1. Restate the Problem

2. Provide a Concrete Example Scenario

    - In Project 1, which VMs did you have on the network?
    - Which tools did you use to control access to and from the network?
    - If you didn't use a VPN, what did you use?
    - What disadvantage(s) did your non-VPN solution have?
    - What advantage(s) did your non-VPN solution have?

Employees at a company may be a bit cautious of using a corporate VPN because it allows the company to view your internet browsing while connected to the corporate network. Although this is a valid concern, the advantages of using a corporate VPN should be considered before outright dismissing the idea. A corporate VPN can be beneficial because an attacker will have a much more difficult time understanding the network if that information is kept private. A VPN created in-house has no open-source code that could be posted on the internet or shared between attackers. The main advantage of a corporate VPN is that it protects and disguises the network from attackers with a changing IP address. This would protect against a large amounts of attacks because it prevents the attacker from being able to track and save the company IP addresses.

In Project 1 I did not use a VPN in my network because I already created security rules to deny anyone access except for specific IP addresses. This prevents unwanted people from accessing my network and causing harm. Another tool I used in my network is the Load Balancer (LB) which automatically distributes traffic between my Web VM's. This access control allows us to be sure that one VM is not overrun with large amounts of traffic. As you can see from my network diagram, the load balancer is placed after the firewall to ensure it's not distributing dangerous software or malicious IP's. This leads me to my last access control used, the firewall! It automatically detects when an attack is being attempted and aims to deny it. In this case, all safe traffic will be distributed to the load balancer which will then distribute the traffic to my 3 web VM's.

Of course, this solution is not fool-proof. Our firewall can still be bypassed by a persistent hacker. At this point, the load-balancer would not protect us from an attack. For example, let's say an attacker is attempting a DDoS attack and has bypassed our firewall. The DDoS attack can be centered at the load balancer which would then just distribute the packets to both VM's. This may take a bit longer to achieve, but eventually the attack would render our Web VM's useless. It's for this reason that a corporate VPN can be extremely advantageous. A corporate VPN installed on our network would ensure that the attacker has an extremely difficult time trying to locate our IP address. Because of this, a DDoS attack would be difficult to achieve because the attacker cannot pinpoint an address to send the packets.

A corporate VPN, although monitored by the company, can be extremely useful. It allows the IT department at the company to set up specific alarms to trigger when an attack could be

coming. This allows the company to protect against threats before they're presented by moving to a backup server or just stopping the server altogether. It gives the company much more control over who can enter the network; and more importantly, what is being sent from the network.