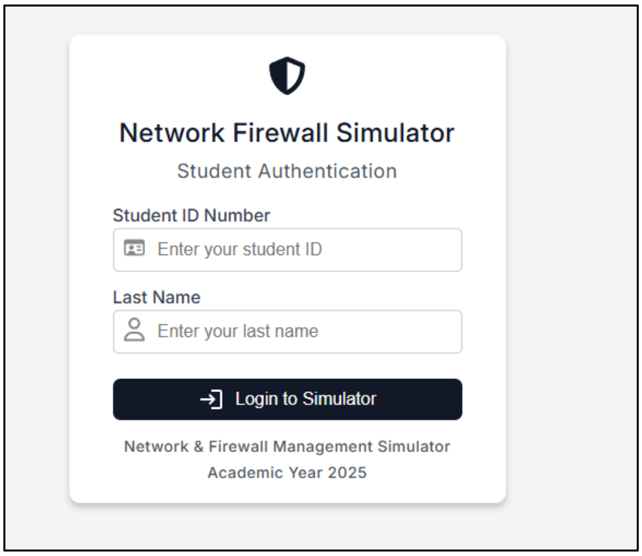
User Guide

1. Login

- The application uses a student ID system

- Enter your student ID (must be between 270000 and 280000) and your surname(last name)

- The system will automatically create a session for you



Network Firewall Simulator

Student Authentication

Student ID Number

Enter your student ID

Last Name

Enter your last name

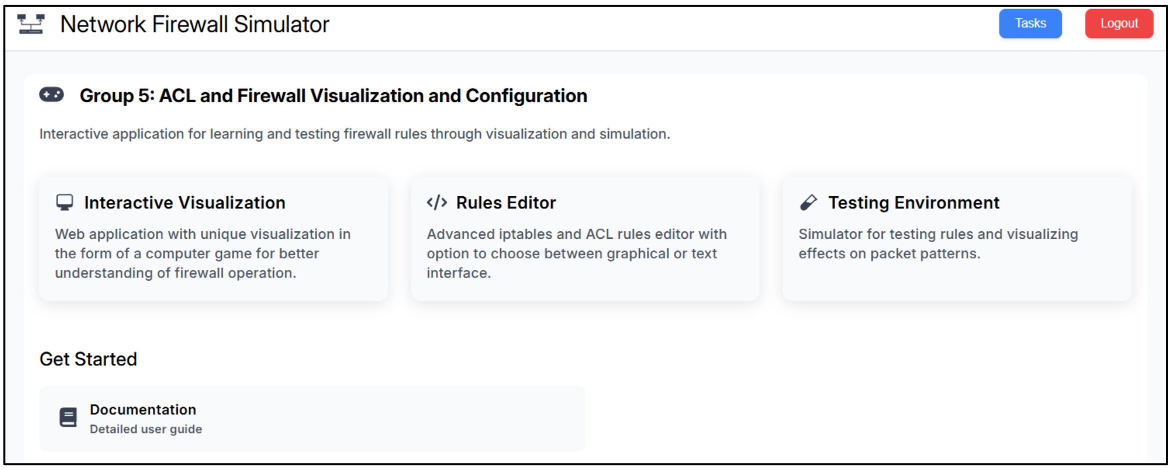
Network & Firewall Management Simulator

Academic Year 2025

2. Main Interface

The main interface consists of several key components:

- Navigation bar with access to different sections (tasks/logout or “network firewall simulator to go back to Main”)



Group 5: ACL and Firewall Visualization and Configuration

Interactive application for learning and testing firewall rules through visualization and simulation.

Interactive Visualization

Web application with unique visualization in the form of a computer game for better understanding of firewall operation.

Rules Editor

Advanced iptables and ACL rules editor with option to choose between graphical or text interface.

Testing Environment

Simulator for testing rules and visualizing effects on packet patterns.

