Ironclad Kernel Firewall: User Manual

Welcome to **Ironclad Kernel**, a high-performance, Zero Trust firewall powered by eBPF technology. This guide will help you install, configure, and master your new security system.

📦 1. Installation Guide

This section explains how to install the firewall on a new computer using the pre-compiled binaries.

Prerequisites

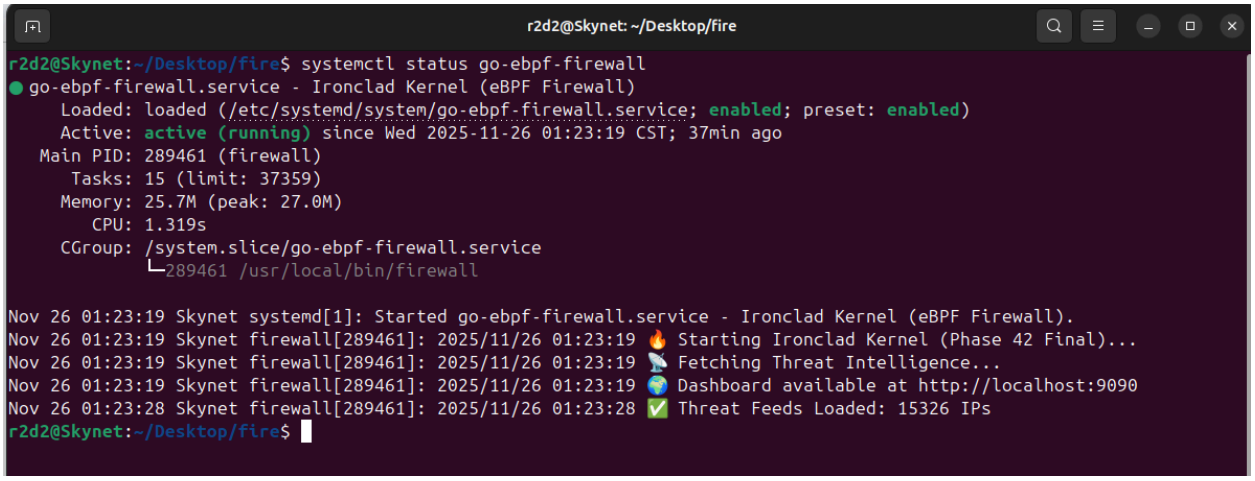
- **Operating System:** Linux (Kernel 5.8 or newer recommended).
- **Privileges:** Root access (sudo) is required.

Step-by-Step Installation

1. Transfer Files:
   Copy the two binary files (firewall and fwctl) and the installer script (install_binaries.sh) from your development machine to the target machine (same folder for all 3).
2. Run the Installer:
   On the target machine, navigate to the folder containing the files and run:
   chmod +x install_binaries.sh
   sudo ./install_binaries.sh

   This script will move the binaries to /usr/local/bin, create the configuration directory at /etc/go-ebpf-firewall, and set up the systemd service.
3. Verify Installation:
   Check if the service is running:
   sudo systemctl status go-ebpf-firewall

   You should see Active: active (running).



🛠️ 2. Patching & Updates

Applying Optional Boot Fix

If threat feeds fail to load on reboot because the network wasn't ready, run this patch script once:
chmod +x fix_boot_race.sh
sudo ./fix_boot_race.sh

This updates the systemd service to wait for a full network connection before starting the firewall.

