



documentação


REGRAS FIREWALL

Instituto Federal Catarinense - Videira

Aluno: Vítor Farias

04/06/2024

Professora: Angelita Rettore

 regras definidas em
<https://github.com/info-ifc-vda/seguranca-angelita/blob/main/labs/lab-firewall.md>.

Regras Caliandra - script e explicações.

SCRIPT:

```
$ firewall-caliandrash
1  #!/bin/bash
2
3  echo 1 > /proc/sys/net/ipv4/ip_forward
4
5  # Configuração de rotas de rede
6  ip route del default
7  ip route add default via 172.0.1.1
8  ip route add 172.0.3.0/24 via 172.0.2.3
9
10 # Permitir todo o tráfego de saída para a Internet
11 iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
12
13 # Permitir conexões HTTP e HTTPS de entrada da RedePan para a Internet (portas 80 e 443)
14 iptables -A FORWARD -p tcp -d 172.0.2.6 -m multiport --dports 80,443 -j ACCEPT
15
16 # Permitir conexões DNS de entrada e saída (porta 53)
17 iptables -A FORWARD -p udp -d 172.0.2.7 --dport 53 -j ACCEPT
18
19 # Permitir tráfego SMTP e IMAP de entrada para e-mail (portas 465, 587, 995, 143, 993)
20 iptables -A FORWARD -p tcp -d 172.0.2.0/24 -m multiport --dports 465,587,995,143,993 -j ACCEPT
21
22 # Restringir o acesso ao banco de dados. Somente o servidor de Aplicações pode acessar o banco de dados postgresql (porta 5432)
23 iptables -A FORWARD -p tcp -s 172.0.2.10 -d 172.0.2.9 --dport 5432 -j ACCEPT
24 iptables -A FORWARD -d 172.0.2.9 -j DROP # Bloquear todo o tráfego para o servidor de banco de dados que não atenda à regra acima
25
26 # Restringir o acesso ao Servidor de Aplicações à Subredelocal
27 iptables -A FORWARD -s 172.0.3.0/24 -d 172.0.2.10 -j ACCEPT
28 iptables -A FORWARD -d 172.0.2.10 -j DROP # Bloquear todo o tráfego para o servidor de aplicações que não atenda à regra acima
29
30 # Permitir tráfego entre subredes internas
31 iptables -A FORWARD -s 172.0.2.0/24 -d 172.0.2.0/24 -j ACCEPT
32 iptables -A FORWARD -d 172.0.2.0/24 -j DROP # Bloquear todo o tráfego de entrada que não atenda à regra acima
33
34 # Configuração padrão para aceitar tráfego de forwarding, necessário revisar conforme a política de segurança
35 iptables -P FORWARD ACCEPT
36
37 # Registrar tentativas de conexões bloqueadas para análise e monitoramento de segurança
38 iptables -A FORWARD -j LOG --log-prefix "Firewall: "
```

EXPLICAÇÕES:

1 - Habilitar o Encaminhamento de Pacotes IPv4

- Habilita o encaminhamento de pacotes IPv4 para permitir que o sistema funcione como um roteador.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2 - Configuração de Rotas de Rede

- Remove a rota padrão existente.
- Define uma nova rota padrão via 172.0.1.1.
- Adiciona uma rota específica para a sub-rede 172.0.3.0/24 através do gateway 172.0.2.3.

```
ip route del default
ip route add default via 172.0.1.1
ip route add 172.0.3.0/24 via 172.0.2.3
```

3 - Permitir Todo o Tráfego de Saída para a Internet

- Aplica mascaramento (NAT) ao tráfego de saída na interface `eth0`, permitindo que os dispositivos internos acessem a Internet com o endereço IP público da interface `eth0`.

```
iptables -t nat -A POSTROUTING -o eth0
-j MASQUERADE
```

4 - Permitir Conexões HTTP e HTTPS de Entrada da RedePan para a Internet

- Permite pacotes TCP destinados ao IP 172.0.2.6 nas portas 80 (HTTP) e 443 (HTTPS), permitindo acesso à web.

```
iptables -A FORWARD -p tcp -d 172.0.2.6 -m
multiport --dports 80,443 -j ACCEPT
```

