STI MEI/MIEBIOM 2022/2023

Practical Exercises #5

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).

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

- 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.

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

  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.

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

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

Goals

Configure network packet filtering and NAT using IPTables

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"