# How to Setup IPFire Free Linux Firewall – A Step by-Step Guide

By Freak Sense


“In this post, I’ll share a step-by-step guide on how to setup IPFire Free Linux Firewall.”

IPFire Linux Firewall is an open-source high-level firewall distribution that is easy to operate and flexib enough to be used by enterprises, authorities, individuals and just about anyone. IPFire has been desi with a modularity and flexibility where it can be deployed on your network as a firewall, proxy server, gateway, DHCP server, Open VPN, monitoring and more.

Before I share how to setup IPFire, let me discuss why you should secure your network with IPFire.

# IPFire Free Linux Firewall: Highlights

“The IPFire development team understands that security means different things to different people ar certainly can change over time. The fact that IPFire is modular and flexible makes it perfect for integra any existing security architecture.

Don’t forget that ease-of-use is a key principle. If all this sounds a little too much for you, IPFire comes great default settings out-of-the-box, meaning it’s a snap to get going quickly.”

The main agenda of IPFire is security and while it forms the base of a secure network, you can easily c the firewall for the type of security that will suit you best. Here I’ll take you through brief color codes o Firewall security in IPFire.

## Stateful Packet Inspection (SPI) firewall in IPFire

IPFire implements SPI in firewall built over the Linux packet filtering framework. In the following insta guide, you’ll see that the network is configured in four segments identified by four colors.

With this segmentation, each machine will have a defined place on the network. Each color segment represents the group of computers that share the common security level on the network.

## A Brief Description of the Segments

1. **Green:** Green is the “safe area” which includes all the regular clients. Here, the clients can easily ac other segments without any restrictions.
2. **Red:** Red is considered the “danger area” or in simple words, connection to the internet. Nothing c through until specified by the administrator.
3. **Blue:** Blue segment represents the “wireless network” and because it poses a potential danger the will require explicit permission before they access the network.
4. **Orange:** Orange is the DMZ or “demilitarized zone”. Any servers which are accessible by the public separated by the rest of the network to prevent the security breaches in the network.

The latest release **IPFire 2.19 with core update 114**, the GUI has been completely rewritten and imm extended with new functionality. Now, you’ll be able to manage groups of hosts or services. This mak

simple for admin to create similar rules and use it for a great number of groups, hosts, and services.

## Other Highlights: Why You Should Install IPFire Linux Firewall

1. **Easy to Administer:** With a state-of-the-art firewall, IPFire makes it easy to administer even the mc complex networks in an enterprise.
2. **Designed Security:** IPFire has been designed with a vision of providing high security with a modul flexibility whether you're an individual or a large enterprise. You can rest assure that IPFire will be a protect the network from various types of attacks.
3. **Package Management System:** IPFire has an integrated packet management system called PakFir can update the whole system with just a single click. It is a faster and quick process to install patch bugfixes and feature enhancements that make IPFire safer and better.
4. **Higher Degree of Performance:** IPFire runs well on embedded software and has been proven to p higher degree of performance and run evenly on all kinds of software.
5. **Easy to Install:** IPFire installation takes 15-20 minutes and it is relatively easier to use for the exper features required in professional networks.
6. **Open Source:** IPFire is a free software released under GPL license. This open-source software has a community of developers and users who are working on improving it every single day.

Now, if you're interested to know more about the raft of features supported by IPFire you must check o detailed features page of the latest release.

For now, let's begin with the next section.

# How to Setup IPFire Free Linux Firewall: Recommended System Requirements (Minimur

- 512 MB RAM
- 2 GB Hard Disk Space
- 2 Network Cards (with 1 GB transfer speed)
- i586 CPU (Intel Pentium 333 MHz)

Now, that you've checked if your system is compatible with IPFire, let's get started with the setup guid

# How to Setup IPFire Free Linux Firewall: Installation Steps

In this installation guide, I'll be using the installation using a CD/DVD. However, you can also use a boo USB drive for the installation as well.

Let's begin.

1. Visit the official downloads page of the IPFire website.
2. Now, select Download IPFire 2.19 and select the appropriate ISO image file for your system and bu the CD/DVD.
3. Now, run the DVD and boot the media on your system.
4. From the screen, select Install IPFire 2.19 to start the installation.
5. Next, select the Language according to your region. Here I'll select English and click Ok.
6. In this step, you can cancel if you don't wish to proceed and reboot your system.
7. Now, accept the license and click OK to proceed. You can select the spacebar on your keyboard to s the option and then click OK.
8. In this step, you'll be issued a warning that all the data on the disk would be destroyed. Select yes t to continue and then click OK.
9. Next, you'll be asked to select the file system. Click on Ext4 and select OK.
10. Once you have selected the file system, the installation will begin. It may take up a few minutes. All data will be formatted and system files will be installed.
11. With this step, IPFire will be installed and you'll be prompted to reboot the machine. Click "Press O reboot".
12. After the system has rebooted successfully, you can proceed with the other steps to configure ISDN passwords and network cards.
13. Now, as the system reboots you'll be prompted with a menu to select the option. Select the default and press enter.
14. Now, select the type of keyboard here as per your discretion. I'll select US and click OK.
15. Here, select the time zone you're in and click OK.
16. In this step, select a hostname for firewall machine. By default, it will be ipfire. If you don't wish to any changes, click OK to proceed.
17. In this step enter the domain name. It should be a valid domain name. If you don't have one, we ca it later on. Now, click OK.
18. Here, enter the root user password for Command-line prompt. Enter a secure password twice and
19. Now, enter another password which must be different from the one you created for command-line This password will be used to log in to the IPFire web administration pages. Enter your password a OK.

20. In this step, I'll proceed with the network configuration settings of IPFire. Here, select **Network Configuration type**. I'll use 2 Ethernet cards in my IPFire Firewall system. The individual network c have to be configured separately. By default, it will pick the GREEN+RED scheme. This means that i connect to the local and WAN server with Internet access.
21. Now, select GREEN+RED for the two network cards and click OK.
22. In the network configuration menu, select Drivers and **Card Assignments** and press OK. This optio help you to select the network which will assign LAN and WAN interfaces.
23. Now, select GREEN and press SELECT to enable an interface for the two network cards.
24. Now repeat the same step for the RED interface and press DONE.
25. Here, select **Address Settings** from the menu and click OK. In this step, I'll assign the IP Addresses network interfaces. Because there are two interfaces, I'll be assigning a different IP for both from va sub-nets.

For instance, if I assign the IP address 192.168.0.100 for RED, I will have to use a different IP for the GRE
In this guide, I'll be using DHCP for the RED interface.

26. Select GREEN and click OK. You'll receive a warning. Click OK to proceed. Provide the localhost IP f which is 192.168.1.1 and click OK.
27. Select RED and click OK. Now here, click DHCP to get the IP address from the ISP provider or you ca the IP manually.
28. After selecting DHCP, press OK and then click DONE.
29. Now, select **DNS and Gateway Settings** and press OK.
30. Here, you can configure your DNS and gateway settings. For ease of user, it is better suited to leave blank and click OK.
31. Press DONE to exit from the DNS settings.
32. In this step, I'll take you through the DHCP configuration process. Here, I need to configure these se for the GREEN interface. DHCP pool range will be from **192.168.1.2 to 192.168.1.100**

**First, enable the DHCP configuration, then enter the following information if you're unsure what**

- Start address: **192.168.1.2**
- End address: **192.168.1.100**
- Primary DNS: 192.168.1.1
- Secondary DNS: 8.8.8.8
- Default lease (mins): 60
- Max Lease (mins): 120
- Domain Name Suffix:

Now click OK.

33. For the final step, press OK to complete the IPFire setup.
34. Now the computer will reboot for the final changes to take place. After the reboot, you'll get the co line access by entering the password you had set earlier during the installation process.
    Enter root as admin and your selected password.

    If entered correctly, you'll be able to access the CLI of IPFire easily.
35. To access the web interface, enter the URL which was prior used for the GREEN interface (192.168.1 your web browser. You'll be prompted to enter the password you had set for accessing the IPFire w administrator page. Click Login.
36. Once you have successfully logged in, you'll be directed to a dashboard of the IPFire web interface.

There are multiple features in the IPFire including Advanced Web proxy, Bandwidth Monitoring, Log co Memory services, DNS forwarding, DNS server, Update accelerator, Content filtering, Connection sche and a lot more.

It's up to you and your definition of "security" to enable the versatile features and functionality in the open-source IPFire Linux Firewall.

# How to Setup IPFire Free Linux Firewall: Summa

IPFire Linux Firewall is the best and most effective security solution for any individual or an enterprise network. I hope with this guide you learned how to setup IPFire free Linux firewall for your network as

Did you find this tutorial helpful or you have some questions? Drop in your quick comments below an try to help you out.

For more such articles, stay connected with Freaksense.

**Freak Sense**

*https://freaksense.com*