



# IPTables



Aluno: Kelton Martins Dias  
Professor: Adriano Antunes

# Introdução ao IPTables

## 01

### O que é?

O ipTables é uma ferramenta de firewall para sistemas Linux que permite controlar o tráfego de rede, atuando como um "guarda" que decide quais pacotes de dados podem entrar ou sair do sistema. Ele utiliza regras definidas pelo usuário, organizadas em tabelas e cadeias, para permitir ou bloquear conexões, garantindo a segurança e integridade da rede ao proteger contra acessos não autorizados e atividades maliciosas.

## 02

### Tables and chains

O ipTables possui quatro tabelas principais. A tabela filter é a mais comum e utilizada para filtrar pacotes, com as chains INPUT, OUTPUT e FORWARD. A tabela nat lida com a tradução de endereços de rede (NAT), com as chains PREROUTING, OUTPUT e POSTROUTING. A tabela mangle permite a modificação de cabeçalhos de pacotes, contendo as chains PREROUTING, INPUT, FORWARD, OUTPUT e POSTROUTING. Por fim, a tabela raw controla o rastreamento de conexões, com as chains PREROUTING e OUTPUT.

# Table Filter



## INPUT

Controla o tráfego de entrada, verificando todos os pacotes que chegam à máquina. As regras aqui determinam se um pacote será aceito ou bloqueado, sendo essencial para proteger o sistema contra acessos não autorizados ou ataques externos.



## OUTPUT

Gerencia o tráfego de saída, controlando os pacotes gerados pela própria máquina. Permite definir regras para restringir ou permitir a comunicação com redes externas, útil para limitar acessos a sites ou serviços indesejados.



## FORWARD

Lida com o tráfego que atravessa o sistema sem ser destinado a ele. Usada quando a máquina atua como um roteador, a chain FORWARD permite controlar o fluxo de pacotes entre diferentes redes, garantindo segurança no encaminhamento do tráfego.

# Table Filter Exemplos



## INPUT

1. Permitir conexões SSH
2. Bloquear acessos de IPs específicos
3. Permitir tráfego HTTP e HTTPS
4. Dropar pacotes com portas inválidas
5. Redirecionar tráfego para um servidor proxy



## OUTPUT

1. Bloquear acesso a sites específicos
2. Permitir comunicação com servidores DNS
3. Controlar o tráfego de aplicativos específicos
4. Limitar o uso da banda de internet
5. Registrar conexões de saída para auditoria



## FORWARD

1. Criar uma VPN para conectar redes separadas
2. Implementar NAT para traduzir endereços IP
3. Criar regras de firewall para tráfego de rede interna
4. Gerenciar o tráfego entre diferentes sub-redes
5. Bloquear pacotes maliciosos que tentam passar pela sua máquina

# Parâmetros

| Parâmetro      | Descrição                       |
|----------------|---------------------------------|
| <b>-p</b>      | Define o protocolo do pacote    |
| <b>-s</b>      | Define o endereço IP de origem  |
| <b>-d</b>      | Define o endereço IP de destino |
| <b>-j</b>      | Define a ação a ser tomada      |
| <b>--dport</b> | Define a porta de destino       |
| <b>--sport</b> | Define a porta de origem        |

# Exemplo dos parâmetros

|                | INPUT   | OUTPUT   | FORWARD   |
|----------------|---|--|---|
| <b>-p</b>      | iptables -A INPUT -p tcp -j ACCEPT            | iptables -A OUTPUT -p udp -j ACCEPT            | iptables -A FORWARD -p icmp -j ACCEPT           |
| <b>-s</b>      | iptables -A INPUT -s 192.168.1.10 -j DROP     | iptables -A OUTPUT -s 192.168.1.15 -j DROP     | iptables -A FORWARD -s 192.168.2.0/24 -j DROP   |
| <b>-d</b>      | iptables -A INPUT -d 192.168.1.20 -j ACCEPT   | iptables -A OUTPUT -d 203.0.113.5 -j ACCEPT    | iptables -A FORWARD -d 10.0.0.1 -j ACCEPT       |
| <b>-j</b>      | iptables -A INPUT -p icmp -j REJECT           | iptables -A OUTPUT -p tcp -j REJECT            | iptables -A FORWARD -p tcp -j REJECT            |
| <b>--dport</b> | iptables -A INPUT -p tcp --dport 22 -j ACCEPT | iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT | iptables -A FORWARD -p tcp --dport 53 -j ACCEPT |
| <b>--sport</b> | iptables -A INPUT -p tcp --sport 8080 -j DROP | iptables -A OUTPUT -p tcp --sport 443 -j DROP  | iptables -A FORWARD -p tcp --sport 1234 -j DROP |



Obrigado!