COOP 2: Network Setup Lab

The goal of the lab is to familiarize you with the real world applications of the topics you learn about in class. While this lab will only use a small test environment it's easy to see how the system may work in an actual production environment with many users.

This lab will detail how to setup a simple firewall, expand on the ideas of subnetting and introduce many of you to virtualization. The software utilized by this lab is widely used in the real world. The main software used is **pfSense**, a Linux based firewall and router. Furthermore, **Zenmap**, a GUI front end for the popular **nmap** software, and Ubuntu Linux will also be used. VMWare's Workstation 11 will serve as the hypervisor.

The lab is broken down into a few parts. They are:

1. **Prelab** – This will lay the ground work for the lab and introduce you to the environment.
2. **Initial pfSense configuration** – This portion involves basic setup of pfSense for the first time and getting things up and running.
3. **pfSense GUI** – This section focuses on more granular setup and tailoring this installation of pfSense for this specific usage case.
4. **Explore** – Now that the environment is working it's time to investigate and learn what is happening behind the scenes.

Throughout the lab a series of questions will be posed. Those questions have been reproduced here should you prefer that. The questions will become clearer later within the context of the lab.

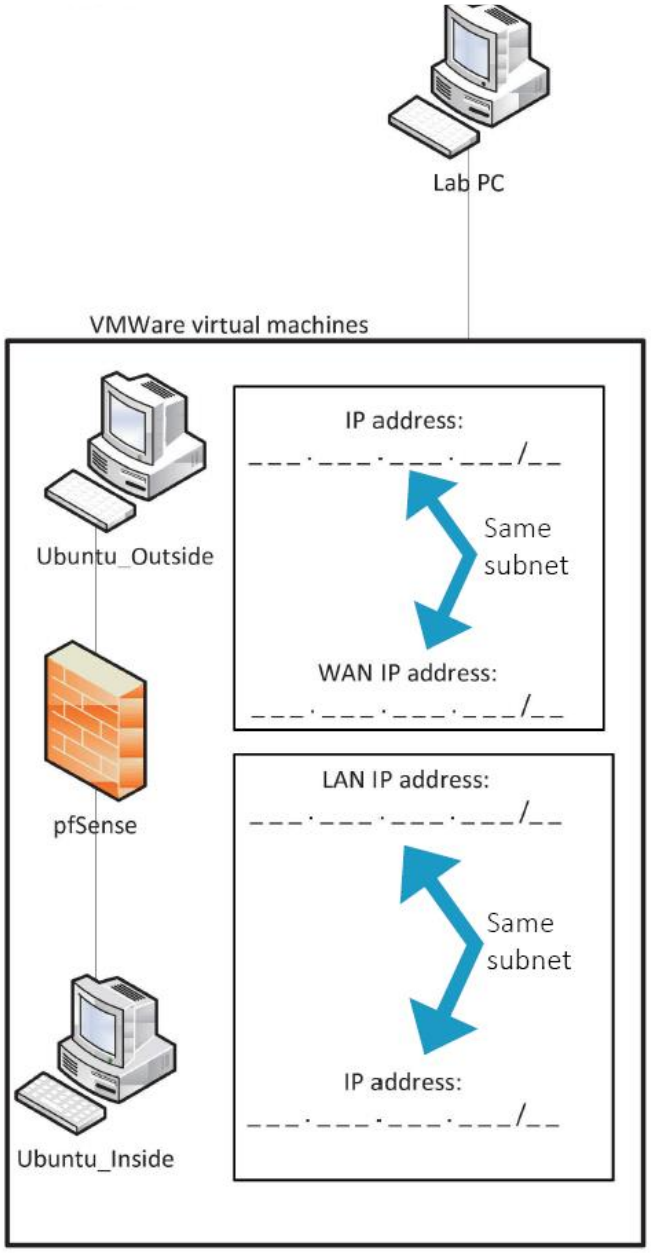
1. Why is blocking FTP a good idea? Use Wireshark and Follow TCP Stream with the sample packet to find out.

2. pfSense is providing an IP address and routing for Ubuntu_Inside but which DNS servers are being used?

3. What does the scan tell us about the firewall?

4. The scan will come back with nothing. Pinging the WAN IP will also come back with nothing.
   Why?

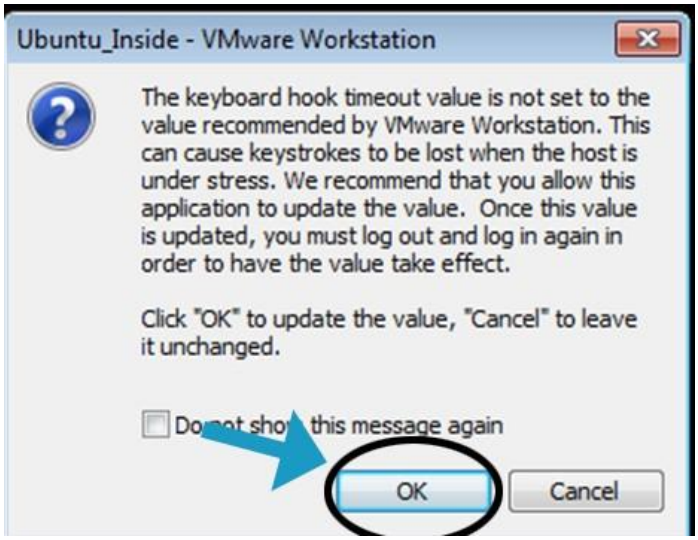
This is an overview of the virtual environment in which the lab takes place. Please fill in the IP addresses of the various machines as appropriate.



