

Tecnologias Avançadas de Redes

3º Trabalho

Compreensão do framework NETFILTER



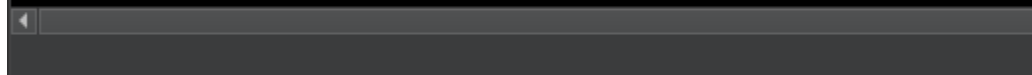
Aluno: João Dragovic nº48015

Docente: Pedro Ribeiro

Neste trabalho pretende-se que se obtenha prática com a gestão de tabelas e regras associadas ao módulo Linux NETFILTER, entendendo o modelo de operação deste nos processos de filtragem de pacotes e NAT.

```
root@deb11-client:~# ping -c 3 172.16.0.14
PING 172.16.0.14 (172.16.0.14) 56(84) bytes of data.
64 bytes from 172.16.0.14: icmp_seq=1 ttl=64 time=0.222 ms
64 bytes from 172.16.0.14: icmp_seq=2 ttl=64 time=0.365 ms
64 bytes from 172.16.0.14: icmp_seq=3 ttl=64 time=0.246 ms

--- 172.16.0.14 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.222/0.277/0.365/0.062 ms
root@deb11-client:~#
```



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 20 14:40:40 WEST 2023 on tty1
root@deb11-router:~# ping -c 3 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=47 time=5.34 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=47 time=2.75 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=47 time=2.50 ms

--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.499/3.528/5.340/1.285 ms
root@deb11-router:~#
```

Figura 1 - Confirmação dos Pings (Cliente-Router e Router-Internet)

1-O cliente não possui conectividade devido a não conhecer o caminho até a internet, a rota é desconhecida:

```
root@deb11-client:~# ping -c 3 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.

--- 1.1.1.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2028ms

root@deb11-client:~# _
```

Figura 2 - Ping do Cliente Até "Internet" sem router configurado

2. Concluimos que devido aos comandos feitos na alínea anterior o cliente conseguiu ter conexão à “internet”, e com este comando conseguimos ver os detalhes sobre a conexão ping, como está na figura:

```
root@deb11-client:~# ping -c 3 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=16.2 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=501 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=27.8 ms

--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 16.215/181.776/501.283/225.975 ms
root@deb11-client:~#
```

Figura 3 - Ping do Cliente até a "Internet" com router configurado.

```
root@deb11-router:~# tcpdump -pn -i any icmp
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
10:32:49.834431 eth1 In IP 172.16.0.1 > 1.1.1.1: ICMP echo request, id 47027, seq 1, length 64
10:32:49.834455 eth0 Out IP 10.0.3.15 > 1.1.1.1: ICMP echo request, id 47027, seq 1, length 64
10:32:49.850314 eth0 In IP 1.1.1.1 > 10.0.3.15: ICMP echo reply, id 47027, seq 1, length 64
10:32:49.850338 eth1 Out IP 1.1.1.1 > 172.16.0.1: ICMP echo reply, id 47027, seq 1, length 64
10:32:50.834990 eth1 In IP 172.16.0.1 > 1.1.1.1: ICMP echo request, id 47027, seq 2, length 64
10:32:50.835007 eth0 Out IP 10.0.3.15 > 1.1.1.1: ICMP echo request, id 47027, seq 2, length 64
10:32:51.336041 eth0 In IP 1.1.1.1 > 10.0.3.15: ICMP echo reply, id 47027, seq 2, length 64
10:32:51.336058 eth1 Out IP 1.1.1.1 > 172.16.0.1: ICMP echo reply, id 47027, seq 2, length 64
10:32:51.835228 eth1 In IP 172.16.0.1 > 1.1.1.1: ICMP echo request, id 47027, seq 3, length 64
10:32:51.835245 eth0 Out IP 10.0.3.15 > 1.1.1.1: ICMP echo request, id 47027, seq 3, length 64
10:32:51.862861 eth0 In IP 1.1.1.1 > 10.0.3.15: ICMP echo reply, id 47027, seq 3, length 64
10:32:51.862878 eth1 Out IP 1.1.1.1 > 172.16.0.1: ICMP echo reply, id 47027, seq 3, length 64
```

Figura 4 - Análise do ping feito do cliente para a internet

3. Com estes comandos feitos observamos que o primeiro pacote é apanhado na “rede” da regra OUTPUT, o que significa que qualquer pacote que sai pelo output é aceite:

```
[1:84] -A OUTPUT -j ACCEPT
```

Como o primeiro pacote foi aceite os outros seguem pela regra ESTABLISHED, pois agora os cliente apenas podem receber tráfego dessa ACL:

```
[9:756] -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Também podemos ver que na parte do NAT foi feita uma conexão:

```
:OUTPUT ACCEPT [1:84]
:POSTROUTING ACCEPT [1:84]
```

