Lab 2: Setting up and configuring a pfSense firewall

Introduction

In this lab, we will discuss the details of deploying a software-based firewall—pfSense—and see how to configure it to start sending events such as blocked and allowed connections and other interesting information to a syslog (or SIEM) server.

I chose the pfSense software-based firewall because it is the most versatile, stable, expandable, and configurable firewall; putting no money down will buy you. A pfSense VM can conveniently add a firewall, routing, network address translation (NAT), and event DPI (through additional add-ons) to a lab setup.

Objectives for this assignment:

1. Deploying the pfSense VM
2. Configuring pfSense
3. Configuring log forwarding to syslog (Security Onion)

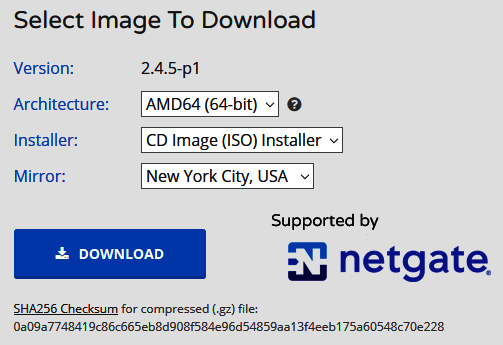
**Submission:** You need to submit a detailed lab report, with screenshots, to describe what you have done and observed. Questions will be defined as you progress through the lab. The lab report will be compiled as a Word document and submitted on Brightspace by **MONTH DAY at TIME AM/PM.**

Objective 1: Deploying the pfSense VM

We will now deploy a Security Onion VM for our lab environment. Follow along with the next process to get the VM up and running.

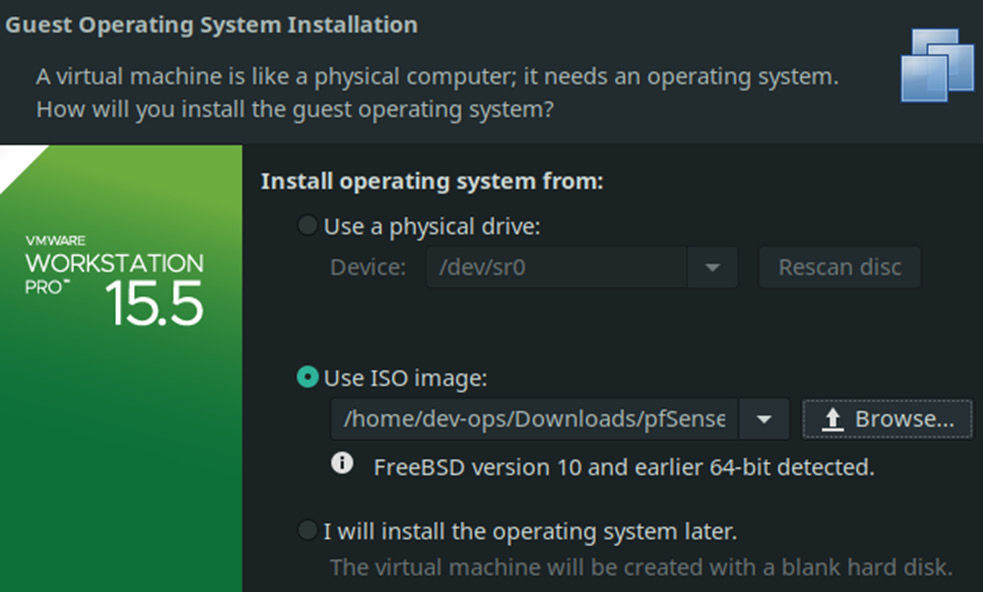
1. Head on over to https://www.pfsense.org/download/ and download the latest version of the pfSense install ISO file. Make sure to select the proper architecture for your hardware (**AMD64** if you install on a virtual platform) as well as choosing the **CD Image (ISO) Installer** media, as illustrated in the following screenshot:

