IPFire

Your Presentation Title

An optional subtitle for more context

Your Name | IPFire Project

February 18, 2026

Agenda

Introduction

Content Examples

Closing

Introduction

Background & Motivation

What is IPFire?

IPFire is a hardened, versatile, state-of-the-art Open Source firewall based on Linux. Its ease of use, high performance in any scenario and extensibility make it usable for everyone.

- Stateful Packet Inspection (SPI) Firewall
- Intrusion Detection and Prevention
- Web Proxy with Content Filtering
- VPN support (IPsec, OpenVPN, WireGuard)

IPFire at a Glance

Designed for security

- Minimal attack surface
- Regular security updates
- Kernel hardening

Community-driven

- Open Source (GPL)
- Active mailing lists & forums
- ipfire.org

Key Principle

Security by Default

IPFire ships in a secure configuration out of the box. Administrators open only what is explicitly needed — not the other way around.

Important

Always keep your IPFire installation up to date to benefit from the latest security patches.

Content Examples

Demos, code, and data

Checking Firewall Status

You can inspect the active firewall rules from the shell:

```
# List all iptables rules with counters
iptables -nvL --line-numbers

# Check INPUT chain only
iptables -nvL INPUT

# Show NAT rules
iptables -t nat -nvL
```

How IPFire Handles a Packet

1. Packet arrives on an interface

How IPFire Handles a Packet

1. Packet arrives on an interface
2. Connection tracking checks state table

How IPFire Handles a Packet

1. Packet arrives on an interface
2. Connection tracking checks state table
3. Firewall rules evaluated top-to-bottom

How IPFire Handles a Packet

1. Packet arrives on an interface
2. Connection tracking checks state table
3. Firewall rules evaluated top-to-bottom
4. Intrusion detection inspects payload (optional)

How IPFire Handles a Packet

1. Packet arrives on an interface
2. Connection tracking checks state table
3. Firewall rules evaluated top-to-bottom
4. Intrusion detection inspects payload (optional)
5. Packet forwarded, dropped, or rejected

Stateful Inspection

IPFire tracks connection state so return traffic for established connections is allowed automatically — without explicit rules.

Closing

Summary

- IPFire is a production-ready, hardened Linux firewall distribution
- Zone-based architecture provides clear network separation
- Regular updates and an active community keep it secure
- Extensible via Add-ons without compromising core security

Get Involved

- Website: www.ipfire.org
- Development: git.ipfire.org
- Community: community.ipfire.org

Questions?

Your Name