5 - Permitir Conexões DNS de Entrada e Saída

- Permite pacotes UDP destinados ao IP 172.0.2.7 na porta 53, permitindo consultas DNS.

```
iptables -A FORWARD -p udp -d 172.0.2.7  
--dport 53 -j ACCEPT
```

6 - Permitir Tráfego SMTP e IMAP de Entrada para E-mail

- Permite pacotes TCP destinados à rede 172.0.2.0/24 nas portas usadas por serviços de e-mail (SMTP, IMAP).

```
iptables -A FORWARD -p tcp -d 172.0.2.0/24  
-m multiport --dports 465,587,995,143,993  
-j ACCEPT
```

7 - Restringir o Acesso ao Banco de Dados

- Permite apenas que o servidor de aplicações (172.0.2.10) acesse o banco de dados PostgreSQL no servidor 172.0.2.9 na porta 5432. Todo outro tráfego para 172.0.2.9 é bloqueado.

```
iptables -A FORWARD -p tcp -s 172.0.2.10  
-d 172.0.2.9 --dport 5432 -j ACCEPT  
  
iptables -A FORWARD -d 172.0.2.9 -j DROP
```

8 - Restringir o Acesso ao Servidor de Aplicações

- Permite apenas que dispositivos na sub-rede 172.0.3.0/24 acessem o servidor de aplicações em 172.0.2.10. Todo outro tráfego para 172.0.2.10 é bloqueado.

```
iptables -A FORWARD -s 172.0.3.0/24  
-d 172.0.2.10 -j ACCEPT
```

```
iptables -A FORWARD -d 172.0.2.10  
-j DROP
```

9 - Permitir Tráfego entre Sub-redes Internas

- Permite o tráfego interno dentro da sub-rede 172.0.2.0/24. Todo outro tráfego destinado a essa sub-rede é bloqueado.

```
iptables -A FORWARD -s 172.0.2.0/24  
-d 172.0.2.0/24 -j ACCEPT  
  
iptables -A FORWARD -d 172.0.2.0/24  
-j DROP
```

10 - Configuração Padrão para Aceitar Tráfego de Forwarding

- Define a política padrão para aceitar o encaminhamento de pacotes. Esta configuração deve ser revisada conforme a política de segurança da organização.

```
iptables -P FORWARD ACCEPT
```

11 - Registrar Tentativas de Conexões Bloqueadas

- Registra todas as tentativas de conexões bloqueadas para análise e monitoramento de segurança, prefixando os logs com "Firewall: ".

```
iptables -A FORWARD -j LOG  
--log-prefix "Firewall: "
```

Regras Caiman - script e explicações.

SCRIPT:

```
$ firewall-caiman.sh
1  #!/bin/bash
2
3  # Habilita o encaminhamento de pacotes IP no kernel
4  echo 1 > /proc/sys/net/ipv4/ip_forward
5
6  # Configuração de roteamento padrão
7  ip route del default
8  ip route add default via 172.0.2.2
9
10 # NAT para tráfego saindo pelo eth0
11 iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
12
13 # Permitir conexões de saída da estação de trabalho para a Internet para HTTP, HTTPS (portas 80 e 443)
14 iptables -A FORWARD -p tcp -s 172.0.3.0/24 -m multiport --dports 80,443 -j ACCEPT
15
16 # Permitir tráfego de saída para serviços de e-mail (SMTP, IMAP, POP nas portas 465, 587, 995, 143, 993)
17 iptables -A FORWARD -p tcp -s 172.0.3.0/24 -m multiport --dports 465,587,995,143,993 -j ACCEPT
18
19 # Restringir o acesso ao banco de dados. Somente o servidor de Aplicações pode acessar o banco de dados postgresql (porta 5432)
20 iptables -A FORWARD -d 172.0.2.9 -j DROP
21
22 # Restringir o acesso às portas 80 e 443 da SubredeLocal
23 iptables -A FORWARD -p tcp -d 172.0.3.0/24 -m multiport --dports 80,443 -j DROP
24 iptables -A FORWARD -p udp -d 172.0.3.0/24 -m multiport --dports 80,443 -j DROP
25
26 # Restringir o acesso ao Servidor de Aplicações à SubredeLocal
27 iptables -A FORWARD -s 172.0.3.0/24 -d 172.0.2.10 -j ACCEPT
28 iptables -A FORWARD -d 172.0.2.10 -j DROP
29
30 # Permitir todo o tráfego entre a rede local e a Internet
31 iptables -A FORWARD -s 172.0.3.0/24 -d 172.0.2.0/24 -j ACCEPT
32 iptables -A FORWARD -s 172.0.2.0/24 -d 172.0.3.0/24 -j ACCEPT
33
34 # Bloquear qualquer acesso direto da Internet para a estação de trabalho
35 iptables -A FORWARD -d 172.0.3.0/24 -j DROP
36
37 # Política padrão para aceitar o tráfego de FORWARD (deve ser revisado para maior segurança)
38 iptables -P FORWARD ACCEPT
```

