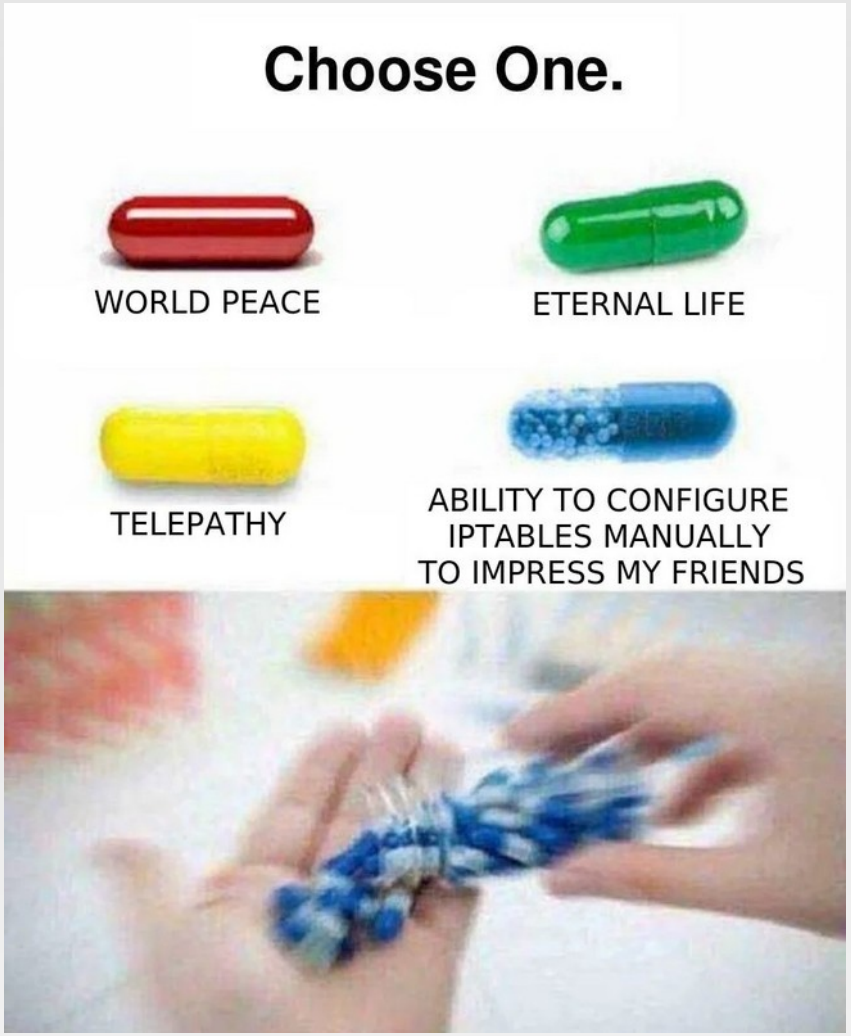
Apresentação
Firewall - Iptables

- Introdução
- Conceitos
- Regras e sintaxe
- Configuração
- Exemplos
- Laboratório
- Atividades adicionais

Intro

- Projeto Netfilter
- Iptables é o programa em user space para configurar regras IPv4
- Outros: arptables, ebtables, ip6tables, etc
- Uso de tabelas (nat, filter, mangle, security e raw) com cadeias de regras para os diversos módulos
- Outros sistemas: PF, IPFW, IPF, etc

Intro



nftables vem substituir ao iptables

Conceitos

- Firewall pode ser stateful e stateless
- Hardware appliance ou software
- Application level e NGFW
- Sistemas derivados, e.g. NIDS.

