



Redes de Computadores II

C.T. Informática para Internet
Prof. Vinícius Alves Hax



Antes

- Firewall (teoria)
- Auditoria (prática)

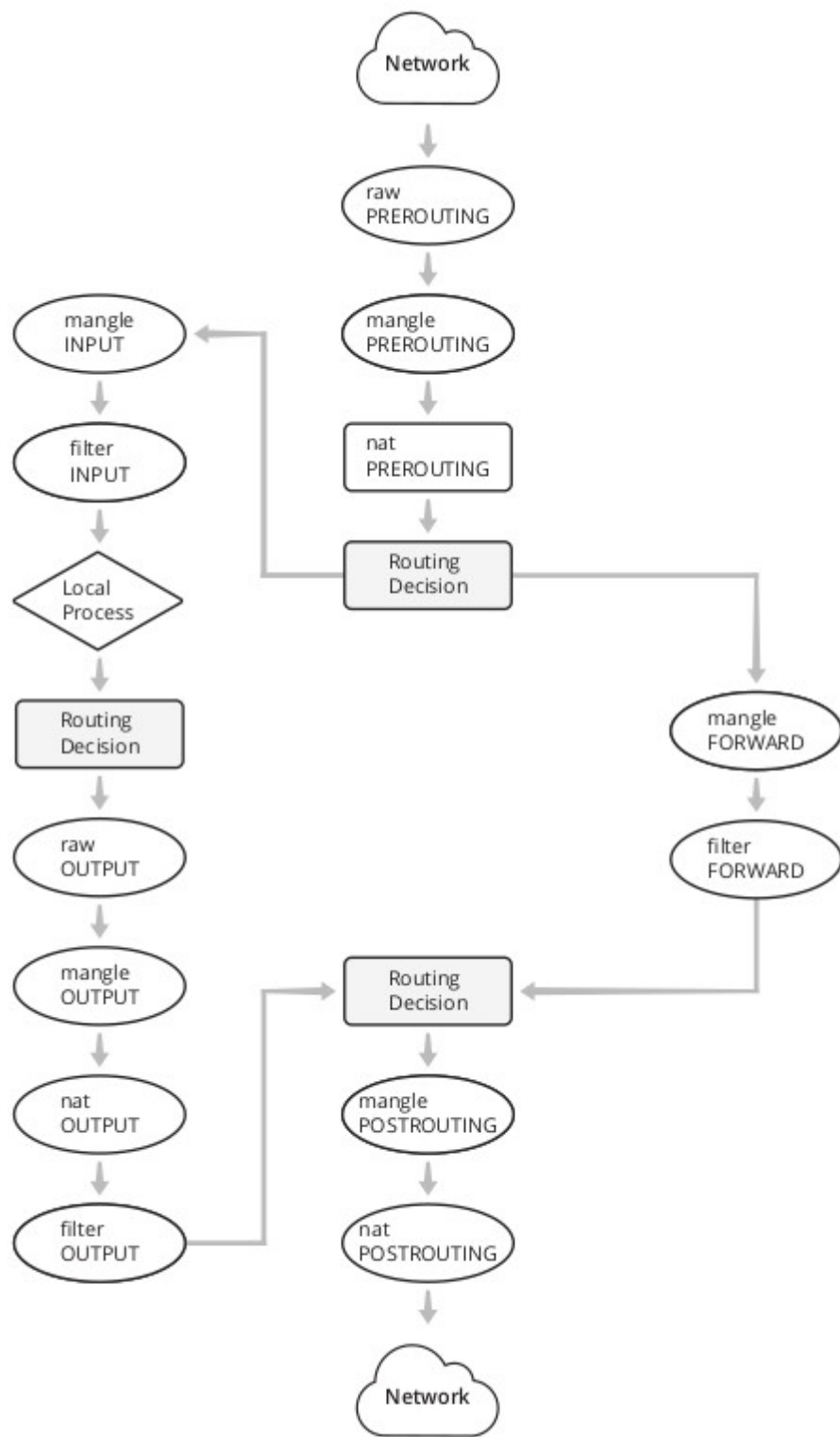


Hoje

- Firewall (prática)
- Planejamento viagem pra reitoria


Terminologia iptables

- Policy: Geralmente traduzida como política. É o comportamento padrão para cada chain
- Rule: Cada regra do iptables
- Chain: Conjunto de regras
- Drop: Quando um pacote é descartado por não obedecer alguma regra
- Reject: Semelhante ao 'drop', porém o remetente é avisado que sua mensagem não chegou ao destino



Iptables

- Principal software para firewall em servidores
- Sintaxe básica:
 - `iptables -A|D|L [-d|s IP] [-p TCP|UDP --sport|dport ??] -j DROP|REJECT|ACCEPT|LOG`

- 
- Lista as regras
 - sudo iptables -L
 - Apaga as regras
 - sudo iptables -F

Define as políticas

- Definindo política de saída como ACCEPT
- `sudo iptables -P OUTPUT ACCEPT`
- Definindo política de saída como DROP
- `sudo iptables -P OUTPUT DROP`

Drop p/ host específico

- Pelo IP
- `sudo iptables -A OUTPUT -d 200.19.1.202 -j DROP`
- Pelo hostname
- `sudo iptables -A OUTPUT -d ifsul.edu.br -j DROP`

Drop em portas específicas

- Bloqueando a porta 80
- `sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP`
- Bloqueando porta 80 de um host específico
- `sudo iptables -A OUTPUT -d 194.5.156.92 -p tcp --dport 80 -j DROP`

Log de conexões

- `sudo iptables -A OUTPUT -d 200.19.1.195 -j LOG`
- `$ cat /var/log/syslog | grep TTL`



Bloqueando uma subrede


- `sudo iptables -A OUTPUT -d 200.19.1.202/24 -j DROP`

Deletando regras específicas

- Mostrando o número
- `sudo iptables -L --line-numbers`
- Apagando a partir do número
- `sudo iptables -D OUTPUT 3`

Ordem das regras

- "As regras são lidas de cima para baixo. Então, a primeira condição que bater, será aplicada."
- Exemplo
 - sudo iptables -A OUTPUT -d 200.19.1.195 -j DROP
 - sudo iptables -A OUTPUT -d 200.19.1.195 -j ACCEPT
- Vai bloquear ou aceitar?

- 
- Valor: 5 pontos (exercício a e b)
 - Data de entrega: 15/fevereiro
 - Exercício a) Escolha um site da sua preferência, descubra o IP do mesmo e descubra se o mesmo está servindo o site no protocolo HTTP ou HTTPS. Informe qual o comando para bloquear somente o acesso à essa porta desse host usando iptables.
 - PS: Evite sites muito grandes (escolha um site .br) que possuem múltiplos ips para um mesmo domínio (pois nesse caso o teste no browser podem não funcionar muito bem)
 - Exercício b) Qual o comando iptables para bloquear todos os hosts no intervalo entre 142.251.0.128 até 142.251.0.143?
 - Elabore um relatório de até uma página (um relatório para ambos os exercícios) mostrando os comandos para resolução dos exercícios a e b, e a explicação dos passos realizados para a realização do exercício.



Dúvidas?

Fontes

- <https://mateusmuller.me/2018/10/18/o-guia-completo-do-iniciante-em-iptables/>
- <https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules-pt>
- IPTables:
Peixinho, I.; Fonseca, F. e Lima, F. Segurança de Redes e Sistemas. Escola Superior de Redes.