1. Power on the pfSense virtual machine you created in Week 2. Connect to the management interface.
2. Explore the menus and configuration options looking for VPN related settings.
   1. What VPN protocols does pfSense support? OpenVPN, Wireguard, IPsec, and L2TP
   2. Do any of these protocols not support encryption? L2TP does not support encryption on it’s own. It must be paired with another protocol to encrypt traffic.
3. Review the *Virtual Private Networks* chapter in the [pfSense book](https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf).
   1. What protocol is considered the best for interoperability? IPSec is considered the best for interoperability because almost all devices that can support a VPN include IPSec.
   2. What protocol typically is the most firewall friendly for remote access scenarios? OpenVPN is the most firewall-friendly VPN as it uses a single UDP or TCP port number that is not normally restricted by default NAT functions.
   3. What are the common ways pfSense is deployed to provide VPN functionality? Site-to-site connectivity, remote access, protection for wireless networks, and a secure relay.
   4. Does pfSense provide the opportunity to control authorization of VPN traffic with firewall rules? How? PFSense does provide the opportunity to control authorization of VPN traffic with firewall rules as the firewall rules within pFsense can be configured based on the source of the traffic, such as VPN traffic.
4. pfSense supports using certificates during authentication processes for VPN connection
   1. Are certificates a form of symmetric or asymmetric encryption? Certificates can be a form of symmetric or asymmetric encryption depending on the VPN application and what is needed from the VPN.
   2. What protections do they provide? Certificates provide a trusted session between two end points.
   3. Why are these protections vital to the ability to have VPNs that are secure? VPN services need to ensure that traffic sent is secure from on-path attacks and ensuring the identity of the VPN user (their location) remains hidden.