Cloud Security

There is a lot of pros and cons to using a company VPN, but when should we be using one and what is the best time to deploy one. In project 1 for the ELK-stack project we had multiple machines running which consisted of JumpBox-Provisoner(20.102.74.211), Web-1(52.224.110.129), Web-2(52.224.110.129) and lastly the Elk Virtual Machine (20.119.180.182). The tools we used to access any of the Virtual Machines we used were SSH and accessing our containers. We would SSH into our machines which ever we needed at the period by SSH azureuser@ipadress than accessing our containers by adding our docker and attaching it. By attaching the docker we will get access to our root user, to access it would be Sudo docker start (CONTAINER) and Sudo docker attach (CONTAINER). Personally, gaining access was a little challenge at first, I was lost, but as time progressed, I was starting to get the hang of accessing each VM and attaching my docker as well as starting my dockers, but did not use a VPN. Using a VPN is an immediate action people need to do, when you think of data leaks, cyberattacks, personal info accessed you think "that will never happen to me right" but in a blink of an eye it can. In the project I did not deploy a VPN but rather used an SSH, a SSH runs on an application layer of a network, as for a VPN it runs on that transport layer. If a user is trying to gain that SSH on a company's private network you need that VPN, creating that layer for your company's data to push it through. There are some disadvantages to using a VPN, like people say it will slow down your internet speed and can cause attention on whatever activity you are working on. Also using certain apps on that VPN like banking apps, work apps and any apps containing data but should have a certain layer or barrier between the VPN and any apps. But for the project not having a VPN and using a SSH user it would leave it open for attacks through my VM and leaving the public and private IP’s open for an attack. But the advantage of my non- VPN would probably be gaining access to the dockers, but there definitely is more disadvantages to not using a VPN rather that advantage solutions. A VPN does meet the access control in project 1. Access control can identify users by multiple log ins. Log ins that may include usernames and passwords and well as Multifactor Authentication that does require multiple methods to verify that integrity of the user such as a captcha. To get people onboard and get on the wave to our new VPN system wouldn't be a choice but a requirement. A requirement that protects the user and integrity of the company from any data leaks or cyberattacks. Take it in a sense of say if someone stood on a corner and has your address your bank information your family your social security numbers your bank statements, you would be upset right? Exactly, so if a VPN was there imagined someone painting over that board hiding confidential information, then scribbling all over that is what a VPN is like. There are tools to deploy on Azure to execute in the Virtual Machine. One that I would personally deploy would be Microsoft Defender for Cloud, and which is a cloud security posture management. it is a cloud protection that its solution by finding vulnerable spots and strengthens the security of the cloud environment and protects the workloads across multiple environments. it is definitely worth the added price to protect certain areas. Is there really a time where VPN can be too much and be overkill? The answer is No, never in my opinion. Even to leave a VPN on all the time it decreases the chances of a data leak or even cyber-attacks. Say you are searching the web and come across a website and notice there is no HTTPS extension, being a https extension on blocks from you and the website you are on. But using a VPN encrypts all the connections. People also say a VPN can also slow down your Internet but others say they don’t see a noticeable difference between the speed when a VPN is always running. There are 3 types of access controls to think about, there is Mandatory Access Control which controls the system with restrictive protections. Another access control can be Discretionary Access Control and although it’s in the owner's hands it can be controlled on what is accessible and what resources someone can access. Last is Role-Based Access Control and it has a goal of only letting certain users that have roles and is only necessary for that user. Last but not least a VPN is a good key to follow when under the occurrence of a data breach or if a user is connected to a public WI-FI. Using that VPN is also a subtitle way of by-passing any firewalls, and or browsing the internet anonymously without any worries. So, ending we now know that VPNs do a lot of work on keeping us safe and blocking any negative or suspicious activity. The future is still ahead and technology is barley getting started, computers are growing with more and more intelligence, CPU, etc. Each year. It's safe to take precautions now rather than later when you find yourself in a sticky situation.