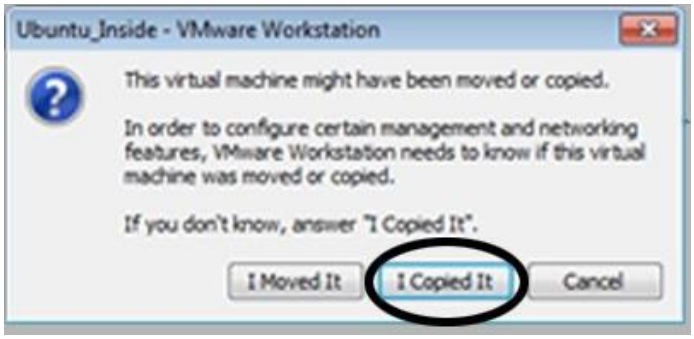
Before beginning it is important to grasp the difference between the two subnets. Ubuntu_Outside is on a NAT subnet generated by VMWare. In other words, Ubuntu_Outside already has a router, IP address, and can reach the Internet. On the other hand, Ubuntu_Inside is a host only subnet. This means that Ubuntu_Inside can’t reach the Internet; its network only exists on your particular computer.

Section 0: Helpful Hints

1. **Alt** + **Ctrl** releases your mouse from the current VM.
2. If you see a message about keyboard timeout value, click OK.



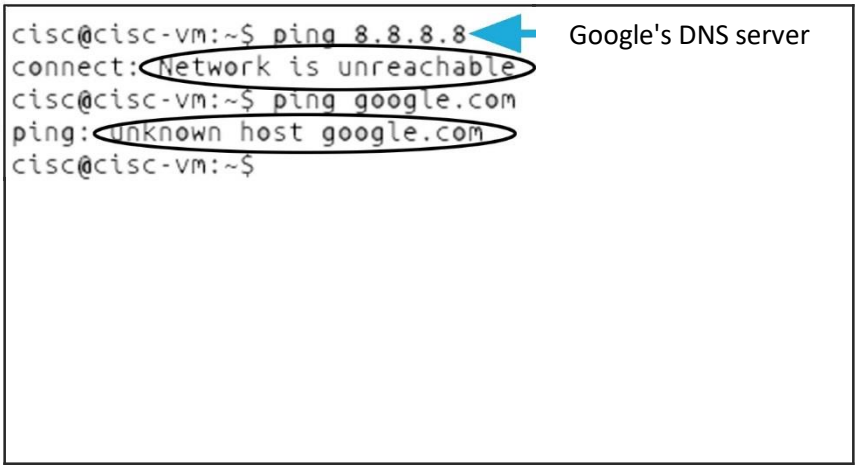
3. If you see a message about virtual machine being moved, clicked "I Copied It"



4. To launch a VM, click the green triangle in the upper menu bar.

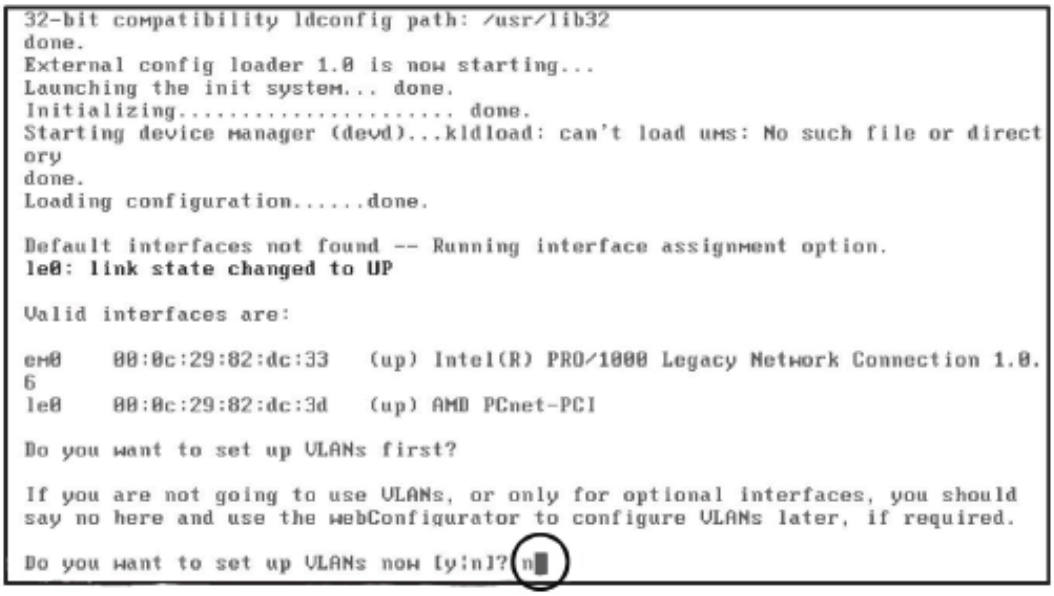
Section 1: Prelab

1. Open VMWare Workstation.
2. Launch the Ubuntu Inside virtual machine.
3. Open Terminal. It is the black icon in the dock on the left.
4. Verify the machine has no network connectivity.



Section 2: Initial Configuration

5. Launch the pfSense_CISC250 virtual machine.
6. You will now begin the setup process for **pfSense**, a combination of router and firewall.
7. The first step of configuring pfSense is deciding if you want VLANs. We do not.



