Lab 2:

Installing   
pfSense as  
virtual machine   
using VMware

Linux Server Security  
 2024-2025

© Daan Pareit

## Introduction

# Lab concept

During this lab, we will create a new VM running pfSense, a network platform for NAT/firewall/… . The pfSense machine will have two interfaces. One connected to VMware’s default NAT network (VMnet8), which will be pfSense’s WAN interface. And another interface connected to a local virtual network, which will be pfSense’s LAN interface. Our test environment will thus be extended as shown in the figure below.



# Learning goals

* Creating a VMnet
* Installing pfSense within VMware
* Basic configuration of pfSense via CLI and web interface

# Practicalities and prerequisites

You’ll need the following:

* About 2.5 GB free disk space
  + 700 MB for the pfSense ISO file
  + 1.5 GB for the pfSense VM after installation
* Download the Community Edition of **pfSense 2.7.2** from <https://www.pfsense.org/> . Choose the ‘AMD64 ISO IPMI/Virtual Machines’ installation image. You’ll have a checkout chart of $0.00
* Unzip the downloaded ISO file (using 7-zip or similar application)

## Create a VMnet in VMware Workstation/Fusion

Your pfSense -which you’ll create in a few moments- is connected to two virtual switches in VMware (see figure in the ‘Lab concept’ section). At its WAN side, it will be connected to the existing NAT network (a.k.a. VMnet8). At its LAN side it needs to be connected to another virtual switch which will serve another local virtual network. We will create the latter switch/network now:

In VMware Workstation (Windows or Linux):

1. In VMware Workstation, go to the ***Virtual Network Editor*** and add a new VMnet (e.g. VMnet5 or whatever unused VMnet so far)
2. Set this VMnet to be host-only and give it subnet **192.168.11.0/24.** This is the IP subnet we’ve chosen to use for our internal network
3. **Disable** the DHCP server for this subnet. (We will let pfSense act as DHCP server instead.)

A screenshot of a computer

Description automatically generated

In VMware Fusion (Mac):

1. In VMware Fusion, go the ***Network*** settings and click the plus (+) button to add a new vmnet (e.g. vmnet3)
2. Disable the NAT
3. Enable the “Connect the host Mac to this network”
4. Disable the DHCP

## Installing pfSense

1. In VMware Workstation click on the menu item “**New Virtual Machine**” to create a new virtual machine (VM). The wizard will help you with this.

* Choose for ***Typical installation***
* Choose ***I will install the operating system later***
* Choose for ***Other*** as OS and choose for **“FreeBSD 14 64-bit**”
* Enter a name (e.g. ***pfSense***) for your VM
* Choose a **hard disk of 20 GB** (default) and choose to save the virtual disk **as a single file**.
* Click on ***Customize hardware*** and:
  + increase memory to **512 MB**
  + add a **second Network Adapter**.
* Connect the second Network Adapter **into your new custom VMnet**.
* Click on the **Finish** button

1. Connect the downloaded (and uncompressed) ISO file of pfSense to the CD/DVD of your VM in VMware Workstation. You can do that via the settings menu of your VM.
2. Power on your VM.
3. Accept the disclaimer and choose to install pfSense.

A screenshot of a computer

Description automatically generated

1. Select ‘em0’ as WAN interface.
2. Proceed with default settings for interface ‘em0’ as WAN interface.
3. Select ‘em1’ as LAN interface.
4. Change the settings for ‘em1’ as follows:
   1. IP Address: The address 192.168.1.1/24 is proposed. However, we have chosen 192.168.11.0/24 to be our internal IP network (and you’ve created therefore a custom VMnet earlier in this assignment). We want to give our pfSense **LAN interface** the IP address **192.168.11.254/24** (the last available IP address in our subnet).
   2. DHCPD Range: this range now also needs to be within the network we’ve chosen. Choose **192.168.11.100** as start address and **192.168.11.200** as end address.
5. Confirm your configuration for ‘em1’ and ‘em0’.
6. An Internet connection to Netgate Servers will be made. Then, choose to install the free CE (‘Community Edition’).
7. Continue with the default options for file system type and partitioning (ZFS and GPT).
8. Choose ‘stripe’ as ZFS configuration.
9. Confirm the ‘da0’ selected disk for installation. (Disk should be selected by default, if not hit space bar to select.)
10. The warning about destroying current contents is of course about your virtual disk, not about your laptop disk 😉, thus safe to accept
11. Select the latest current stable release to be installed.
12. Reboot into your freshly installed pfSense.