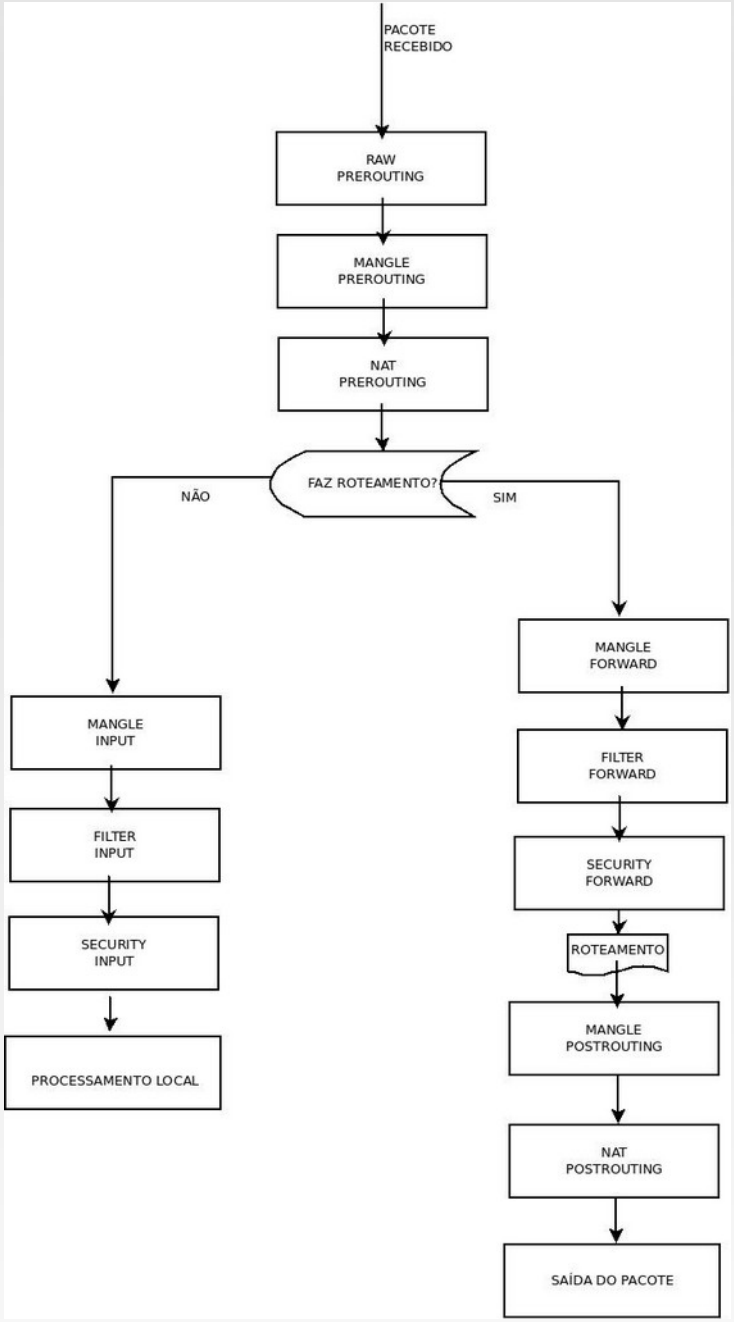
Conceitos

- Regras em cadeias
- Cadeias, por sua vez, estão em tabelas
- Regras são interpretadas de forma sequencial dentro das cadeias
- Toda cadeia deve ter uma política padrão

