

# Trabalho 3 - Implementação de um Firewall

H. de M. O. Lima – 211055281, L. P. Torres – 222011623, and M. N. Miyata – 180126890

## I. INTRODUÇÃO

O presente trabalho tem como objetivo a implementação de um firewall utilizando o iptables em um ambiente Linux. O firewall será configurado para controlar o tráfego de rede, permitindo ou bloqueando conexões com base em regras específicas.

No ambiente experimental, utilizaremos três máquinas virtuais: uma atuando como roteador/firewall, outra como cliente interno e a terceira como servidor interno. Em seguida, detalharemos as regras implementadas no firewall, a metodologia utilizada para testar sua eficácia e a análise dos resultados obtidos.

## II. FUNDAMENTAÇÃO TEÓRICA

Um firewall é um sistema de segurança de rede que monitora e controla o tráfego de entrada e saída com base em regras de segurança predefinidas. Ele atua como uma barreira entre redes confiáveis e não confiáveis, protegendo os sistemas internos contra acessos não autorizados e ameaças externas.

No Linux, o iptables é uma ferramenta amplamente utilizada para configurar firewalls. Ele permite a criação de regras que definem como o tráfego deve ser tratado, seja permitindo, bloqueando ou redirecionando pacotes de dados.

## III. AMBIENTE EXPERIMENTAL

Como mencionado anteriormente, o ambiente experimental consiste em três máquinas virtuais: Roteador/Firewall, Cliente Interno e Servidor Interno. A máquina Roteador/Firewall está configurada para atuar como o ponto central de controle do tráfego de rede entre o Cliente Interno e o Servidor Interno. Além disso, todos foram configurados com endereços IP estáticos para garantir a comunicação adequada entre eles.

## IV. ROTEADOR/FIREWALL

Os scripts de configuração do firewall estão contidos em três arquivos principais: 00\_enable\_routing.sh, 01\_setup\_firewall.sh e 02\_cleanup\_firewall.sh. A máquina virtual é um Debian sem interface gráfica, configurada com dois adaptadores de rede: um em modo “Rede Interna” (conectado ao Cliente e Servidor Internos) e outro em modo “NAT” (conectado à Internet). Os detalhes de configuração do firewall são apresentados nas próximas subseções.

### A. Roteamento e NAT

O script 00\_enable\_routing.sh ativa o encaminhamento de pacotes IP no sistema. Três variáveis principais são definidas: WAN\_IF (interface de rede conectada à Internet), LAN\_IF (interface de rede conectada à rede interna) e LAN\_IP (endereço IP da interface LAN). A seguir, o script configura o endereço IP da interface LAN, ativa o encaminhamento de pacotes e configura o NAT (Network Address Translation) para permitir que os dispositivos na rede interna acessem a Internet através do roteador/firewall.

```
1 #!/bin/bash
2 # Habilita roteamento e NAT de forma persistente.
3
4 # Interface de saída para a internet, conectada ao
   provedor
5 WAN_IF="${WAN_IF:-enp0s3}"
6 # Interface de rede interna, utilizada pelos
   clientes para se conectar ao roteador
7 LAN_IF="${LAN_IF:-enp0s8}"
8 # Endereço IP da rede interna (LAN)
9 LAN_IP="${LAN_IP:-192.168.50.1/24}"
10
11 echo "[+] Ativando roteamento IPv4..."
12 sysctl -w net.ipv4.ip_forward=1
13 sed -i 's/^#\?net.ipv4.ip_forward.*/net.ipv4.
   ip_forward=1/' /etc/sysctl.conf
14
15 echo "[+] Configurando IP da LAN..."
16 ip addr add $LAN_IP dev $LAN_IF
17 ip link set $LAN_IF up
18
19 echo "[+] Limpando regras antigas..."
20 iptables -t nat -F
21
22 echo "[+] Ativando NAT (masquerade) na interface
   $WAN_IF..."
23 iptables -t nat -A POSTROUTING -o $WAN_IF -j
   MASQUERADE
24
25 echo "✓[] Roteamento e NAT configurados."
```