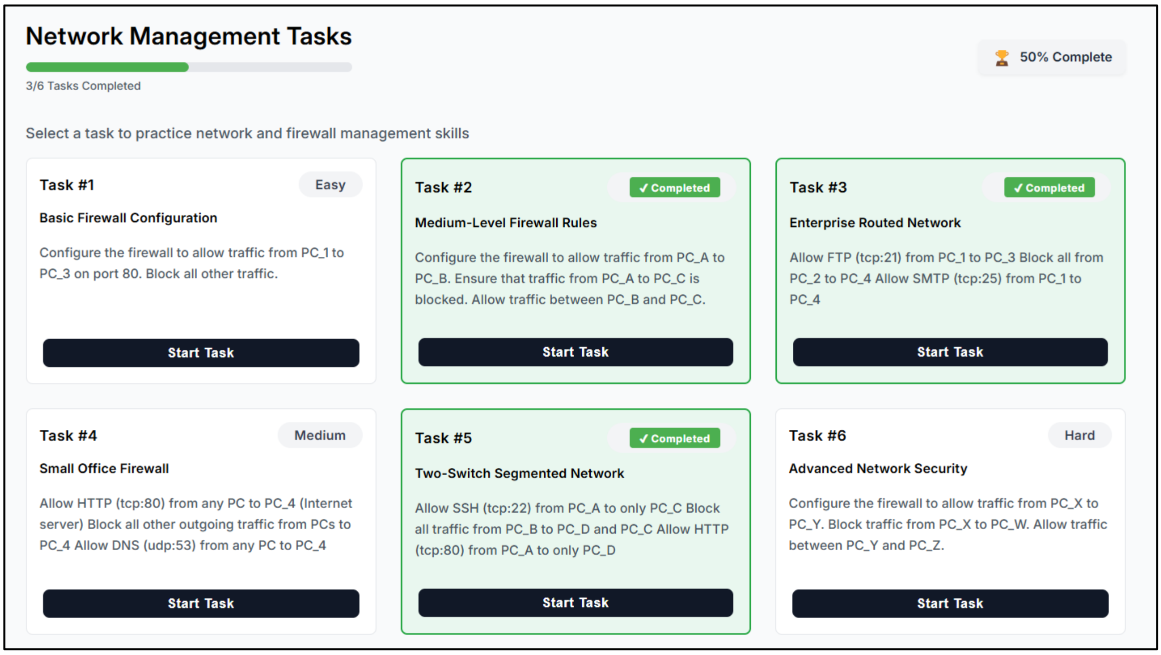
Get Started

Documentation

Detailed user guide

3. Tasks

The simulator includes multiple tasks of varying difficulty:



Network Management Tasks

3/6 Tasks Completed

50% Complete

Select a task to practice network and firewall management skills

Task #1 — Easy

Basic Firewall Configuration

Configure the firewall to allow traffic from PC_1 to PC_3 on port 80. Block all other traffic.

Start Task

Task #2 — ✓ Completed

Medium-Level Firewall Rules

Configure the firewall to allow traffic from PC_A to PC_B. Ensure that traffic from PC_A to PC_C is blocked. Allow traffic between PC_B and PC_C.

Start Task

Task #3 — ✓ Completed

Enterprise Routed Network

Allow FTP (tcp:21) from PC_1 to PC_3 Block all from PC_2 to PC_4 Allow SMTP (tcp:25) from PC_1 to PC_4

Start Task

Task #4 — Medium

Small Office Firewall

Allow HTTP (tcp:80) from any PC to PC_4 (Internet server) Block all other outgoing traffic from PCs to PC_4 Allow DNS (udp:53) from any PC to PC_4

Start Task

Task #5 — ✓ Completed

Two-Switch Segmented Network

Allow SSH (tcp:22) from PC_A to only PC_C Block all traffic from PC_B to PC_D and PC_C Allow HTTP (tcp:80) from PC_A to only PC_D

Start Task

Task #6 — Hard

Advanced Network Security

Configure the firewall to allow traffic from PC_X to PC_Y. Block traffic from PC_X to PC_W. Allow traffic between PC_Y and PC_Z.

Start Task

4. Using the Console

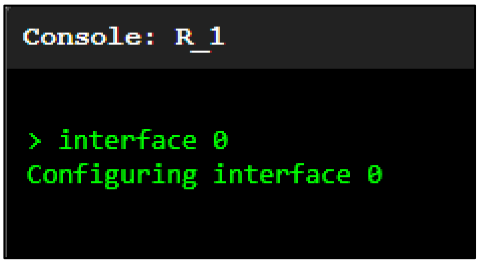
The console interface allows you to configure network devices:

Available Commands:

1. Interface Configuration:

interface <number>

- Switches to interface configuration mode
- Used to configure specific network interfaces



```
Console: R_1

> interface 0
Configuring interface 0
```

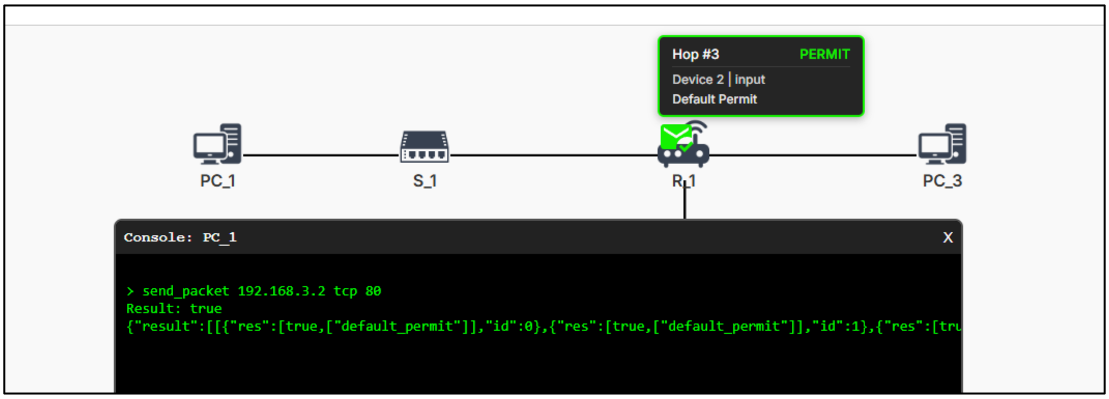
2. Packet Testing:

send_packet <destination_device_id> <protocol> <port>

- Tests network connectivity

- Example:

on PC_1 ` send_packet 192.168.3.2 tcp 80`

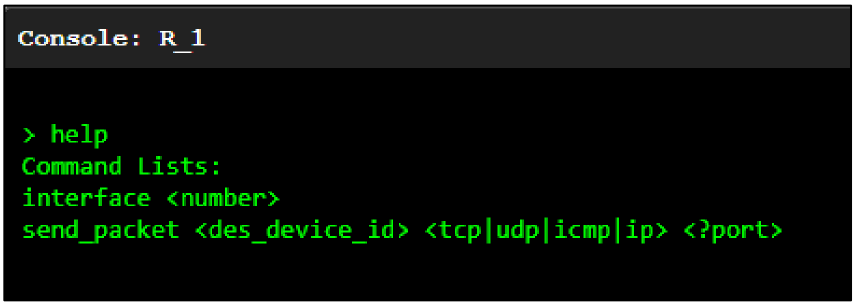


```
> send_packet 192.168.3.2 tcp 80
Result: true
{"result":[[{"res":[true,["default_permit"]],"id":0},{"res":[true,["default_permit"]],"id":1},{"res":[tru
```

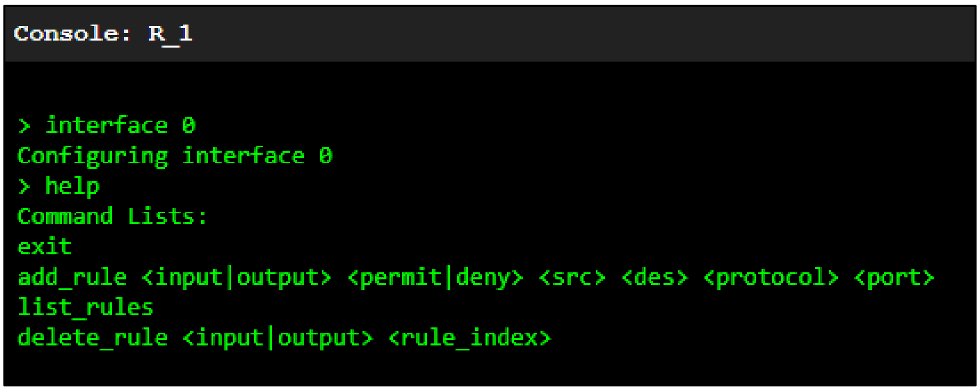
3. Help Command:

