FSI LEI 2025/2026

Practical Exercises #3 Resolution examples

Goals

Configure network packet filtering and NAT using IPTables

Configure network packet filtering and NAT using IPTables

- Configure a Linux system to operate as a router (by **enabling packet forwarding**) between two IPv4 networks: 10.254.0.0/24 (representing the internal network) and 172.16.1.0/24 (the external network).

```
Para controlar o forwarding de pacotes:
systemctl -w net.ipv4.ip_forward=1
ou
echo 1 > /proc/sys/net/ipv4/ip_forward
ou
adicionar linha "net.ipv4.ip_forward = 1" a /etc/sysctl.conf
```

- **Clear** your IPTables (firewall) configuration

```
iptables -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

- Create a network firewall configuration to implement the following **security policy**:

  Authorize the following communications between the two networks (**direct IP communications**, therefore without NAT):

  - DNS queries from hosts on the internal network to DNS servers on the external network.
  - Network time synchronization requests from hosts on the internal network to NTP servers on the external network.

```
iptables -A FORWARD -s 10.254.0.0/24 -d 172.16.1.0/24 -p udp --dport
domain -j ACCEPT
iptables -A FORWARD -d 10.254.0.0/24 -s 172.16.1.0/24 -p udp --sport
domain -j ACCEPT

iptables -A FORWARD -s 10.254.0.0/24 -d 172.16.1.0/24 -p udp --dport
ntp -j ACCEPT
iptables -A FORWARD -d 10.254.0.0/24 -s 172.16.1.0/24 -p udp --sport
ntp -j ACCEPT
```

  Authorize the following communications between the two networks using SNAT (**Source NAT**):

  - SSH, HTTP and HTTPS connections from hosts on the internal network to servers on the external network.

```
iptables -A FORWARD -s 10.254.0.0/24 -d 172.16.1.0/24 -p tcp --dport
ssh -j ACCEPT
iptables -A FORWARD -s 10.254.0.0/24 -d 172.16.1.0/24 -p tcp --dport
http -j ACCEPT
iptables -A FORWARD -s 10.254.0.0/24 -d 172.16.1.0/24 -p tcp --dport
https -j ACCEPT
```

Materials

- Red Hat Enterprise Linux Security Guide: 2.8 Firewalls
- The netfilter.org Project
- Linux 2.4 Packet Filtering HOWTO
- Gestão de Sistemas e Redes em Linux, Jorge Granjal, FCA 2010/2013, "Capítulo 12. O Linux como router e firewall"
- Segurança em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, "Capítulo 8. Proteção de Redes"

```
# Neste caso optamos por autorizar de forma mais geral os pacotes
# de ligações já estabelecidas, como alternativa a autorizar seletivamente
# para cada aplicação
iptables -A FORWARD -s 172.16.1.0/24 -p tcp ! --syn -j ACCEPT

 # Outras estratégias alternativas para autorizar o retorno das ligações:
#  • Autorizar recorrendo ao "--sport"
#  • Autorizar recomendo ao módulo de estado:
#  "-m state --state RELATED,ESTABLISHED"

iptables -t nat -A POSTROUTING -s 10.254.0.0/24 -d 172.16.1.0/24 -p
tcp --dport ssh -j SNAT –to-source 172.16.1.254
iptables -t nat -A POSTROUTING -s 10.254.0.0/24 -d 172.16.1.0/24 -p
tcp --dport http -j SNAT –to-source 172.16.1.254
iptables -t nat -A POSTROUTING -s 10.254.0.0/24 -d 172.16.1.0/24 -p
tcp --dport https -j SNAT –to-source 172.16.1.254
```

- FTP connections from hosts on the internal network to a server on the external network (in passive and active modes).

```
Nesta aplicação é necessário adicionar regras para lidar com os modos
passivo e ativo do FTP, bem como ativar os necessários módulos de
"connection tracking", fazendo também uso do "-m state --state
RELATED,ESTABLISHED"
```

Authorize the following communications between the two networks using DNAT (**Destination NAT**):

- SSH connections from hosts on the external network to the IP address of the external interface of the router, which should be redirected to a host on the internal network.

```
iptables -t nat -A PREROUTING -s 172.16.1.0/24 -d 172.16.1.254 -p tcp --
dport ssh -j DNAT –to-destination 10.254.0.1
iptables -A FORWARD -s 172.16.1.0/24 -d 10.254.0.1 -p tcp --dport ssh -j
ACCEPT
iptables -A FORWARD -d 172.16.1.0/24 -s 10.254.0.1 -p tcp --sport ssh -j
ACCEPT
```

All remaining IP communications should be **dropped** by the firewall.

```
iptables -P FORWARD DROP
```

- Test your firewall configuration, e.g. using the **netcat** (**nc**) utility

```
Testes com netcat, no modo cliente:

nc -v <ip address of server> <tcp port>

nc -v -u <ip address of server> <udp port>
```

Testes com netcat, no modo servidor:

nc -v -l <tcp port>

nc -v -l -u <udp port>