Overview sobre Firewall

~~~~~~

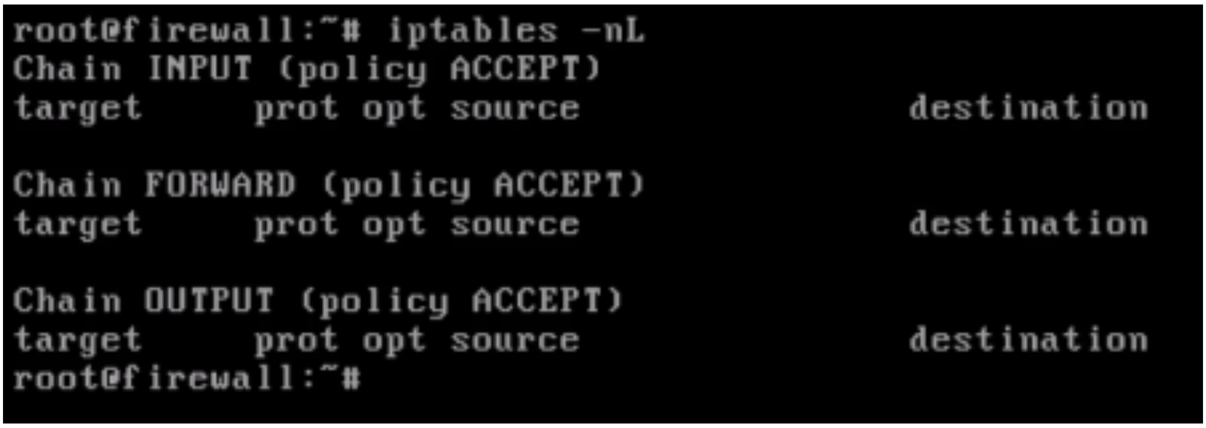
Firewall - Iptables na Prática

~~~~~~

+ iptables é uma ferramenta de Firewall para Linux que, por default, já vem desabilitada (com todas as condições ACCEPT). Ele é como um “guarda de fronteira” enrtre o pc e a internet.

+ `iptables -nL`

→ mostra como estão as regras do firewall na máquina



```
root@firewall:~# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@firewall:~#
```

INPUT → entradas (aceitando qualquer coisa na entrada)
FORWARD → encaminhamento de portas
OUTPUT → saída
todas estão no default que não impede nada.

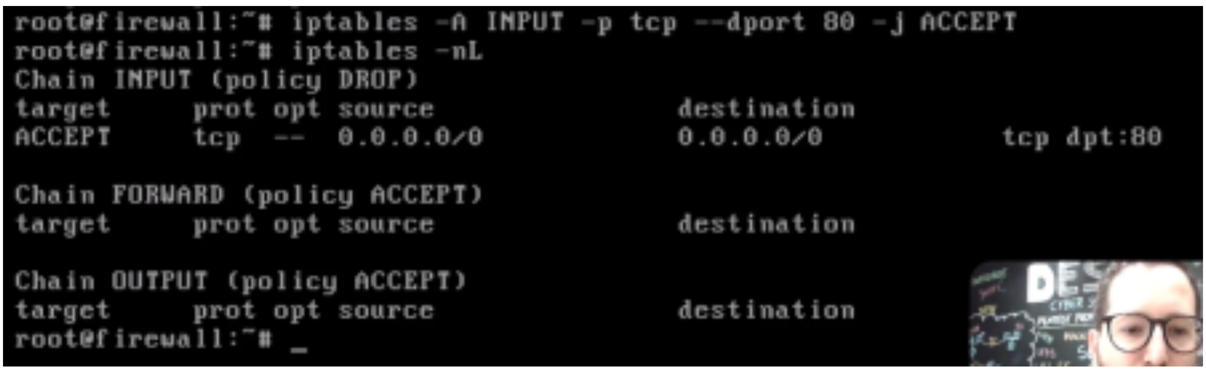
+ `iptables -P INPUT DROP`

→ o -P indica a política que vamos implementar.
→ nesse caso, mudamos a política de ACCEPT para DROP
→ com essa configuração, ele nega tudo
→ O host não poderá mais ser pingado, scaneado ou acessado, mesmo com os serviços ativos.

+ Queremos agora liberar algumas entradas (no caso, vamos liberar a porta 80)

+ `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

→ -p indica o protocolo (que escolhemos o tcp), o 80 é a porta e o -j é a ação que queremos tomar



```
root@firewall:~# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@firewall:~# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:80

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@firewall:~# _
```

→ nesse caso, conseguimos acessar o endereço na internet na porta
→ 80, mas ainda n conseguimos fazer um portscanning ou sequer um
→ ping.

+ Agora faremos a liberação do ping, lembrando que o ping se usa
do protocolo ICMP

+ `iptables -A INPUT -p icmp -j ACCEPT`

+ `iptables -F`

→ Esse último comando faz que o firewall zere as regras (com exceção
→ das políticas já programadas)

+ Existe uma maneira de filtrar não apenas a porta e o protocolo,
mas também o ip de origem.

+ `iptables -A INPUT -p tcp --dport 80 192.168.0.11 -j ACCEPT`

→ aqui o 192.168.0.11 é o ip de origem

+ Filtraremos agora o tipo do protocolo icmp que poderá passar

+ `iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT`

+ Se quiséssemos resolver o host businesscorp.com.br com o comando
host businesscorp.com.br, não conseguiríamos pois o comando host
usa, por default, o protocolo udp.
+ Para habilitar a resolução, devemos habilitar o protocolo udp

```
iptables -A INPUT -p udp -j ACCEPT
```

+ Para filtrar a porta de destino, usamo --dport [n da porta]. Se
fosse a de origem, --sport [n da porta]. s de source