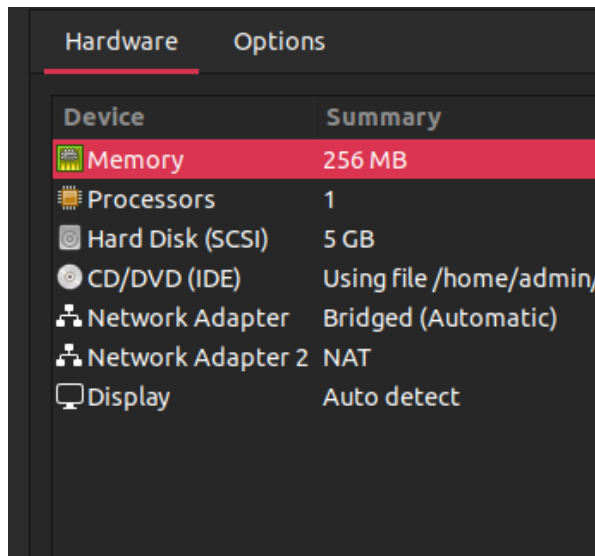


# The Firewall

From a security standpoint, firewalls are some of the most important tools in an enterprise environment. Firewalls allow us to control the traffic that enters and exits our networks by creating rules and setting policies in place to create a safe environment. For this lab, I decided to go with an open-source firewall; pfSense. There are a few reasons as to why I decided to use pfSense. First, the software being open-source means that it is free to download and you can use it as long as you want, unlike other “free” subscription based software. Also, from my research I found that pfSense is relatively easy to implement with VMware Workstation and should function as a normal firewall.

A screenshot of the VMware Workstation 'Hardware' settings window. The window has two tabs: 'Hardware' (selected) and 'Options'. Below the tabs is a table with two columns: 'Device' and 'Summary'. The table lists several hardware components: Memory (256 MB), Processors (1), Hard Disk (SCSI) (5 GB), CD/DVD (IDE) (Using file /home/admin...), Network Adapter (Bridged (Automatic)), Network Adapter 2 (NAT), and Display (Auto detect). The 'Memory' row is highlighted in red.

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	5 GB
CD/DVD (IDE)	Using file /home/admin...
Network Adapter	Bridged (Automatic)
Network Adapter 2	NAT
Display	Auto detect

Configuring pfSense and integrating it into my environment proved to be difficult for a number of reasons. To start, my knowledge on firewalls was very limited to their intended functions and some different types of firewalls. I have never really worked with any before and therefore had to do a lot of research before digging into configuration. After I got a grasp of what my intended outcome was and how I would go about achieving it, I started by downloading the

pfSense Community Edition on my main physical machine. It is important that you download the raw image and the correct version for your machine. I then created a new VM in VMware. You need to choose to install an operating system later, ‘Other’, and ‘FreeBSD 11 64-bit’. Then choose a name for the VM and allocate your resources. I went with 1 CPU, 1 Processor core and 256MB of memory. Next, you need to select a type of network adapter, I chose to go with a bridged adapter (to start). Then, you need to create an IDE virtual disk, set it to 5GB, and choose to store it as a single file. Once this is completed, click finish and enter the virtual machines advanced settings. I opted to

remove unnecessary things like the USB controller and Sound card after I selected the CD/DVD(IDE) and connected it to the ISO for pfSense. All that is left is to make sure that the machine connects at power on.

Once the VM has booted up, it is now time for the actual configuration of the machine. Press enter to accept the copyright notice, choose 'Install' and 'OK'. In the partitioning options choose 'Auto(UFS)' and pfSense should start installing. At the end, it will ask if you want to do any manual configuration, select 'NO' and reboot the system. Once rebooted, pfSense will start its initial configuration phase. The important step here is to make sure to set your WAN adapter to em0, which was the bridged adapter in my case. Once this is done, you will get to a sort of terminal with a number of options. Select 'Halt System' to shut it down. Go back into the advanced settings of the VM and add another ethernet adapter. This time we will be adding a NAT adapter that will function as our LAN adapter. Power the machine on and you should be back at the terminal with all of the options. Select option 2 'Assign Interfaces' and again option 2 for 'LAN(em1)'. At this point you will need to know what the IPv4 settings for the domain controller are and type them all in accordingly. It is important to note that I decided not to use pfSense as a DHCP server because I already configured AD DHCP. Type 'y' to revert to the HTTP webConfigurator protocol and hit enter. To recap what things should look like at this point, my WAN is a 192 address and my LAN is a 172 address.

The final step to setting up pfSense is logging into the web console. For this you will need to be able to access a web browser and simply type the LAN address into the search bar. The first login will be the default credentials of 'admin' as the username and 'pfsense' as the password. Go to system / general setup and enter the correct values for hostname, domain, dns servers, and timezone. Then, navigate to available packages and install 'open-vm-tools'. Finally, go to system / user manager and select the 'admin' account and change the password from the default. Reboot your system and you are all

set. The firewall is finally configured and should now be functioning as intended. At this point, you can apply rules, set different LAN interfaces, and choose how to filter traffic.

# **Resources**

Downloading pfSense on VMware

<https://www.vgemba.net/vmware/pfSense-VMware-Workstation/>