8. Next we need to tell pfSense which network interface is the WAN, in this case **le0**.

```
ory
done.
Loading configuration......done.

Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP

Valid interfaces are:

em0    00:0c:29:82:dc:33   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
le0    00:0c:29:82:dc:3d   (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: le0
```

9. Tell pfSense which interface is the LAN, in this case **em0**.

```
Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP

Valid interfaces are:

em0    00:0c:29:82:dc:33   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
le0    00:0c:29:82:dc:3d   (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0
```

10. pfSense will ask you to verify the interface assignments. Double check them and then proceed.

```
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished) <-- press enter here

The interfaces will be assigned as follows:

WAN  -> le0
LAN  -> em0

Do you want to proceed [y|n]? y
```

11. pfSense will now proceed to its dashboard. From here we want to choose the subnets pfSense will use. Option 2.

```
 7) Ping host                          16) Restart PHP-FPM
 8) Shell


Enter an option:


FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> le0        -> v4/DHCP4: 192.168.29.128/24
 LAN (lan)       -> em0        -> v4: 192.168.1.1/24
 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) pfSense Developer Shell
 4) Reset to factory defaults          13) Upgrade from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell


Enter an option: 2
```

12. We can't change the WAN subnet since another router handles that but we can choose the LAN subnet.

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.29.128/24
 LAN (lan)       -> le0        -> v4: 192.168.1.1/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2
```

Should be (and in all of the following screenshots)
WAN -> le0
LAN -> em0

13. Pick an address space for the LAN. You need not use 10.10.10.0 but you may if you wish.

```
 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.29.128/24
 LAN (lan)       -> le0        -> v4: 10.10.10.1/29
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1
```

14. Choose the subnet size. We want a subnet with **6** addresses.

```
 5) Reboot system                        14) Enable Secure Shell (sshd)
 6) Halt system                          15) Restore recent configuration
 7) Ping host                            16) Restart PHP-FPM
 8) Shell


Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29
```

Also known as the extended network prefix

15. Since we're assigning a LAN simply press enter for none.

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

16. We're only dealing with 1Pv4 so we'll skip the 1Pv6 setup. Press enter to move on.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>
```

17. Ordinarily we would want to use DHCP. It makes adding new network devices much easier and more convenient. However, for this lab we will manually assign addresses for the sake of learning.

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
```

18. Below, write down the starting IP address of the subnet you have chosen. Space is provided should you need to do the calculation in full.

19. Below, write down the ending IP address of the chosen subnet. As above, space is provided if you need to perform the calculations.

20. We do not want to revert to HTTP since it's less secure.

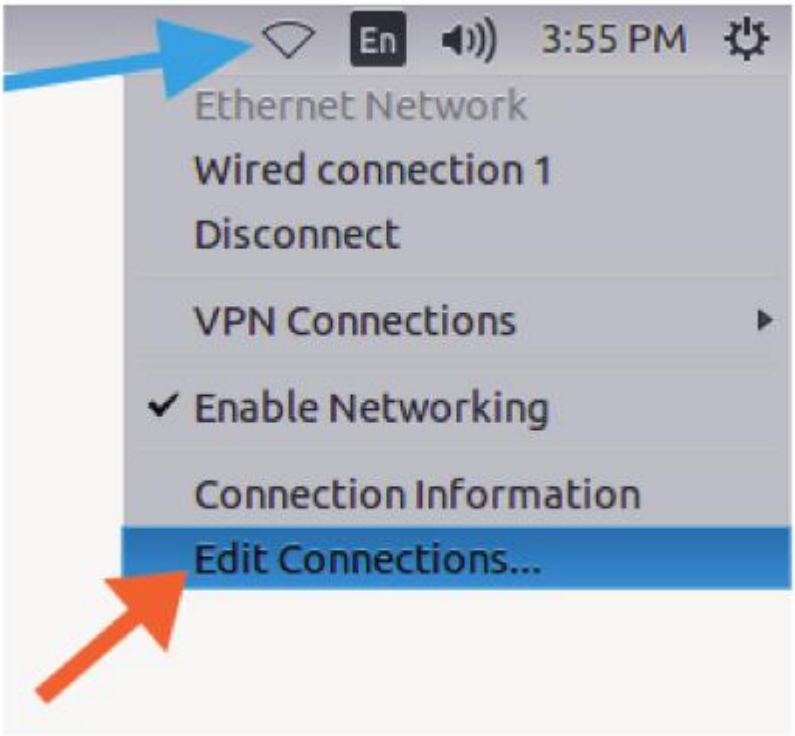
```
2 - LAN (le0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Use https

21. The initial setup of pfSense is complete. The IP address for the pfSense GUI will be displayed.

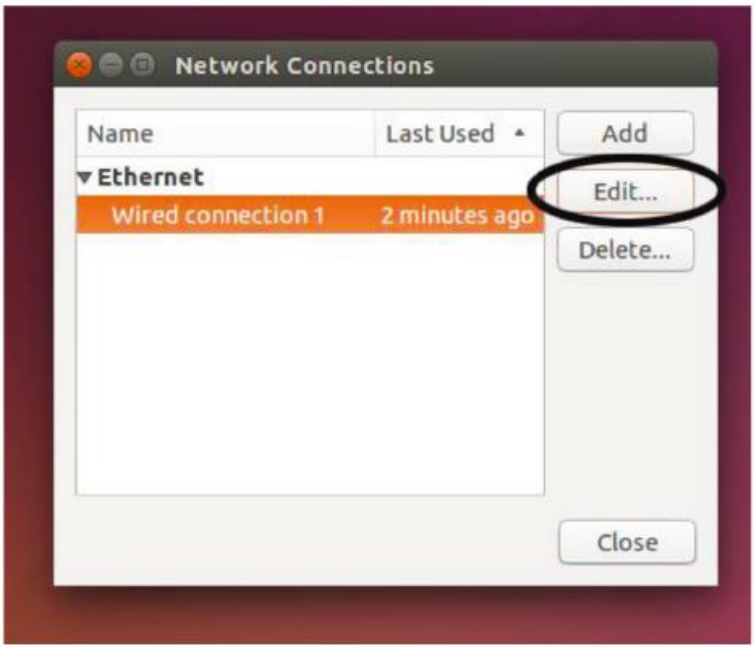
```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 10.10.10.1/29
You can now access the webConfigurator by opening the following URL in your web
browser:
              https://10.10.10.1/

Press <ENTER> to continue.
```