There was a need for a couple of restarts before it actually worked.

## Basic pfSense configuration

1. You should be dropped into a menu which shows the WAN interface (em0) having received an IP address via DHCP in your NAT VMnet. While the LAN interface (em1) has 192.168.1.1/24 . We specified it to be 192.168.11.254/24 during installation, but apparently that didn’t succeed. Probably a bug in the latest installer ISO file.
2. We have chosen 192.168.11.0/24 to be our internal IP network (and you’ve created therefore a custom VMnet earlier in this assignment). We want to give (again) our pfSense **LAN interface** the IP address **192.168.11.254/24** (the last available IP address in our subnet). Select option 2 to do this. You will be asked a few additional questions when setting the IP:
   1. Don’t configure the LAN interface via DHCP but manually assign it its IP address mentioned above. You don’t need to specify a gateway address
   2. Don’t configure the LAN interface via DHCP6, nor assign an IPv6 address manually.
   3. Enable the DHCP server on LAN. Choose 192.168.11.100 as start address and 192.168.11.200 as end address.
   4. Choose ‘yes’ to revert to HTTP as webConfigurator protocol
3. Verify that you can now use a web browser on your laptop to open the web page on your pfSense VM at 192.168.11.254

A screenshot of a computer

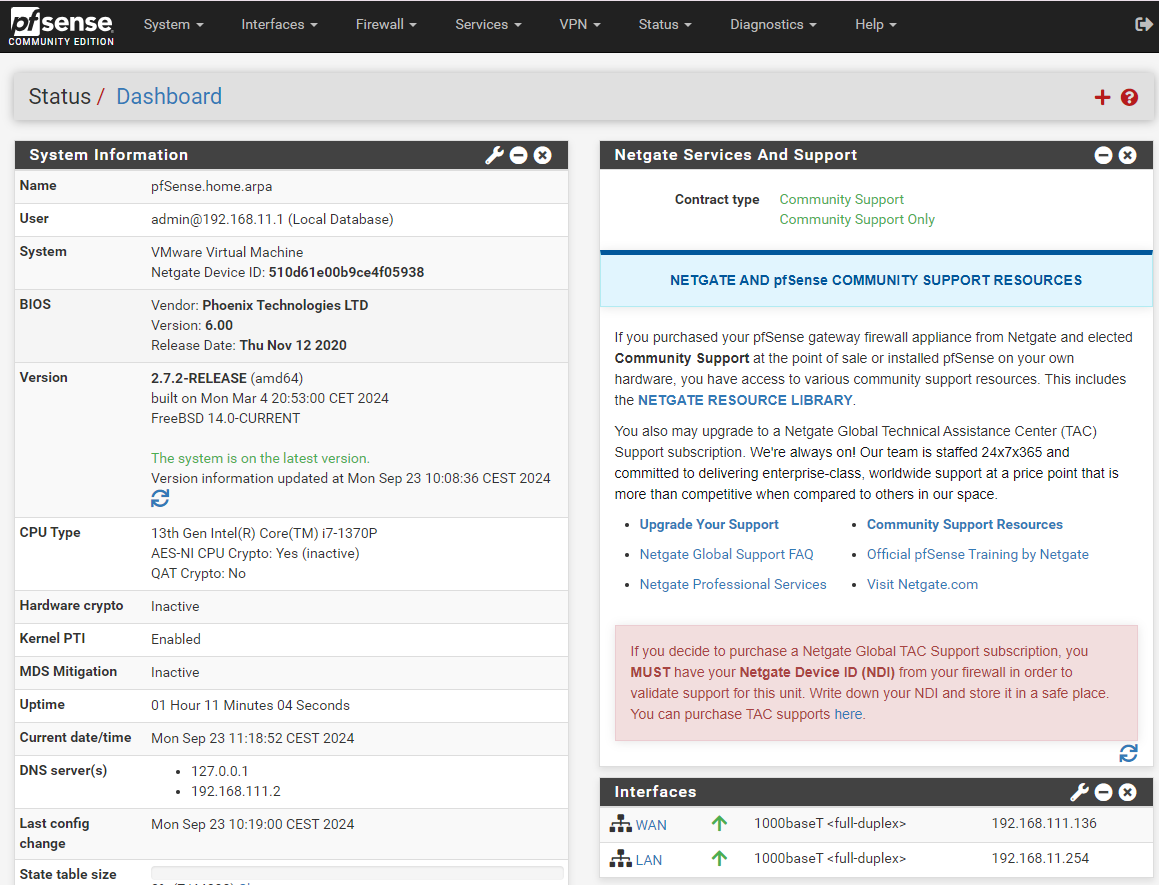
Description automatically generated

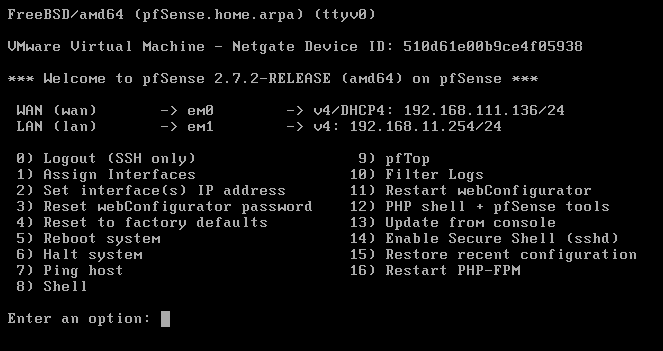
Yes, I can!!!

1. Use *admin* and default password *pfsense* to login to this web page.
2. Walk through the initial wizard. Leave values to default settings. Except for
   1. Step 3: Set timezone to Europe/Brussels
   2. Step 4: **uncheck the last two checkboxes** (‘Block private networks from entering via WAN’ and ‘Block non-Internet routed networks from entering via WAN’). This is because you are using a private IP network in VMware on the WAN interface.
   3. Step 6: choose a new Admin password

