PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004

Department of Applied Mathematics and Computational Sciences

M. Sc (CS) - Semester 5

CONTINUOUS ASSESSMENT TEST 1 Date: 28-October 2025

23XC51 – Network Security

25

Time: 1 hour 30 min. **Maximum Marks: 40**

INSTRUCTIONS:

1. Answer **ALL** questions. Each question carries 20 Marks.
2. Subdivision (a) (i) and (ii) carries 2 marks each, subdivision (b) carries 6 marks each and subdivision (c) carries 10 marks each.
3. Course Outcome Table :

Qn.1	CO.3

Qn.2	CO.5

1.a.(i) Propose a counter measure for SYN flooding. **[L2]** 1

a.(ii) Ilustrate a diagram to evade firewall using VPN along with the flow of informations. **[L4]** 1

b. Design a TCP reset attack on Telnet connections. Give the Scapy code. How to perform reset attack on SSH connections and Video streaming [L4] 4

C. Outline the TLS programming overview for Client and Server. Implement a client program to communicate with real-world web server **example.com** using the TLS protocol and print the Cipher Suite used, TLS Version and the server side certificate of example.com. **[L5]** 8

2.a.(i) Give the applications built on Netfilter framework. **[L2]** 2

a.(ii) Give a rule using iptables conntrack module to drop new connections if a single IP address attempts to open more than 50 simultaneous TCP connections, helping to mitigate DoS attacks**[L4]**. 1

b) Discuss on the types of IDS. What are the performance metrics for evaluating IDS? How to evade an IDS?[L2] 4

C . (i) Consider the diagram below where a packet filtering firewall (FW1) is running on router R2. The "internal" networks are on the left of the firewall (that is, connected to interface 1 of router R2). Each IP network is identified by a letter (e.g. "Network A"), and each host on a particular network is identified by a number (e.g. **"Host A.4"**). You can refer to "any" value using * (e.g. **"A .* "** meaning all hosts on network A). For the following scenarios, complete the necessary firewall rules in the table provided **[L5]** 5

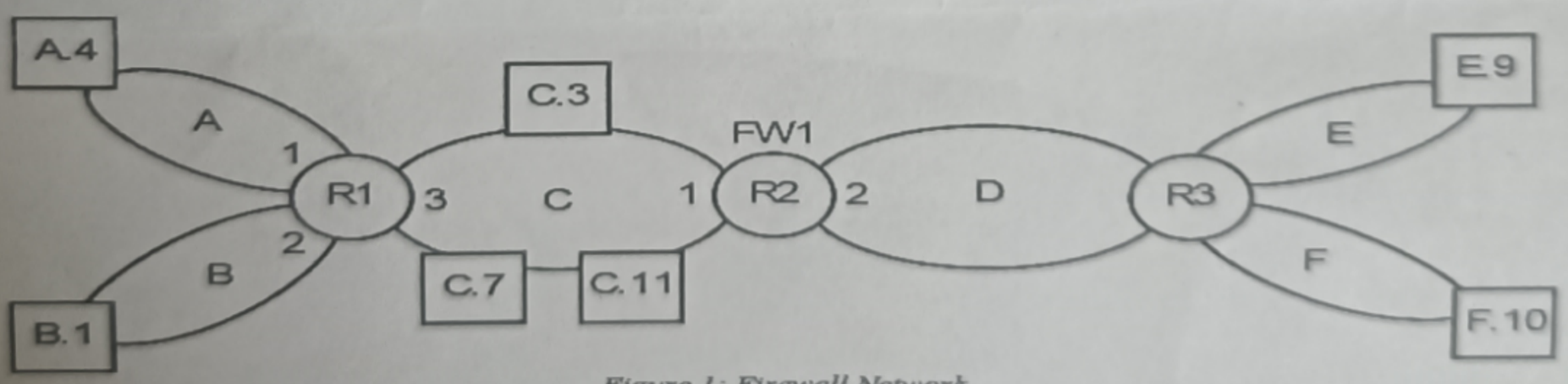

Figure 1: Firewall Network

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

I. Allow all internal hosts to connect to all web servers (0.5)
II. Allow all hosts on network F to connect to SSH server on C.7 (0.5)
III. Allow all hosts on network C , except the servers **C.3** and **C.7** to connect to all email servers. (1)
IV. Block all DNS traffic from any source to any destination. Using IP blocks both DNS name resolution queries on UDP port 53 and DNS zone transfers on TCP port 53. You could also implement this was two separate rules with one for UDP and one for TCP.(2)
V. Rule for default deny(1)

c.(ii). Illustrate and explain the packet Traversal Path in IPtable through the different Chains.(5) **[L2]**