help

- Displays available commands for the current context



```
> help
Command Lists:
interface <number>
send_packet <des_device_id> <tcp|udp|icmp|ip> <?port>
```



```
> interface 0
Configuring interface 0
> help
Command Lists:
exit
add_rule <input|output> <permit|deny> <src> <des> <protocol> <port>
list_rules
delete_rule <input|output> <rule_index>
```

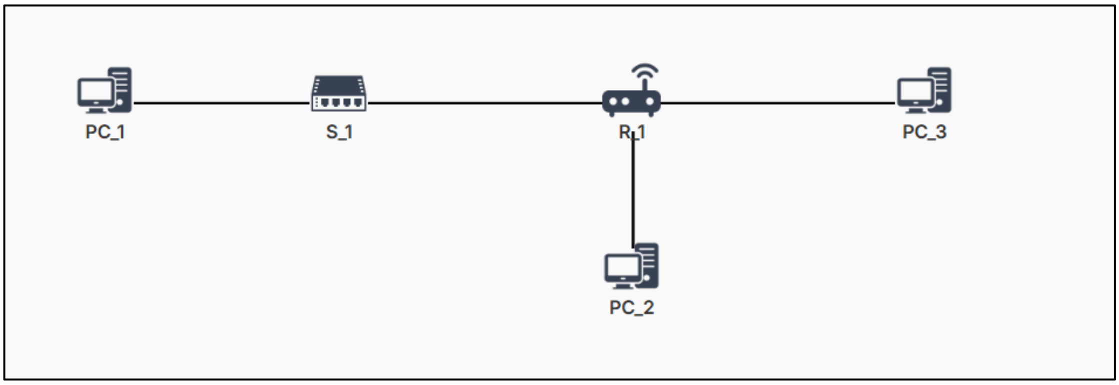
4. Network Topology

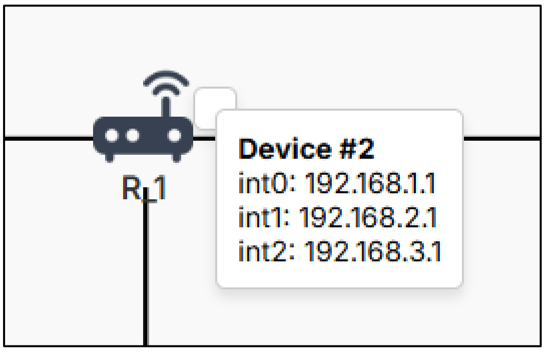
- The topology view shows all network devices and their connections

- Connections are shown as lines between devices

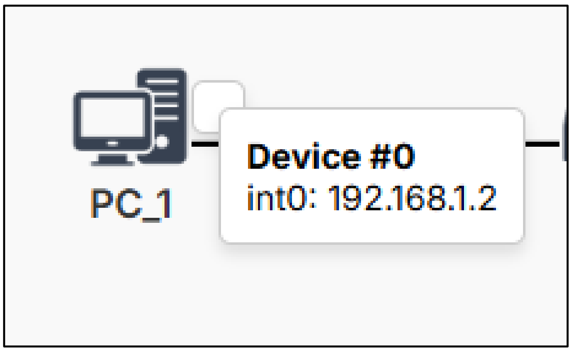
- Click on devices to access their configuration