I am alright with the normal **pfsense** password

1. Finally, finish the wizard.





In this current version of pfSense, there also appears to be a bug concerning the initial configuration of the DHCP range. You specified a range starting at 192.168.11.100 and stopping at 192.168.11.200 during CLI setup in the previous steps. However, this is not applied. Let’s fix that:

1. In the web interface, go to ‘Services > DHCP Server’
2. Within ‘General Options’ you can specify the ‘Range’ again from 192.168.11.100 till 192.168.11.200
3. ‘**Save**’ these changes (blue button at the bottom of the page) and subsequently ‘**Apply**’ the changes (green button at the top of the page).

## pfSense DNS settings

We want future DNS queries arriving at pfSense to be handled by the DNS server of VMware, which is most commonly 192.168.x.2 in VMnet8 (see figure in the ‘Lab concept’ section). Note: this one will in turn of course use the DNS server of the Howest network or your home network.

èBrowse to the web interface of your pfSense VM. Go to ‘Services – DNS Resolver’.

èDisable DNSSEC support

èEnable the DNS Query Forwarding mode in the settings of ‘**DNS Resolver**’

Note: this is **not** ‘Services – DNS Forwarder’, which is a different type of DNS server.

Note: you don’t need to explicitly specify 192.168.x.2 as name server, pfSense will get this information from the DHCP server in VMnet8.

è Finally, we also want pfSense to allow DNS responses with private IP address for internal Howest servers (on campus or over VPN). Therefore, choose to display the custom options. In the textbox add the following:

server:

private-domain: howest.be

è Save these changes.

èThen, you’ll **explicitly also need to apply** these changes.

That’s it for now concerning the initial pfSense installation. You now have a dedicated VM which will act as the gateway/router/firewall/DNS for the other VMs and virtual networks we’ll use in the labs.