4. Neste output temos uma ligação UDP, e 3 pacotes gerados e enviados a partir do router. Também vemos que já houve 4 ACCEPTS o que quer dizer que 4 pacotes foram aceites pois mais nenhuma regras os acusou.

```
[0:0] -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
[0:0] -A INPUT -m pkttype --pkt-type multicast -j ACCEPT
[0:0] -A INPUT -m pkttype --pkt-type broadcast -j ACCEPT
[0:0] -A INPUT -m limit --limit 6/min --limit-burst 20 -j LOG
[0:0] -A INPUT -j DROP
[0:0] -A FORWARD -o eth0 -p udp -m udp --sport 1024:65535 --dport 53 -j ACCEPT
[1:76] -A FORWARD -i eth0 -p udp -m udp --sport 53:65535 --dport 1024:65535 -j ACCEPT
[0:0] -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
[0:0] -A FORWARD -m conntrack --ctstate RELATED -j ACCEPT
[0:0] -A FORWARD -i eth0 -p tcp -m tcp --sport 20 --dport 1024:65535 -j ACCEPT
[0:0] -A FORWARD -o eth0 -p tcp -m tcp --sport 1024:65535 --dport 21 -j ACCEPT
[0:0] -A FORWARD -p icmp -j ACCEPT
[1:76] -A FORWARD -p udp -j ACCEPT
[0:0] -A FORWARD -p tcp -j ACCEPT
[0:0] -A FORWARD -m limit --limit 6/min --limit-burst 20 -j LOG
[0:0] -A FORWARD -j ACCEPT
[41:2779] -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
[0:0] -A OUTPUT -m conntrack --ctstate RELATED -j ACCEPT
[4:258] -A OUTPUT -j ACCEPT
COMMIT
# Completed on Fri Apr 21 11:07:17 2023
# Generated by iptables-save v1.8.7 on Fri Apr 21 11:07:17 2023
*nat
:PREROUTING ACCEPT [1:76]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [3:201]
:POSTROUTING ACCEPT [3:201]
:eth0_internal_masq - [0:0]
[0:0] -A PREROUTING -i eth0 -p tcp -m tcp --dport 122 -j DNAT --to-destination 172.16.0.1:22
[1:76] -A POSTROUTING -s 172.16.0.0/12 -o eth0 -j eth0_internal_masq
[1:76] -A eth0_internal_masq -p udp -j MASQUERADE
[0:0] -A eth0_internal_masq -p tcp -j MASQUERADE
[0:0] -A eth0_internal_masq -p icmp -j MASQUERADE
[0:0] -A eth0_internal_masq -j MASQUERADE
```

5. O contador UDP incrementou de 0 para 1 pois foi preciso usar DNS para ir buscar o IP do site inserido, pois o DNS usa UDP.

6.Observamos que até este ponto já houve 4 conexões UDP e também 15 pacotes foram gerados e enviados do router (OUTPUT, POSTROUTING).

```
[0:0] -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
[0:0] -A INPUT -m pkttype --pkt-type multicast -j ACCEPT
[0:0] -A INPUT -m pkttype --pkt-type broadcast -j ACCEPT
[0:0] -A INPUT -m limit --limit 6/min --limit-burst 20 -j LOG
[0:0] -A INPUT -j DROP
[0:0] -A FORWARD -o eth0 -p udp -m udp --sport 1024:65535 --dport 53 -j ACCEPT
[4:304] -A FORWARD -i eth0 -p udp -m udp --sport 53:65535 --dport 1024:65535 -j ACCEPT
[0:0] -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
[0:0] -A FORWARD -m conntrack --ctstate RELATED -j ACCEPT
[0:0] -A FORWARD -i eth0 -p tcp -m tcp --sport 20 --dport 1024:65535 -j ACCEPT
[0:0] -A FORWARD -o eth0 -p tcp -m tcp --sport 1024:65535 --dport 21 -j ACCEPT
[0:0] -A FORWARD -p icmp -j ACCEPT
[4:304] -A FORWARD -p udp -j ACCEPT
[0:0] -A FORWARD -p tcp -j ACCEPT
[0:0] -A FORWARD -m limit --limit 6/min --limit-burst 20 -j LOG
[0:0] -A FORWARD -j ACCEPT
[41:2779] -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
[0:0] -A OUTPUT -m conntrack --ctstate RELATED -j ACCEPT
[61:3801] -A OUTPUT -j ACCEPT
COMMIT
# Completed on Fri Apr 21 11:17:09 2023
# Generated by iptables-save v1.8.7 on Fri Apr 21 11:17:09 2023
*nat
:PREROUTING ACCEPT [4:304]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [15:1044]
:POSTROUTING ACCEPT [15:1044]
:eth0_internal_masq - [0:0]
[0:0] -A PREROUTING -i eth0 -p tcp -m tcp --dport 122 -j DNAT --to-destination 172.16.0.1:22
[4:304] -A POSTROUTING -s 172.16.0.0/12 -o eth0 -j eth0_internal_masq
[4:304] -A eth0_internal_masq -p udp -j MASQUERADE
[0:0] -A eth0_internal_masq -p tcp -j MASQUERADE
[0:0] -A eth0_internal_masq -p icmp -j MASQUERADE
[0:0] -A eth0_internal_masq -j MASQUERADE
COMMIT
```

7.Este passo não foi possível executar, sem perceber como exatamente.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:92:20:5c brd ff:ff:ff:ff:ff:ff
    altname enp0s8
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic eth0
        valid_lft 81043sec preferred_lft 81043sec
    inet6 fe80::a00:27ff:fe92:205c/64 scope link
        valid_lft forever preferred_lft forever
```

```
root@deb11-client:~# ssh tar@10.0.3.15 -p 22
ssh: connect to host 10.0.3.15 port 22: No route to host
root@deb11-client:~# ssh tar@10.0.3.15 -p 122
ssh: connect to host 10.0.3.15 port 122: No route to host
```

Conclusão

Neste trabalho foi necessário a consulta e aplicação dos conhecimentos aprendidos nas aulas relativamente ao NETFILTER para observar e entender o que cada comando faz e aplicá-lo.

Bibliografia

- PDF sobre ACLs disponibilizado pelo professor.
- www.networklessons.com
- [Man page of IPSET \(netfilter.org\)](http://netfilter.org/man/iptables/)
- [netfilter/iptables project homepage - Documentation about the netfilter/iptables project](http://netfilter.org/iptables/project/homepage)
- [iptables Tutorial 1.2.2 \(frozentux.net\)](http://frozentux.net/iptables-tutorial-1.2.2/)