Lab instructions for Firewall and IPS Technology

1. Introduction

This document details the required lab exercises for the course DTEK8063 Firewall and IPS Technology. The labs are individual assignments, so each student will do their own labs and write their own report.

2. System requirements

The exercises are based on virtual machines. A computer capable of running standard virtual machines on x86 architecture is required. You should be able to get these images running on a M-series Macbook, but there is unfortunately no dedicated support provided for ARM based solutions.

The lab has been tested on VirtualBox 7.1.4. r165100 running on Windows 10. The lab will require at least 4Gb of RAM and 20 GB of disk space.

3. Lab set up

The lab exercises have been tested with VirtualBox VMs. If you use another hypervisor (e.g. Parallels) you will have to figure out the details yourself.

The following VMs are provided for the lab in Moodle:

- TinyCore VM
  - User (for SSH login): fwips PW: Pass1234
- Metasploitable VM
  - User: msfadmin PW: msfadmin

The following disk images (.iso) are provided for the lab in Moodle:

- PFSense
- IPFire

Your host (the computer running the VMs) will require the following capabilities:

- SSH client
- netcat
- Internet connection
- browser

For Windows you can use for example Ncat: https://nmap.org/ncat/ You will need to adjust both Virtualbox and your host computer networking settings depending on the exercise. Virtualbox networking user guide can be found here: https://docs.oracle.com/en/virtualization/virtualbox/7.0/user/networkingdetails.html

4. Lab assignments – Part 1

4.1. Task 1 – Install and configure PFSense firewall

The instructions are relatively detailed to provide you with guidance in the beginning. Later parts are not as well documented and will require you to read documentation and figure things out for yourself.

Objectives:

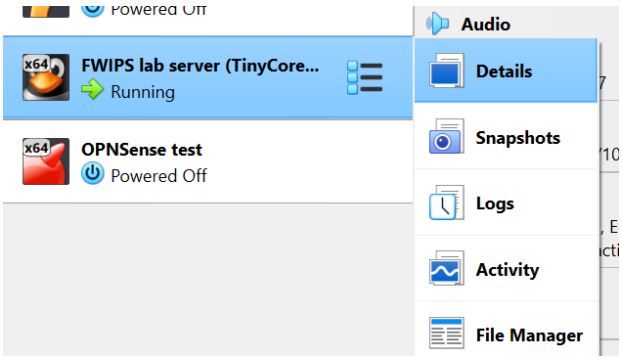
1. Set up PFSense firewall and lab server virtual machines in Virtualbox
2. Configure virtual networking and routing appropriately
3. Log in to the firewall admin console and configure firewall interface settings
4. Test functionality

The firewall ISOs are available in Moodle. Create a new virtual machine in Virtualbox for pfSense with the following settings.

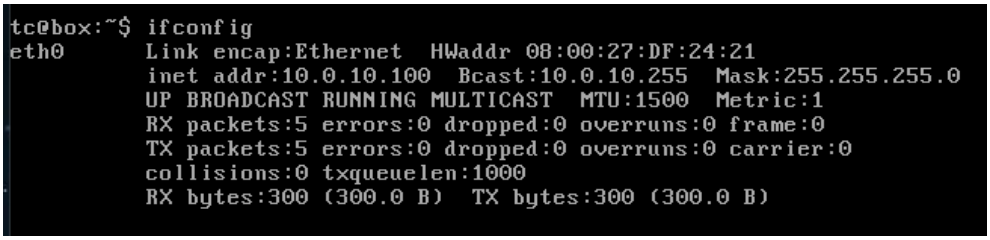
- Operating system: FreeBSD (64bit)
- ISO image: use the ISO provided in Moodle
- Base memory: 1024 MB
- Number of CPUs: 1
- Video memory: 16MB
- Graphics controller: VMSVGA
- Virtual hard disk size: 8GB
- Virtual hard disk type: VDI
- Network adapters: 2 x Intel PRO/1000MT Desktop
    - Adapter 1: Internal network (Use this for WAN)
    - Adapter 2: Host-only network (Use this for LAN)

For this exercise the firewall administrative interface must be accessible from the host computer (the computer running the VMs) and therefore it cannot be in a Virtualbox internal network, which is not accessible by the host.