22. Before using the pfSense GUI we need to assign Ubuntu_lnside an IP address. Begin by clicking the icon on the upper right and selecting "Edit connections" from the drop down menu.

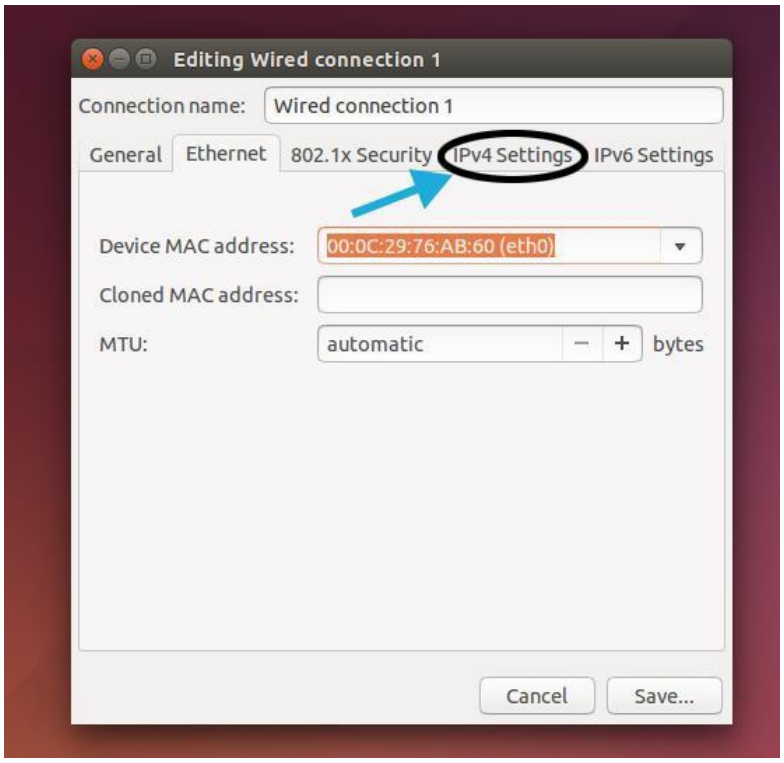


23. Once the "Network Connections" window pops up, click on the connection and click edit.

Note: If there are multiple connections, use the one that was most recently used.

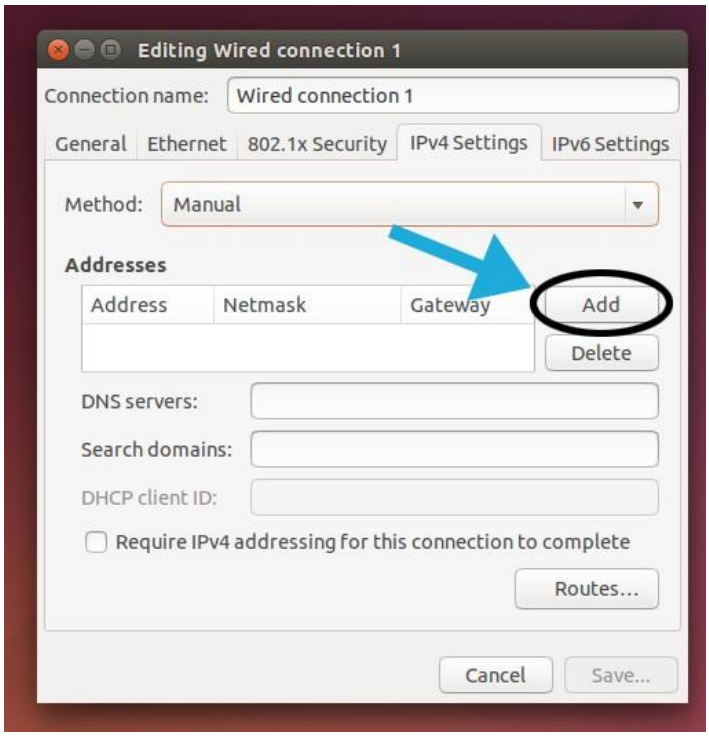


24. Now the Editing window will pop up. Navigate to the “IPv4 Settings” tab along the top.



25. Click the “Method” box and select “Manual.”

26. Under the “Addresses” section, click the “add” button

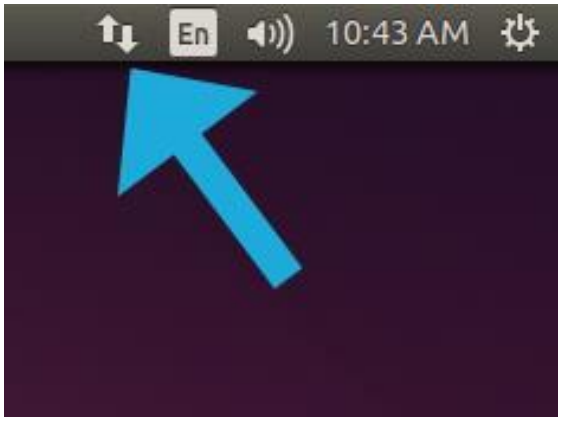


27. Now fill in the appropriate fields. Remember to pick an IP address that's in the subnet.

28. The final step is to tell Ubuntu_Inside which DNS servers to use. The example uses pfSense for DNS but we will return to this topic later on.

