

Download the installer from the pfSense website, taking care to get the version that matches your environment and preferred installation method. Burn the CD or write the image to a USB drive as required.

Boot your device from the installation media you created and wait until it has completed booting, and displays the software license screen. Go through and accept the license terms and move on to the installation. Select “Install” from the menu, choose the correct keyboard layout for your region, then select continue.

From the next menu, select automatic partitioning and hit enter to continue

Configure a computer with a static IPv4 address in the same range as the IPv4 address you assigned to the LAN interface on the firewall. You can connect this computer directly to the LAN port on the firewall (using a crossover cable if you’re working with older hardware that doesn’t support Auto-MDIX) or connect via a switch.

Using your web browser, go to the LAN IPv4 address that we configured in the previous step. Log in using the username “admin” and the default password “pfsense”. You will be presented with the initial setup wizard. Click on next, then next again at the following screen to begin the setup of your new firewall.

Enter the name you want to give your firewall, and the domain associated with your internal office network. We’re going to be boring and use “firewall” for the name, and “local” for the domain, but you should probably come up with something more distinctive

pfSenses is a firewall oriented operating system that acts as a router. This assignment was done in VMware. The first step was to download the community version of pfSense which is shown in the images (this would be the iso image) from there you will create a new virtual machine and do your custom install as you would any other VM (the typical installation). Ensure the ISO image is located and the VM picks up the ISO. After installation you would have to enter pfSense with the default gateway, by default there are two interfaces with the WAN which is configured by DHCP client without VLANs or any additional configuration, LAN is configured with 192.168.1.1/24 and with DHCP enabled , access to administration is allowed whereas access to administration is not allowed for WAN. For this assignment I created a second NAT adapter and that was customized in the VM and connected windows 10 to it.

Once pfsense has been installed on the ASCII text screen I chose option 8, which was the shell to ping a website to ensure WAN connection. pfSense is designed to connect directly to the internet and have the public IP address provided by me, it is very important to have a public IP and not be behind CGNAT, otherwise we will not be able to do port forwarding or remotely access pfSense itself. Once VLAN 20 on em) is created in pfSense I clicked on to save changes.

I should add to in order to configure my pfsense on the same network I changed windows 10 to Vmnet14 as I did in pfsense, this means windows 10 as a client had not internet access but was directly connected to pfSense that operates as a router and a firewall. In Windows 10 I changed the properties of the ethernet connection in ipv4 properties settings and added the default IP of 192.168.1.1 and as a default gateway I changed it to 192.168.1.100 Once that was configured and save I opened a browser and entered the address of the LAN which is 192.168.1.1, which will say it is not a secure sit but check advanced setting and continue to IP which will bring to the pfSense site and for this the default username is admin and password is pfsense.

**To Summarize:**

Install pfSense on your device by downloading the installer from the pfSense website and following the instructions.

Configure the basic networking settings on the console, such as the WAN and LAN interfaces, the IP addresses, and the passwords.

Run the initial configuration wizard on the web interface, which will guide you through the general settings, such as the hostname, the DNS servers, and the time zone.

Optionally, enable IPv6 support if your ISP provides it and you want to use it.

Set up local network services, such as DHCP servers, DNS servers, and NTP servers, for your LAN and any VLANs you want to create.

|  |  |
| --- | --- |
| 1. Edit the network adapter in VM |  |
| 1. Add a Vmnet host-only in VM and disable the dhcp |  |
| 1. Open the VM |  |
| 1. Press installer and next |  |
| 1. Give it a name and click on next |  |
| 1. Configure memory to 2 gb |  |
| 1. Configure processers to 2 |  |
| 1. First network adapter should be bridge |  |
| 1. Add another network adapter and go to custom to chose vmnet2 |  |
| 1. Start running pfsense |  |
| 1. Click on ok |  |
| 1. Click on select |  |
| 1. CHOSE BIOS AND CLICK NEXT |  |
| 1. REBOOT PFSENSE |  |
| 1. Write 7 to check internet working |  |
| 1. Enter the ip address 8.8.8.8 to check if internet working |  |
| 1. Now go to client to check if pfsense work before running check the network adapter and go to custom and put the vmnet2 |  |
| 1. Write the default ip 192.168.1.1 and press advanced to check the fireware |  |
| 1. And her we go enter the username and password by default   “admin”  “pfsense” |  |
| 1. Press on change password |  |
| 1. Put the new password and scroll down to click on save |  |
| 1. The ip address 192.168.1.100 connected to the internet and to pfsense |  |
| 1. Pfsense give me that admin from 192.168.1.100 succsefully login |  |
| 1. Verifiy the internet working in windows server 2019 |  |