Figure 1.1 – Exercise 2: Downloading pfSense



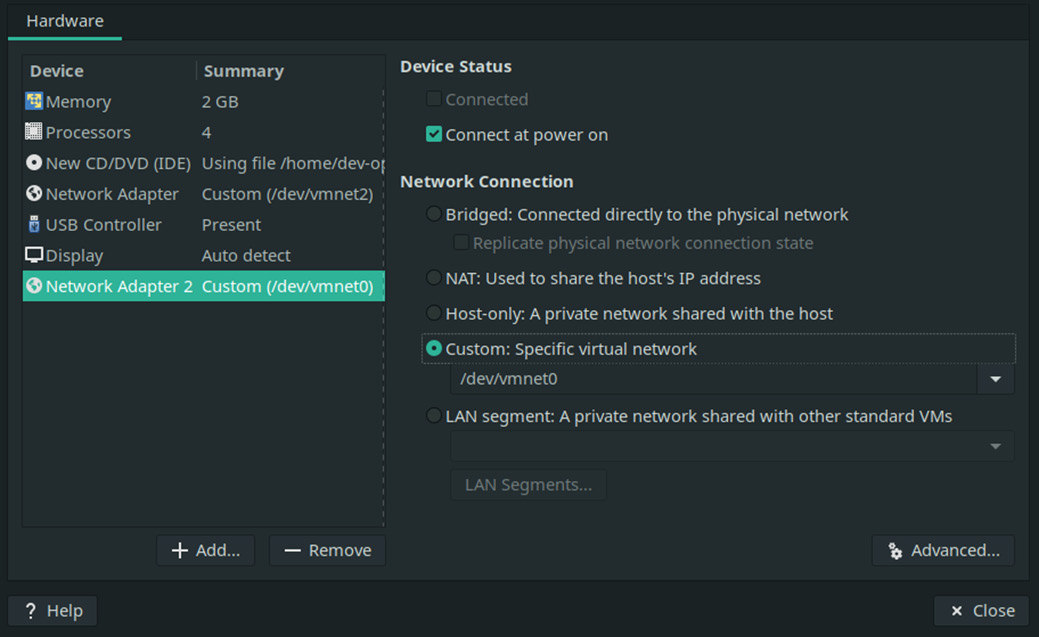
2. As we did in the previous exercise, create a new VM in VMware Workstation and attach the freshly downloaded ISO image to install from. VMware should automatically detect that this is a **FreeBSD** operating system, but if it fails to do so, select **Other – FreeBSD version 10 and earlier 64-bit** in the operating system type screen, as illustrated in the following screenshot:

Figure 1.2 – Exercise 2: Creating a VM



3. Give the VM a name and configure the hardware settings to resemble this, as illustrated in the following screenshot:

Figure 1.3 – Exercise 2: VM hardware settings



Notice that there are two interfaces configured. Add as many as you will need at this point.

4. The VM is now ready to start up. Click the **Power On this Virtual Machine button** and wait until the **pfSense Installer** appears.

5. Simply hit **Accept** on the initial screen, followed by **OK** on the **Welcome** screen, as illustrated in the following screenshot:

Figure 1.4 – Exercise 2: Installing pfSense – Installer screen

A screenshot of a computer

Description automatically generated

6. On the **Keymap Selection** screen, opt for **Continue with default keymap** and click **Select**.

7. On the **Partitioning** screen, stick with the default **Auto (UFS)** option and select **OK**, as illustrated in the following screenshot:

Figure 1.5 – Exercise 2: Installing pfSense – partioning

A screenshot of a computer

Description automatically generated

8. Now, the pfSense operating system is installing, as can be seen in the following screenshot:

Figure 1.6 – Exercise 2: Installing pfSense - installing

A screenshot of a computer

Description automatically generated

9. When it finishes, opt for **No** when asked if manual modifications are required, then click **Reboot** on the final screen, as illustrated in the following screenshot:

Figure 1.7 – Exercise 2: Installing pfSense – rebooting

A screenshot of a computer

Description automatically generated

10. After the VM is completely rebooted, select **2** from the main screen to start the **Set interface(s) IP address** configurationprocess.

11. Select the interface for the LAN side of the firewall (**2**, in my case) and specify the IP address you want to assign to that interface (**172.25.100.1**), as illustrated in the following screenshot:

Figure 1.8 – Exercise 2: Configuring pfSense – LAN IP address

A screenshot of a computer

Description automatically generated

12. Specify a netmask (**24**).

13. Hit *Enter* to skip specifying a gateway and, finally, decide whether you want to enable a **Dynamic Host Configuration Protocol (DHCP)** server on the LAN interface (**y/n**)

14. The settings will be applied, so hit Enter once done to complete the process, as illustrated in the following screenshot:

Figure 1.9 – Exercise 2: Configuring pfSense – IP subnet mask

A screenshot of a computer

Description automatically generated

This concludes the installation of the pfSense VM. Next, we will examine the firewall's basic configuration.