29. Click save in the lower right to close the window and preserve the configuration.

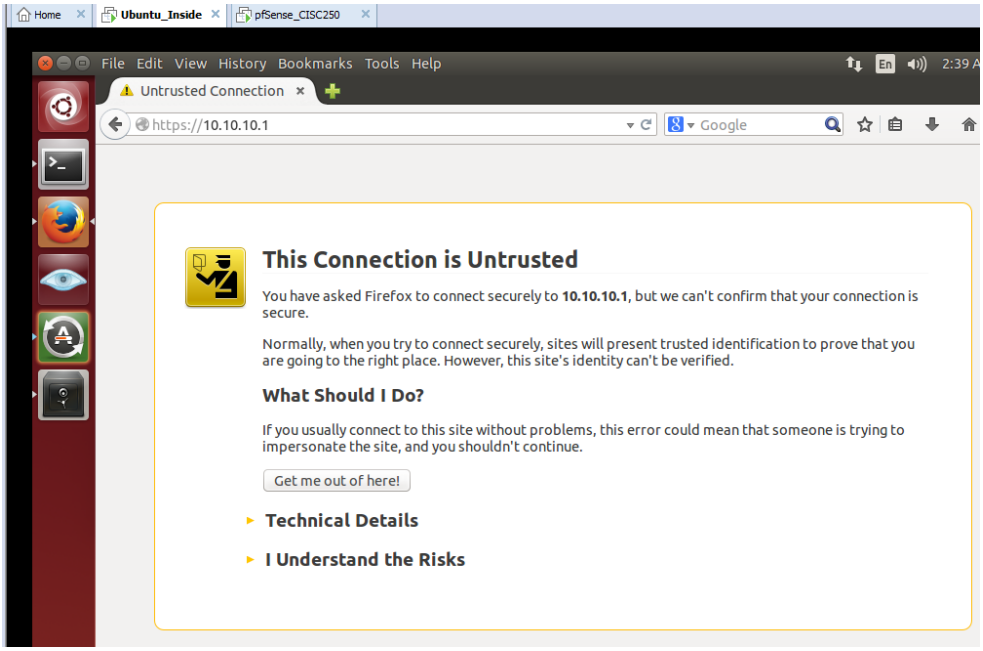
30. If the configuration was done correctly, the cone symbol in the top right will change to two arrows.



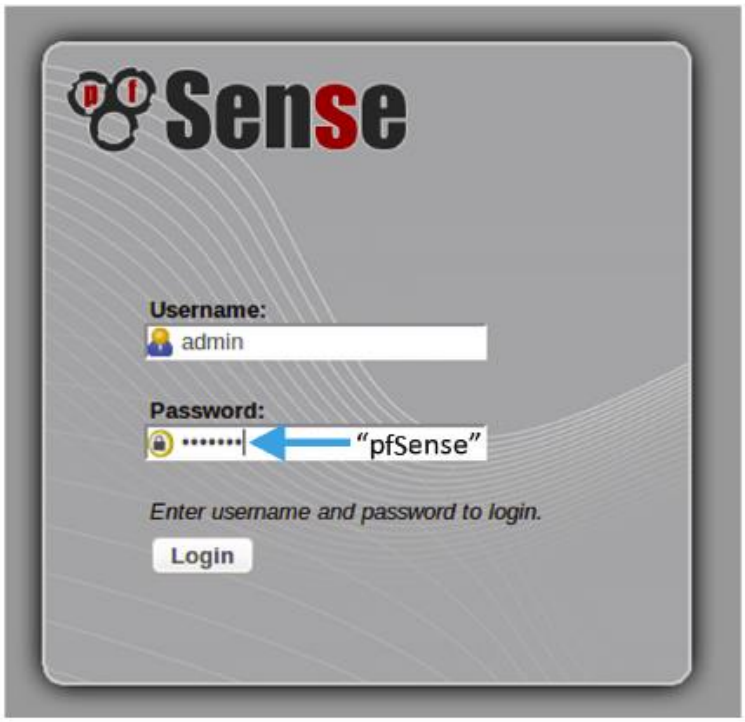
31. Now that Ubuntu_Inside has network connection, we can ping Internet resources.

Section 3: pfSense GUI

32. Open the Web Browser (Firefox) on Ubuntu_Inside. Navigate to the pfSense WebConfigurator IP address (10.10.10.1). Ignore warnings about an untrusted connection. Click on “I Understand the Risks” and then “Add Exceptions”.

