

Network Devices

Lab 12

ITSC 200: Network Protocols and Security

Table of Contents

[Lab Outcome(s) 2](#_Toc465173395)

[Reading 2](#_Toc465173396)

[Introduction 2](#_Toc465173397)

1. [Install, configure, and use a virtual Pfsense firewall 3](#_Toc465173398)

[References 4](#_Toc465173400)

Lab Outcome(s)

* Install Pfsense
* Learn how to do basic configuration of the Pfsense firewall.

Reading

* None

Introduction

This lab is to practice the installation of Pfsense firewall and to do basic configuration and troubleshooting of a virtual install.

1. Installing Pfsense  
   1. Create a Virtualbox VM on your laptop that has two network interface cards. One should be “bridged” and one should be “internal networking”.
   2. You won’t need much RAM or hard drive ( 1024 Mb and 20GB respectively).
   3. Install the Pfsense firewall and when you come to the character-based console, configure the LAN and WAN interfaces. Be careful that the bridged interface is the WAN interface and the LAN interface is “internal networking”.
   4. Allow the WAN interface to be DHCP configured but give the LAN interface a static IP 192.168.1.1/24.
   5. Once it is installed and rebooted, use one of your other local VM’s and change its interface to “internal networking” and choose the same internal network as the LAN interface of Pfsense.
   6. Make sure you give the second VM a static IP address of 192.168.1.2/24 and use the LAN IP of the Pfsense as the default gateway. The DNS can be 8.8.8.8 (Google’s public DNS server).
   7. Open the web browser on you second VM and point it at 192.168.1.1. The default username is “admin” and the default password is “pfsense”. The wizard will run to change this.
   8. Set up a firewall rule that blocks incoming https connections but allows everything else including http.
   9. From your second VM, go to [www.](http://www.cnn.com/)weevil.info (http). Did it work ? Go to [www.google.ca](http://www.google.ca/) (https). Did it work ?
   10. Check the log files of the Pfsense firewall. Was there any information there ?
   11. Do step 1.9 again but this time capture the WAN interface traffic, download it, and bring it into Wireshark.
   12. Try setting up a “captive portal” on Pfsense. (this is similar to trying to access the Internet from inside a hotel. You are automatically directed to their website first).

Lab Submission : No lab submission.

References

<https://www.tecmint.com/monitor-ethernet-activity-in-linux/>

<http://www.faqs.org/docs/securing/chap14sec117.html>

<https://adamscheller.com/systems-administration/fail2ban-ssh-ubuntu-debian-mint/>

<https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-14-04>

Blank page if necessary to make pages an even number

**DO NOT DELETE THE SECTION BREAK BELOW. DELETING IT MAY IMPACT THE FORMATTING IN THIS DOCUMENT.**