
SOC Analyst
Firewalls
THINKCYBER

Table of Contents

Firewalls – The Core of Network Security 3
What is a Firewall? 3
Types of Firewalls 3
What is pfSense and Why is it Widely Used? 4
pfSense Installation 6
Install pfSense on Physical Hardware 7
Install pfSense on a Virtual Machine 8
Installation Process 9
pfSense Configuration 13
Components and Their Role 13
Configuring Interfaces using pfSense Console 14
Configuring IP Addresses for Interfaces 16
Accessing the Console and Disabling the Firewall 18
Accessing the WebConfigurator 18
Basic pfSense Configuration via the Web GUI 19
Adding Rules for Service Access 27
Firewall NAT Configuration in pfSense 31
pfSense Shell Commands 34
Basic Shell Navigation and Management 34
Firewall and NAT Commands 35
System and Performance Monitoring Commands 35
User and Process Management Commands 36
Backup and Restore Commands 37
Testing and Diagnostics Commands 38
Managing Packages in pfSense 39
Introduction to the pfSense Package Manager 39
Navigating the Package Manager 39
Working with Packages: Installation and Management 40
Managing Installed Packages 41
Popular Packages and Use Cases 41
pfBlocker-NG (Ad-blocking and GeoIP Filtering) 42
ntopng (Network Traffic Analyzer) 42
OpenVPN Client Export Utility 42
Managing Packages via the Command Line 42

Firewalls – The Core of Network Security

Firewalls are an essential component of modern network security. Acting as a gatekeeper between internal and external networks, firewalls control the flow of traffic based on predefined rules. They are vital for protecting systems from unauthorized access, preventing attacks, and enforcing network segmentation.

What is a Firewall?

A firewall is a security device—either software-based or hardware-based—that monitors and controls incoming and outgoing network traffic. It acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet. Firewalls enforce **access control policies** by filtering traffic based on rules defined by the administrator. The goal is to allow legitimate traffic while blocking or restricting unauthorized or malicious connections.

Firewalls help mitigate various threats, including:

- **Unwanted traffic** from external networks
- **Unauthorized access** to internal resources
- **Distributed Denial-of-Service (DDoS) attacks**
- **Malware and malicious traffic** trying to exploit vulnerabilities in systems

Firewalls not only protect individual systems but also serve as the foundation for secure networking, including **virtual private networks (VPNs)** and **intrusion prevention systems (IPS)**.

Types of Firewalls

There are several types of firewalls, each serving specific roles in network security. Depending on the organization's needs, firewalls may be deployed at multiple points across the network to enforce security at different levels.

Packet-Filtering Firewalls

These firewalls analyze the headers of incoming and outgoing packets based on parameters such as **source and destination IP addresses, ports, and protocols**. They are efficient but limited, as they do not inspect the contents of packets beyond the header.

Stateful Inspection Firewalls

Stateful firewalls keep track of active connections and ensure that only legitimate traffic associated with established sessions is allowed through. They evaluate both packet headers and connection states, making them more secure than packet-filtering firewalls.

Application Layer Firewalls (Proxy Firewalls)

These firewalls operate at the **application layer** and inspect the content of data packets. They can block or allow traffic based on specific application behaviors, such as HTTP requests. Application firewalls

offer deeper insights into network activity, but they may introduce latency due to their processing overhead.

Next-Generation Firewalls (NGFWs)

NGFWs combine traditional firewall features with **intrusion detection (IDS)**, **intrusion prevention (IPS)**, **content filtering**, and **threat intelligence**. These firewalls provide comprehensive protection against modern cyber threats.

What is pfSense and Why is it Widely Used?

pfSense is a free, open-source firewall and router software distribution based on **FreeBSD**. Designed to be both powerful and user-friendly, pfSense provides **enterprise-level functionality** for network security, routing, and management. It can be deployed on physical hardware, virtual machines, or dedicated network appliances, making it an extremely versatile solution for both **small networks** and **large enterprise environments**.

pfSense is more than just a basic firewall; it offers **a comprehensive suite of networking and security features** that are typically found only in high-end commercial firewalls. It is widely recognized for its **ease of use**, **customizability**, and **modular architecture**. Administrators and SOC analysts rely on pfSense to **protect, manage, and monitor networks efficiently**, and its flexibility allows it to be tailored to meet specific security and performance requirements.

Key Features of pfSense

- **Firewall and Router**: At its core, pfSense provides powerful **stateful firewall capabilities** that monitor and control traffic based on rules defined by the administrator. It also functions as a **router**, enabling network segmentation, NAT (Network Address Translation), and static or dynamic routing.
- **WebGUI Interface**: pfSense's WebGUI is a standout feature, making it easy to manage the firewall and router configuration through a browser without needing to use the command line. This **user-friendly interface** makes pfSense accessible even to non-experts.
- **Advanced Security with Packages**: pfSense supports a wide range of **security-focused packages**, such as **Snort** for intrusion detection and **pfBlockerNG** for IP and domain blocking. This allows organizations to **extend pfSense's functionality** to meet evolving security needs.
- **VPN Capabilities**: pfSense offers robust **VPN support** with tools like **OpenVPN** and **IPsec**, providing secure remote access and site-to-site connectivity. It is often used by businesses to **create secure tunnels** between remote locations and to allow employees to work remotely.

- **High Availability and Load Balancing**: pfSense supports **failover and load balancing** configurations, ensuring uninterrupted network access. It can manage multiple WAN connections, automatically switching between them if one fails, making it a reliable solution for mission-critical environments.
- **Built-in Monitoring and Diagnostics**: pfSense includes **real-time monitoring tools** and detailed logs that help administrators quickly detect network issues or intrusions. The platform offers features like **packet capture**, traffic graphs, and alerts to aid in troubleshooting and security analysis.

Use Cases for pfSense

1. Small Business Firewall: pfSense is widely used by small businesses as a **cost-effective firewall solution**. With built-in VPN capabilities, it allows employees to work remotely and access internal resources securely.

2. Network Segmentation in Enterprises: Large enterprises use pfSense to **segment internal networks**, preventing lateral movement by attackers. By isolating critical systems, they reduce the attack surface.

3. ISP and Data Center Operations: Internet Service Providers (ISPs) and data centers use pfSense to manage **bandwidth, route traffic**, and provide **secure internet access** to customers.

4. Educational Institutions: Schools and universities use pfSense to implement **content filtering** and manage bandwidth, ensuring a safe and productive online environment for students.

5. Home Network Security Enthusiasts: Tech-savvy home users install pfSense on small appliances or old PCs to create **secure home networks** with advanced features like **ad-blocking**, **intrusion detection**, and **VPNs**.

pfSense Installation

Preparing for the Installation

Before starting the installation, it's essential to prepare the necessary hardware or virtual environment. pfSense can be installed on both **physical hardware** and **virtual machines**.

Hardware Requirements

To run pfSense efficiently, ensure your system meets the minimum requirements:

- **CPU**: At least 1 GHz processor (multi-core recommended for larger networks)
- **RAM**: Minimum 1 GB (2 GB or more recommended)
- **Storage**: At least 4 GB (SSD recommended for better performance)
- **Network Interface Cards (NICs)**: One NIC for WAN and one NIC for LAN. Additional NICs are required for more complex setups like multiple WANs or VLANs.

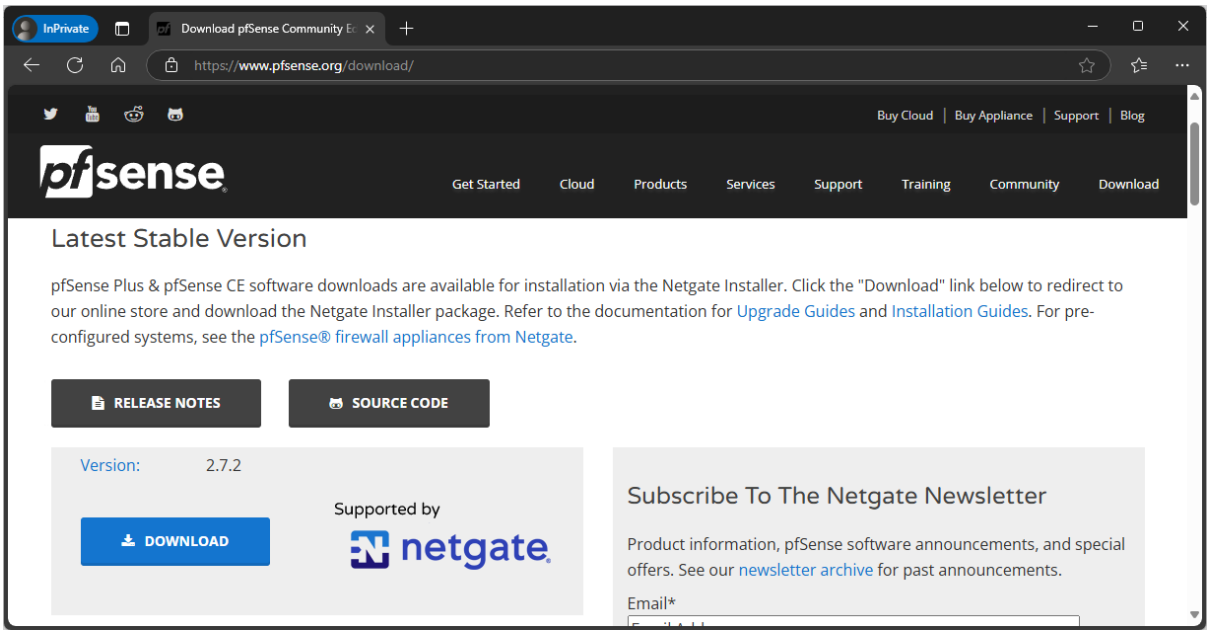
Virtual Machine Requirements

If installing pfSense on a virtual machine (VM), ensure your VM environment is configured with:

- **2+ CPU cores**
- **4+ GB of RAM**
- **2+ network interfaces** (one for WAN and one for LAN)
- **Virtual Disk** of at least 20 GB

Downloading pfSense ISO Image

Visit the official pfSense website to download the **ISO image** for installation.

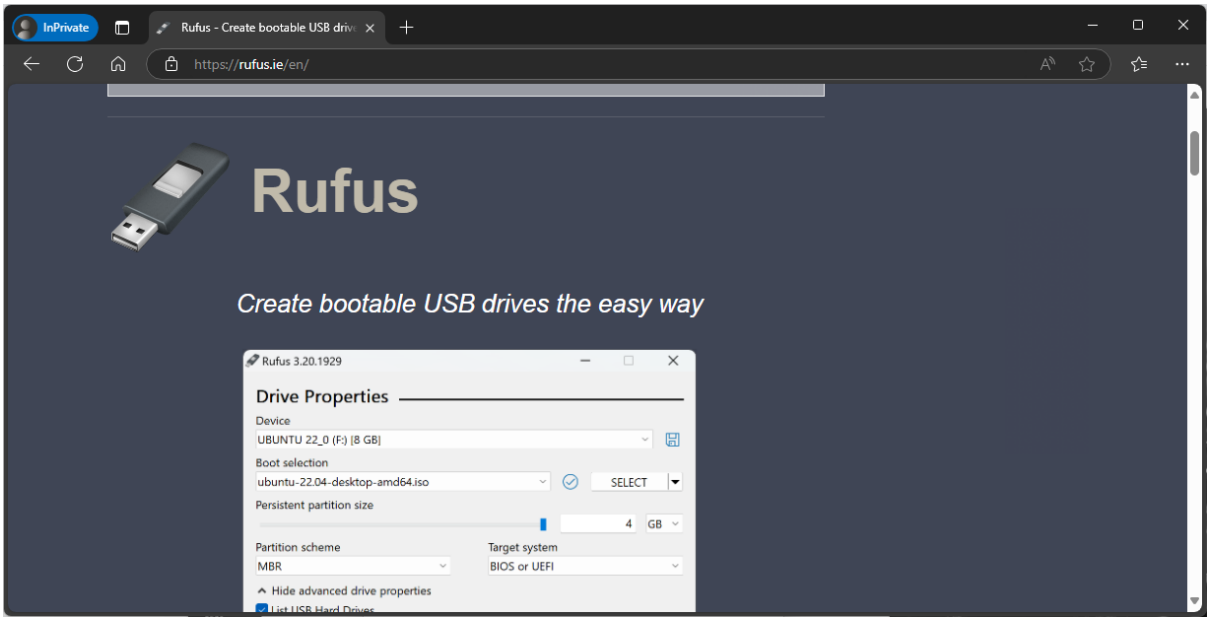


Install pfSense on Physical Hardware

Creating a Bootable USB (for physical installations)

If installing pfSense on physical hardware, you'll need to create a **bootable USB drive** from the downloaded ISO file.

A. Use tools like **Rufus** or **Etcher** to create the bootable USB.



B. Insert the USB drive into your machine and open Rufus.

C. Select your USB drive and the pfSense ISO file, then click **Start** to create the bootable USB.

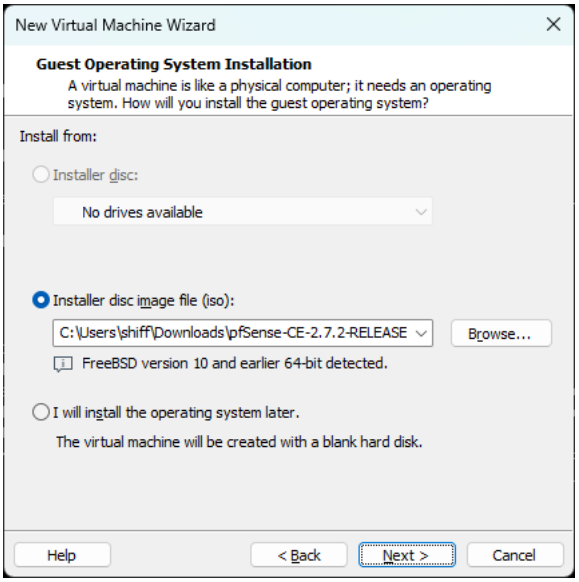
Once the USB is ready, insert the **bootable USB drive** into your machine and power it on.

Enter the BIOS/UEFI setup and set the system to boot from USB.

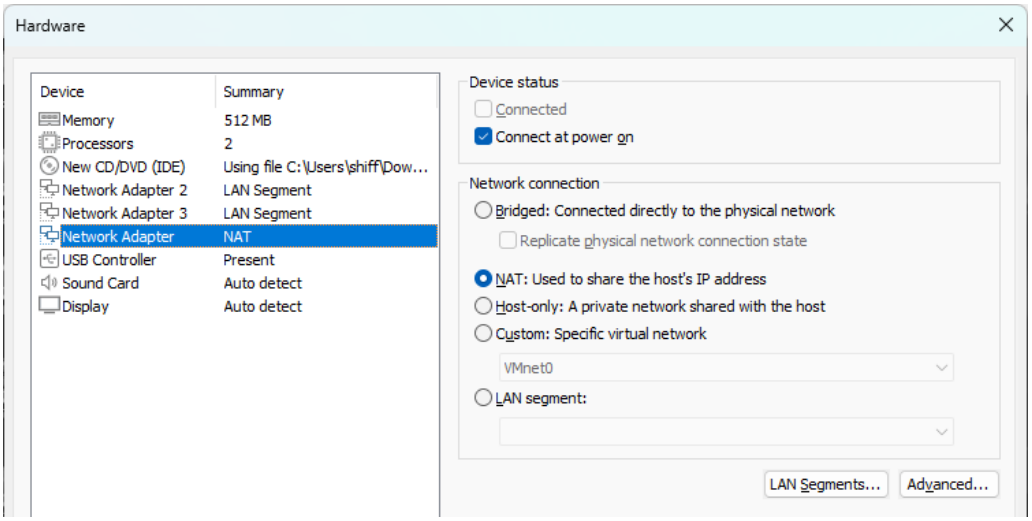
Once the pfSense installer starts, you will see the pfSense logo followed by the prompt to **Install pfSense**.

Install pfSense on a Virtual Machine

1. Create a **new virtual machine** in your hypervisor (e.g., VMware, VirtualBox, Hyper-V).
2. Attach the pfSense **ISO file** as the virtual optical drive.