After you have installed the firewall, it's a good idea to take a snapshot of the virtual machine in its initial state. If something goes wrong, you can always return to the snapshot state easily. Snapshots can be found in the VM menu.

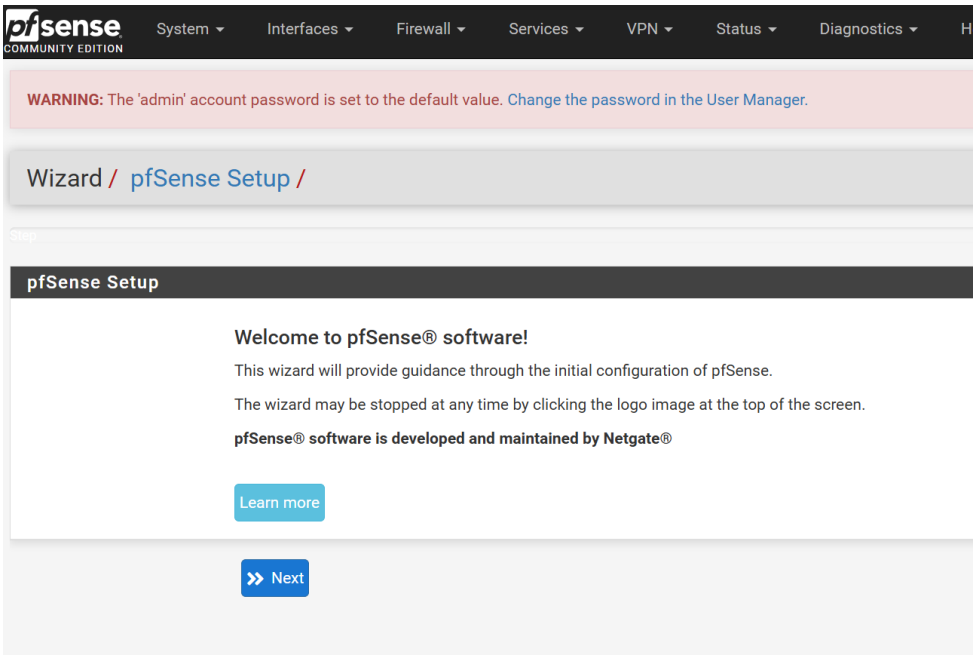


Next, import the TinyCore lab server VM. Connect the network interface to the Internal network. Start the VM. Verify that it runs and has static IP address 10.0.10.100.



From the console, configure the PFSense firewall LAN adapter to use DHCP.

Now you can access the firewall admin console with a browser. The IP address is the one assigned to the LAN interface via DHCP, and the default credentials are (usr:pwd) *admin:pfsense*.



Proceed through the wizard. Use defaults, except for the following:

- Hostname: <your name>-PFSense
- WAN adapter settings
    - Static IP address 10.0.10.1
    - Subnet mask: 24
    - Block private networks and loopback addresses: NOT selected
    - Block bogon networks: NOT selected
- Verify that LAN subnet mask is also 24
- Change admin password to *Pass1234*

Add upstream route to the lab server from System->Routing. Add new gateway with the following information:

- Interface: WAN
- Address family: IPv4
- Name: lab
- Gateway: 10.0.10.100

Set default IPv4 gateway to “lab”, save and apply changes. Check from Interfaces->WAN that the IPv4 upstream gateway is selected correctly.

Finally, because the lab WAN IP addresses are in a non-routable address space, you will have to configure a static route from your host computer to the Virtualbox LAN. In these examples the firewall LAN adapter has IP address 192.168.56.101, but use the correct address for your system.

Windows: (as admin) *route add 10.0.10.0 MASK 255.255.255.0 192.168.56.101*

Linux: *sudo ip route add 10.0.10.0/24 via 192.168.56.101 dev eth0*

MacOS: *sudo route -n add 10.0.10.0/24 192.168.56.101*

Test the connection from your host to the server in the internal network by pinging the TinyCore server at 10.0.10.100 from your host computer. If you do not get a reply, you can try pinging the server from the firewall. If you get a response there but not from your host, the traffic is not getting through the firewall.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> route add 10.0.10.0 MASK 255.255.255.0 192.168.56.101
 OK!
PS C:\WINDOWS\system32> ping 10.0.10.100