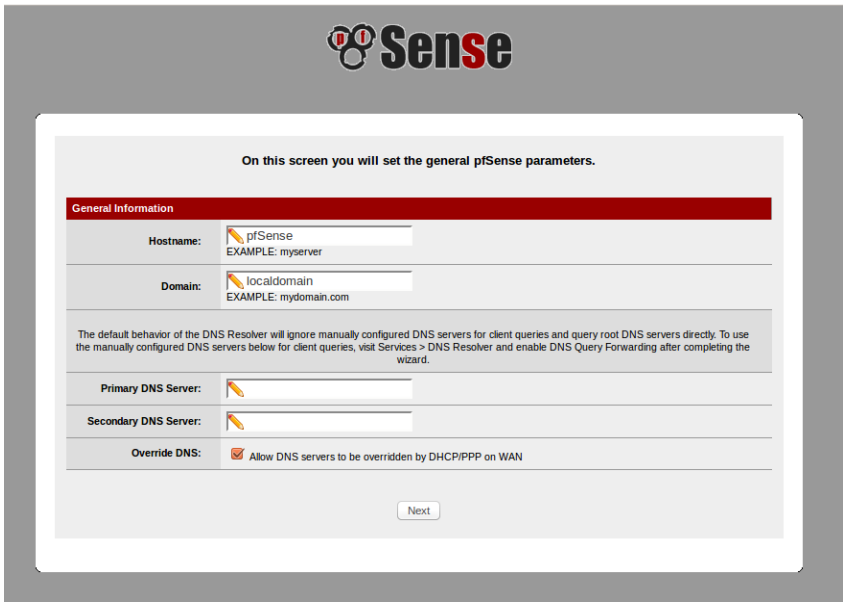


33. Log in to pfSense. The default credentials are "**admin**" and the password is "**pfsense**" (all **<u>lower case</u>** letters).

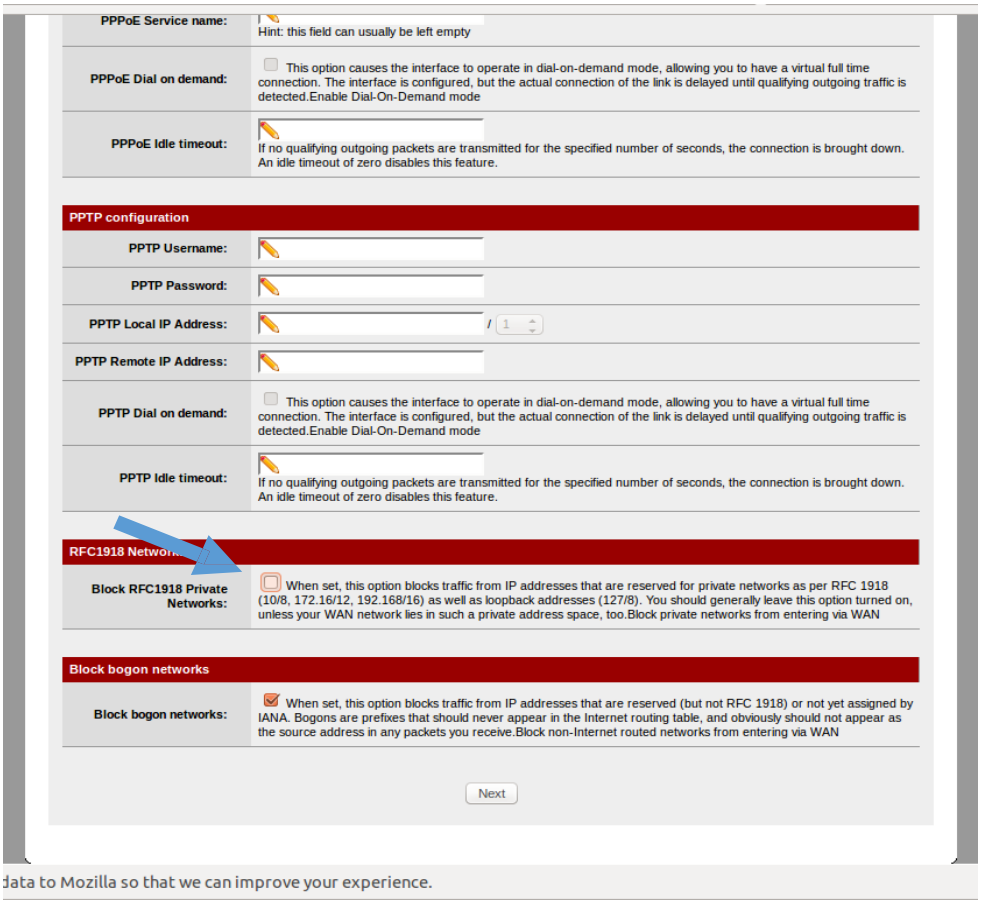


34. Begin the pfSense WebConfigurator setup wizard.

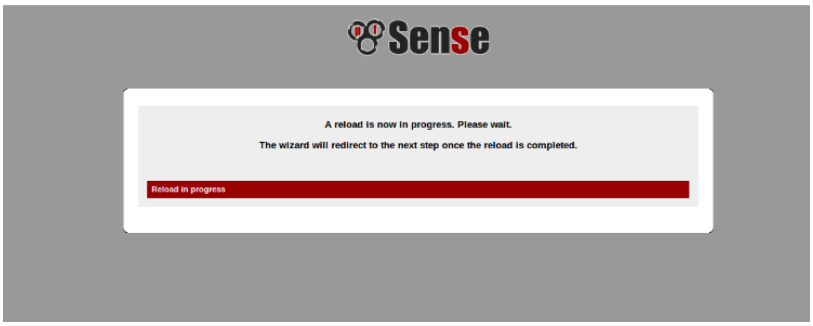
35. Use the defaults; press next to move on.