3. Allocate the CPU, memory, and storage as discussed earlier.

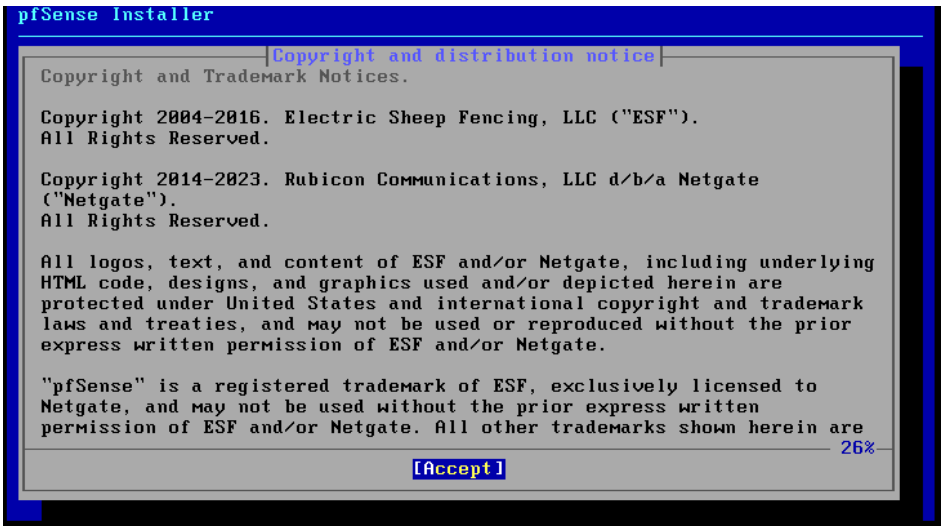


4. Boot the VM and start the pfSense installation.

Installation Process

After booting your device using the **pfSense ISO** (from a USB or virtual disk), the first screen you encounter is the **Copyright and Trademark Notice**.

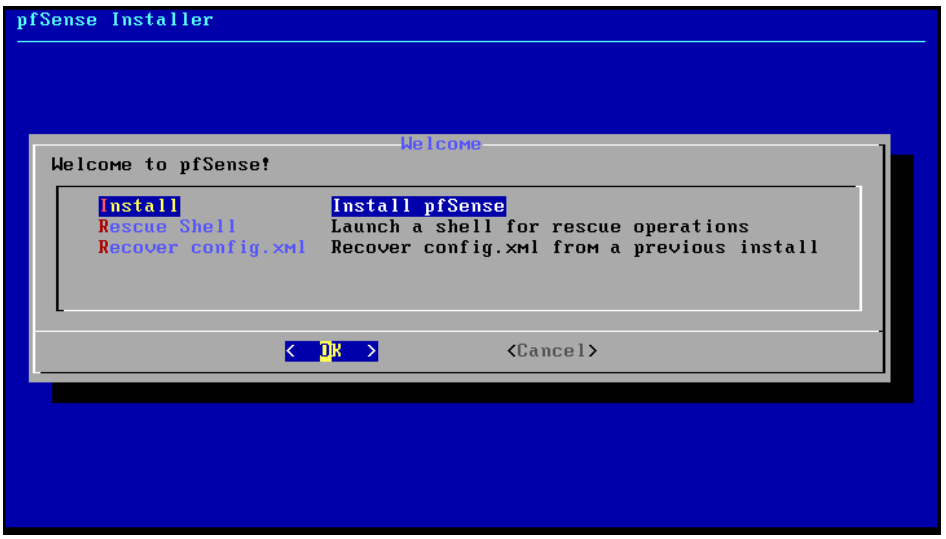
1. Review the copyright information. This confirms the legitimacy of the software and shows the legal information regarding pfSense.
2. **Select [Accept]** to proceed. This takes you to the **Welcome screen** of the installer.



The **installer menu** offers three choices:

- **Install**: This option launches the pfSense installation process.
- **Rescue Shell**: This is used for troubleshooting or running system-level commands manually if there are problems with an existing installation.
- **Recover config.xml**: This option restores configuration settings from a previous installation.

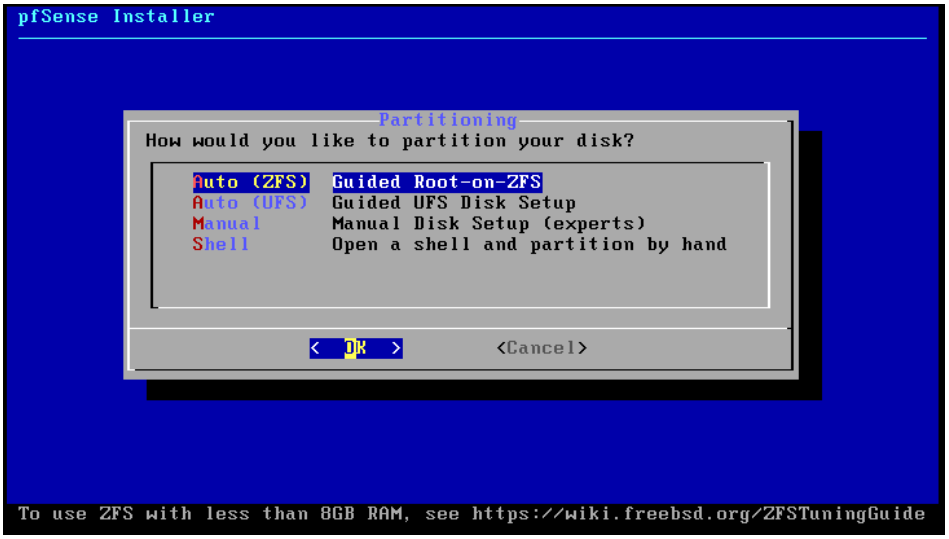
For a new setup, select **Install** and press **Enter** to continue.



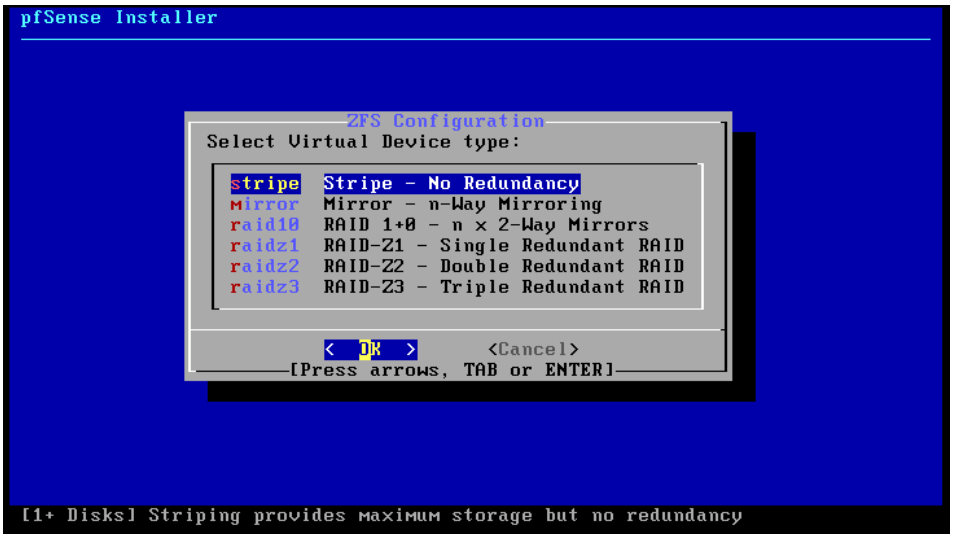
The next step asks how you want to **partition your disk**. You have several options, but most users should go with **Auto (ZFS)**, which uses the ZFS filesystem, known for its stability and redundancy.

- **Auto (ZFS)**: Guided ZFS setup, ideal for most users.
- **Auto (UFS)**: Uses UFS, a simpler but less modern file system.
- **Manual**: Advanced partitioning, recommended only for experts.
- **Shell**: Opens a terminal for manual disk partitioning.

Select **Auto (ZFS)** and press **Enter** to continue.

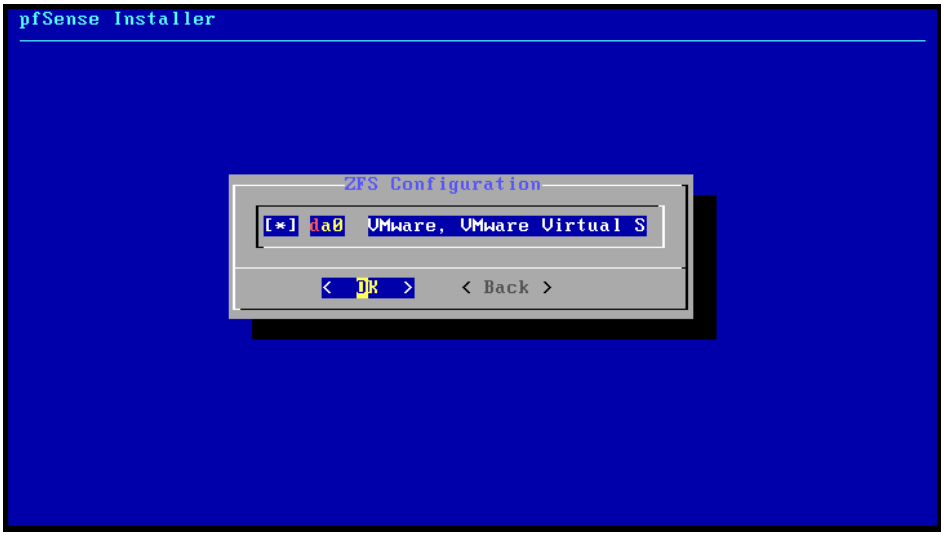


If you select **ZFS**, the installer will ask you to choose a **ZFS virtual device type**. ZFS offers several RAID-like options that determine how redundancy and fault tolerance are handled. For a single-disk installation, select **Stripe** and press **Enter**. If you have multiple disks, you can choose a RAID option.



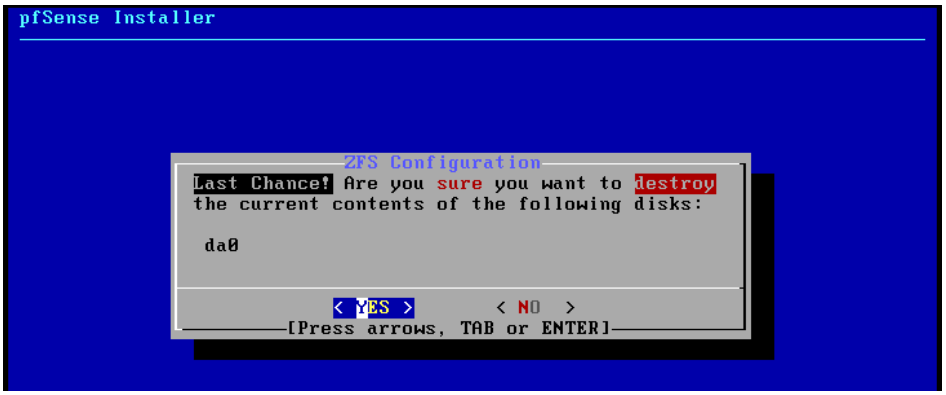
You will now see a list of **available disks**. Select the disk you want to install pfSense on. The installer will label it (e.g., da0), indicating the disk's identifier.

- Use the **arrow keys** to select the appropriate disk.
- Press **Enter** to confirm your selection.

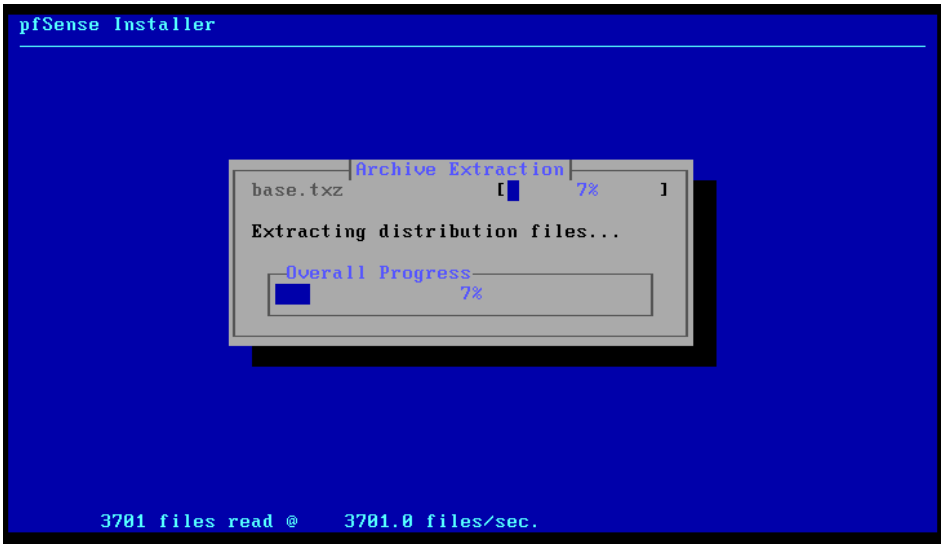


The installer will warn you that the disk will be **wiped**, and all existing data will be destroyed. This is your **last chance** to back out if you've selected the wrong disk.

- Select **Yes** to proceed with the installation.



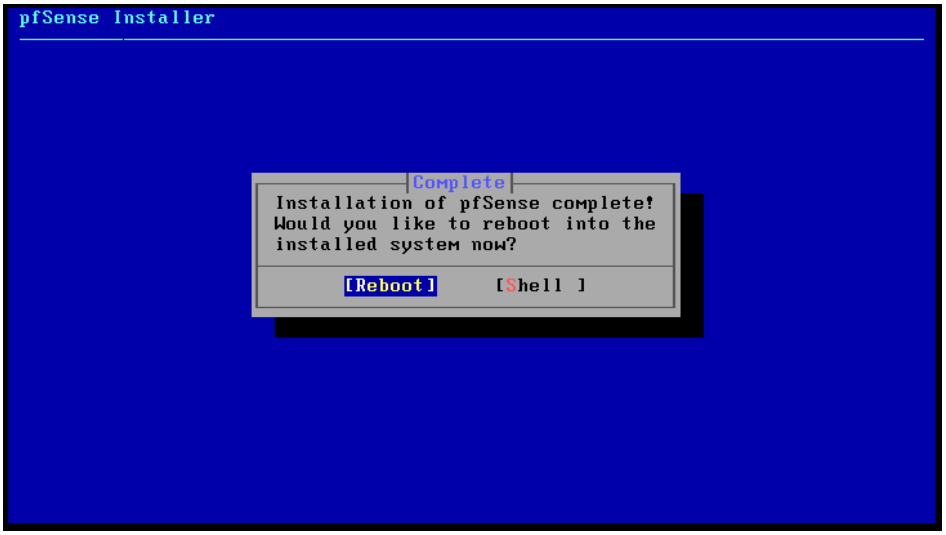
You'll see a **progress bar** indicating the percentage of files extracted. Once the process is complete, the installer will automatically proceed to the next step.



After extracting the files, the installer will display a message confirming that the installation is complete.

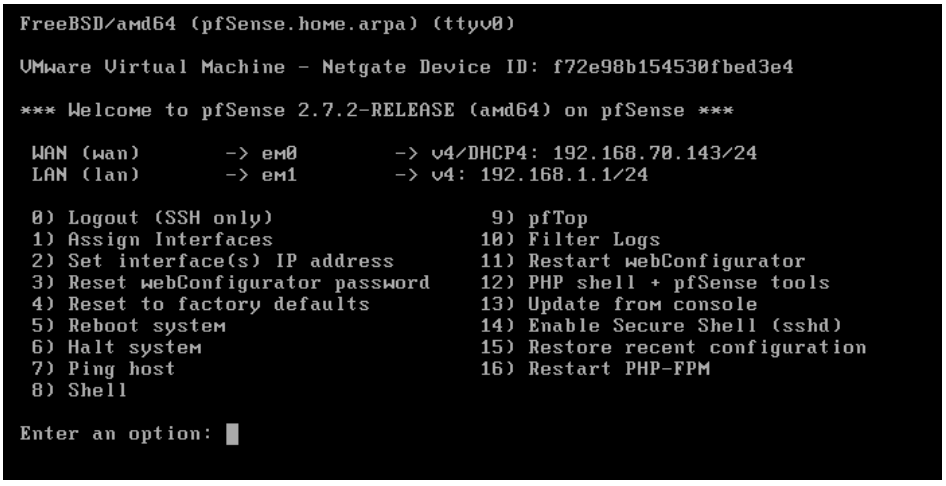
- **Select [Reboot]** to restart the system and boot into the installed pfSense environment.
- Remove the **USB drive** (or disconnect the ISO) to avoid booting back into the installer.

Alternatively, you can access the **Shell** at this point to run any additional commands if needed.