### B. Regras do Firewall

O script 01\_setup\_firewall.sh é responsável por configurar as regras do firewall utilizando o iptables. As cadeias de entrada (INPUT), encaminhamento (FORWARD) e saída (OUTPUT) são configuradas com políticas padrão seguras, bloqueando todo o tráfego por padrão. Em seguida, regras específicas são adicionadas para permitir o tráfego necessário e bloquear conexões indesejadas:

**INPUT:** Permite o tráfego de loopback, conexões estabelecidas e acesso ao servidor web na porta 8000.

No entanto, o tráfego ICMP (ping) é permitido apenas para a rede interna.

```
1 echo "[+] INPUT: Permitir tráfego de loopback"
2 iptables -A INPUT -i lo -j ACCEPT
3
4 echo "[+] INPUT: Permitir conexões estabelecidas"
5 iptables -A INPUT -m conntrack --ctstate
6     ESTABLISHED,RELATED -j ACCEPT
7
8 echo "[+] INPUT: Permitir acesso ao servidor web (
9     porta 8000)"
10 iptables -A INPUT -s $REDE_INTERNA -p tcp --dport
11     8000 -m state --state NEW -j ACCEPT
12
13 echo "[+] INPUT: Permitir Ping (ICMP) da rede
14     interna"
15 iptables -A INPUT -s $REDE_INTERNA -p icmp --icmp-
16     type echo-request -j ACCEPT
```

**FORWARD:** Permite conexões estabelecidas, bloqueia DNS para redes sociais específicas (Facebook e TikTok) utilizando correspondência de strings, permite DNS de saída (UDP e TCP), permite HTTP e HTTPS de saída, e gerencia o tráfego ICMP (ping) de forma controlada.

```
1 echo "[+] FORWARD: Permitir conexões estabelecidas"
2 iptables -A FORWARD -m conntrack --ctstate
3     ESTABLISHED,RELATED -j ACCEPT
4
5 echo "[+] FORWARD: Bloqueando DNS para redes
6     sociais (String Match)"
7 iptables -A FORWARD -s $REDE_INTERNA -p udp --
8     dport 53 -m string --string "facebook" --algo
9     bm -j REJECT
10 iptables -A FORWARD -s $REDE_INTERNA -p udp --
11     dport 53 -m string --string "tiktok" --algo
12     bm -j REJECT
13
14 echo "[+] FORWARD: Permitir DNS (UDP e TCP) de
15     saída (Geral)"
16 iptables -A FORWARD -s $REDE_INTERNA -p udp --
17     dport 53 -m state --state NEW -j ACCEPT
18 iptables -A FORWARD -s $REDE_INTERNA -p tcp --
19     dport 53 -m state --state NEW -j ACCEPT
20
21 echo "[+] FORWARD: Permitir HTTP e HTTPS de saída"
22 iptables -A FORWARD -s $REDE_INTERNA -p tcp --
23     dport 80 -m state --state NEW -j ACCEPT
24 iptables -A FORWARD -s $REDE_INTERNA -p tcp --
25     dport 443 -m state --state NEW -j ACCEPT
26
27 echo "[+] FORWARD: ICMP (Ping) gerenciado"
28 iptables -A FORWARD -s $REDE_INTERNA -d
29     $SERVIDOR_INTERNO -p icmp --icmp-type echo-
30     request -j ACCEPT
31 iptables -A FORWARD -s $REDE_INTERNA -p icmp --
32     icmp-type echo-request -j REJECT --reject-
33     with icmp-host-prohibited
```

**OUTPUT:** Aceita todo o tráfego de saída sem restrições. Essa escolha visa garantir que o firewall não interfira nas conexões iniciadas pela própria máquina roteadora/firewall, permitindo que ela se comunique livremente com outros dispositivos na rede ou na Internet.

## V. ANÁLISE DE RESULTADOS E DESAFIOS ENFRENTADOS

## VI. CONCLUSÃO

## VII. REFERÊNCIAS