A VPN or a virtual private network extends across a public network and enables the user to receive or send data across shared or public networks as if their computers were directly connected. Using a VPN can be beneficial because it encrypts your data and hides your IP address by bouncing your network activity through a secure chain to another server miles away. Some main advantages to a VPN are ability to use while on public wifi networks, it hides your private information, and prevents data throttling. Disadvantages of a VPN include websites that block VPN users, some countries consider VPNs illegal and VPNs may log and sell browsing data to third parties. While doing my Elk stack project I had my jumpbox provisioner on the subnet and I used my ansible container to connect to my web 1 and web 2 VM. If I hadn’t used my containers they would have been exposed and a potential hacker would be able to work their way into my PC. A VPN would have been able to provide similar security when accessing my Web1 and Web 2 VMs. A VPN would still allow me to achieve online privacy by masking my browsing activity from potential eavesdroppers. Azure provides Cloud based VPN access such as Azure VPN Gateway, with high availability and is easy to manage. The way I would encourage others to use a VPN is to first help them become aware of some of the vulnerabilities associated with not using one such as wifi spoofing and then show how user friendly a VPN is and lastly I would remind that VPNs are not expensive. Most VPNs are fairly inexpensive or sometimes free. ProtonVPN is a VPN service by a Swiss company. They recently received 4 out 5 stars in a review by TechRadar in 2019. ProtonVPN has no bandwidth limits, decent speeds and a good privacy policy. When using a VPN your traffic gets encrypted so no one can intercept it via public Wi-Fi, therefore it is a big advantage for the user. Without a VPN protection your login details, passwords or other private information could be stolen. A VPN can prevent data throttling and minimizes bandwidth congestion. Netflix blocks VPN users and is not able to access their site. In China VPNs are illegal and if used are tightly controlled. Some free VPNs may be selling users browsing data in the background. It is better to do your research when first using a VPN and it is important to understand how it works. Overall I believe with being in the cybersecurity field it is necessary to have a VPN because we are often engaging with various potential threats and a VPN is a good layer of defense against them.