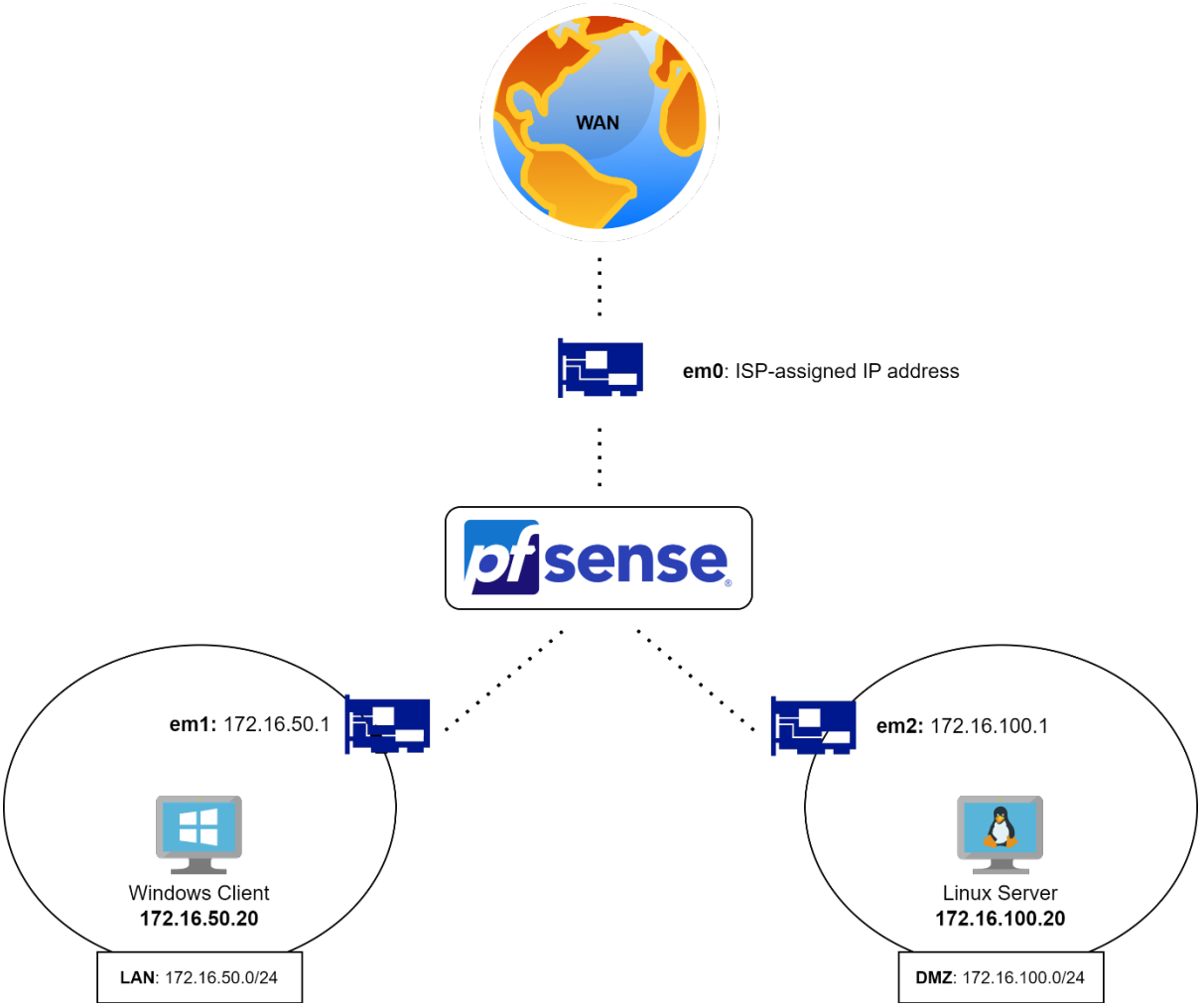
After rebooting, pfSense will load, and you'll be presented with the **console menu**. This menu allows you to perform initial configurations and troubleshooting tasks.

At this point, you can configure the **WAN** and **LAN** interfaces if necessary. Once the interfaces are assigned and configured, you can access the WebGUI via the **LAN interface IP address** (e.g., 192.168.1.1).



pfSense Configuration

The diagram provided presents a **network architecture built around a pfSense firewall** that connects multiple network segments: **WAN, LAN, and DMZ**. This setup demonstrates how pfSense serves as the **core firewall and router**, managing traffic between internal, external, and isolated networks. The design reflects a common structure used by organizations to **segregate critical services, enhance security, and control network access**.



Components and Their Role

WAN (Wide Area Network) – Interface em0

- This interface connects the **pfSense firewall to the Internet** through an ISP (Internet Service Provider).
- **em0** is the **WAN interface**, configured with an **ISP-assigned IP address**. This is the gateway for all outgoing and incoming traffic from the external Internet.
- **Firewall rules** on the WAN interface control access to internal resources from external sources, ensuring only permitted services are accessible.

LAN (Local Area Network) – Interface em1

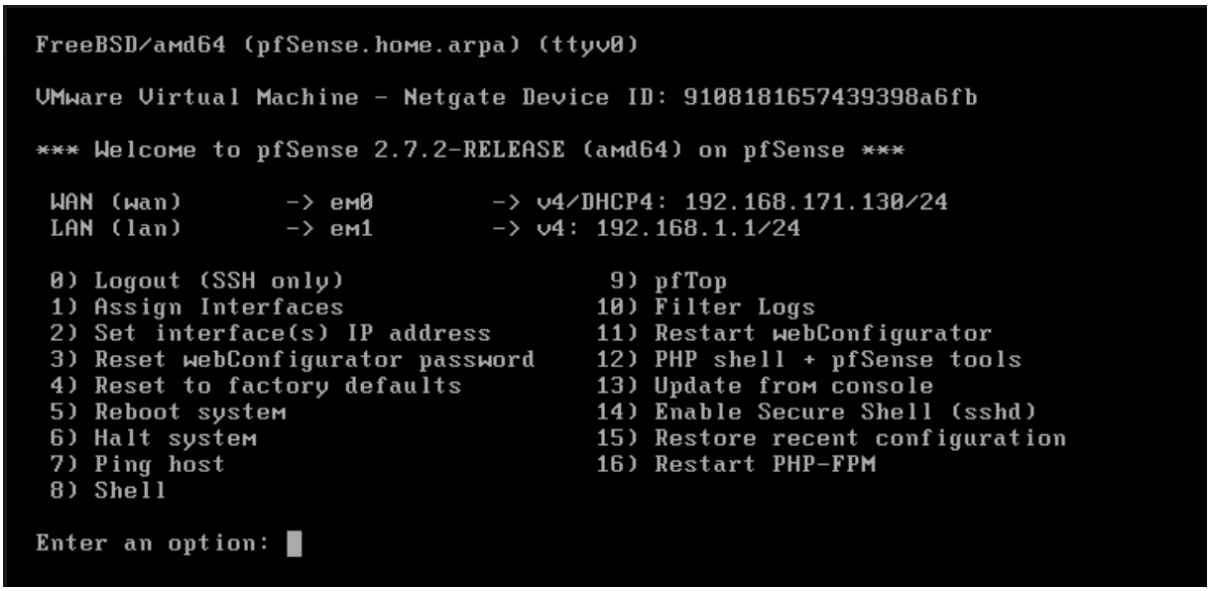
- The **LAN network** (172.16.50.0/24) is an internal network where local devices reside.
- The **Windows client (172.16.50.20)** connects to this segment through **interface em1** with the pfSense firewall acting as the **gateway (172.16.50.1)**.
- The **LAN network is usually trusted**, and devices within this network can access external Internet resources via the **WAN interface**, as well as internal services hosted in the DMZ.

DMZ (Demilitarized Zone) – Interface em2

- The **DMZ network (172.16.100.0/24)** is an isolated segment where **public-facing services** are hosted. In this example, the **Linux server (172.16.100.20)** resides in the DMZ and can be accessed externally.
- **Interface em2** connects the DMZ to pfSense, with the firewall serving as the gateway **(172.16.100.1)**.
- The DMZ isolates **public-facing services** (such as web or mail servers) from the LAN, ensuring that if these services are compromised, internal resources remain protected.

Configuring Interfaces using pfSense Console

Assigning Interfaces



1. From the **main console menu**, select **Option 1 – Assign Interfaces**.
2. When prompted about setting up **VLANs**, type **n** (unless VLANs are needed).
3. Enter the following assignments based on your setup:

- **WAN Interface**: em0
  (Enter **em0** when prompted for the WAN interface)
- **LAN Interface**: em1
  (Enter **em1** for the LAN interface)
- **Optional 1 Interface (DMZ)**: em2
  (Enter **em2** to assign DMZ as Optional 1)

```
 6) Halt system                          15) Restore recent configuration
 7) Ping host                            16) Restart PHP-FPM
 8) Shell

Enter an option: 1


Valid interfaces are:

em0     00:0c:29:35:1a:67   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1     00:0c:29:35:1a:71   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2     00:0c:29:35:1a:7b (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a):
```

4. Review the assigned interfaces:
   - WAN → em0
   - LAN → em1
   - OPT1 (DMZ) → em2
5. If everything is correct, type **y** to proceed. The interface assignments will now take effect.

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2

Do you want to proceed [y|n]? y
```

Configuring IP Addresses for Interfaces

1. After assigning the interfaces, return to the **main menu** and select **Option 2** – **Set Interface(s) IP Address**.

```
 5) Reboot system                    14) Enable Secure Shell (sshd)
 6) Halt system                      15) Restore recent configuration
 7) Ping host                        16) Restart PHP-FPM
 8) Shell

Enter an option: 2
```

2. **Configuring WAN Interface**:
    - Enter **1** to select the WAN interface.
    - When asked if you want to configure the IPv4 address via **DHCP**, type **y**.
    - For **IPv6 DHCP**, type **n** (if you're not using IPv6).
    - Leave the **manual IP fields blank** for DHCP.
    - You will be asked if you want to **revert to HTTP** for the WebConfigurator. Type **n** to keep the default HTTPS configuration.

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
```

3. **Configuring LAN Interface**:
    - Enter **2** to select the LAN interface.
    - When asked if you want to configure via DHCP, type **n**.
    - Enter the **new LAN IP address**: 172.16.50.1
    - Set the **subnet mask**: 24
    - For the **gateway**, press **Enter** (no gateway needed for LAN).
    - When prompted to enable the **DHCP server**, type **n** (unless needed).

```
Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.50.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.16.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.16.50.1/
```

4. **Configuring DMZ Interface (Optional)**:
    - Enter **3** to configure the DMZ (Optional 1).
    - Type **n** when asked about DHCP.
    - Enter the **DMZ IP address**: 172.16.100.1
    - Set the **subnet mask**: 24
    - Leave the **gateway** field blank by pressing **Enter**.
    - Type **n** for DHCP setup unless required.

```
Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 172.16.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24
```

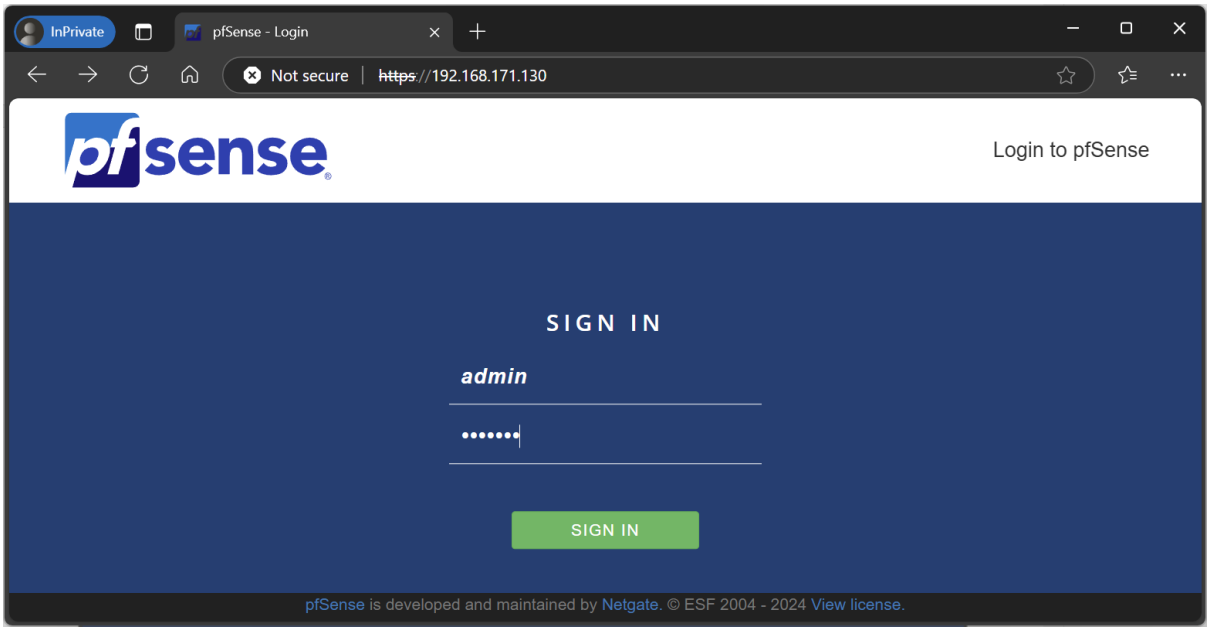
Accessing the Console and Disabling the Firewall

Disabling the firewall with the pfctl -d command during the initial setup of pfSense can be a crucial step, especially when trying to access the **WebGUI** for the first time. This will temporarily disable all firewall rules until re-enabled.

```
pfctl -d
```

Accessing the WebConfigurator

1. Now that the LAN is configured, you can access the **pfSense WebConfigurator** from a browser.
    - Open a browser and go to **https://172.16.50.1**
    - **Username**: admin
    - **Password**: pfsense



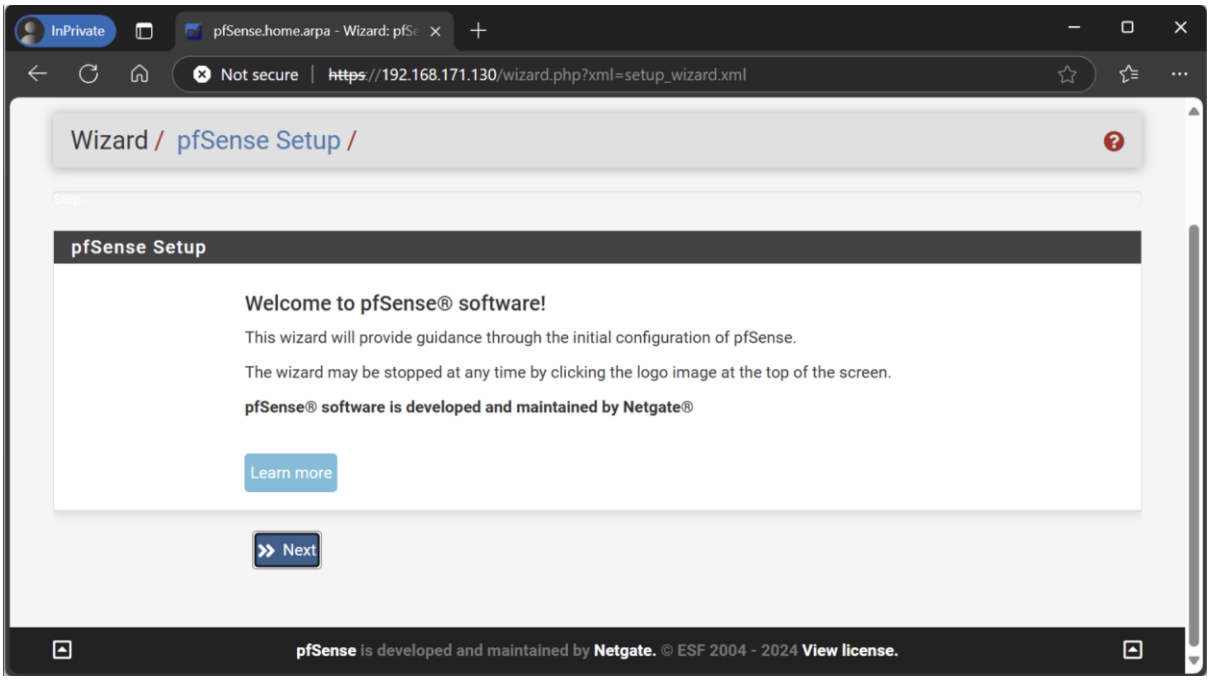
2. Once inside the WebConfigurator, further configurations (like **firewall rules** and **routing**) can be done more conveniently.

