



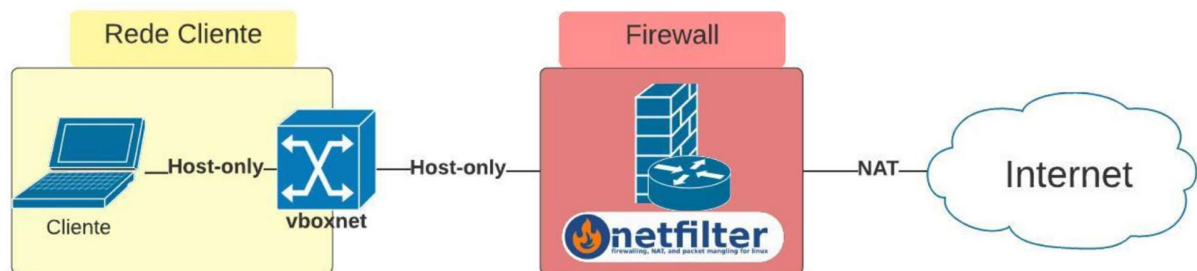
Universidade Federal do Ceará

Disciplina: Segurança da Informação

Professor: Marcos Dantas Ortiz

Exercícios – Iptables

- 1) Criar regras necessárias para implantar as seguintes políticas de segurança no Firewall, utilizando cenário de rede virtualizado (virtualbox):



Obs.: adicione nas respostas as regras e os prints dos tráfegos (quando possível)

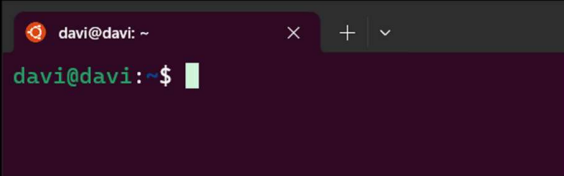
- a) Permitir o acesso ao firewall via SSH.

Testar: `ssh user@ip_do_firewall`

```
davi@davi:~$ sudo iptables-save
# Generated by iptables-save v1.8.7 on Fri Aug 23 16:17:24 2024
*filter
:INPUT DROP [6:1962]
:FORWARD DROP [318:19364]
:OUTPUT DROP [676:70056]
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
COMMIT
```

```
davi@davi:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-08-21 23:30:12 UTC; 17min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 643 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 686 (sshd)
      Tasks: 1 (limit: 2219)
     Memory: 6.7M
        CPU: 130ms
   CGroup: /system.slice/ssh.service
           └─686 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 21 23:30:11 davi systemd[1]: Starting OpenBSD Secure Shell server...
Aug 21 23:30:12 davi sshd[686]: Server listening on 0.0.0.0 port 22.
Aug 21 23:30:12 davi sshd[686]: Server listening on :: port 22.
Aug 21 23:30:12 davi systemd[1]: Started OpenBSD Secure Shell server.
Aug 21 23:44:13 davi sshd[1240]: Accepted password for davi from 192.168.243.1 port 62136 ssh2
Aug 21 23:44:13 davi sshd[1240]: pam_unix(sshd:session): session opened for user davi(uid=1000) by
lines 1-19/19 (END)
```



b) Por padrão, o Firewall deve descartar todos os pacotes. (Política DROP)

```
davi@davi:~$ history | grep DROP
 98 sudo iptables -P INPUT DROP OUTPUT DROP FORWARD DROP
 99 sudo iptables -P INPUT DROP
100 sudo iptables -P OUTPUT DROP
101 sudo iptables -P FORWARD DROP
131 history | grep DROP
davi@davi:~$ _

davi@davi:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
davi@davi:~$ _
```

c) Permitir o tráfego loopback no host do firewall.

Testar com ping (ICMP) para o próprio host - 127.0.0.1

```
-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
```

```
davi@davi:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.167 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.270 ms
^C
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.043/0.135/0.270/0.091 ms
davi@davi:~$
```

- d) Habilitar a realização de pings do Firewall para uma máquina remota na Internet.

Testar com ping (ICMP) do cliente para o firewall

```
davi@davi-firewall:~$ sudo iptables-save | grep icmp
-A INPUT -p icmp -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
davi@davi-firewall:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=46.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=46.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 46.697/48.873/53.180/3.045 ms
davi@davi-firewall:~$
```

```
davi@davi-client:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=47.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=48.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=48.9 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 47.147/48.025/48.889/0.711 ms
davi@davi-client:~$
```

- e) Permitir que o firewall faça requisições DNS.