36. Towards the bottom of the page, uncheck Block Private Networks. Without this pfSense won't work.

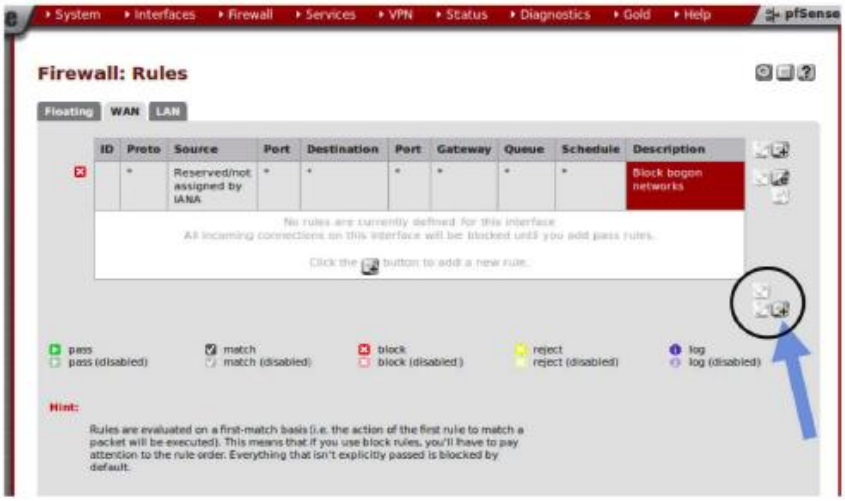


37. Click next and the wizard will finish.



38. Once at the dashboard, go to the Firewall tab on top and click **Rules**.

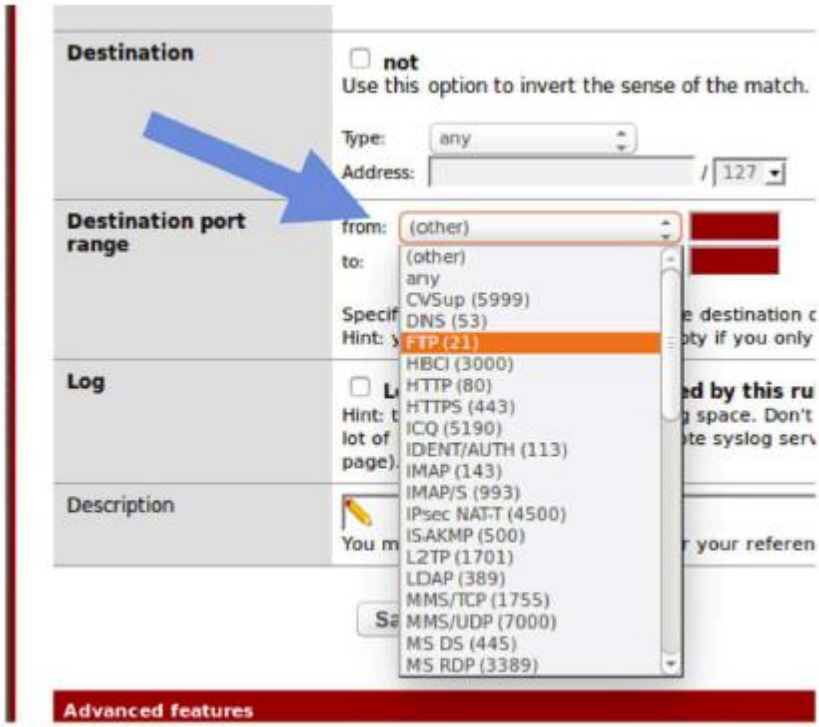
39. Click the+ icon to create a new rule.



40. We want to create a new rule to stop certain packets leaving or entering the firewall. Pick Reject for the action.

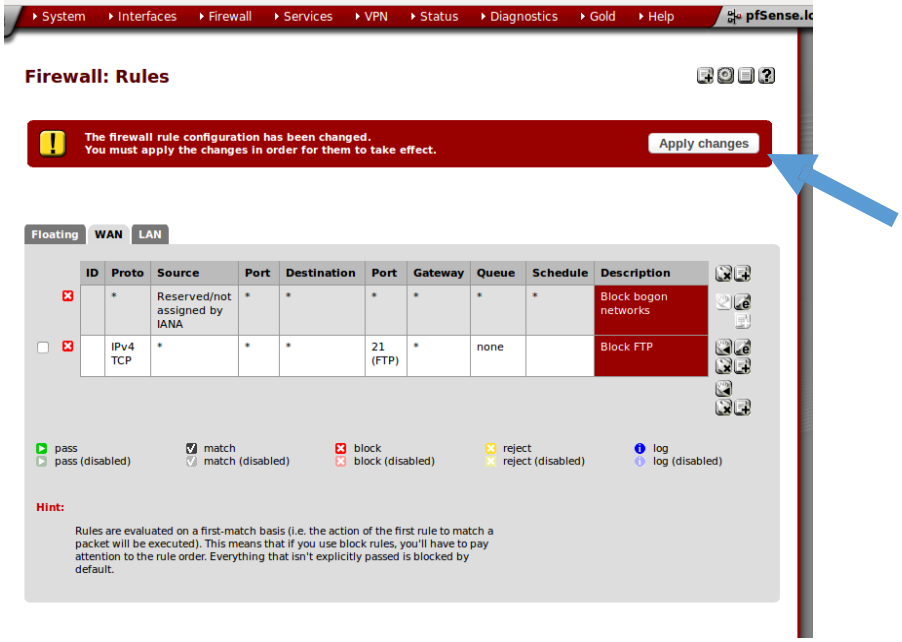
Note: the difference between block and reject is what feedback the sender receives. If we choose "block" then the sender will receive an error code back. Reject will drop the packets without alerting the sender.