Basic pfSense Configuration via the Web GUI

The Web GUI (Graphical User Interface) in pfSense plays a critical role in managing and configuring the firewall efficiently. While pfSense offers a command-line interface (CLI) for initial setup or troubleshooting, the Web GUI provides a much more intuitive and user-friendly way to access and modify advanced features.

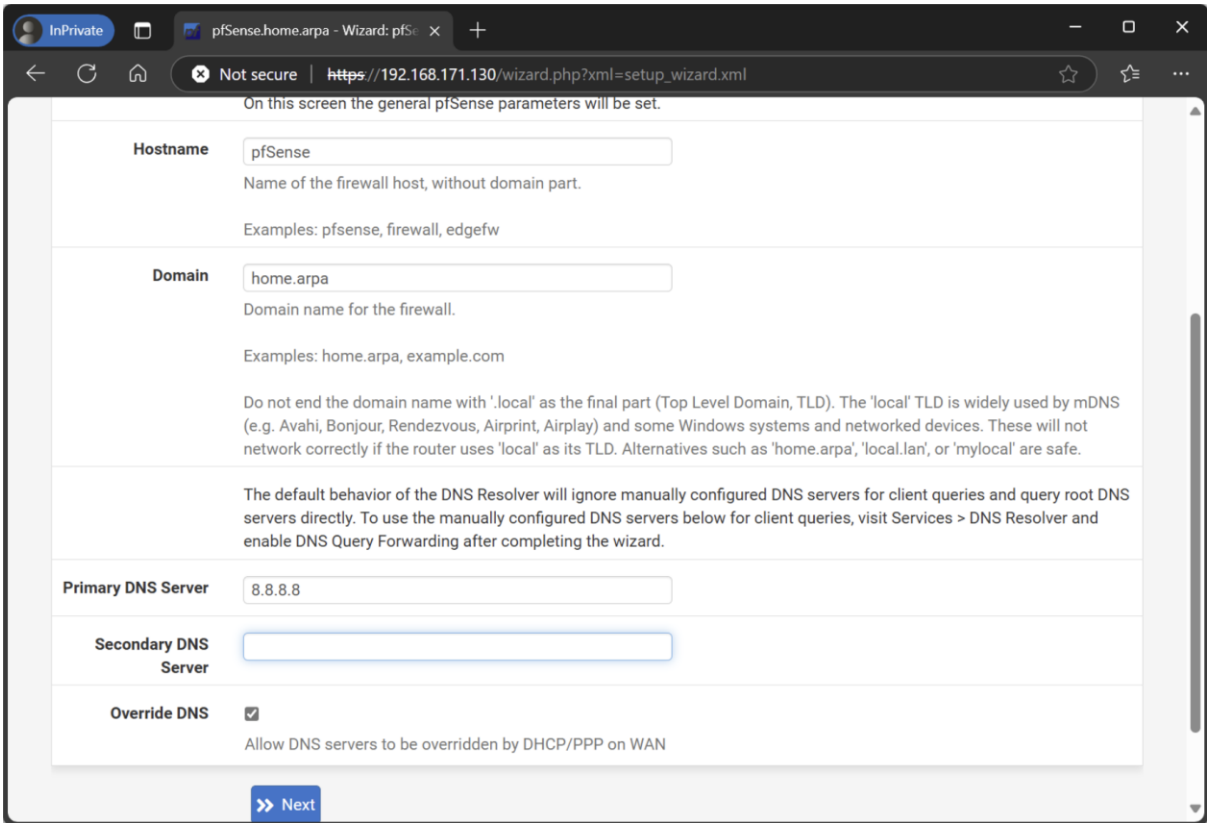
Step 1: Welcome Wizard

1. The wizard begins with an introduction. Click **Next** to proceed through the steps.



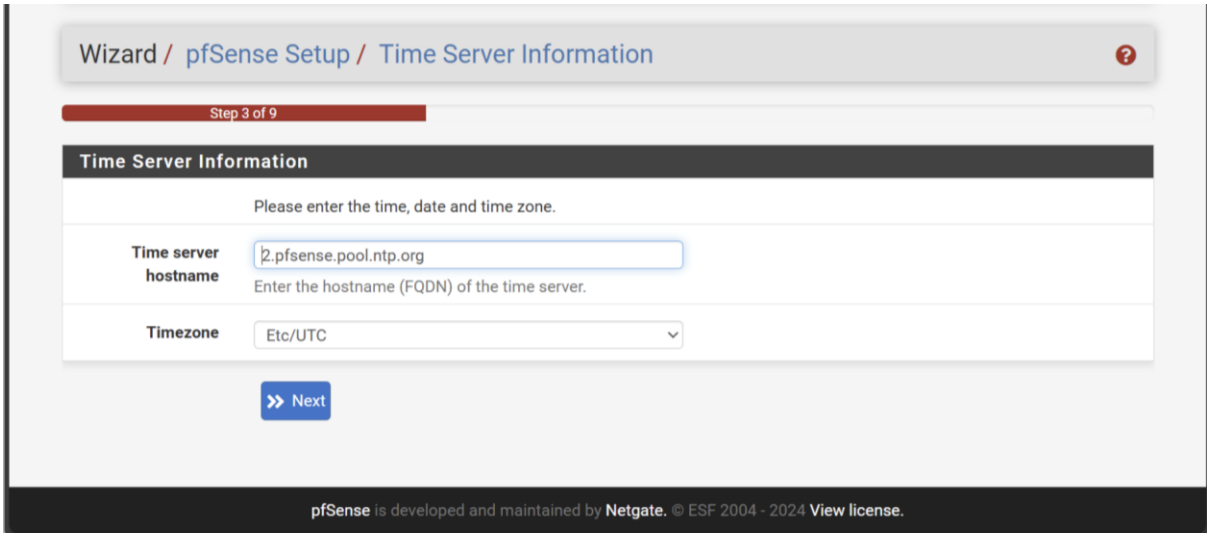
Step 2: Configure General Settings

1. **Hostname**: Enter a name for your pfSense router (e.g., pfSense).
2. **Domain**: Set your network's domain (e.g., home.arpa).
3. **Primary DNS Server**: Use a reliable DNS server such as 8.8.8.8 (Google DNS).
4. You can also enter a **Secondary DNS Server** if needed.
5. Enable or disable the **Override DNS** option depending on whether you want to allow DHCP to override these settings.
6. Click **Next** to proceed.



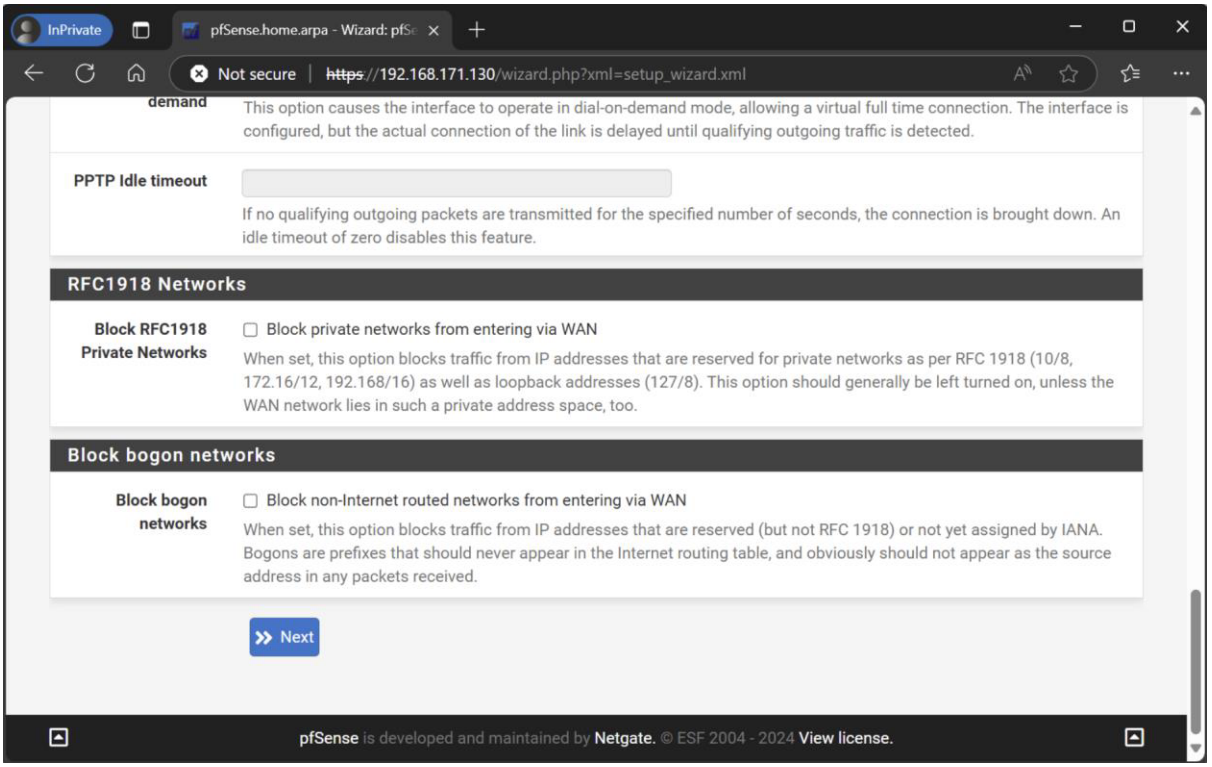
Step 3: Time Server Configuration

1. Ensure your time settings are correct by setting:
    - **Time server hostname**: 2.pfsense.pool.ntp.org
    - **Timezone**: Select the appropriate timezone (e.g., Etc/UTC).
2. Click **Next** to save and continue.



Step 4: WAN Interface Configuration

1. **Configure your WAN settings to allow internal access:**
    - **Unblock RFC1918 Networks**: **Uncheck** this box to **allow** private IP addresses (such as 10.x.x.x, 172.16.x.x, and 192.168.x.x) to access the firewall over the WAN interface. This is necessary when configuring the firewall from within a private or internal network.
    - **Unblock bogon networks**: **Uncheck** this option to **allow** traffic from IP ranges that may not be publicly routable. This can be useful for testing, lab environments, or internal network setups.

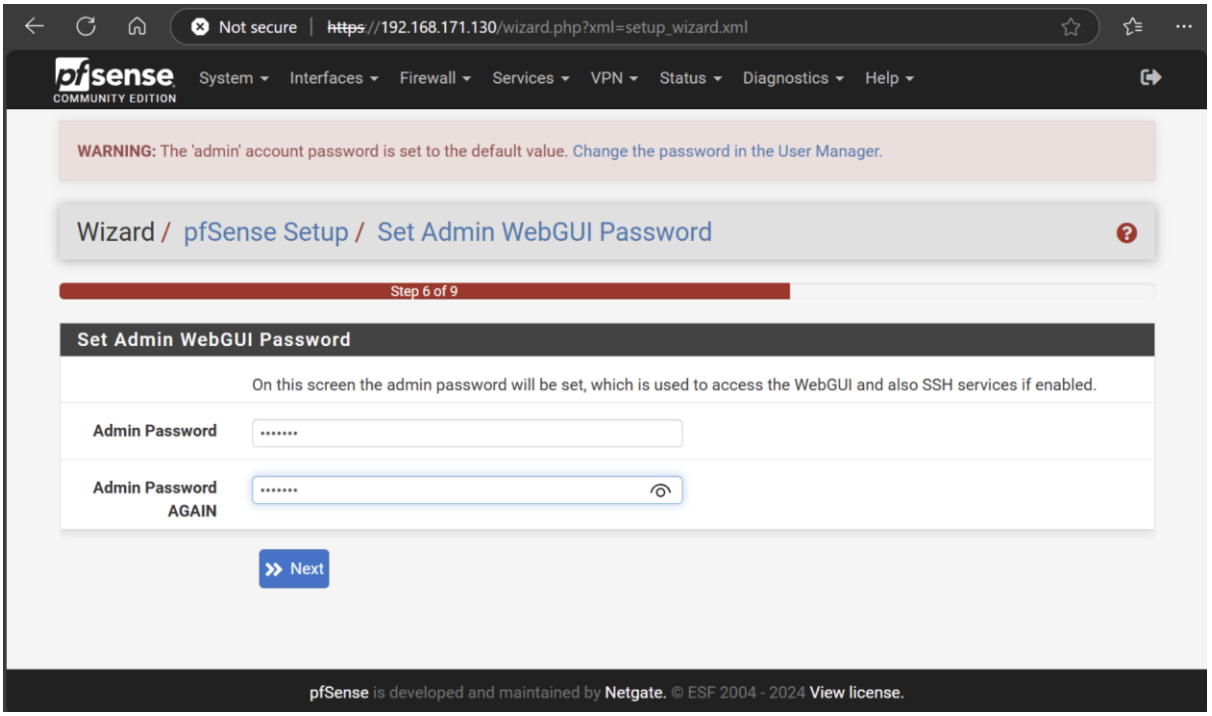


2. **Click Next to continue.**

By unchecking both options, users inside the private network can connect to the pfSense firewall through the WAN interface to complete the configuration. This is especially useful during the initial setup phase or when access to the LAN interface is unavailable. However, remember to reconfigure these settings appropriately once the setup is complete to ensure proper security.

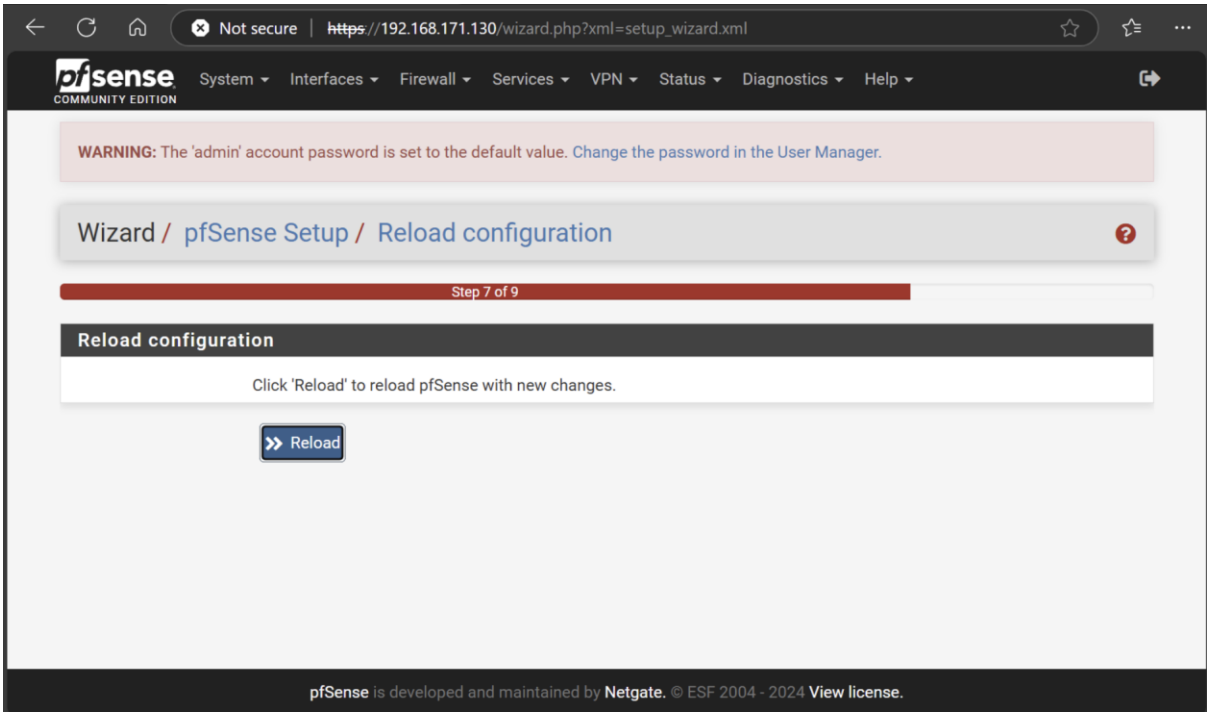
Step 5: Set Admin Password

1. On this step, create a new admin password for accessing the Web GUI and SSH.
2. Enter the password twice to confirm.
3. Click **Next** to proceed.



