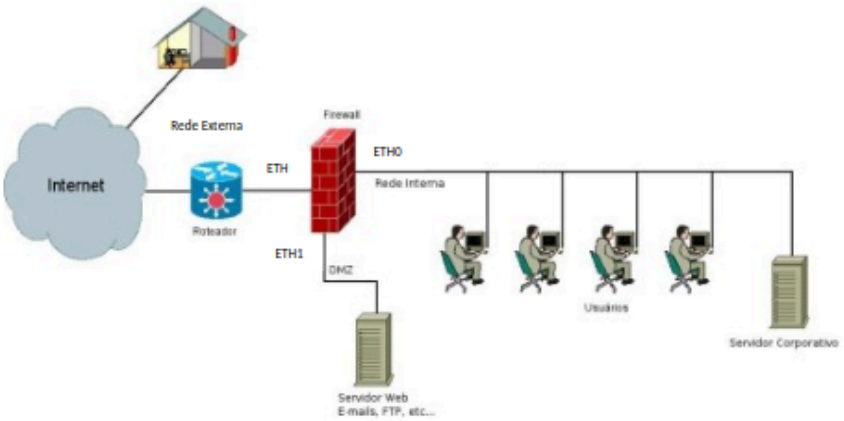
# Firewall IPTABLES - Lista de Exercícios

1) Dado a topologia de rede a seguir:




Configuração das redes:

| | |
|---|---|
| Rede Interna: 10.1.1.0/24 | ETH0: 10.1.1.1/24 |
| DMZ: 192.168.1.0/24 | ETH1: 192.168.1.1/24 |
| Rede Externa: 200.20.5.0/30 | ETH2: 200.20.5.1/30 |

Elabore as regras necessárias para implementar os seguintes controles. Utilize para isso as regras do firewall Linux (netfilter/iptables).

**I. Libere qualquer tráfego para interface de loopback no firewall.**

iptables - t filter - A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

**II. Estabeleça a política DROP (restritiva) para as chains INPUT e FORWARD da tabela filter.**

iptables - t filter - P  INPUT DROP // usar - P ao invé de -A
iptables -t filter  - P  FORWARD ACCEPT

**III. Possibilita que usuários da rede interna possam acessar o serviço WWW, tanto na porta (TCP) 80 como na 443. Não esqueça de realizar NAT já que os usuários internos não possuem um endereço IP válido.**

- Uso das interfaces com base nos modelos acima!!!

iptables -t filter -A FORWARD -i ethO -o eth2 -p tcp --dport 80 -j ACCEPT
iptables-t filter -A FORWARD -i ethO -o eth2 -p tcp --dport 443-j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o ethO -p tcp --sport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o ethO -p tcp -sport 443 -j ACCEPT

**IV. Faça LOG e bloqueie o acesso a qualquer site que contenha a palavra "games"**

iptables -t filter -| FORWARD -o eth2 -p tcp --dport 80 -m string --algo bm --string "games"- j LOG

iptables -tfilter -I FORWARD -o eth2 -p tcp --dport 80 -m string --algo bm --string "games"— j DROP

**V. Bloqueie acesso para qualquer usuário ao site www.jogosonline.com.br, exceto para seu chefe, que possui o endereço IP 10.1.1.100**

iptables -t filter -| FORWARD -o eth2 -s 10.1.1.100 -d www.jogosonline.com.br-ptcp--dport 80 -j ACCEPT

iptables -t filter -| FORWARD -o eth2 -s 10.1.1.0/24-d www.jogosonline.com.br-ptcp-dport 80-j DROP

**VI. Permita que o firewall receba pacotes do tipo ICMP echo-request (ping), porém, limite a 5 pacotes por segundo.**

iptables -t filter -| INPUT -p icmp --icmp-type -echo-request-m limit--limit 5/s -j ACCEPT

**VII. Permita que tanto a rede interna como a DMZ possam realizar consultas ao DNS externo, bem como, receber os resultados das mesmas.**

iptables -t filter - I FORWAR -o eth2 -p udp -dport 53 -j ACCEPT
iptables -t filter - I FORWAR -i eth2 -p udp -sport 53 -j ACCEPT

**VIII. Permita o tráfego TCP destinado à máquina 192.168.1.100 (DMZ) na porta 80, vindo de qualquer rede (Interna ou Externa).**

iptables -t filter -| FORWARD -d 192.168.1.100 -p tcp --dport 80 -j ACCEPT

**IX. Redirecione pacotes TCP destinados ao IP 200.20.5.1 porta 80, para a máquina 192.168.1.100 que está localizado na DMZ.**

iptables -t nat -A PREROUTING -i eth2 -d 200.20.5.1 -p tcp --dport 80 -j DNAT --to 192.168.1.100

**X. Faça com que a máquina 192.168.1.100 consiga responder os pacotes TCP recebidos na porta 80 corretamente.**

iptables -t filter -| FORWARD -s 192.168.1.100 -p tcp -sport 80 -j ACCEPT