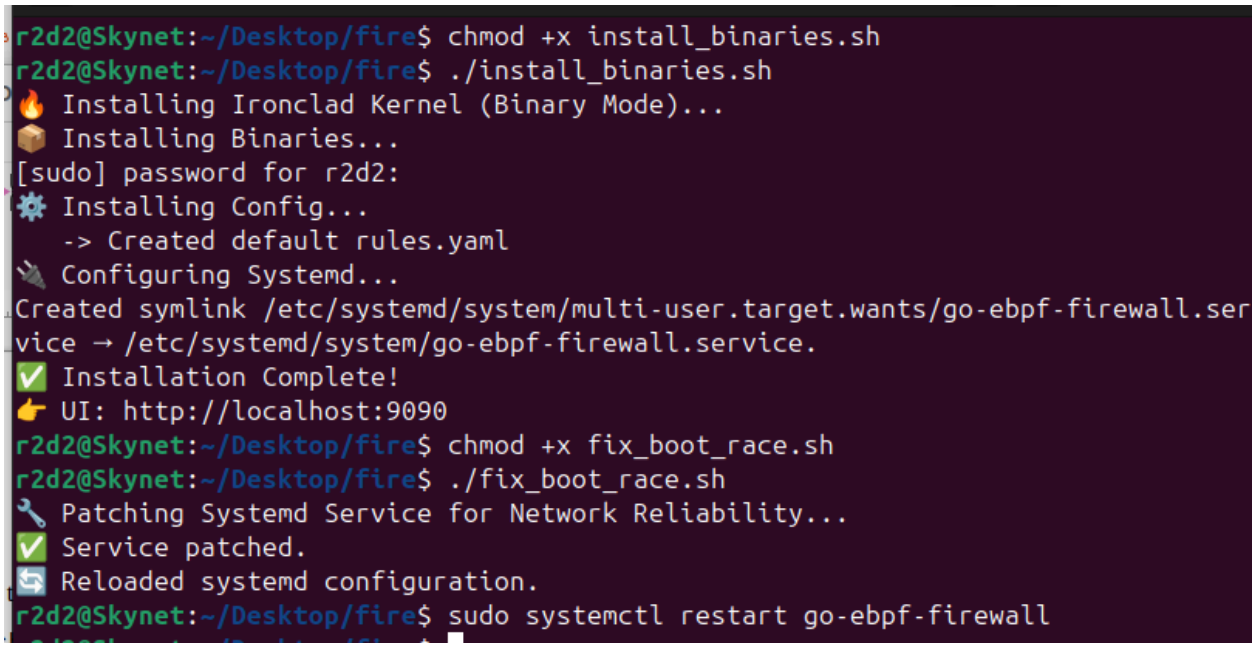
Updating the Firewall

To update to a newer version:

1. Stop the current service:
   sudo systemctl stop go-ebpf-firewall

2. Overwrite the old binaries in /usr/local/bin/ with the new ones.
3. Restart the service:
   sudo systemctl restart go-ebpf-firewall

A perfect install and update looks like this:



🖥️ 2. Using the Dashboard (UI)

The Ironclad Kernel comes with a built-in web dashboard for real-time monitoring and control.

Accessing the Dashboard

Open your web browser and navigate to:
👉 http://localhost:9090
(Note: If accessing from a remote machine, replace localhost with the server's IP address, e.g., http://192.168.1.50:9090)

Dashboard Features

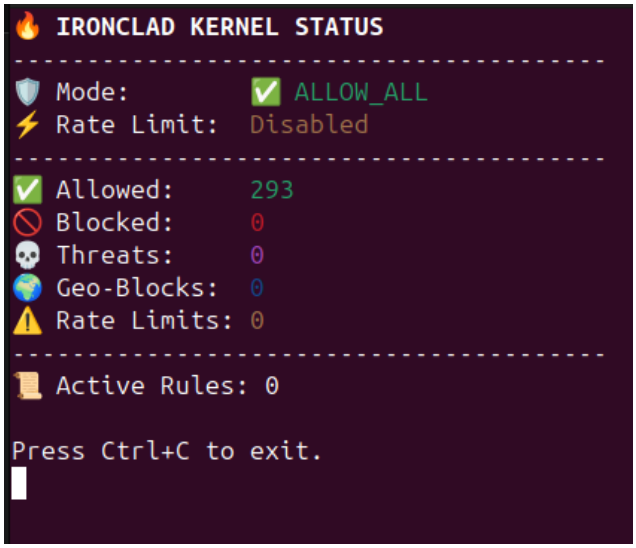
Feature	Description
🛡️ **Mode Toggle**	Switch between **Default Allow** (Green) and **Zero Trust / Default Deny** (Red). **Warning:** Zero Trust blocks *everything* not explicitly allowed.
⚡ **Rate Limit**	Use the slider to set a global connection limit (e.g., 50 conn/sec) to prevent DDoS attacks.
Traffic Overview	A real-time line chart showing allowed vs. blocked traffic volume.
Live Event Feed	A scrolling log of every connection attempt.
Action Buttons	Click **Block** next to an allowed connection to instantly ban that process.
Geo-Blocking	Enter a 2-letter Country Code (e.g., CN, RU) to block all IP addresses from that nation.
Payload Inspector	Scroll through the "Details" column to see DNS queries or TLS headers (SNI) for encrypted traffic.

⌨️ 3. CLI Command Reference

For quick checks or headless servers, use the fwctl command-line tool.

Live Monitor

View a real-time, auto-updating dashboard in your terminal (similar to top or htop).
sudo fwctl monitor



Snapshot Stats

Get a one-time dump of current statistics (useful for scripts or logs).
sudo fwctl stats

Reload Rules

Force the daemon to re-read the configuration file without restarting.
sudo fwctl reload

❓ Troubleshooting

Q: The dashboard is blank or won't load.

- **Check Status:** Is the firewall running? (sudo systemctl status go-ebpf-firewall)
- **Check Port:** Is port 9090 blocked by another firewall (like ufw)? Try sudo ufw allow 9090.
- **Check Binding:** Run sudo ss -tulpn | grep 9090 to ensure it's listening on :::9090 or 0.0.0.0:9090.

Q: I blocked everything and locked myself out!

- **Emergency Reset:** Restarting the service clears all *runtime* blocks (like Geo-blocks and manual bans) but keeps the persistent rules.yaml configuration.
  sudo systemctl restart go-ebpf-firewall

- **Manual Config Edit:** If you added a bad rule to rules.yaml, edit /etc/go-ebpf-firewall/rules.yaml manually and remove the offending line, then restart.

Q: Threat Feeds show "0 IPs".

- **Check Internet:** Does the server have internet access?
- **Check Logs:** Run sudo journalctl -u go-ebpf-firewall -f and restart the service. Look for "Fetching Threat Intelligence...". If it fails, it will log the error there.