeita o pacote e mas avisa)
- DROP (rejeita e não dá sinal de vida)
- LOG (registra o fato no /var/log/messages (tem q rodar o syslogd))
- MASQUERADE (permite NAT)
- REDIRECT (redireciona o pacote)

# Exemplos:

Liberando navegação:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/255.0.0.0 -o eth1 -j  
MASQUERADE
```

Onde: 10.0.0.0/255.0.0.0 = endereço da rede local  
eth1 interface exposta a internet

Não esquecer de setar 1 em /proc/sys/net/ipv4/ip\_forward  
echo 1 > /proc/sys/net/ipv4/ip\_forward

## Exemplos:

Proxy transparente

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --  
dport 80 -j REDIRECT --to-port 3128
```

Assumindo eth0 a interface da rede local

O squid ou outro proxy está ouvindo na porta 3128

## Exemplos:

Abrindo a porta de ssh

```
iptables -A INPUT -p tcp -s 192.168.0.45 --dport  
22 -j ACCEPT
```

## Exemplos:

Redirecionar uma porta para outro host da rede:

```
iptables -t nat -A PREROUTING -s ppp0 -i eth0 -j DNAT  
--to 192.168.1.5
```

```
iptables -t nat -A POSTROUTING -s ppp0 -o eth0 -p tcp  
--dport <PORTA> -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.5 -o ppp0  
-j SNAT --to ppp0
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.5 -o ppp0  
--p tcp --dport <PORTA> -j ACCEPT
```

## Exemplos:

Gerando logs

```
iptables -A INPUT -p tcp --dport 22 -j LOG --log-  
prefix "Tentaram acessar SSH -"
```

## Exemplos:

Bloqueando o que não foi liberado:

```
iptables -A INPUT -p tcp --syn -j DROP
```

# Desativando o firewall

```
iptables -t nat -F  
iptables -F
```