Objective 2.0: Configuring pfSense

As the preceding screenshot in the previous section shows, the **WebConfiguration** address for the newly created pfSense firewall is **https://172.25.100.1.** We will be using this **Uniform Resource Locator (URL)** to configure the firewall. The first time we log in to the **WebConfigurator** portal (the default credentials are **admin** and **pfsense**), we are presented with some initial configuration steps. The login screen is shown in the following screenshot:

Figure 1.10 – Exercise 2: Configuring pfSense – web portal login

A login screen with a green button and white text

Description automatically generated

Once we are logged in, the initial configuration process starts automatically. Follow the next instructions to get through these initial configuration steps:

1. On Step 1, click **Next**.
2. In Step 2, specify a name for the server and enter the primary and secondary DNS servers to use. I specified **1.1.1.1** as the primary server and **9.9.9.9** as the secondary one. Leave the **Allow DNS servers to be overridden by DHCP/PPP on WAN** box checked, and click Next.
3. On Step 3, select the **Coordinated Universal** **Time (UTC)** time zone from the dropdown (in order to have the correct timestamp generated with events that we will be sending to Security Onion, we need to set the time zone for the pfSense firewall to **UTC**, a format that is universally accepted as default by many network and security devices and that allows for convenient synchronization of event log timestamps across multiple systems and devices).
4. On Step 4, define the **wide area network** (**WAN**) interface setup (**DHCP**, in my case) and click **Next**.
5. On Step 5, define the LAN Interface (already done earlier) and click **Next**.
6. On Step 6, change the default admin password to something more secure than **pfsense**, then click **Next**.
7. On Step 7, click **Reload**.

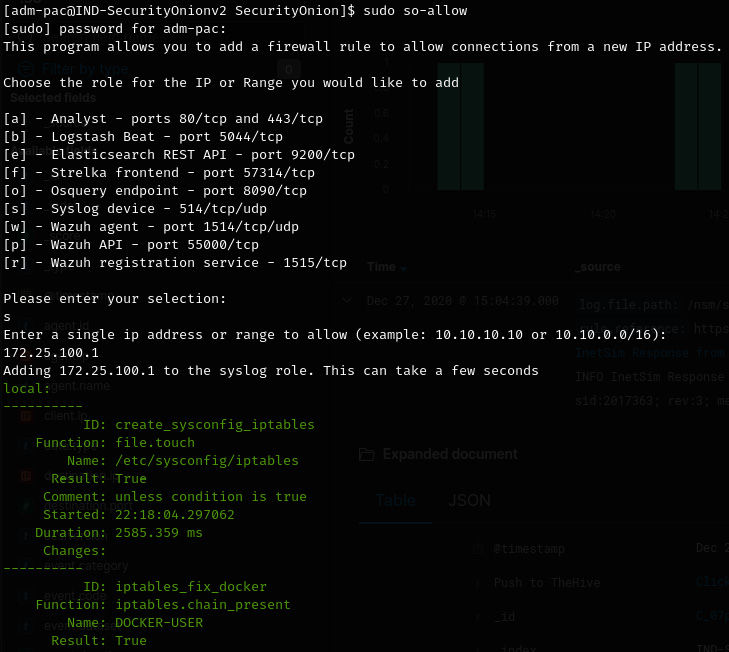
Our pfSense firewall VM is now built and has an initial configuration, ready to start handling traffic. Let's next configure event log forwarding so that we can include data from our firewall in Security Onion searches and dashboards.