Pinging 10.0.10.100 with 32 bytes of data:
Reply from 10.0.10.100: bytes=32 time=1ms TTL=63
Reply from 10.0.10.100: bytes=32 time=1ms TTL=63
Reply from 10.0.10.100: bytes=32 time=2ms TTL=63
Reply from 10.0.10.100: bytes=32 time=2ms TTL=63
```

4.2. Task 2 – Set up firewall rules for PFSense

Now that we have a functioning firewall and a server in WAN, it is time to set up firewall rules. The objectives in task 2 are

1. Configure the LAN rules so that **All outbound SSH and HTTP connections are logged**
2. Configure **WAN interface to allow ICMP Ping replies** to the 10.0.10.1/24 segment and to log such connections
3. Test outbound HTTP
   3.1. From your host computer, open a connection to 10.0.10.100 in the browser
   3.2. Check that the connection is logged by the firewall
4. Check that outbound SSH connections are logged
   4.1. Log in to 10.0.10.100 using the credentials fwips:Pass1234
   4.2. Verify from the firewall system logs that this connection is logged
5. Test WAN Ping rule
   5.1. Ping your firewall WAN interface from the server. You can use the SSH shell you just opened.
   5.2. Note that you receive a reply and that the connection is logged

4.3. Task 3 – Port forwarding

Now it is time to configure inbound traffic rules. We will open a port in the firewall so that the server in WAN can connect to your host computer using netcat. The objectives in task 3 are

1. Redirect incoming connections to the firewall WAN adapter, port 8080, to your host computer, port 8080. Use the Virtualbox host-only network adapter IP address as your IP. Log these connections.
2. Set up netcat to listen to port 8080 on your host computer.

3. Make a new SSH connection to 10.0.10.100. From there, use netcat to connect to your host and send a message to the listening terminal.
4. Make sure that the connection is logged.

4.4. Task 4 – IPFire setup

Now it is time to set up the same environment using the IPFire firewall. The objectives of task 4 are:

1. Shut down the PFSense VM
2. Create a new virtual machine and install IPFire on it
3. Set up interfaces similarly to PFSense: WAN interface is in Internal and LAN is in host-only network
4. Recreate the same environment using IPFire and do the same tests.
   4.1. UPDATE 13.12.2024: IPFire has a peculiar design philosophy where the WAN interface always replies to ping requests, regardless of firewall rules. Therefore it is not possible to do parts 2 and 5 of task 2 with IPfire, you can ignore the ping related rules and tests. [Instructor note: I did not test this beforehand because of course I thought that IPFire would behave like any other firewall. Assumptions can betray you. :)]

UPDATE 12.12.2024: The following instructions may help you when dealing with IPFire.

- IPFire uses different terminology for networks. Green = LAN, Red = WAN.
- For IPFire, create a new host-only network in the network manager. Set the IP address for the Virtualbox adapter to a suitable subnet and make it **something else than xyz.xyz.xyz.1.** Configure the Green adapter to use this host-only network and assign the first address to it. For example, here the address for the host adapter is 192.168.130.10 and IPFire Green adapter is given the address 192.168.130.1.

- Also remember to update the static route on your host computer to reflect the change of IP address for the host-only network. In this case the new static route would be (for Windows hosts, adjust accordingly for other OSs)

  route add 10.0.10.100 MASK 255.255.255.0 192.168.130.1

4.5. Network diagram

Draw a network diagram of your lab network. Include interfaces and addresses for each interface.

4.6. Optional task – firewall clustering

This task is optional. Students that finish this will get a small bonus in their grades, but finishing this task is **not mandatory**. The objectives for this task are

1. Create another PFSense virtual machine
2. Add a third interface to both firewalls (for synchronization)
3. Configure the second firewall to act as a backup firewall using CARP
   3.1. Note that the sync network needs to be separate from the others. Choose the network freely
   3.2. For the second firewall WAN interface IP address, use 10.0.10.2
4. Criteria for success: CARP configured and firewalls form a functional cluster
5. Update your network diagram to reflect the cluster setup

Option: you can also do this with IPFire if you wish. One implementation is enough for the bonus.

Part 2 of the instructions is ~~coming soon~~ available in Moodle.