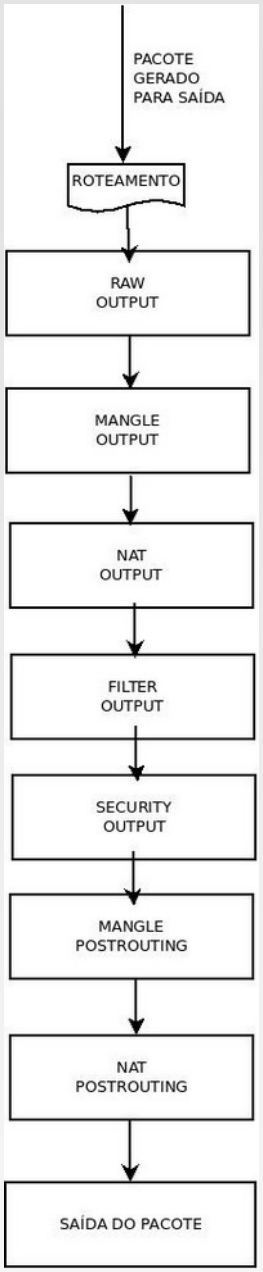
Conceitos

- Pacotes percorrem todas as cadeias das tabelas padrões + tabelas e cadeias configuradas pelo usuário
- A política padrão deve ser aplicada caso a inspeção de um pacote não case com nenhuma regra
- Módulos podem ser carregados no kernel para habilitar capacidades adicionais

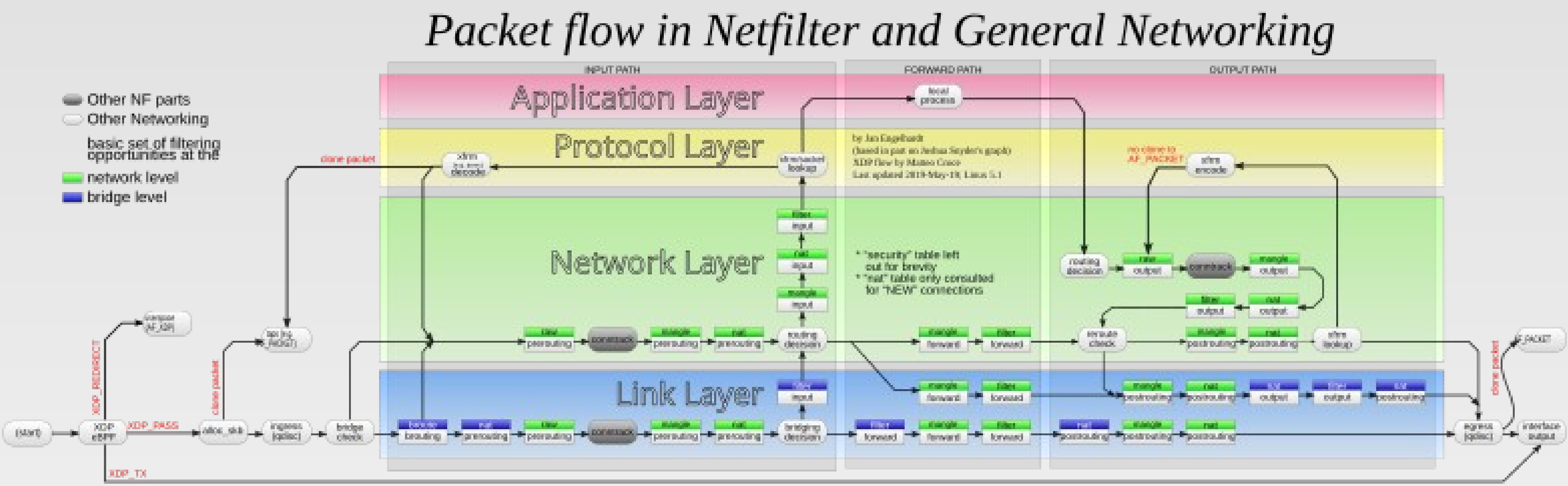
Conceitos


PACOTE RECEBIDO
RAW PREROUTING
MANGLE PREROUTING
NAT PREROUTING
FAZ ROTEAMENTO?
NÃO
SIM
MANGLE INPUT
FILTER INPUT
SECURITY INPUT
PROCESSAMENTO LOCAL
MANGLE FORWARD
FILTER FORWARD
SECURITY FORWARD
ROTEAMENTO
MANGLE POSTROUTING
NAT POSTROUTING
SAÍDA DO PACOTE

Conceitos


PACOTE
GERADO
PARA SAÍDA
ROTEAMENTO
RAW
OUTPUT
MANGLE
OUTPUT
NAT
OUTPUT
FILTER
OUTPUT
SECURITY
OUTPUT
MANGLE
POSTROUTING
NAT
POSTROUTING
SAÍDA DO PACOTE