Objective 3.0: Configuring log forwarding to syslog (Security Onion)

In order to start forwarding pfSense firewall logs to our Security Onion syslog server, we need to first allow (expose) the service to be contacted by the pfSense firewall. In order to do this, follow these next steps:

1. SSH into the Security Onion VM (ssh adm-pac@172.25.100.250) and run the sudo so-allow command.
2. Choose selection s for Syslog Device—port 514/tcp/udp.
3. Specify the LAN IP address of the pfSense firewall as the allowed IP address (172.25.100.1).
4. Confirm the configuration by hitting Enter. The process is illustrated in the following screenshot:

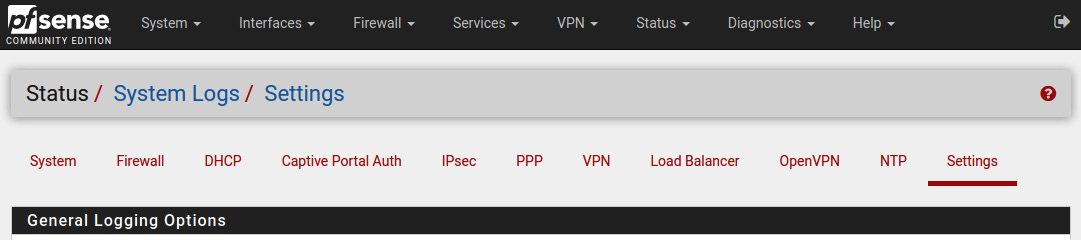
Figure 1.11 – Exercise 2: Security Onion – allowing syslog access



That takes care of allowing access to the syslog server on our Security Onion VM. Next, we need to configure pfSense to start forwarding events to the external syslog server. To accomplish this, follow these instructions:

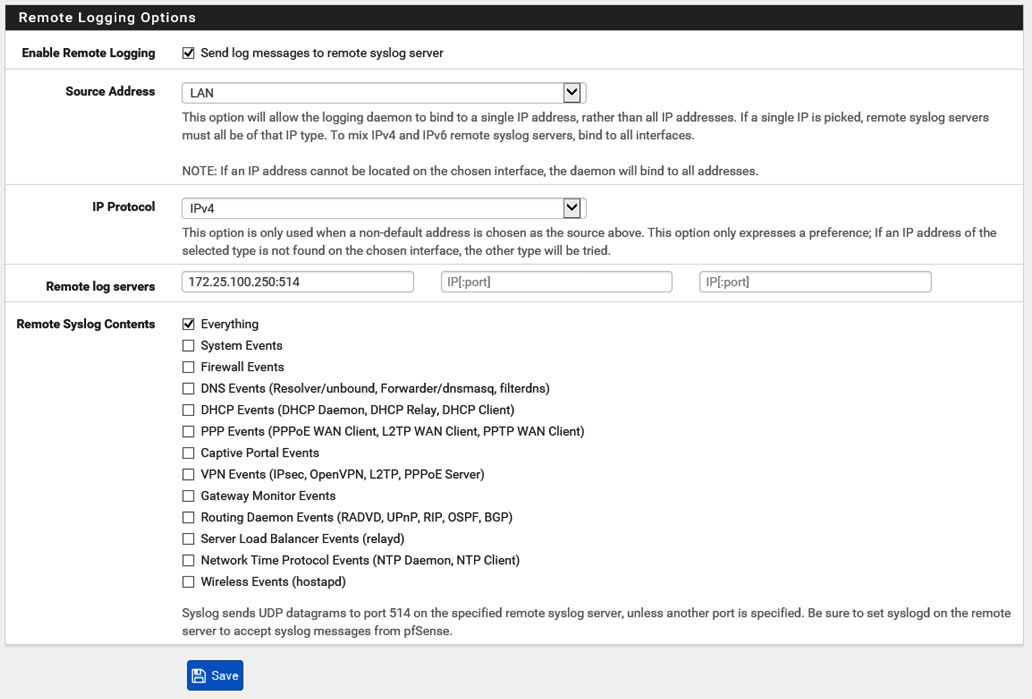
1. Navigate to the pfSense **WebConfigurator** portal at **https://172.25.100.1** and log in to the portal.
2. Head on over to **Status/ System Logs/ Settings**, as illustrated in the following screenshot:

Figure 1.12 – Exercise 2: System Logs settings



1. Scroll to the bottom of this configuration screen and enable **Send log messages to the remote syslog server**.
2. Fill out the configuration options as shown in the following screenshot, to send everything to the Security Onion syslog server at **172.25.100.250:514:**

Figure 1.13 – Exercise 2: Configuring pfSense – setting up syslog forwarding



1. Click **Save** to complete the configuration process.

That's it: we now have a functioning pfSense virtual firewall VM in our lab setup and have configured event forwarding to the Security Onion appliance we built in Exercise 1 – Setting up and configuring Security Onion.