41. We want to block any FTP packets. To do this select FTP in the Destination Port Range. The rest will be autofilled.



42. Write a description for the rule then scroll to the bottom and click save.

43. Follow the prompts to apply the changes.



Section 4: Exploring

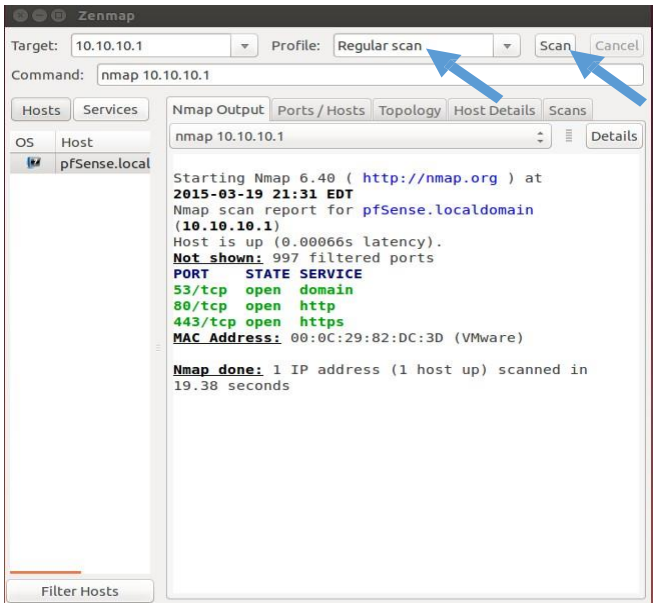
Question 1: Why is blocking FTP a good idea? Use Wireshark and Follow TCP Stream with the sample packet (available on Canvas->Files->Lab) to find out.

Question 2: pfSense is now configured and ready to go. Now return to the Ubuntu_Inside virtual machine. pfSense is providing an IP address and routing for Ubuntu_Inside but which DNS servers are being used?

Question 3:

- Launch the Ubuntu_Outside virtual machine. Verify that it too has an IP address and connectivity.
- Take a minute to fill out the network diagram with the proper IP addresses.
- Return to the Ubuntu_Inside virtual machine.
- Launch **Zenmap**. It is the eyeball icon in the dock on the left.
- We want to scan the open ports of the firewall from the LAN side.
- Input the WebConfigurator's IP into the Target box and select Regular Scan from the profile list. Click Scan.

What does the scan tell us about the firewall?

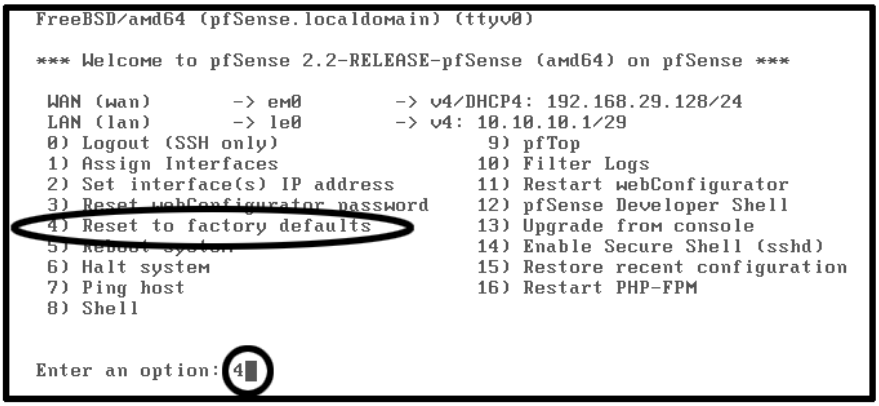


Question 4:

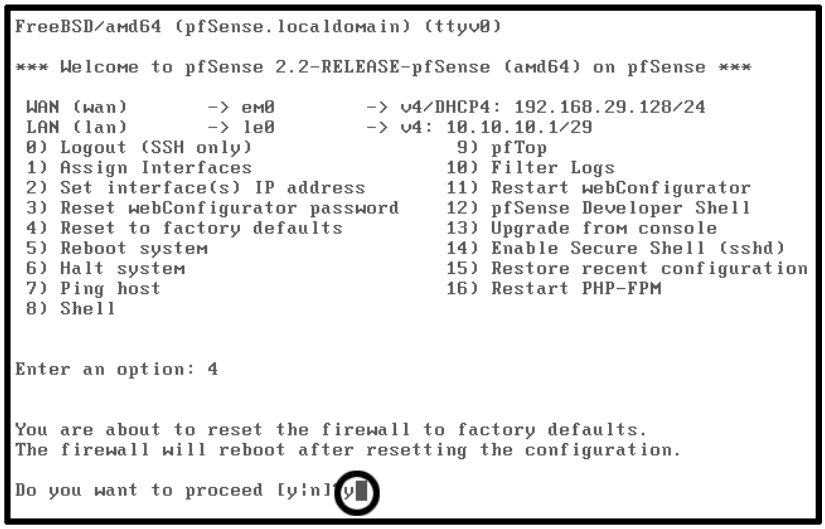
- Launch the Ubuntu_Outside virtual machine.
- Launch **Zenmap**. Same as before it's the eyeball icon in the dock on the left.
- Put pfSense's WAN IP as the target. This should be in your network diagram. Choose Regular and then Scan.

The scan will come back with nothing. Pinging the WAN IP will also come back with nothing. Why?

Finally, return pfSense to its factory defaults.



When asked to proceed, do so to continue with the reset.



Shutdown any remaining open virtual machines.