|  |
| --- |
|  |
| PfSense Firewall  Installation and setup |
| |  |  |  | | --- | --- | --- | | Case Study 1 -Group 10 |  | User Manual | |

Table of Content

[1. Introduction 2](#_Toc98251305)

[2. Requirements 2](#_Toc98251306)

[3. Installation 2](#_Toc98251307)

[4. Configuration 4](#_Toc98251308)

## Introduction

The Internet is a scary place these days. Almost daily, a new zero-day, security breach, or ransomware occurs leaving many people wondering if it is possible to secure their systems. Many organizations spend hundreds of thousands, if not millions, of dollars trying to install the latest and greatest security solutions to protect their infrastructure and data. PfSense is a FreeBSD based open-source firewall solution. The distribution is free to install on one’s own equipment

## Requirements

Minimum system specifications to run PfSence Firewall:

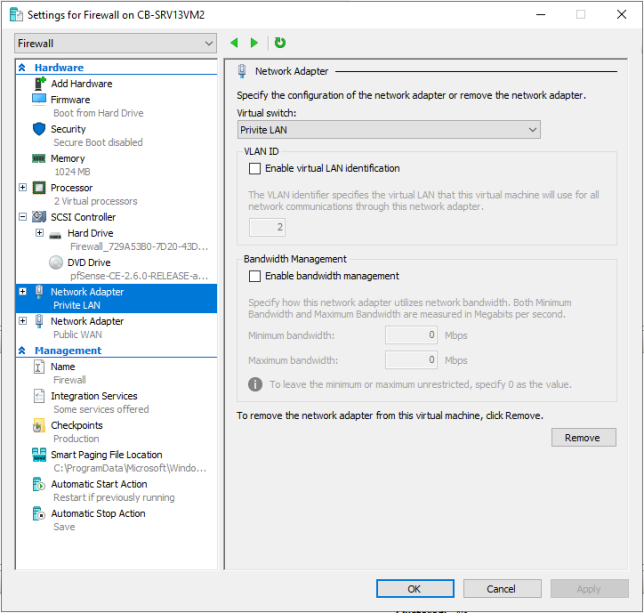
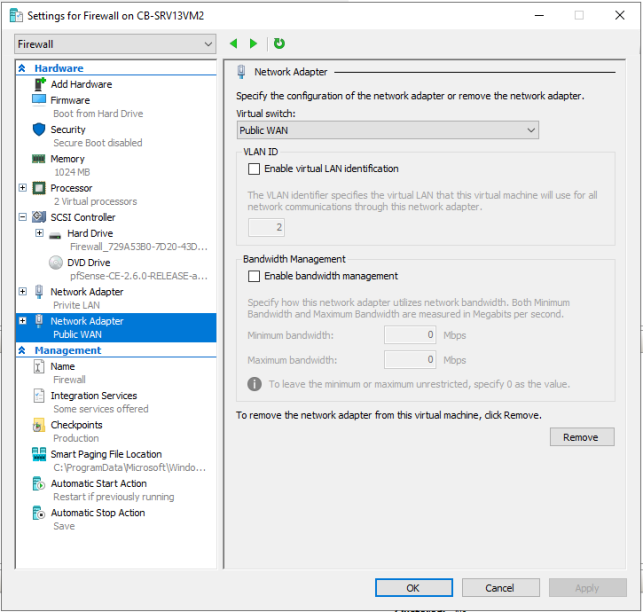
* 500 mhz CPU
* 1 GB of RAM
* 4GB of storage
* 2 network interface cards

## Installation

Graphical user interface, application, website

Description automatically generated‘PfSense’ Firewall is installed from the official website: <https://www.pfsense.org/download/>

A new virtual machine is created in Hyper-V manager. During the configuration process, the OS file that is used the .iso file which was download from the ‘PfSense’ webpage. To make Firewall works, two virtual network switches are added – Public WAN (for the external connection) and Private LAN (for the internal/private connection)



After the configuration of the machine is done, it must be installed. To do that, just boot the newly created VM and follow the installation steps.

Graphical user interface, text, application, email

Description automatically generatedA picture containing text

Description automatically generatedTip: Do not change any setting during the installation. Leave everything by default.

## Configuration

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generatedAfter the installation is completed, it is time to configure the Firewall settings. The first thing to be done is to connect properly the network adapters. Check the MAC address of both and make sure you connect them to the correct interface.

Click on ‘y’ to proceed and to save the current settings. After that, a list of command will pop up on the screen. If the shown IP addresses are not the correct once, select number 2 to change them.

Text

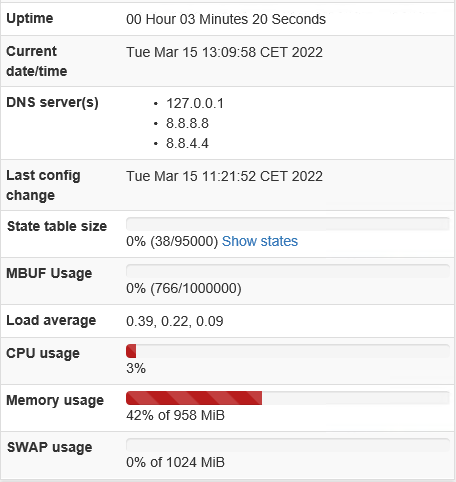
Description automatically generated

Text

Description automatically generatedTo check whether everything is alright, try to ping host. To do this, select number 7 and type the IP address (in our case it is Google.com)

Ping is successful.

The last step is to finish the setup of the Firewall from the webpage. For this purpose, open the browser and type the IP of the private interface (in our case: 192.168.0.1/24). Complete the steps and the Firewall will be fully configured.



**Note**: Text

Description automatically generatedIf the private environment has a DHCP server it could enable it by changing the IP settings. Select number 2 and follow the steps to enable DHCP server.

**Note**: To be able to ping WAN, new rules must be created from the home page of the Firewall

Text

Description automatically generatedBy default, pinging the WAN interface on a Firewall is disabled:

In this assignment we need to access to WAN interface. By default, this is disabled so, in order to overrule the default settings a new rule needs to be created.

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text

Description automatically generated

As the ping uses the ICMP protocol the new rule will need to pass packets from this protocol. The rule we created and added to the pfSense® Firewall allows any packet using this protocol, coming to the WAN interface and to this Firewall to be passed through regardless of source.

Text

Description automatically generatedAs a result, we were able to ping the Firewall successfully: