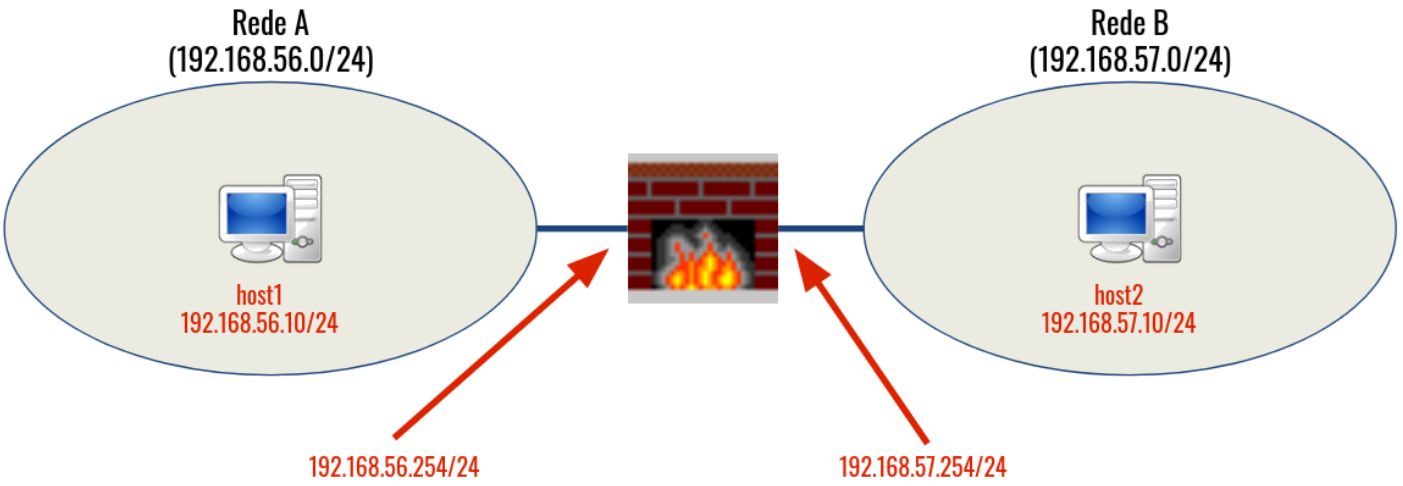
Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Segurança e Preservação de Dados

Atividade Prática em Laboratório (Roteiro) - Firewalls com Iptables - Parte 01

Utilizando contêineres docker vamos montar o seguinte cenário:



1) Crie um arquivo para montar este cenário usando uma imagem leve do Linux Debian e configurando adequadamente as interfaces de rede. O arquivo docker-compose.yml para isso deve ter o seguinte conteúdo (logo a seguir está o link para baixar o arquivo pronto para facilitar):

```
services:
  fw:
        image: debian:12-slim
        container_name: fw
        cap_add:
        - NET_ADMIN
        networks:
        rede-a:
        ipv4_address: 192.168.56.254
        rede-b:
        ipv4_address: 192.168.57.254
        command: /bin/bash -c "tail -f /dev/null"

  host-1:
        image: debian:12-slim
        container_name: host-1
        cap_add:
        - NET_ADMIN
        networks:
        rede-a:
        ipv4_address: 192.168.56.10
        depends_on:
        - fw
        command: /bin/bash -c "tail -f /dev/null"

  host-2:
        image: debian:12-slim
        container_name: host-2
        cap_add:
        - NET_ADMIN
        networks:
        rede-b:
        ipv4_address: 192.168.57.10
        depends_on:
        - fw
        command: /bin/bash -c "tail -f /dev/null"

networks:
  rede-a:
        driver: bridge
        ipam:
        config:
        - subnet: 192.168.56.0/24
  rede-b:
        driver: bridge
        ipam:
        config:
        - subnet: 192.168.57.0/24
```

https://www.segurancaderedes.com.br/spd/pratica06/docker-compose.yml

2) Execute/ative os contêineres:

```
$ docker compose up -d
```

3) Atualize os pacotes e a base APT em todos os contêineres:

```
$ docker exec -it fw bash
# apt update
```

```
$ docker exec -it host-1 bash
```

```
# apt update
```

```
$ docker exec -it host-2 bash
# apt update
```

4) Instale os pacotes iproute2 (para configuração das interfaces) e iputils-ping (para executar o ping) nos dois hosts:

```
$ docker exec -it host-1 bash
# apt install iproute2 iputils-ping
```

```
$ docker exec -it host-2 bash
# apt install iproute2 iputils-ping
```

5) Instale os pacotes iproute2 (para configuração das interfaces), iputils-ping (para executar o ping) e iptables (para configurar as filtragens no firewall) no contêiner fw:

```
$ docker exec -it fw bash
# apt install iproute2 iputils-ping iptables
```

6) Remova a rota padrão (gateway) dos dois hosts, que apontam para a 'máquina real' e insira uma rota padrão nova informando como gateway o firewall:

```
$ docker exec -it host-1 bash
# ip route del default
# ip route add default via 192.168.56.254
```

```
$ docker exec -it host-2 bash
# ip route del default
# ip route add default via 192.168.56.254
```

7) Teste a conectividade:

- Execute o ping do host-1 para o fw
- Execute o ping do host-1 para o host-2

Inserindo Regras de Firewall (Iptables)

8) Conecte em um terminal no host-1 e deixe o ping ativado com destino ao host-2 para visualizar quando o bloqueio for efetivado:

```
$ docker exec -it host-1 bash
# ping 192.168.57.10
```

9) Conecte em um terminal no firewall e bloqueie todos os pacotes que são repassados (política default = DROP):

```
$ docker exec -it fw bash
# iptables -P FORWARD DROP
```

10) Acesse o terminal onde está executando o host-1 e verifique que o ping não responde mais!!!