- Hover on devices to display their interfaces and IP’s





Device #2
int0: 192.168.1.1
int1: 192.168.2.1
int2: 192.168.3.1



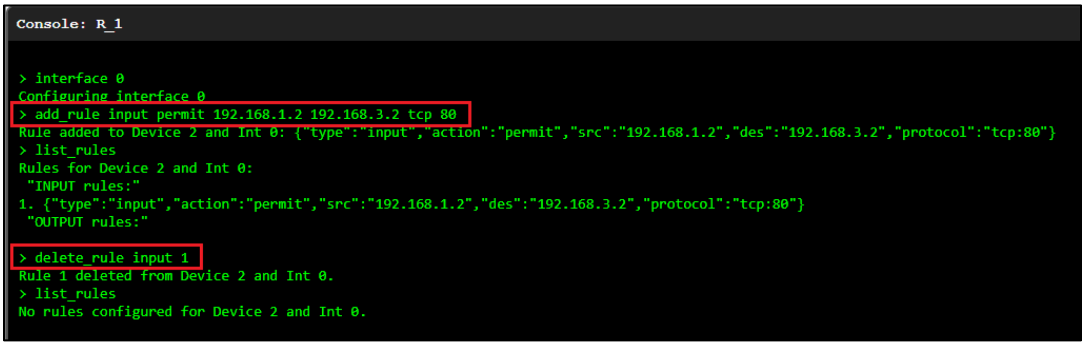
Device #0
int0: 192.168.1.2

5. Firewall Rules

When configuring firewall rules, you can:

- Add new rules

- Remove rules



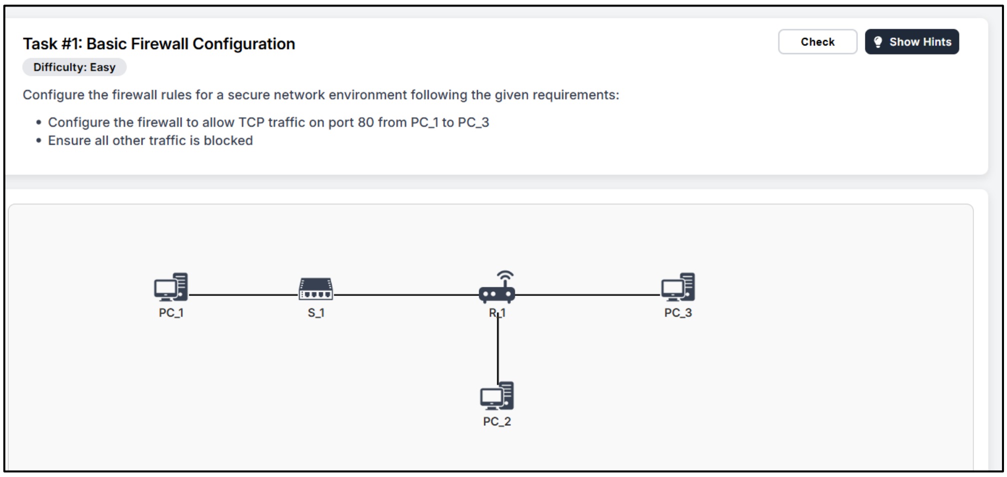
```
Console: R_1

> interface 0
Configuring interface 0
> add_rule input permit 192.168.1.2 192.168.3.2 tcp 80
Rule added to Device 2 and Int 0: {"type":"input","action":"permit","src":"192.168.1.2","des":"192.168.3.2","protocol":"tcp:80"}
> list_rules
Rules for Device 2 and Int 0:
 "INPUT rules:"
1. {"type":"input","action":"permit","src":"192.168.1.2","des":"192.168.3.2","protocol":"tcp:80"}
 "OUTPUT rules:"

> delete_rule input 1
Rule 1 deleted from Device 2 and Int 0.
> list_rules
No rules configured for Device 2 and Int 0.
```

6. Testing Your Configuration

Use the built-in Check to validate your configuration



Task #1: Basic Firewall Configuration

Difficulty: Easy

Configure the firewall rules for a secure network environment following the given requirements:

- Configure the firewall to allow TCP traffic on port 80 from PC_1 to PC_3
- Ensure all other traffic is blocked

Additional Resources

- Use the hints provided in each task

- Refer to the task description for specific requirements