**Learning About pfSense**

Open the pfSense Book and review the “Introduction>Common Deployment”s section.

* How/where is pfSense typically deployed as a firewall? pfSense is typically deployed as a perimeter firewall being used as a LAN or WAN router.
* What “special” roles can it play as an appliance? pfSense can have the special role of a VPN, Sniffer, and DHCP server appliance.

In the pfSense Book, review the first three pages of the “Firewall” section/chapter

* What type of filtering from the textbook does pfSense offer? pfSense is defined as a Stateful firewall which means as connections come through, pfSense builds a table of the connections coming through in a State Table.
* Would you consider rejecting traffic you deem to be dangerous rather than blocking it? Why or why not? I would consider blocking traffic I deem to be dangerous because when traffic is rejected, a malicious attacker can know that destination they are trying to reach is at least real.
* What is the default Ingress filtering policy on WAN interfaces? Block private networks and block bogon networks.
  + Why does this make sense from a security perspective? Before any configurations are made on the firewall, this will allow the firewall to be online while still blocking all traffic.
* What is the default Egress filtering policy on LAN interfaces? The Anti-Lockout Rule
  + Provide 2 reasons why we would probably want to make adjustments to this default filtering policy. Two reasons to make adjustments to this default filtering policy is prevent admins from locking them selves out