Step 6: Reload Configuration

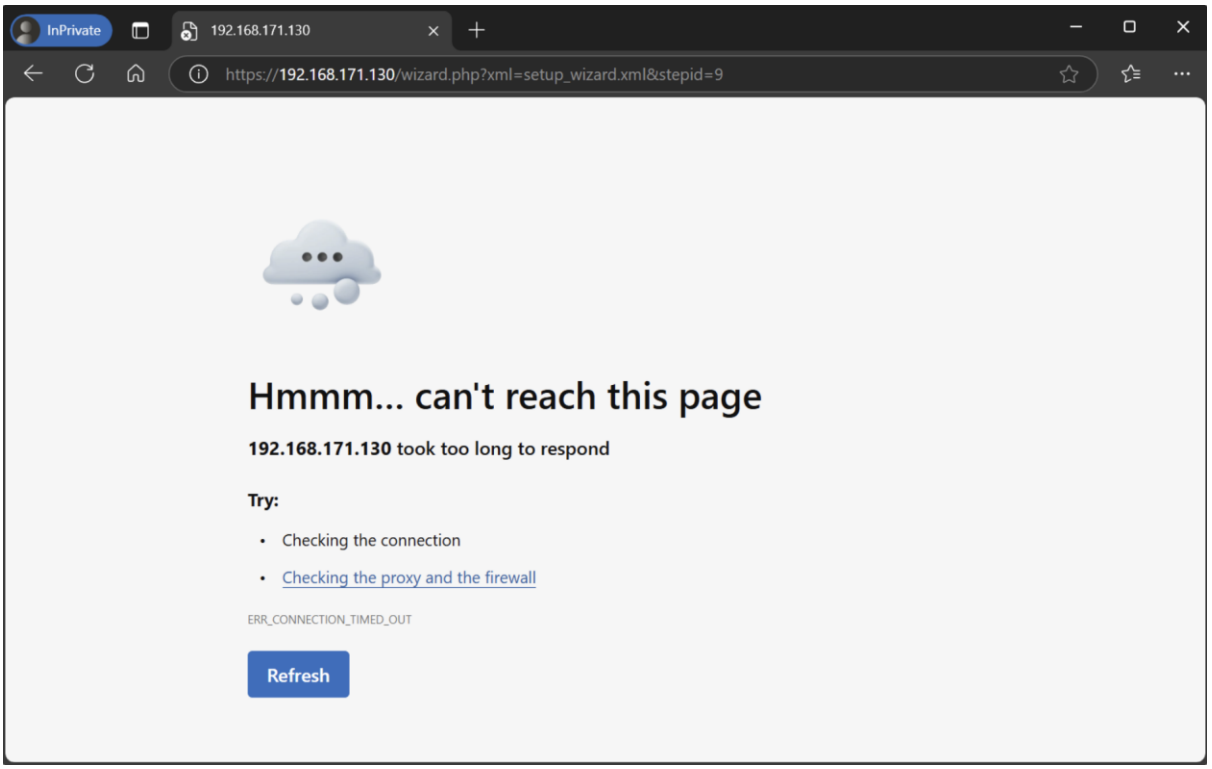
1. Click **Reload** to apply the new settings.
2. The system will reload the configuration and return to the final setup steps.



Step 7: Finalize Configuration

1. **Disable the Firewall Temporarily**

   The firewall is set to turn on on reboot.

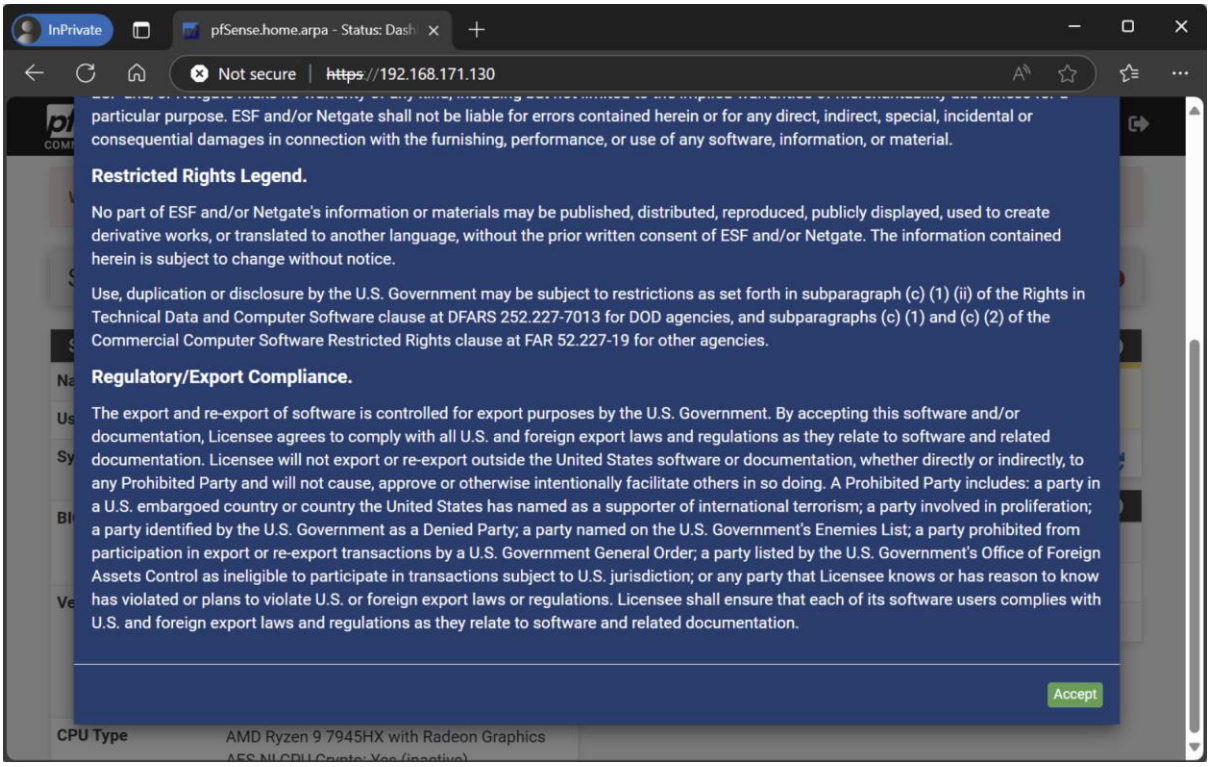


   To ensure uninterrupted access to the Web GUI during the final steps, you will need to disable the firewall again:

   - Access the **CLI** (either via the console or SSH).
   - Enter the command:

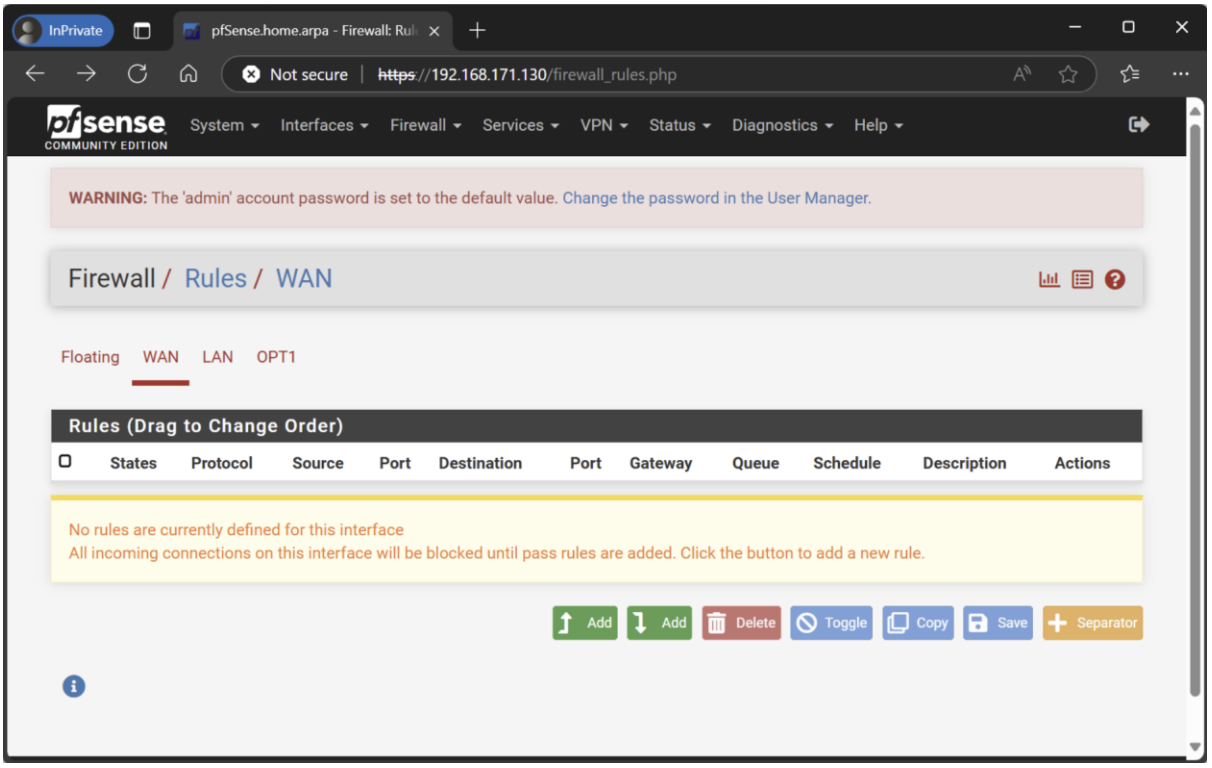
```
pfctl -d
```

2. This ensures no traffic restrictions block your access to the Web GUI while you finalize the configuration.
3. **Access the Completion Screen**
   - After the configuration reloads, you will see the **Congratulations! pfSense is now configured** screen.
   - Click **Finish** to exit the wizard and proceed to the dashboard.



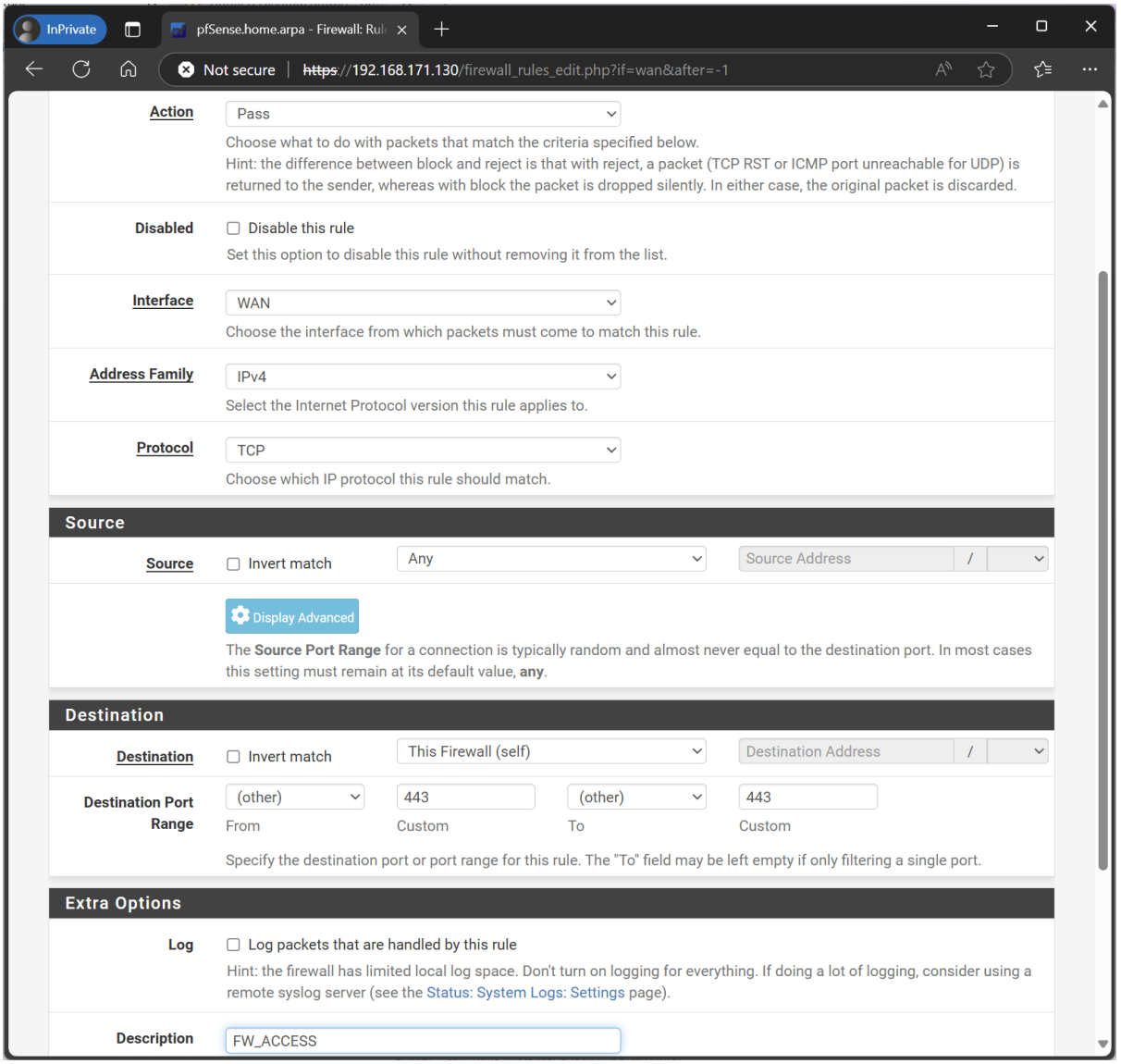
Step 8: Verify Web GUI and Firewall Access

1. **Check Firewall Rules**
    - Navigate to **Firewall > Rules** in the Web GUI.

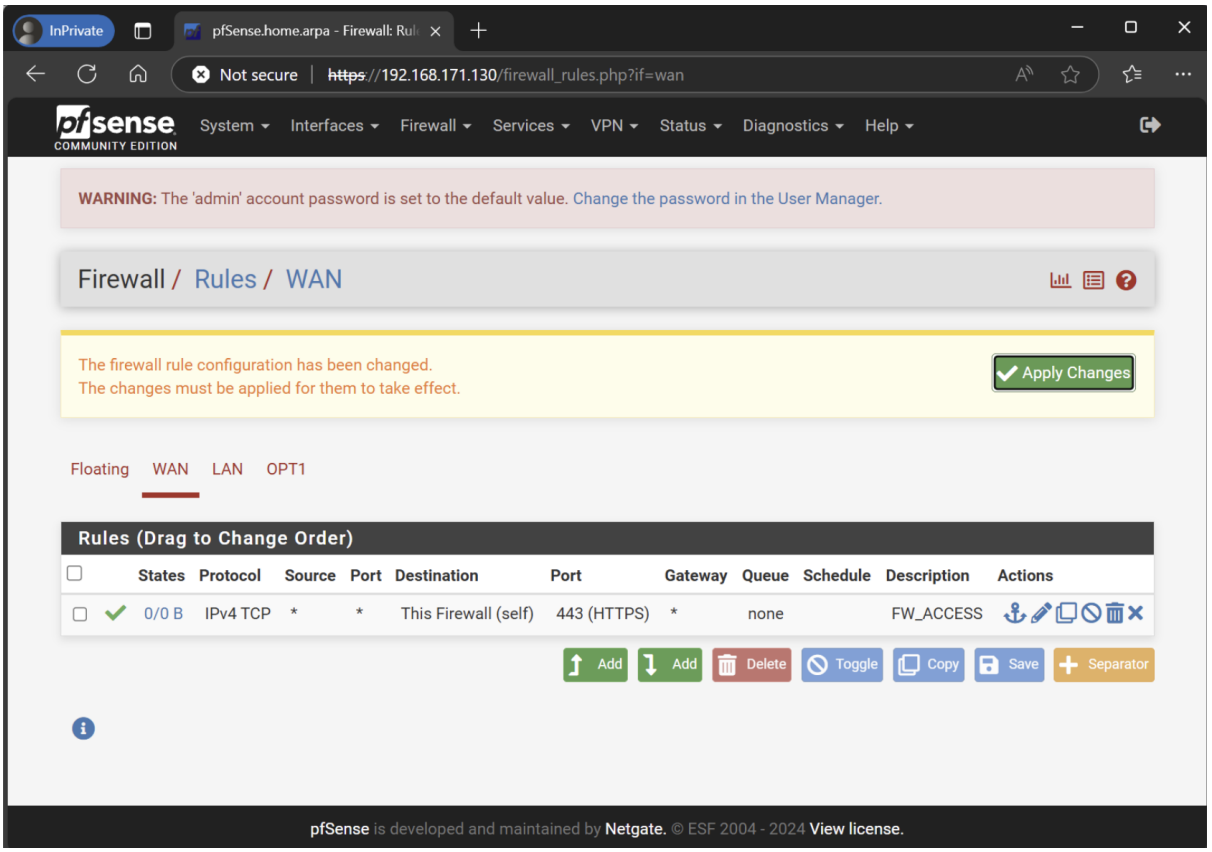


Step 9: Apply Firewall Rules for Permanent Access

1. **Create a Permanent Web GUI Access Rule**
    - Go to **Firewall > Rules > WAN**.
    - Click **Add** to create a new rule:
        - **Action**: Pass
        - **Interface**: WAN
        - **Protocol**: TCP
        - **Destination**: This Firewall (self)
        - **Destination Port**: HTTPS (443)
        - **Description**: Web GUI Access
    - Click **Save** and then **Apply Changes**.



