Cheatography

IPtables Cheat Sheet

by apavanello via cheatography.com/59386/cs/15576/

Composição do comando

```
iptables [-t tabela] [opção] [chain] [dados] -j [ação]
Sendo
  [-t tabela] -> a tabela a ser criada, filter é a default
  [opção] -> Opções como criar ou deletar regras
  [chain] -> Chain a ser usada
  [dados] -> Destinos e origens
  -j [ação] -> Ação a fazer com o pacote
Ex.: iptables -t filter -A FORWARD -d 192.168.1.1 -j DROP
#Dropa todos os pacotes que devem ser encaminhados para o 192.168.1.1
```

Tabelas

filter	Tabela default, faz filtragem dos pacotes simples
nat	Efetua as operações com nat
mangle	para alterações avançadas nos pacotes

Na ausencia do parametro de tabela, a tabela filter é selecionada
As tabelas são sempre escritas no comando na forma minuscula
Ex.:

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

regra para abilitar o nat na porta eth0

Chains

INPUT	Regras que atuarão na entrada de pacotes no FW Tabelas Filter e Mangle
FORWARD	Regras que atuarão no redirecionamento de pacotes no FW Tabelas Filter e Mangle
OUTPUT	Regras que atuarão no saida de pacotes no FW Tabelas Filter, Mangle e NAT
PREROUTING	Regras que atuarão no pacote antes do processo de roteamento Tabelas NAT e Mangle
POSTROUTING	Regras que atuarão no pacote depois do processo de roteamento Tabelas NAT e Mangle

INPUT e OUTPUT a origem é o próprio FW
FORWARD o pacote passa através do FW
Chains são sempre escrita em **MAIÚSCULO**

Comandos Basicos - Visualizar Regras

iptables -L	Lista as regras da tabela **FILTER**
iptables -t nat -L	Lista as regras da tabela **NAT**
iptables -L -n	Lista as regras da tabela **FILTER** sem resolver os nomes e numeros de portas

Ao não definir uma tabela a filter é a**padrão**
Atenção para letras maiúsculas e minúsculas

Comandos Basicos - Criar Regras

-A *chain*	Cria a regra na CHAIN informada
-I *chain num*	Cria a regra na *chain* informada e coloca na posição*num*
-d *IP*	IP de destino
-s *IP*	IP de origem
-p *protocolo*	protocolo (TCP, UDP, ICMP)
--sport *porta*	Porta de origem (necessario usar junto do -p)
--dport *porta*	Porta de destino (necessario usar junto do -p)
-i *int*	Interface de entrada de dados(ex.: ETH0)
-o *int*	Interface de saida de dados(ex.: ETH0)
-j *ação*	ação a ser tomada (ACCEPT, REJECT,DROP)
-D *num*	Deleta a regra de numero *num*
-F	apaga todas as regras

Substituir o que este em*itálico* pela opção informada
ex.: -A *chain* na INPUT ficaria:
iptables -A INPUT

AÇÕES

ACCEPT	Aceita os pacotes
DROP	Descarta o pacote
REJECT	Rejeita o pacote
MASQUERADE	Usado na tabela NAT para aplicar a mascara NAT
DNAT	efetua o nat reverso, é necessario usar junto do comando --to-destination *IP:port*