Conceitos



Packet flow in Netfilter and General Networking
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
Other NF parts
Other Networking
basic set of filtering opportunities at the
network level
bridge level
local process
routing decision
bridging decision
prerouting
forward
input
output
postrouting
conntrack
XDP eBPF
XDP_PASS
XDP_REDIRECT
XDP_TX
clone packet
ingress (qdisc)
egress (qdisc)
interface output
bridge check
* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections

Regras e sintaxe

- Listagem

```
#> iptables -L -n
#> iptables -t nat -L -n
#> iptables -L -n –line-numbers
#> iptables -L -v -n –line-numbers
```

Regras e sintaxe

- Mais regras

#> iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

#> iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

#> iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT

#> iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j ACCEPT

#> iptables -A INPUT -i eth0 -p tcp -s 192.168.200.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

#> iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

Regras e sintaxe

- Policy

#> iptables -P INPUT ACCEPT

- Regra

  #> iptables -A INPUT -p tcp –dport 80 -j DROP

  #> iptables -I INPUT 1 -p tcp –dport 80 -j DROP

Regras e sintaxe

- Mais regras

#> iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

- Cadeias personalizadas

#> iptables -N LOGGING_SSH

#> iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW -j LOGGING_SSH

#> iptables -A LOGGING_SSH -m limit --limit 120/min -j LOG --log-prefix "NEW SSH CONNECTION: " --log-level 7

#> iptables -A LOGGING_SSH -m limit --limit 120/min -j ACCEPT

#> iptables -A LOGGING_SSH -j DROP

Regras e sintaxe

- NAT

#> iptables -t nat -A POSTROUTING -p TCP -j MASQUERADE --to-ports 1024-31000

#>iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to-source 67.215.65.132

Regras e sintaxe

- NAT

#> iptables -t nat -A PREROUTING -p tcp -d 67.215.65.132 --dport 110 -j DNAT --to-destination 10.15.100.110

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

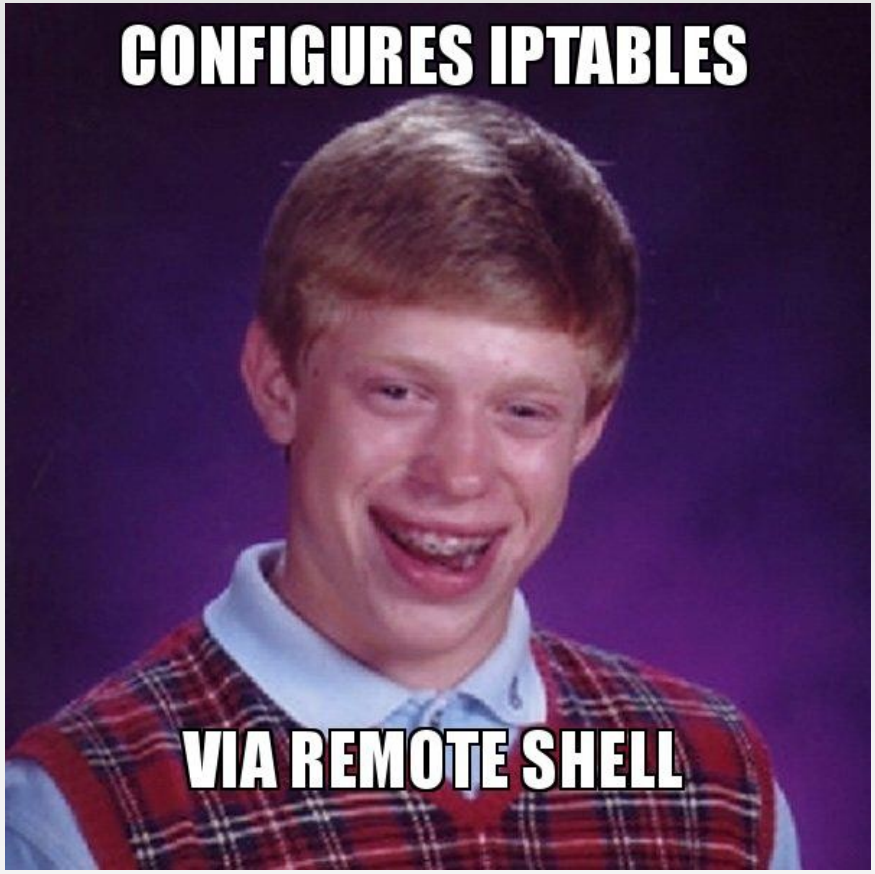
#>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 3128