By following these steps, you'll have a fully configured pfSense firewall that allows access through the Web GUI without requiring frequent firewall disabling.



Adding Rules for Service Access

In any network environment, security is paramount, and firewalls like pfSense play a crucial role in controlling what traffic enters or leaves the network. One of the key features of pfSense is its capability to filter traffic based on rules set by the administrator. These rules can be configured to allow or deny access to specific services, ensuring a balance between network security and accessibility. For example, you might need to permit SSH access to your router from a remote location over the WAN for remote management purposes.

Understanding the Logic and Need

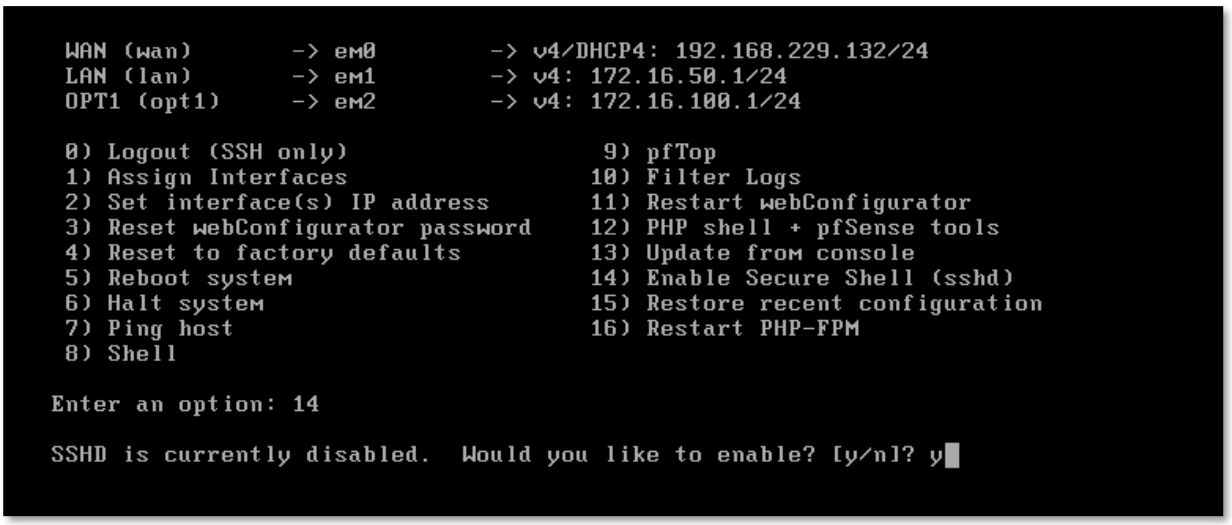
Why Do We Need Rules?

- **Access Control**: Rules allow you to define what traffic should be permitted or blocked based on criteria such as source/destination IP, port, protocol, and more.
- **Granular Control**: By creating custom rules, you can control exactly who has access to specific services and from where.
- **Minimizing Attack Surface**: By default, pfSense blocks unsolicited connections from the WAN for security. Manually configuring rules to allow necessary services ensures only desired traffic can reach your network.
- **Security and Management**: Allowing SSH access for administrative purposes can be critical but must be done with security measures in place, such as limiting access to trusted IP addresses.

Prerequisites

Before configuring rules, ensure:

1. You have administrative access to pfSense.
2. SSH is enabled on the pfSense device, if necessary.



3. You understand the security implications of opening services to the WAN.

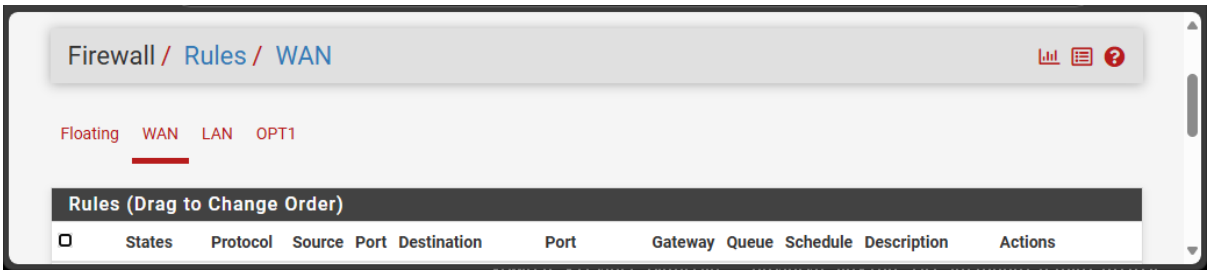
Configuring the Rule

1. Access the Firewall Rules Section

- Log in to your pfSense web interface.
- Navigate to **Firewall > Rules**.

2. Select the WAN Interface

- Since we are creating a rule to allow traffic from the WAN, click on the **WAN** tab.



3. Add a New Rule

- Click the **+ Add** button to create a new rule.

4. Configure Basic Settings

- **Action**: Select **Pass** to allow traffic that matches this rule.
    - This setting ensures that traffic matching the rule criteria is allowed through the firewall.
- **Disabled**: Ensure this is **unchecked** so the rule is active.
- **Interface**: Select **WAN**.
    - This defines that the rule applies to traffic coming in from the WAN interface.
- **Address Family**: Select **IPv4**.
    - This setting specifies that the rule applies to IPv4 traffic. Adjust accordingly if you are using IPv6 or dual-stack.
- **Protocol**: Select **TCP**.
    - SSH uses TCP as the transport protocol.

5. Source Configuration

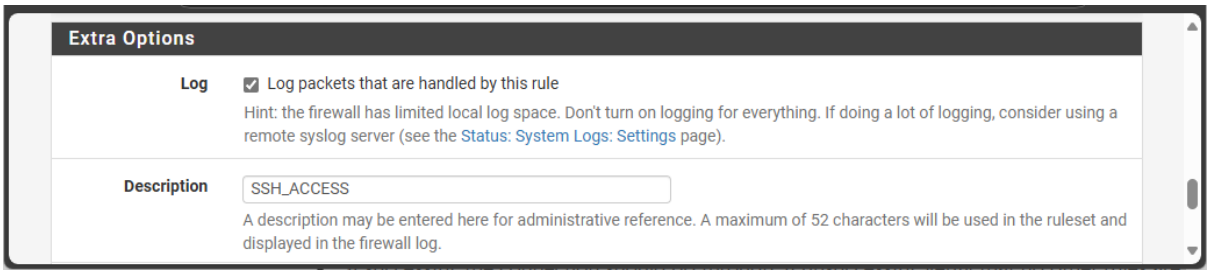
- **Source**: Leave as **Any**.
    - This setting allows traffic from any source to reach the specified destination. For a more secure configuration, you could specify a trusted IP address or subnet here.
- **Source Port Range**: Leave this as **any** (default setting).

6. Destination Configuration

- **Destination**: Set this to **Any** (this can be modified if you want to specify the pfSense IP address or a different destination).
- **Destination Port Range**: Set this to **22** in both the **From** and **To** fields.
    - This restricts access to port 22, which is used by SSH.

7. Extra Options

- **Log**: Check **Log packets that are handled by this rule**.
    - Enabling logging helps track access attempts for monitoring and security auditing purposes. Be mindful of excessive logging if resources are limited.
- **Description**: Enter a meaningful description like **SSH_ACCESS** to easily identify the purpose of the rule.



8. Save and Apply Changes

- Click **Save** to save the rule.
- Click **Apply Changes** at the top of the page to apply the configuration.

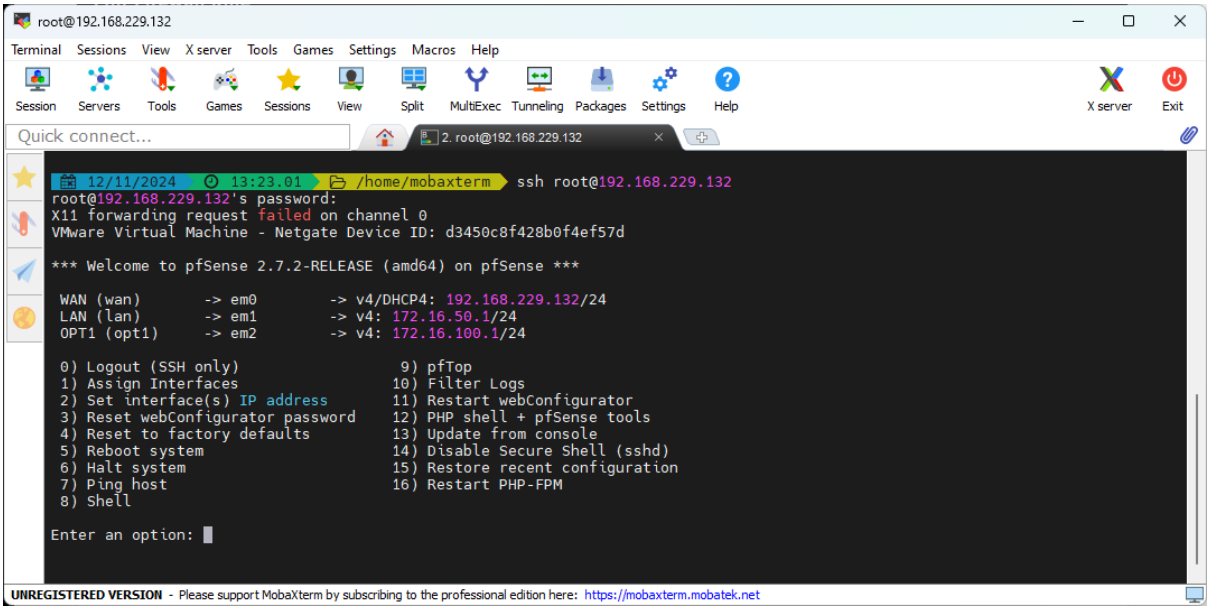
Testing the SSH Configuration After pfSense Firewall Rule Setup

After setting up a rule to allow SSH access to your pfSense device from the WAN, it's important to verify that the rule works as intended and provides the expected level of access.

Steps for Verification

1. **Initiate SSH Connection**
    - Use your preferred SSH client (e.g., MobaXterm, PuTTY, or the built-in terminal on Linux/macOS) to connect to your pfSense WAN IP address.
    - Use the **root** username and the appropriate password (default is **pfsense**, unless it has been changed).

For example: **ssh root@192.168.229.132**



Security Recommendations

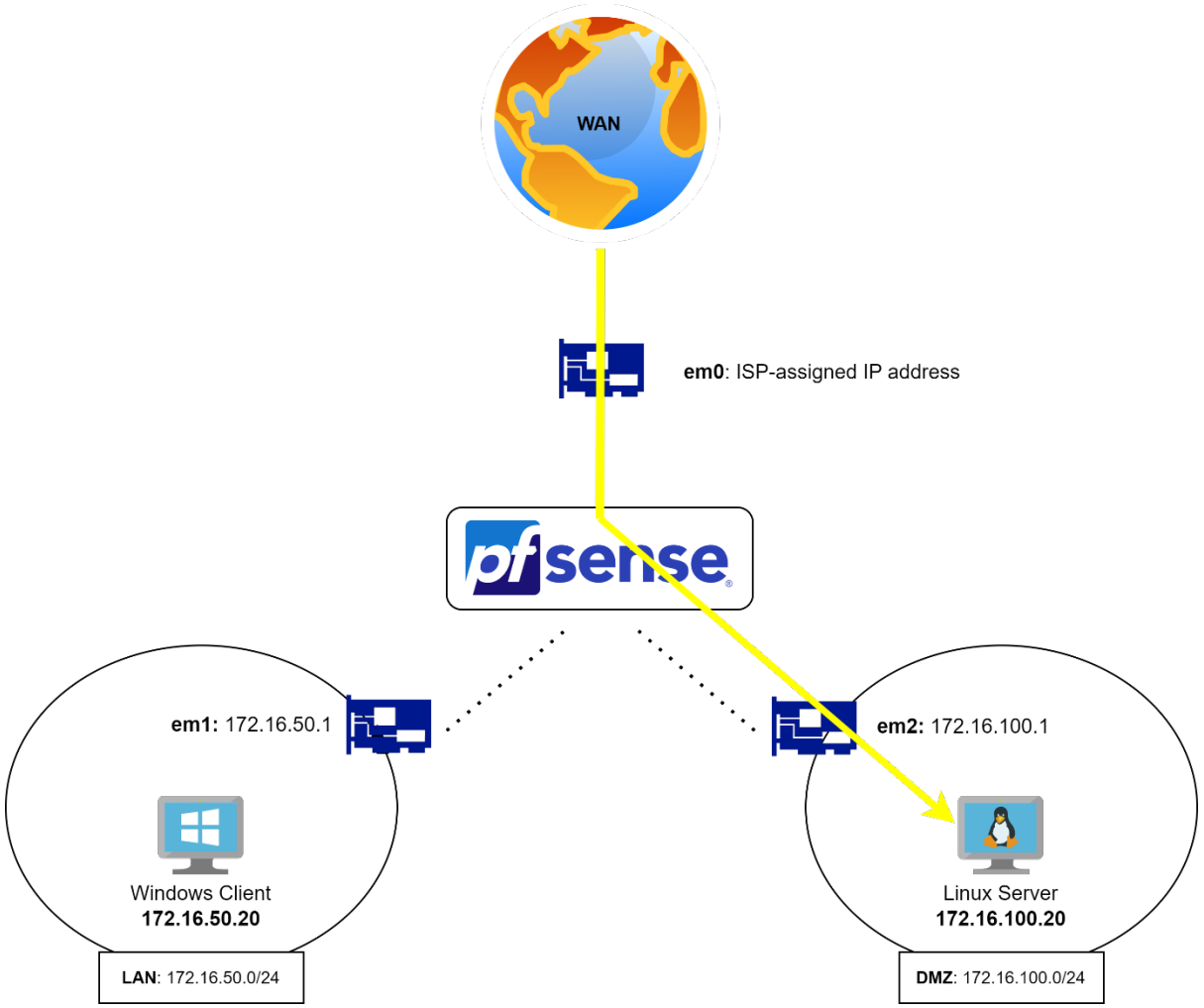
- **Restrict Source IPs**: If possible, limit the source address to a specific trusted IP or subnet to reduce the risk of unauthorized access.
- **Use Strong Authentication**: Utilize strong passwords or SSH keys to secure access.
- **Monitor Logs**: Regularly check logs to detect any suspicious access attempts.

Firewall NAT Configuration in pfSense

Firewall Rules and Network Address Translation (NAT) are two key elements in pfSense that control how traffic flows between interfaces, networks, and devices. While firewall rules define **what traffic is allowed or blocked**, NAT rules translate IP addresses and ports, ensuring correct routing between private and public networks. Understanding how these components work together is essential to configure secure and efficient network traffic.

Firewall Rules vs. NAT Rules

- **Firewall Rules**: Control access by defining which traffic is allowed or denied across interfaces (WAN, LAN, DMZ). These rules are applied to the **interfaces**, such as LAN or WAN, and they work in a **top-down** order.
- **NAT Rules**: NAT manages the translation of IP addresses and ports to facilitate communication between private networks (e.g., LAN or DMZ) and public networks (e.g., WAN). **Port Forwarding** is a common use case for NAT, where incoming WAN traffic is forwarded to an internal server (e.g., the DMZ Linux server).



