17GIIN - NETWORK FUNDAMENTALS

Activity # 4 – Competency Unit 4

Activity:

Firewall Implementation and TCP/IP Network Monitoring

Degree in Computer Engineering

Professor José Pirrone

April, 2025

viu Universidad Internacional de Valencia

CONTENT

INTRODUCTION

Computer and communications security is crucial in the implementation and operation of computer networks. While this topic can reach a significant level of complexity (so much so that it would require a separate course for that topic), this Network Fundamentals course takes an introductory approach, focusing primarily on the topic of ***firewalls*** (firewall), and two key functions to be fulfilled by these elements: the **packet filtering** and the **address translation**.

Packet filtering refers to the action of accepting or denying the passage of a network packet through the firewall, depending on the criteria that can be programmed into the firewall. In most cases, these criteria will depend on values that can be read in the packet headers, at all levels of the protocol stack. Thus, rules can be programmed that take into account basic parameters such as: **source or destination addresses** (MAC at the link layer, IP at the network layer, ports at the transport layer, etc.), to more complex parameters such as fragmentation fields in the IP header, TCP flags at the transport layer, source and destination subnets, etc.

By address translation (*Network Address Translation*, NAT) we understand the possibility of changing the destination IP addresses (DNAT or *Destination NAT*) for redirecting packets to destinations other than those indicated by the packet-generating node; or the source IP addresses (SNAT or *Source NAT*), for "masking" the source addresses encoded in the packets.

To put all this into practice, the GNU/Linux-based platform that has been worked on throughout the course is proposed, this time using a new command: ***iptables***.
The proposed activity for this last unit of competence will then be based on the use of this command for programming packet filtering and NAT rules on a modification of Activity # 2.

Additionally, the topic of monitoring TCP/IP networks will be worked on. With the SNMP protocol (*Simple Network Management Protocol*) will be activated **SNMP agents** in the critical elements of the network (firewall, router and servers), and a monitoring station with an NMS will be implemented (*Network Management System*) from which these critical elements will be monitored.

Activity description

1. Implementing packet filtering and NAT in a Firewall

For implementation, it is proposed to resume the topology of activity # 2 and make the following modifications:

1. Router R1 will now become a*Firewall*, on which packet filtering and address translation (NAT) rules will be programmed, which are specified below.

2. The client (host) on LAN1 will become a**monitoring station**, for which the NMS PRTG will be installed (https://www.paessler.com/prtg).

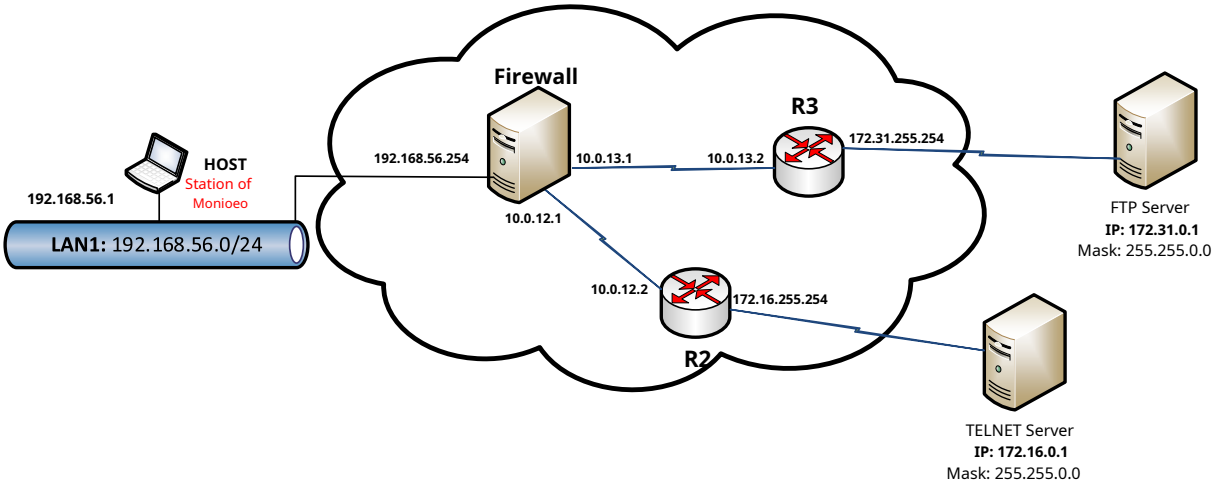

Figure 1: Activity topology with the inclusion of a firewall and a monitoring station

1. It is requested to implement the following rules:**packet filtering**ON THE FIREWALL:

- Block pings (ICMP protocol) against the firewall.
- Deny pings to the FTP server only from LAN1.
- Allow pings against the TELNET server.
- Allow connections to the FTP service at 172.31.0.1 and the TELNET service at 172.16.0.1. (NOTE: Disable any other services that are not applicable on each server. That is, the FTP server should NOT have any processes listening on port 23/TCP (Telnet), and the TELNET server should NOT have any processes listening on ports 20/TCP or 21/TCP (FTP))

2. It is requested to implement the following rules:**DNAT**ON THE FIREWALL:

- All connections from LAN1,**directed to the FTP service**(ports 20 and 21 over TCP) with a destination IP**different from 172.31.0.1**, should be redirected to this IP.
- All transmissions from any LAN, directed to the TELNET service (port 23 over TCP) with a destination IP**different from 172.16.0.1**, should be redirected to this IP.

2. Implementation of Monitoring with SNMP (Optional)

In order to implement monitoring of critical network elements, the following is required:

1. Implement SNMP agents on critical elements: FIREWALL, routers (R2 and R3) and servers.

2. Deploy PRTG NMS on the host:https://www.paessler.com/prtg
3. Configure the NMS to monitor, using the SNMP protocol, the following parameters (at least) on the requested critical elements:
    a. % CPU usage
    b. % hard disk occupancy
    c. % RAM usage
    d. Network connection status (connected or not connected)

Description of the delivery method

Develop a**PRESENTATION**(delivered in .PPT or .PDF formats) with the following parts:

- Front page.
- Index.
- Introduction.
- Description of the implementation process for the topology in Figure 1. (Suggestion: Use tables to list commands, where applicable)
    - either Host implementation.
    - either Implementation of the firewall and all its interfaces.
    - either Commands used to configure IP addresses in each element.
    - either Installing SNMP agents. Installing
    - either the NMS.
- Description of the configuration of packet filtering rules.
- Description of NAT Rule Configuration
- Description of SNMP Agent Configuration
- Description of NMS configuration.
- Conclusions.

GRADES :

- Please accompany the presentation explanations with screenshots where appropriate.

- Upload the presentation in the section**Activities**scheduled on the virtual campus.
- Proposed deadline:**Wednesday, May 16, 2025**