Firewall - PFSense

Description

You will experiment with a Firewall in this lab.

Create a new vm. Doesn’t need too much RAM, 512MB. 16GB HD. Needs 2 nics. The first one should be bridged. The other can be Internal. (You will eventually be using a second GUI machine that should also be on the Internal network). (Probably Kali)

Install using the pfSense iso. You can just accept all the default options.

Your first nic (bridged) should be your Wan interface. Your other nic should be for the Lan (internal), and your other GUI vm is also on this network.

Make sure the other GUI machine can ping the pfsense machine. (Probably a 192.168.1.1 address). See if you can load the web interface on your GUI machine (http://192.168.1.1 or whatever your address is). You should be able to login with admin/pfsense.

Rules

Create a rule that will apply to your WAN network:

- I don’t like accessing the pfsense web page from inside a vm. Configure a rule to allow access to port 80 of your pfsense machine from anywhere on your WAN network. Then (maybe) you could pull it up on a browser from your local machine and administer it.
- Allow access to port 445

Create several rules that will apply to your LAN network:

- Block outgoing pings from your LAN network
- Create a schedule of your choice that will block outgoing access to port 80 during that timeslot.

Test all your rules!!

NAT

Appropriately configure port forwarding so that when trying to ssh to port 2786 of the pfsense machine on the WAN side, it will redirect you to the Kali instance (may have to enable ssh on Kali)

TO pass off

Take screenshots of your rules and schedules page. Put your screenshots in a single pdf and upload to canvas.