EXPLICAÇÕES:

1 - Habilitar o Encaminhamento de Pacotes IPv4

- Habilita o encaminhamento de pacotes IPv4 para permitir que o sistema funcione como um roteador.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2 - Configuração de Roteamento Padrão

- Remove a rota padrão existente.
- Define uma nova rota padrão via 172.0.2.2.

```
ip route del default
ip route add default via 172.0.2.2
```

3 - NAT para Tráfego Saindo pelo `eth0`

- Aplica mascaramento (NAT) ao tráfego de saída na interface `eth0`, permitindo que os dispositivos internos acessem a Internet com o endereço IP público da interface `eth0`.

```
iptables -t nat -A POSTROUTING -o
eth0 -j MASQUERADE
```

4 - Permitir Conexões de Saída da Estação de Trabalho para a Internet

- Permite pacotes TCP provenientes da sub-rede 172.0.3.0/24 destinados às portas 80 (HTTP) e 443 (HTTPS), permitindo acesso à web.

```
iptables -A FORWARD -p tcp -s 172.0.3.0/24
-m multiport --dports 80,443 -j ACCEPT
```

5 - Permitir Tráfego de Saída para Serviços de E-mail

- Permite pacotes TCP provenientes da sub-rede 172.0.3.0/24 destinados às portas usadas por serviços de e-mail (SMTP, IMAP, POP).

```
iptables -A FORWARD -p tcp -s 172.0.3.0/24
-m multiport --dports 465,587,995,143,993
-j ACCEPT
```

6 - Restringir o Acesso ao Banco de Dados

- Bloqueia todo o tráfego destinado ao servidor de banco de dados em 172.0.2.9, exceto para conexões específicas permitidas (nenhuma especificada no script atual, então presume-se bloqueio total).

```
iptables -A FORWARD -d 172.0.2.9 -j DROP
```

7 - Restringir o Acesso às Portas 80 e 443 da Subrede Local

- Bloqueia pacotes TCP e UDP destinados à sub-rede 172.0.3.0/24 nas portas 80 e 443.

```
iptables -A FORWARD -p tcp -d 172.0.3.0/24  
-m multiport --dports 80,443 -j DROP
```

```
iptables -A FORWARD -p udp -d 172.0.3.0/24  
-m multiport --dports 80,443 -j DROP
```

8 - Restringir o Acesso ao Servidor de Aplicações

- Permite apenas que dispositivos na sub-rede 172.0.3.0/24 acessem o servidor de aplicações em 172.0.2.10. Todo outro tráfego para 172.0.2.10 é bloqueado.

```
iptables -A FORWARD -s 172.0.3.0/24 -d  
172.0.2.10 -j ACCEPT
```

```
iptables -A FORWARD -d 172.0.2.10 -j DROP
```

9 - Permitir Todo o Tráfego entre a Rede Local e a DMZ

- Permite tráfego bidirecional entre a sub-rede local (172.0.3.0/24) e a DMZ (172.0.2.0/24).


```
iptables -A FORWARD -s 172.0.3.0/24 -d  
172.0.2.0/24 -j ACCEPT
```

```
iptables -A FORWARD -s 172.0.2.0/24 -d  
172.0.3.0/24 -j ACCEPT
```

10 - Bloquear Qualquer Acesso Direto da Internet para a Estação de Trabalho

- Bloqueia todo o tráfego destinado à sub-rede 172.0.3.0/24 vindo da Internet.

```
iptables -A FORWARD -d 172.0.3.0/24  
-j DROP
```

11 - Política Padrão para Aceitar o Tráfego de Forwarding

- Define a política padrão para aceitar o encaminhamento de pacotes. Esta configuração deve ser revisada conforme a política de segurança da organização.

```
iptables -P FORWARD ACCEPT
```