Testar com nslookup

```
davi@davi-firewall:~$ sudo iptables-save | grep 53
[sudo] password for davi:
:FORWARD DROP [845:49534]
-A INPUT -p udp -m udp --sport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
davi@davi-firewall:~$ nslookup google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.78.206
Name:   google.com
Address: 2800:3f0:4004:802::200e
```

- f) Permitir que o firewall faça requisições HTTP.

Testar com wget

```
davi@davi-firewall:~$ sudo iptables-save | grep 80
-A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
davi@davi-firewall:~$ wget http://httpforever.com/
--2024-08-25 19:01:43-- http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0:
:1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 5124 (5.0K) [text/html]
Saving to: 'index.html.1'

index.html.1      100%[=====>]  5.00K  --.-KB/s   in 0s

2024-08-25 19:01:44 (149 MB/s) - 'index.html.1' saved [5124/5124]

davi@davi-firewall:~$
```

- g) Permitir que o host do firewall faça requisições HTTPS.

Testar com wget

```
davi@davi-firewall:~$ sudo iptables-save | grep 443
-A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
davi@davi-firewall:~$ wget https://dontpad.com/testes
--2024-08-25 19:07:18-- https://dontpad.com/testes
Resolving dontpad.com (dontpad.com)... 76.76.21.21
Connecting to dontpad.com (dontpad.com)|76.76.21.21|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3276 (3.2K) [text/html]
Saving to: 'testes'

testes            100%[=====>]  3.20K  --.-KB/s   in 0s

2024-08-25 19:07:18 (47.8 MB/s) - 'testes' saved [3276/3276]

davi@davi-firewall:~$
```

- h) Rejeite o envio de e-mails a partir do host do firewall.

```
davi@davi-firewall:~$ sudo iptables-save | grep REJECT
-A OUTPUT -p tcp -m tcp --dport 25 -j REJECT --reject-with icmp-port-unreachab
le
-A OUTPUT -p tcp -m tcp --dport 465 -j REJECT --reject-with icmp-port-unreacha
ble
-A OUTPUT -p tcp -m tcp --dport 587 -j REJECT --reject-with icmp-port-unreacha
ble
davi@davi-firewall:~$
```


i) Repita os itens d) a h) para tráfego da rede cliente para máquinas remotas na Internet.

d)

```
davi@davi-firewall:~$ sudo iptables-save | grep "p icmp"
-A INPUT -p icmp -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
davi@davi-firewall:~$
```

```
davi@davi-client:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=47.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=49.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=47.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 47.017/47.951/49.246/0.945 ms
davi@davi-client:~$
```

e)

```
root@davi-firewall: /home/davi# iptables-save | grep "port 53"
-A INPUT -p udp -m udp --sport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 53 -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -p udp -m udp --sport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
root@davi-firewall: /home/davi#
```

```
davi@davi-client:~$ nslookup google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.79.174
Name:   google.com
Address: 2800:3f0:4004:802::200e
```

f)

```
davi@davi-firewall:~$ sudo iptables-save | grep "port 80"
-A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -p tcp -m tcp --sport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
davi@davi-firewall:~$
```

```
davi@davi-client:~$ wget http://httpforever.com/
--2024-08-25 19:20:11-- http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0:
:1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 5124 (5.0K) [text/html]
Saving to: 'index.html'

index.html      100%[=====>]  5.00K  --.-KB/s    in 0.001s

2024-08-25 19:20:11 (3.70 MB/s) - 'index.html' saved [5124/5124]
```

g)

```
davi@davi-firewall:~$ sudo iptables-save | grep 443
-A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -p tcp -m tcp --sport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
davi@davi-firewall:~$
```

```
davi@davi-client:~$ wget https://donthpad.com/testes
--2024-08-25 19:22:54-- https://donthpad.com/testes
Resolving donthpad.com (donthpad.com)... 76.76.21.21
Connecting to donthpad.com (donthpad.com)|76.76.21.21|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3276 (3.2K) [text/html]
Saving to: 'testes'

testes          100%[=====>]  3.20K  --.-KB/s    in 0s

2024-08-25 19:22:55 (26.7 MB/s) - 'testes' saved [3276/3276]

davi@davi-client:~$
```

h)

```
davi@davi-firewall:~$ sudo iptables-save | grep REJECT
-A FORWARD -i enp0s8 -o enp0s3 -p tcp -m tcp --dport 25 -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -i enp0s8 -o enp0s3 -p tcp -m tcp --dport 465 -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -i enp0s8 -o enp0s3 -p tcp -m tcp --dport 587 -j REJECT --reject-with icmp-port-unreachable
```