**Student Name:** Coleton Sanheim / D’artagnan Boocock **Weight: 5%**

**Student ID:** 000862545 **Marks: /**

# Objective

Design a layered network security defense.

# Introduction

**Defense in depth** is a strategy that is widely adopted by organizations to protect their information systems. Layers of defense are used to slow down and wear out an attacker’s momentum, which buys reaction time and allows security to counter an attack.

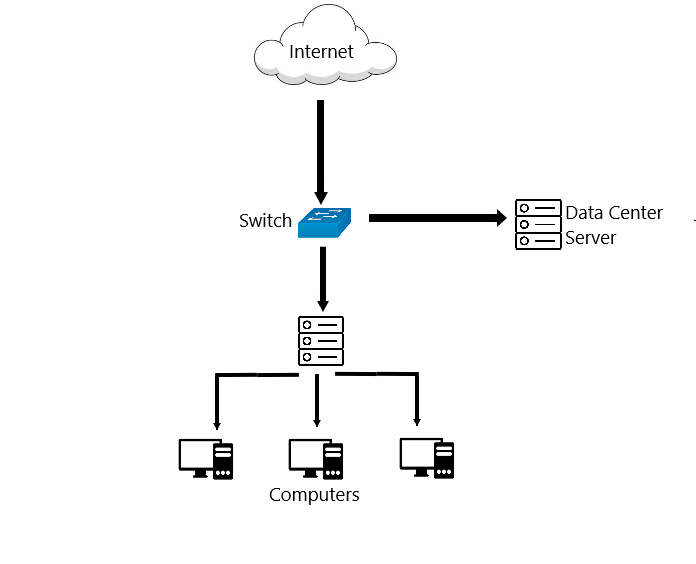
In network security, defense in depth is often used at the security perimeter, especially between the Internet, the DMZ and the internal networks. Different security controls are employed in layers to create a multi-layer defense environment, protecting the security perimeter and internal network resources.

# Instructions

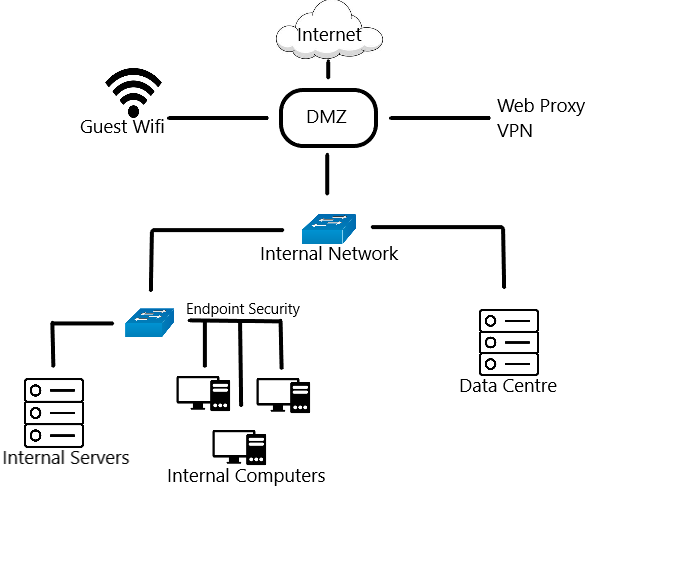
For this mini project, design a plan with respect to each of the areas listed below that uses defense in depth layered security control for the organization network.

In your plan, include a logical diagram that shows the security control, the security zones, the network segments and the IP address assignments.

1. External Internet to the DMZ
2. DMZ services (Web proxy, VPN)
3. DMZ to the internal network
4. Guest WiFi network
5. Sensitive financial database servers in the data centre
6. Network switches
7. Computers



As you can see in this diagram, there no layers of security between an attacker and sensitive data in either the data center or internal network. This is a very bad example of proper defense in depth security. An attack (such as MAC spoofing, phishing attacks on the personal computers, or DDos attacks) could completely compromise the entire system.



In this diagram there is much better designed system for protecting data. All connections to the internal network is filtered through the DMZ, which contains various security applications such as a Web Proxy and a VPN. The internal network is structured into two separate sections, so that if one is compromised then the other can still be secure. On one side there is the secure data centre, which contains its own physical and digital security to protect its sensitive data. On the other section we have the personal computers and servers of the company, which will be installed with various endpoint security to ensure they themselves cannot be the vector of attack into the internal network.