

AI-03018 pfSense Setup

Owner	© Rigel Arcayan
Tags	Project
Created time	@September 21, 2025 11:02 AM

What is pfSense? What is the story behind pfSense? Is pfSense really free? How pfsense owner generates revenue? What commercial products that are based in pfSense? List top use case for pfsense (self-hosted and Aure). Create a step by step pfsense deployment (bare metal and hyper-v)

pfSense is a free and open-source firewall and router software distribution based on FreeBSD. It can be installed on a physical computer or a virtual machine to create a dedicated network firewall and router. It offers a wide array of features typically found in expensive commercial firewalls, including VPN support, traffic control, and intrusion detection.

The Story Behind pfSense

The history of pfSense dates back to 2000 as a fork of **m0n0wall**, another popular open-source firewall project. The goal was to improve upon m0n0wall's capabilities and address its limitations. It was developed by Chris Buechler and Scott Ullrich, who officially released the first version in 2006. The name "pfSense" comes from the packet-filtering tool "PF" (Packet Filter) used by many BSD-based platforms. In 2012, **Netgate** became the official host of the pfSense project and has since supplied most of the engineering and support for it.

Free and Revenue Model

pfSense Community Edition (CE) is indeed free and open-source, and there are no licensing costs. The company behind pfSense, Netgate, generates revenue primarily through:

- **Selling hardware appliances:** Netgate sells pre-configured hardware devices with the commercial version of the software, **pfSense Plus**, pre-installed.

- **Support and services:** They offer paid support subscriptions and professional services for businesses and enterprises.
- **Commercial software licenses:** The pfSense Plus software is a commercial product with a different license from the free CE version. It is often included with Netgate appliances and is also available for purchase for cloud deployments on platforms like AWS and Azure.

Commercial Products Based on pfSense

Netgate is the primary company that develops and sells commercial products based on pfSense. Their product line includes a range of **Netgate appliances** that come pre-loaded with **pfSense Plus** software. These appliances are designed for various use cases, from home and small businesses to large enterprises and data centers.

Top Use Cases for pfSense

Self-Hosted (Bare Metal/Virtual Machine)

- **Home/SOHO (Small Office/Home Office) Firewall:** Replacing a standard consumer-grade router for more advanced security, VPN, and network control.
- **VPN Server/Client:** Creating secure remote access to a network or connecting multiple sites via a site-to-site VPN.
- **Traffic Shaping and QOS (Quality of Service):** Prioritizing network traffic for specific applications or users, ensuring a smooth experience for critical services like VoIP or streaming.
- **Intrusion Detection and Prevention (IDS/IPS):** Using packages like Snort or Suricata to monitor network traffic for malicious activity.
- **Multi-WAN Load Balancing and Failover:** Connecting to multiple internet service providers for redundancy and increased bandwidth.

Azure Cloud

- **Securely Connecting On-Premise to the Cloud:** Using pfSense as a firewall and VPN gateway to create a secure tunnel between a physical office network

and a virtual network in Azure.

- **Protecting Cloud-Based Applications:** Deploying pfSense as a virtual network appliance to act as a firewall for cloud workloads and applications, providing stateful filtering and packet inspection.
- **Providing Secure Remote Access:** Enabling secure remote access for users to connect to their cloud-based applications and data via VPN.

Step-by-Step pfSense Deployment

The following steps provide a general overview of a pfSense installation. Specific details may vary based on your hardware and network configuration.

Bare Metal (Physical Machine) Deployment

1. **Download pfSense:** Download the pfSense CE installer from the official website. You'll typically want the AMD64 (64-bit) installer.
2. **Create Bootable Media:** Use a tool like Rufus or Etcher to create a bootable USB drive from the downloaded ISO file.
3. **Boot the Machine:** Insert the USB drive into your target machine and boot from it. You may need to change the boot order in the machine's BIOS/UEFI settings.
4. **Installer Wizard:** Follow the on-screen instructions. The installer will guide you through partitioning the disk and copying the necessary files.
5. **Assign Interfaces:** After the installation, the system will reboot and prompt you to assign network interfaces. You'll need at least two: one for the WAN (Wide Area Network) and one for the LAN (Local Area Network).
6. **Initial Configuration:** The system will boot into the console. You can set up basic network settings from here, but the primary configuration is done through the web interface.
7. **Access Web GUI:** Connect a computer to the LAN port of the pfSense machine. The pfSense machine will act as a DHCP server and assign an IP to your computer. Open a web browser and navigate to the default pfSense IP address (usually 192.168.1.1).

8. **Run the Setup Wizard:** Log in with the default credentials (admin/pfsense) and follow the initial setup wizard to change the default password, configure DNS, and set up your WAN connection.
-

Hyper-V Deployment

1. **Download pfSense:** Download the pfSense CE installer ISO file.
2. **Create a Virtual Machine:** In Hyper-V Manager, create a new virtual machine.
 - **Generation:** Select **Generation 2**.
 - **Memory:** Assign at least 1 GB of RAM (2 GB is recommended for a more responsive interface and to run packages).
 - **Networking:** Connect the first network adapter to an **External Virtual Switch** (this will be your WAN).
 - **Hard Disk:** Create a virtual hard disk with at least 10-20 GB of space.
 - **Installation:** Select to install an operating system from a bootable image file and point it to the pfSense ISO.
3. **Add a Second Network Adapter:** After creating the VM, go to its settings and add a second network adapter. Connect this one to an **Internal** or **Private Virtual Switch** (this will be your LAN).
4. **Boot the VM:** Start the virtual machine and follow the on-screen installation wizard, similar to the bare metal installation.
5. **Assign Interfaces:** When prompted, assign the network adapters you created in Hyper-V Manager to the WAN and LAN roles within pfSense.
6. **Access Web GUI:** Connect another VM or a physical machine to the LAN virtual switch. Use a web browser to access the pfSense web interface and complete the initial configuration wizard.

This video provides a practical walkthrough for installing and configuring pfSense as a firewall within a Hyper-V environment.

How to Install and Configure pfSense Firewall on Hyper-V

How many physical and virtual ethernet ports needed for a hyper-v pfsense deployment. I'm using a laptop for testing.

For a basic Hyper-V pfSense deployment on a laptop, you'll need at least **one physical Ethernet port** and **two virtual Ethernet ports**. Here's why:

- **1 Physical Port (Your Laptop's Ethernet Port):** This will be your **WAN** (Wide Area Network) connection. You will create an **External Virtual Switch** in Hyper-V that is bound to this physical port. This allows the pfSense VM to get its internet connection from your modem or existing router.
- **2 Virtual Ports (within the pfSense VM):**
 - **WAN Port:** This is the first virtual network adapter you assign to the pfSense VM. You connect it to the External Virtual Switch you created in the step above. This adapter gets the public IP from your internet provider.
 - **LAN Port:** This is the second virtual network adapter. You connect it to a **Private** or **Internal Virtual Switch** in Hyper-V. This switch is what your other virtual machines will connect to for internet access. The pfSense VM will act as the firewall and router for this virtual network, providing services like DHCP and NAT.

While a single physical port is the minimum for this setup, using an additional USB Ethernet adapter is a common and recommended practice. This would allow you to dedicate one physical port to the WAN and a second to the LAN, making the setup cleaner and separating the host's traffic from the virtual network's.

The provided video offers a step-by-step guide on how to install and configure pfSense on a Hyper-V virtual machine, which is relevant to your use case.