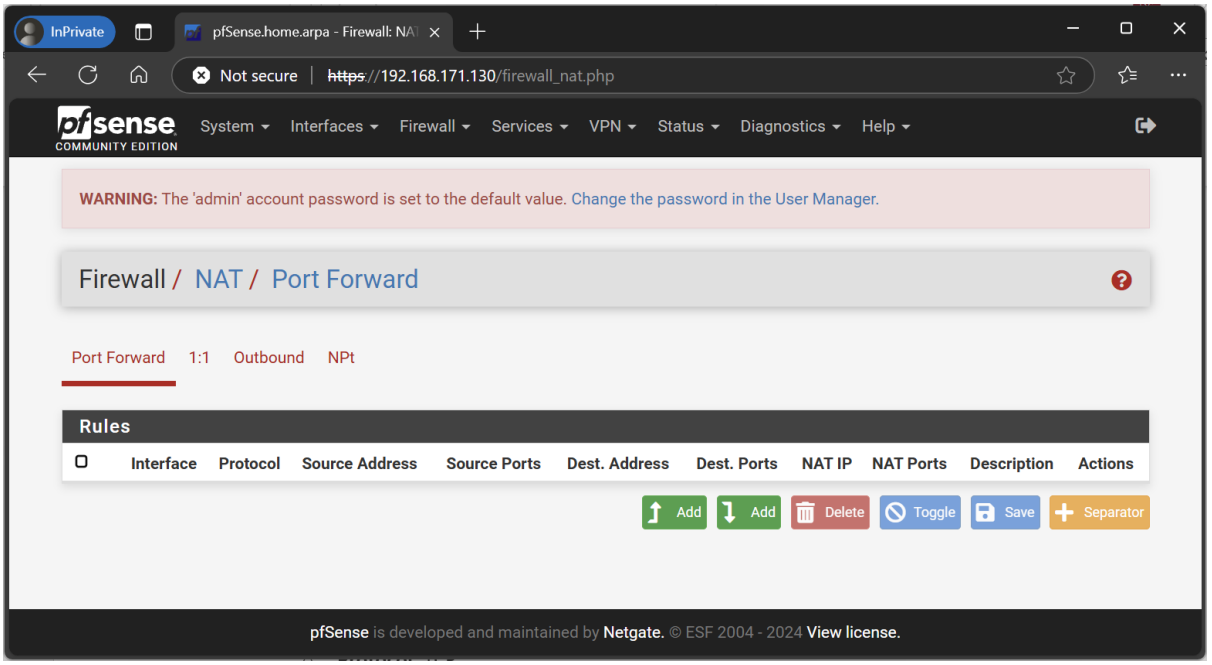
Firewall Rules Configuration

You must configure **firewall rules** to ensure that WAN traffic can reach the DMZ Linux server. Below are the steps:

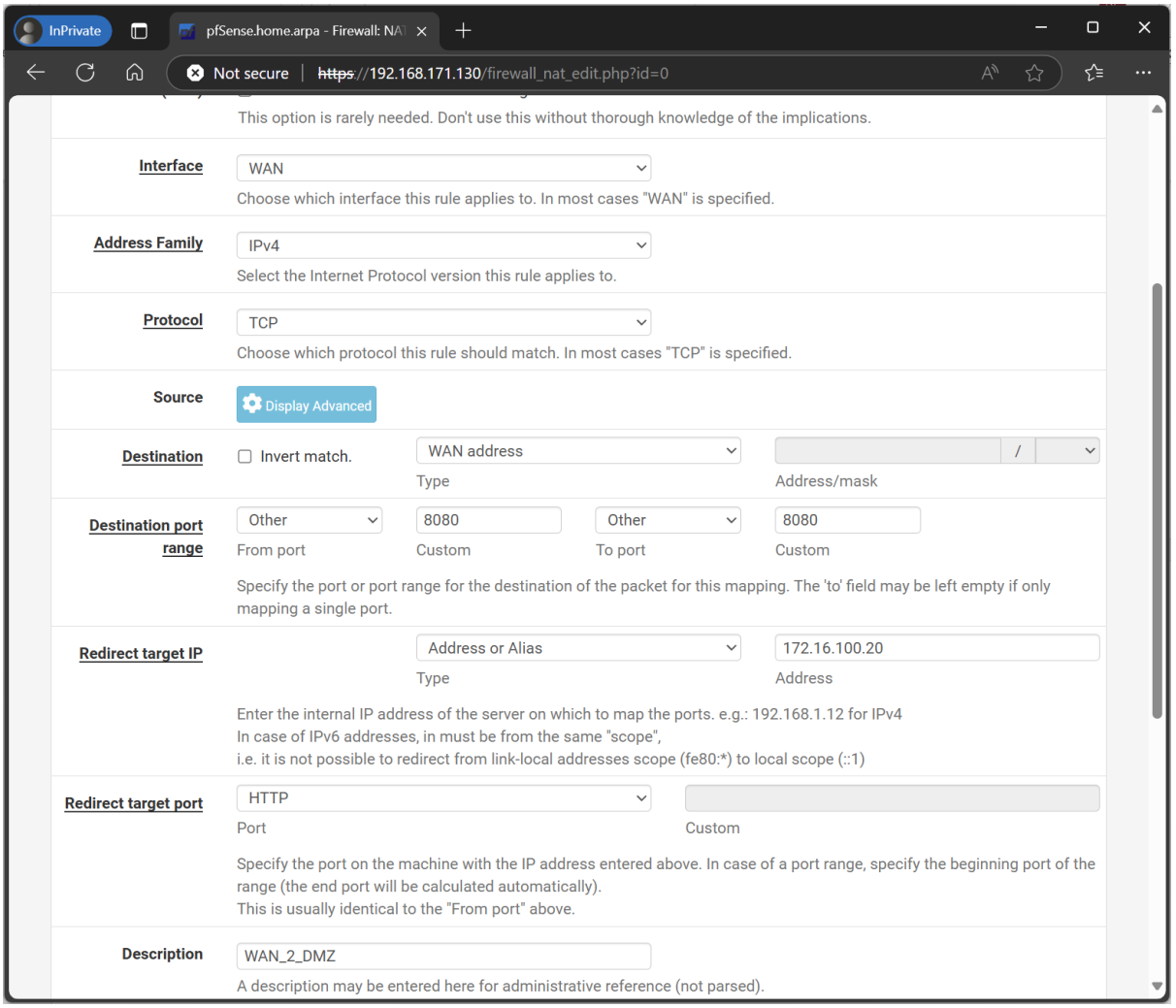
Configuring NAT for Port Forwarding

To allow external users to access the Linux server in the DMZ through the WAN interface, you need to configure **Port Forwarding** in pfSense. Here's how:

1. Go to **Firewall > NAT > Port Forward**.



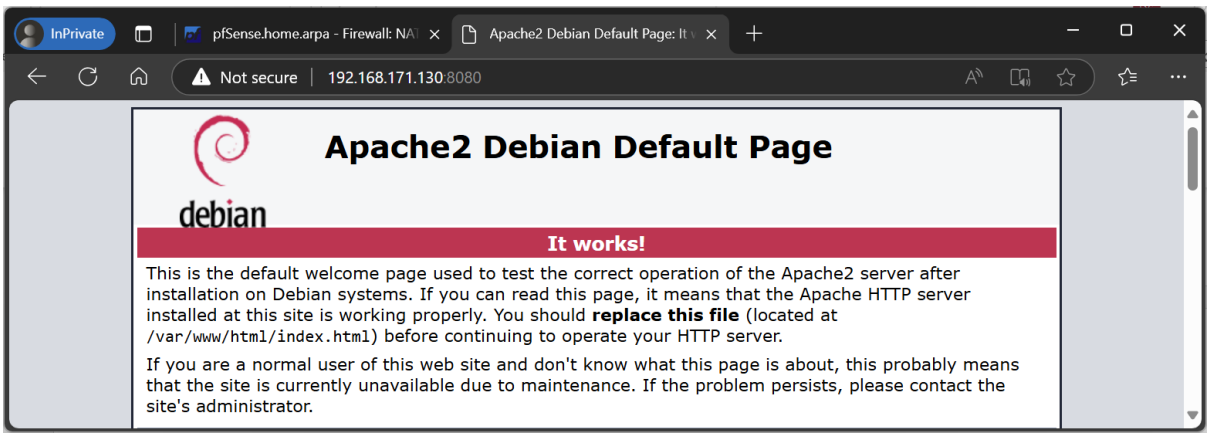
2. Click **Add** to create a new NAT rule.
3. **Configure the Rule:**
    - **Interface**: WAN
    - **Protocol**: TCP
    - **Destination**: WAN Address (This Firewall)
    - **Destination Port Range**: 8080 or the port you want to forward
    - **Redirect Target IP**: 172.16.100.20 (IP address of the DMZ Linux server)
    - **Redirect Target Port**: 80
    - **Description**: "Forward HTTP to DMZ Linux Server"



4. **Save** the rule and click **Apply Changes**.

Testing the Configuration

From a client outside your network, attempt to access the DMZ server by entering the WAN IP address followed by the port (e.g., http://<WAN_IP>:80). Verify that you can connect to the Linux server inside the DMZ.



pfSense Shell Commands

The pfSense shell provides powerful command-line tools for **troubleshooting**, **network monitoring**, and **configuration management**. Analysts and administrators can leverage these commands for quick diagnostics and analysis when working with the firewall. This chapter introduces essential pfSense shell commands, categorized by use case, with examples.

Basic Shell Navigation and Management

These commands help analysts navigate the pfSense shell and manage system services.

- **Enter the shell:** From the pfSense menu, select **Option 8** to access the shell.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.171.130/24
 LAN (lan)       -> em1        -> v4: 172.16.50.1/24
 OPT1 (opt1)     -> em2        -> v4: 172.16.100.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8
```

- **Check pfSense for updates:**

```
pfSense-upgrade -c
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.171.130/24
 LAN (lan)       -> em1        -> v4: 172.16.50.1/24
 OPT1 (opt1)     -> em2        -> v4: 172.16.100.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfSense-upgrade -c
>>> Updating repositories metadata... done.
Your system is up to date
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Checks for available upgrades and the current version of pfSense.

- **Reboot the system:**

```
reboot
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: reboot
```

Firewall and NAT Commands

Commands in this section are useful for managing and troubleshooting **firewall rules** and **NAT settings**.

- **Disable the firewall (for troubleshooting):**

```
pfctl -d
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Temporarily disables the pfSense firewall to allow unrestricted access. Use with caution.

- **Re-enable the firewall:**

```
pfctl -e
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -e
pf enabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

System and Performance Monitoring Commands

These commands help analysts monitor the performance of pfSense and identify potential issues.

- **Monitor CPU and memory usage:**

```
top
```

```
last pid: 96562;  load averages:  0.57,  0.72,  0.37    up 0+00:03:58  17:16:39
46 processes:  2 running, 44 sleeping
CPU:  3.8% user,  0.1% nice,  2.5% system,  0.9% interrupt, 92.7% idle
Mem: 74M Active, 532K Inact, 31M Laundry, 77M Wired, 2488K Free
ARC: 31M Total, 18M MFU, 11M MRU, 568K Anon, 217K Header, 1238K Other
     18M Compressed, 45M Uncompressed, 2.50:1 Ratio
Swap: 1024M Total, 81M Used, 943M Free, 7% Inuse

  PID USERNAME    THR PRI NICE   SIZE    RES STATE    TIME    WCPU COMMAND
  254 unbound       1  20    0    40M  4096B kqread   0:00   0.00% <unbound>
62946 root          5  68    0    13M  1056K uwait    0:00   0.00% dpinger
96123 root          1 108   20   166M   102M RUN      0:00   0.00% netstat
 4932 root          1  20    0    19M  1224K select   0:00   0.00% ntpd
37449 root          1  20    0    13M  1660K pause    0:00   0.00% tcsh
35587 root          1  68   20    13M   864K piperd   0:00   0.00% sh
13973 root          1  20    0    13M   964K bpf      0:00   0.00% filterlog
  402 root          1  20    0   185M  1208K kqread   0:00   0.00% php-fpm
53934 root          1  20    0    13M   796K select   0:00   0.00% syslogd
 4309 root          1  20    0    13M  4096B nanslp   0:00   0.00% <cron>
96562 root          1  20    0    14M  2668K RUN      0:00   0.00% top
79608 root          2  68    0    13M   888K piperd   0:00   0.00% sshg-blocker
  601 root          1  20    0    14M   800K select   0:00   0.00% devd
77552 root          1  68    0    13M  4096B wait     0:00   0.00% <login>
79916 root          1  68    0    13M  4096B wait     0:00   0.00% <sh>
79580 root          1  64    0    19M   872K piperd   0:00   0.00% sshg-parser
```

Provides a real-time view of system resource usage.

- **View disk space usage:**

```
df -h
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: df -h
Filesystem                          Size    Used   Avail Capacity  Mounted on
pfSense/ROOT/default                 16G    817M     15G     5%    /
devfs                               1.0K      0B    1.0K     0%    /dev
pfSense/tmp                          15G    176K     15G     0%    /tmp
pfSense/home                         15G     96K     15G     0%    /home
pfSense/var                          15G    260K     15G     0%    /var
pfSense                              15G     96K     15G     0%    /pfSense
pfSense/reservation                  17G     96K     17G     0%    /pfSense/re
servation
pfSense/var/cache                    15G     96K     15G     0%    /var/cache
pfSense/var/log                      15G    200K     15G     0%    /var/log
pfSense/var/db                       15G    756K     15G     0%    /var/db
pfSense/var/empty                    15G     96K     15G     0%    /var/empty
pfSense/var/tmp                      15G    104K     15G     0%    /var/tmp
pfSense/ROOT/default/cf              15G    268K     15G     0%    /cf
pfSense/ROOT/default/var_cache_pkg   15G     96K     15G     0%    /var/cache/
pkg
pfSense/ROOT/default/var_db_pkg      15G    4.8M     15G     0%    /var/db/pkg
tmpfs                               4.0M    100K    3.9M     2%    /var/run
devfs                               1.0K      0B    1.0K     0%    /var/dhcpd/
dev
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Displays the amount of used and available disk space in a human-readable format.

- **Monitor network traffic in real-time:**

```
tcpdump -i em1
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: tcpdump -i em1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on em1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Captures and displays network traffic on the em1 interface. Use CTRL+C to stop.

- **Check system uptime:**

```
uptime
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: uptime
 5:19PM  up 7 mins, 1 user, load averages: 0.61, 0.60, 0.37
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Displays how long the system has been running since the last reboot.

User and Process Management Commands

These commands allow you to manage users and processes effectively.

- **View currently logged-in users:**

```
who
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: who
root             ttyv0        Oct 29 17:13
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

- **List all running processes:**

```
ps aux
```

```
root    56638   0.0  0.0  12656    4  -  IW   -       0:00.00 minicron: helper
root    56951   0.0  0.0  12656    4  -  IWs  -       0:00.00 /usr/local/bin/mi
root    57278   0.0  0.0  12656    4  -  IW   -       0:00.00 minicron: helper
root    62946   0.0  0.3  13508  652  -  Is   17:13   0:00.17 /usr/local/bin/dp
root    79140   0.0  0.0  13320    4  -  IWs  -       0:00.00 /bin/sh /usr/loca
root    79251   0.0  0.2  12660  380  -  I    17:13   0:00.00 /bin/cat
root    79580   0.0  0.2  19324  416  -  IC   17:13   0:00.00 /usr/local/libexe
root    79608   0.0  0.3  13268  652  -  IC   17:13   0:00.01 /usr/local/libexe
root    79686   0.0  0.0  13320    4  -  IW   -       0:00.00 /bin/sh /usr/loca
root    80049   0.0  0.2  13320  380  -  I    17:13   0:00.00 /bin/sh /usr/loca
root    80139   0.0  0.9  12656 1692  -  INC  17:21   0:00.00 sleep 60
root    35587   0.0  0.5  13320  920 v0- IN   17:13   0:00.02 /bin/sh /var/db/r
root    37449   0.0  0.8  13792 1684 v0  S    17:13   0:00.04 /bin/tcsh
root    77552   0.0  0.0  13204    4 v0  IWs  -       0:00.00 login [pam] (logi
root    79916   0.0  0.0  13320    4 v0  IW   -       0:00.00 -sh (sh)
root    80547   0.0  1.5  13388 2976 v0  R+   17:21   0:00.00 ps aux
root    80836   0.0  0.0  13320    4 v0  IW   -       0:00.00 /bin/sh /etc/rc.i
root    77859   0.0  0.2  12788  380 v1  Is+  17:13   0:00.00 /usr/libexec/gett
root    77957   0.0  0.2  12788  380 v2  Is+  17:13   0:00.00 /usr/libexec/gett
root    78293   0.0  0.2  12788  380 v3  Is+  17:13   0:00.00 /usr/libexec/gett
root    78351   0.0  0.2  12788  380 v4  Is+  17:13   0:00.00 /usr/libexec/gett
root    78598   0.0  0.2  12788  376 v5  Is+  17:13   0:00.00 /usr/libexec/gett
root    78642   0.0  0.2  12788  376 v6  Is+  17:13   0:00.00 /usr/libexec/gett
root    78941   0.0  0.2  12788  380 v7  Is+  17:13   0:00.00 /usr/libexec/gett
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Displays all active processes along with their resource usage.

Backup and Restore Commands

These commands are useful for backing up or restoring pfSense configurations.

- **Backup the current configuration:**

```
cp /cf/conf/config.xml /root/config_backup.xml
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: cp /cf/conf/config.xml /root/confi
g_backup.xml
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Creates a backup of the current configuration file.

