

Linux Iptables GUI Manager - User Guide

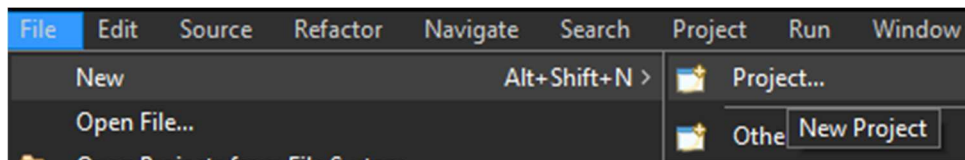
Introduction

Linux Iptables GUI Manager is a user-friendly, Java-based graphical interface designed to help users manage firewall rules using iptables. Rather than relying on complex terminal commands, users can create, view, and delete rules directly from an intuitive graphical interface. The application is ideal for system administrators and learners who want to manage their firewall configurations effectively without deep command-line knowledge.

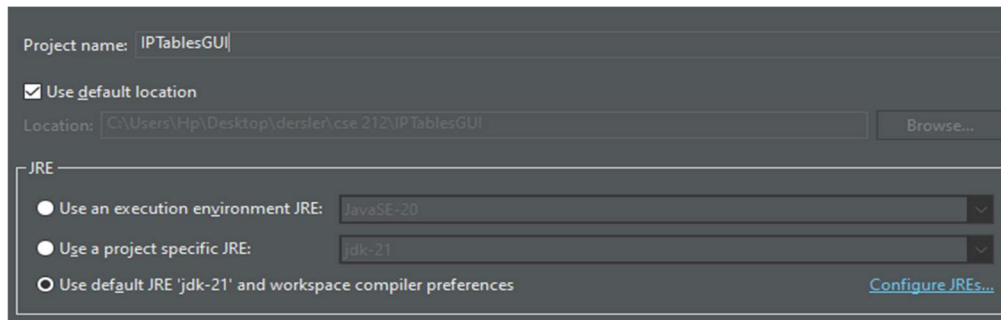
Launching the Application

To start the application using a Java IDE (such as IntelliJ IDEA, Eclipse, or NetBeans):

1. Open your preferred Java IDE.
2. Import the project or create a new project and add all source files.



Then choose the “java Project” option .

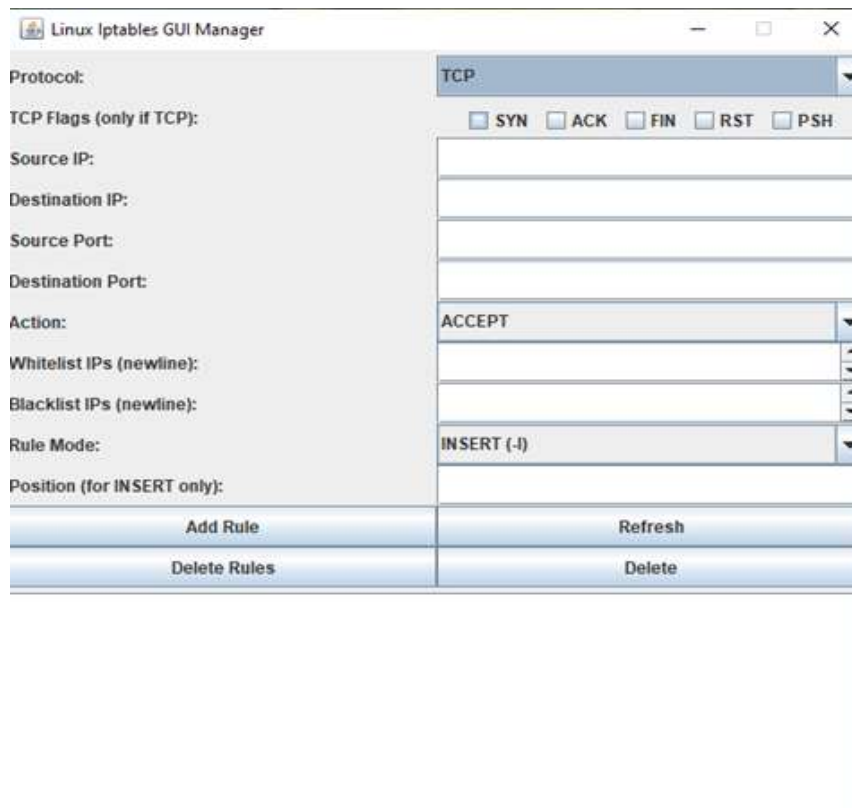


3. Ensure that your main class (e.g., Main.java) has the correct main method entry point.
4. Right-click on the Main class and select **Run 'Main'** (or the equivalent option in your IDE).
5. Upon startup, a prompt will appear asking for your sudo password. This is essential, as modifying iptables rules requires superuser privileges. Your password will be stored securely within the session and used by the program to execute privileged commands.



GUI Overview

The application window is structured into labeled fields, checkboxes, combo boxes, and buttons. Below is a detailed explanation of each section:



Section	Description
Protocol	Select the network protocol: either TCP or UDP. TCP enables additional TCP flag configuration.
TCP Flags (only if TCP)	Checkboxes for flags like SYN, ACK, FIN, etc. These are used to match specific types of TCP traffic.
Source IP / Destination IP	Enter IPv4 addresses to define where packets originate or are heading. Leave blank for wildcard (match all).
Source Port / Destination Port	Specify ports to filter traffic by application-level protocol (e.g., HTTP = 80). Leave blank to apply to all ports.
Action	Choose to ACCEPT (allow) or DROP (block) matching packets.
Whitelist IPs	A multi-line input area. Enter IPs you want to allow unconditionally. Each IP should be on a separate line.
Blacklist IPs	Similar to whitelist, but these IPs will be explicitly blocked from communication.
Rule Mode	Select either INSERT (-I) to place the rule at a specific position or APPEND (-A) to add it to the end.
Position (for INSERT only)	If INSERT is selected, you must specify the position number to place the rule in the chain.

Buttons and Their Functions

Button	Function
Add Rule	Constructs and adds a new iptables rule using the specified settings. Also applies whitelist/blacklist IPs.
Refresh	Displays the current list of active firewall rules in the text area below.
Delete Rules	Clears all configured firewall rules. Use with caution!
Delete	Prompts the user to enter the rule number (as shown in iptables -L --line-numbers) to remove a specific rule.i

Example Usage Scenarios

1. Allow HTTP Traffic (Port 80)

To allow web traffic:

- Protocol: TCP
- Destination Port: 80
- Action: ACCEPT
- Click Add Rule

2. Block a Malicious IP Address

To block traffic from a specific IP:

- Add 192.168.1.200 to the Blacklist IPs field (on a new line)
- Click Add Rule

This creates a DROP rule for the IP.

3. Insert Rule with High Priority

To insert a rule at the top:

- Rule Mode: INSERT (-I)
- Position: 1
- Fill in your rule details
- Click Add Rule

This ensures the rule has higher precedence.

Notes and Tips

- Leaving IP or port fields blank allows the rule to match all sources/destinations or ports.
- Ensure that all entered IP addresses and ports are valid. Invalid entries will be rejected.
- TCP flags are only effective when the protocol is TCP.
- The whitelist and blacklist functionality automatically translates each IP into an ACCEPT or DROP rule.
- The order of rules matters in iptables. Rules added earlier are evaluated first.