**INFORMATION SECURITY**



**Session 2023 - 2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza Iqbal

**Course:**

Information Security

Department of Computer Science

**University of Engineering and Technology**

**Lahore Pakistan**

Contents

[ Basic Rules 3](#_Toc196038217)

[ Advanced Rules 3](#_Toc196038218)

**Assignment 3: Firewall Practice Set**

# Basic Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule No. | Action | Protocol | Source IP | Destination IP | Port(s) | Description |
| 1 | Allow | TCP | Any | 192.168.1.100 | 80, 443 | Allow HTTP/HTTPS to web server |
| 2 | Allow | TCP | 192.168.2.50 | 10.0.0.5 | 22 | Allow SSH from specific IP |
| 3 | Allow | TCP | 10.1.1.20 | Any | 25 | Allow SMTP from internal mail server |
| 4 | Deny | Any | 192.168.3.0/24 | Any | Any | Block all from specific IP range |
| 5 | Allow | UDP | Any | 8.8.8.8 | 53 | Allow DNS to DNS server |

# Advanced Rules

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule No. | Action | Protocol | Source IP | Destination IP | Port(s) | Description |
| 1 | Allow | TCP | Any | Web Server IP | 80, 443 | HTTP/HTTPS from any source |
| 2 | Allow | TCP | Specific IP | Server IP | 22 | SSH from specific IP |
| 3 | Allow | TCP | Internal Mail IP | Any | 25 | SMTP to internet |
| 4 | Deny | Any | 192.168.3.0/24 | Any | Any | Block incoming from range |
| 5 | Allow | UDP | Any | 8.8.8.8 | 53 | DNS from any source |
| 6 | Allow | TCP | Specific IP | FTP Server IP | 21 | FTP from specific user IP |
| 7 | Allow | ICMP | Any | Host IP | Echo Req. | Allow ping to host |
| 8 | Allow | TCP/UDP | Any | Server IP | Specific | Allow specific port |
| 9 | Allow | Any | Internal Network | Specific IP/Domain | Any | Allow outbound to specific destination |
| 10 | Deny | TCP | Any | Internal Network | Ports | Block sensitive ports |
| 11 | Limit | TCP/UDP | Any | Service IP | Port | Rate limit for service |
| 12 | Allow | Any | Country IP Block | Network | Any | Geo-based access |
| 13 | Allow | UDP | Internal Network | VoIP Provider IP | Ports | VoIP outbound |
| 14 | Deny | Any | Internal Network | Domains | Ports | Block domains except on specific ports |
| 15 | Allow | TCP | Management IP | Server IP | Port | Remote access from specific IP |
| 16 | DNAT | TCP | Any | Public IP | Port | Port forward to internal IP |
| 17 | Allow | Any | Any | Any | Protocols | Allow/block by protocol/application |
| 18 | SNAT | Any | Internal Network | Internet | Any | NAT for outbound traffic |
| 19 | Allow | Any | Authenticated User | Any | Any | Traffic based on user/group |
| 20 | Allow | Any | Any | Any | Any | Schedule-based rules |