- **Restore a previous configuration:**

```
cp /root/config_backup.xml /cf/conf/config.xml && reboot
```

Restores a backup and reboots the system to apply the changes.

Testing and Diagnostics Commands

Analysts often need to verify connectivity and troubleshoot network issues. These commands provide useful tools for that.

- **Test DNS resolution:**

```
nslookup google.com
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: nslookup google.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.75.46
Name:   google.com
Address: 2a00:1450:4028:806::200e

[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Tests if DNS resolution is working correctly.

- **Test HTTP service on a remote server:**

```
curl -I http://172.16.100.20
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: curl -I http://172.16.100.20
HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 17:24:36 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Tue, 28 May 2024 05:59:08 GMT
ETag: "29cd-6197d550c6ce0"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html

[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Checks the HTTP response headers of the Linux server in the DMZ.

Managing Packages in pfSense

The power of **pfSense** lies not only in its robust firewall and routing capabilities but also in the extensive features offered through the **Package Manager**. The package manager allows administrators to install, manage, and upgrade additional software modules, bringing advanced features like network monitoring, intrusion detection, ad-blocking, and VPN utilities to the firewall.

Introduction to the pfSense Package Manager

The **Package Manager** provides a modular approach to pfSense, enabling users to extend its core functionality. Packages are software add-ons that cover a variety of uses, such as security monitoring, traffic analysis, or VPN setup. This flexibility makes pfSense adaptable for both small networks and complex enterprise environments.

The package manager is split into two main sections:

- **Installed Packages:** Displays packages currently installed on your pfSense system.
- **Available Packages:** Offers a list of packages you can install to extend pfSense's functionality.

Navigating the Package Manager

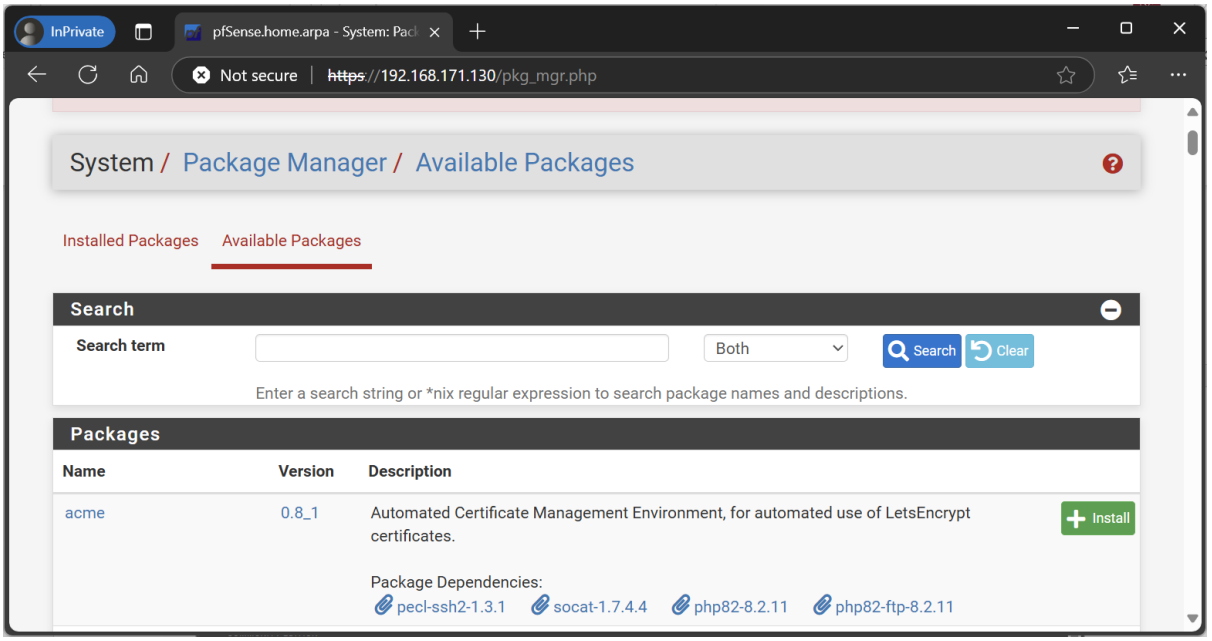
Accessing the Package Manager

To begin managing packages:

1. **Login** to the pfSense Web GUI.
2. Navigate to **System** > **Package Manager**.

You will find two tabs:

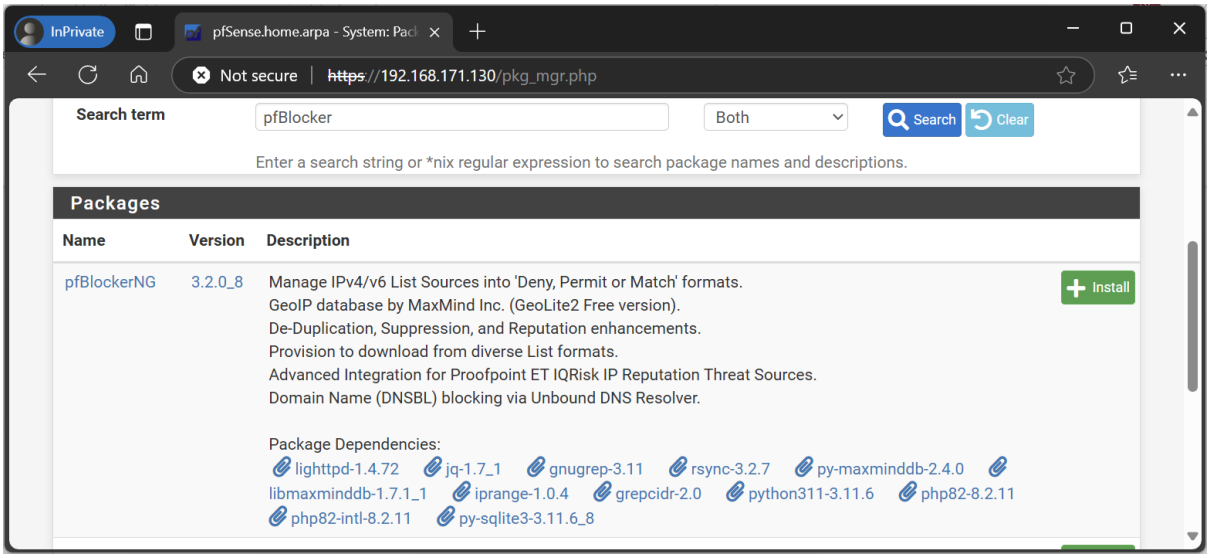
- **Installed Packages:** View and manage the installed packages.
- **Available Packages:** Search for and install new packages.



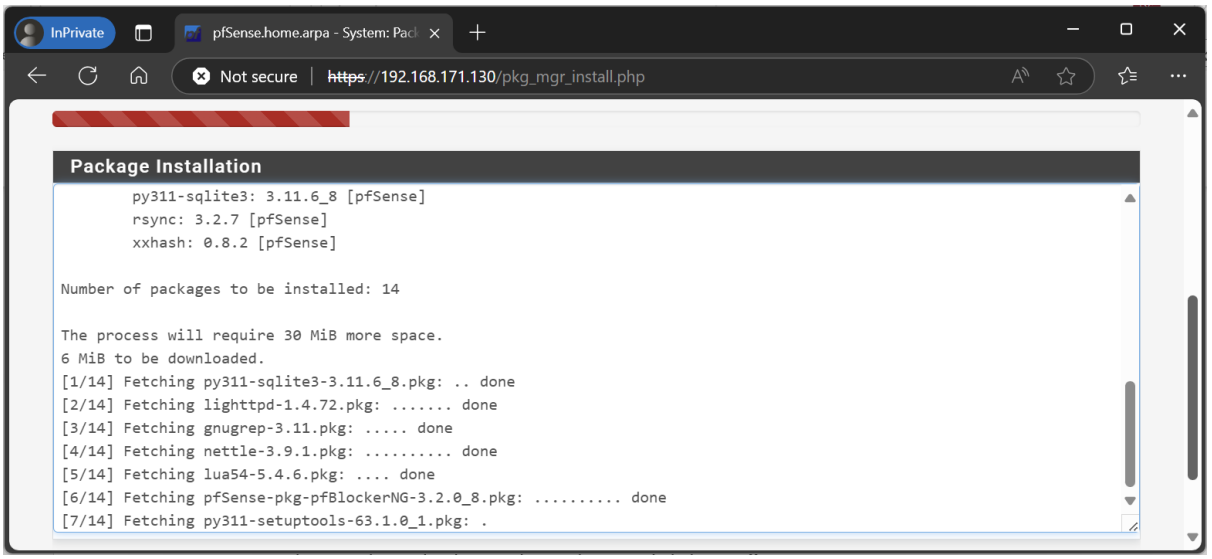
Working with Packages: Installation and Management

Installing a New Package

1. Navigate to **System** > **Package Manager** > **Available Packages**.
2. In the **Search** box, enter the name or a keyword related to the desired package.
3. Click **Search**.



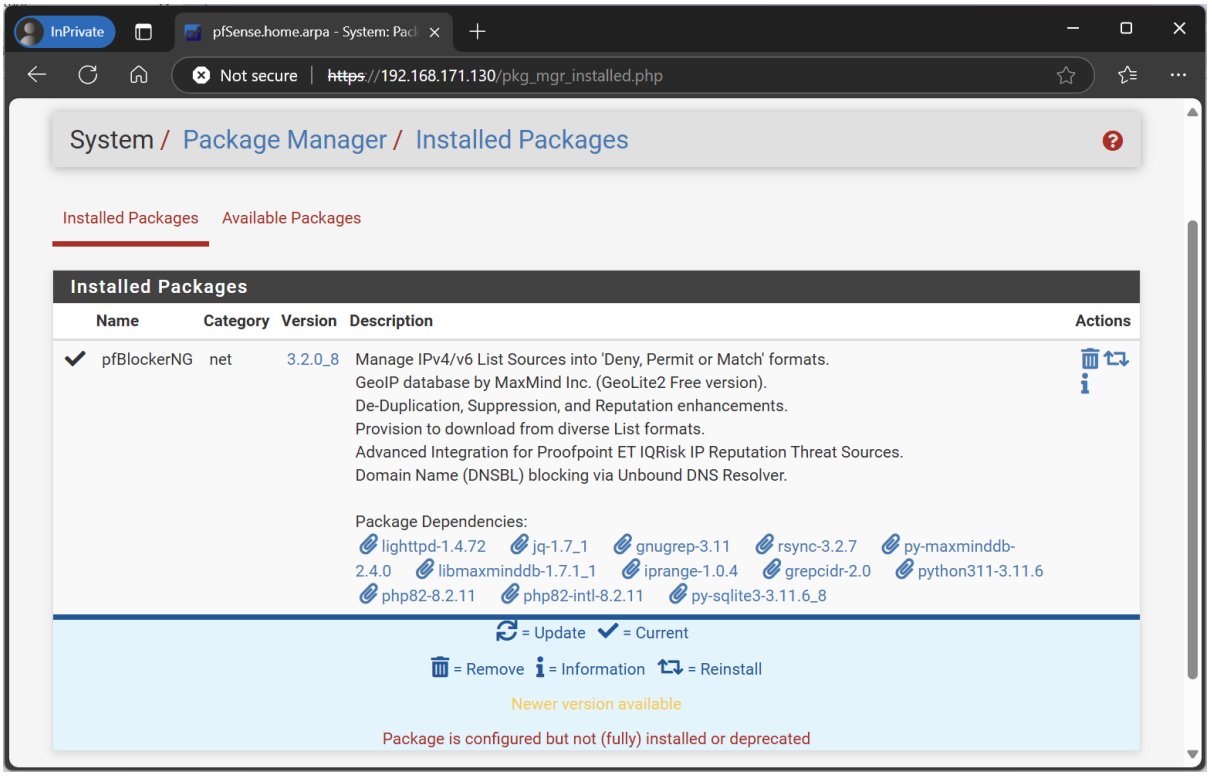
4. In the search results, locate the package and click **Install**.
5. Confirm the installation and monitor the progress.



Tip: Packages like **Suricata** or **pfBlocker-NG** may require additional configuration under the **Services** menu after installation.

Managing Installed Packages

1. Go to **System** > **Package Manager** > **Installed Packages**.
2. Review the list of installed packages with their current versions.
3. From this view, you can:
    - **Update:** Install the latest version if an update is available.
    - **Reinstall:** Reinstall a package if it encounters issues.
    - **Remove:** Uninstall a package no longer in use.



Popular Packages and Use Cases

Here are some of the most widely used packages that provide advanced features to pfSense users:

Suricata (Intrusion Detection and Prevention System)

- **Description:** Suricata monitors network traffic for malicious activity and can block threats in real-time.
- **Use Case:** Ideal for security analysts who need to detect suspicious activities and log them.
- **Command Example:**

```
suricata -r /var/log/packets.pcap
```

This command runs Suricata against a packet capture file for offline analysis.

pfBlocker-NG (Ad-blocking and GeoIP Filtering)

- **Description:** Blocks ads and manages IP filtering based on geographic location or threat intelligence feeds.
- **Use Case:** Security administrators can use pfBlocker-NG to prevent connections to malicious domains and optimize network performance.

ntopng (Network Traffic Analyzer)

- **Description:** Provides in-depth visibility into network traffic and usage trends.
- **Use Case:** Network administrators use ntopng to identify bandwidth hogs, troubleshoot performance issues, and analyze traffic patterns.

OpenVPN Client Export Utility

- **Description:** Simplifies the export of OpenVPN configuration files for clients.
- **Use Case:** Facilitates easy deployment of VPN configurations for end users.

Managing Packages via the Command Line

While the Web GUI is the primary way to manage packages, the **shell interface** offers more control for advanced users. Below are some useful commands to manage packages through the shell.

Basic Package Commands

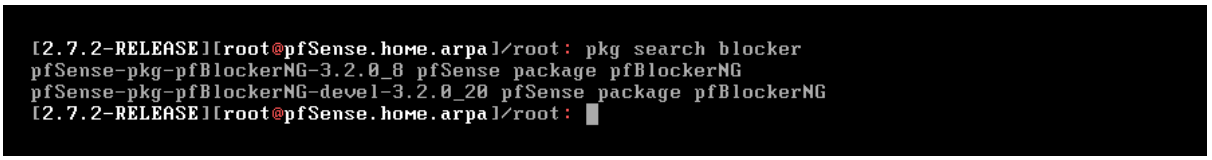
- **List Installed Packages:**

```
pkg info
```

```
ed
rrdtool-1.8.0_2                 Round Robin Database Tools
rsync-3.2.7                     Network file distribution/synchronization utility
scponly-4.8.20110526_5          Tiny shell that only permits scp and sftp
smartmontools-7.4               S.M.A.R.T. disk monitoring tools
sqlite3-3.43.1,1                SQL database engine in a C library
ssh_tunnel_shell-0.2_1          SSH tunnel shell
sshguard-2.4.2_2,1              Protect hosts from brute-force attacks against SS
H and other services
strongswan-5.9.11_3             Open Source IKEv2 IPsec-based VPN solution
uclcmd-0.2.20211204             Command line tool for working with UCL config fil
es
unbound-1.18.0_1                Validating, recursive, and caching DNS resolver
voucher-0.1_3                   Voucher support
vstr-1.0.15_1                   General purpose string library for C
whois-5.5.7                     Marco d'Itri whois client
wol-0.7.1_4                     Tool to wake up Wake-On-LAN compliant computers
wpa_supplicant-2.10_9           Supplicant (client) for WPA/802.1x protocols
wrapalixresetbutton-0.0.8       Utility to detect platform reset button state for
 use in scripting
xinetd-2.3.15_2                 Replacement for inetd with better control and log
ging
xxhash-0.8.2                    Extremely fast non-cryptographic hash algorithm
zstd-1.5.5                      Fast real-time compression algorithm
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

- **Search for a Package:**

```
pkg search <package_name>
```



- **Install a Package:**

```
pkg install <package_name>
```

- **Remove a Package:**

```
pkg delete <package_name>
```

- **Update the Package List:**

```
pkg update
```

- **Upgrade All Packages:**

```
pkg upgrade
```

Note: Using the command line allows for quick troubleshooting if the Web GUI is unavailable or if you encounter errors during the package installation process.