

0

Aluno: Kelton Martins Dias

Professor: Adriano Antunes

Introdução ao IPTables

21

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

- Permitir conexões SSH
- Bloquear acessos de IPs específicos
- Permitir tráfego HTTP e **HTTPS**
- Dropar pacotes com portas inválidas
- um servidor proxy



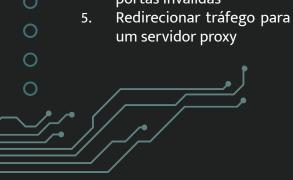
OUTPUT

- Bloquear acesso a sites específicos
- Permitir comunicação com servidores DNS
- Controlar o tráfego de aplicativos específicos
- Limitar o uso da banda de internet
- Registrar conexões de saída para auditoria



FORWARD

- Criar uma VPN para conectar redes separadas
- Implementar NAT para traduzir endereços IP
- Criar regras de firewall para tráfego de rede interna
- Gerenciar tráfego entre 0 diferentes sub-redes
- Bloquear pacotes maliciosos que tentam passar pela sua máquina





Parâmetros

Parâmetro	Descrição	
-р	Define o protocolo do pacote	
-s	Define o endereço IP de origem	
-d	Define o endereço IP de destino	
-j	Define a ação a ser tomada	
dport	Define a porta de destino	
sport	Define a porta de origem	



Exemplo dos parâmetros

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



Obrigado!