Configurações e Melhores Práticas

- Utilizar shell scripts para criação de regras
- Utilizar algum aplicativo suporte para gravar regras de forma não volátil
- Ao realizar bloqueio prefira DROP em detrimento de REJECT
- Compile o Kernel do Linux com os módulos netfilter desejados para a funcionalidade do firewall

Configurações e Melhores Práticas

- Cautela ao fazer a limpeza/reset de cadeias



Exemplos

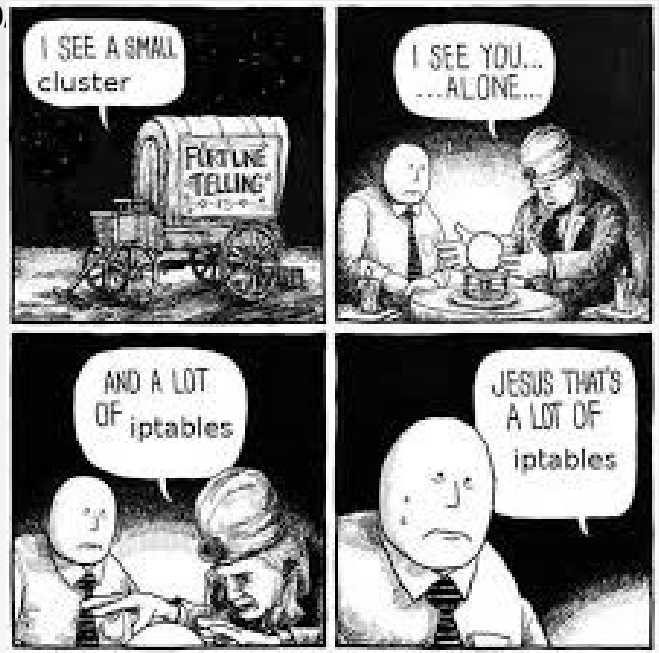
```
#!/bin/bash
INTERNAL_IFACE="eth1"
EXTERNAL_IFACE="eth0"

iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT
iptables -A FORWARD -p tcp -i "$INTERNAL_IFACE" -o "$EXTERNAL_IFACE" -j ACCEPT
iptables -A FORWARD -p udp -i "$INTERNAL_IFACE" -o "$EXTERNAL_IFACE" -j ACCEPT
iptables -A FORWARD -p icmp -j DROP
iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -P FORWARD DROP
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
echo "iptables forwarding rules applied."
```

Exemplos

#> iptables -L FORWARD -v -n

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
0	0	ACCEPT	tcp	--	eth1	eth0	0.0.0.0/0	0.0.0.0/0
0	0	ACCEPT	udp	--	eth1	eth0	0.0.0.0/0	0.0.0.0/0
0	0	DROP	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0



Laboratório

- Configurar bloqueio da tabela filter entrada e saída
- Configurar permissão de tráfego específico
- Configurar filtro de encaminhamento
- Configurar o NAT para comunicação externa

Atividade Extra

- Utilize a referência para entender os comandos e opções possíveis

https://www.linux.co.cr/distributions/review/2002/red-hat-8.0/rhl-rg/s1-iptables-options.html

- Faça o exercício extra em http://rzuolo.com/2025/grs/atividade-extra-04-IPTABLES.pdf

The End