**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 exists.
* 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? Block private networks makes sense from a security perspective as any inbound network with an IP range reserved for private networks will be blocked. The second rule, block bogon networks, blocks traffic from networks that should not be seen on the internet. Meaning, traffic from these networks cannot be verified.
* 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. Adjustments would want to be made to the anti-lockout to rule to only allow trusted hosts within the LAN to access administrative functions of the pfSense firewall. Adjusting the rule to make a separate, isolated management network.