**Student Name:** Ahmed **Weight: 5%**

**Student ID:** 651096 **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.

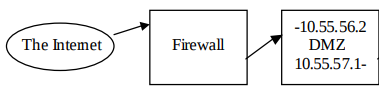
# Instructions

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

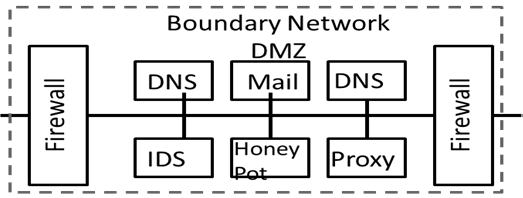
A DMZ separates an external network from directly referencing an internal network. Most of the time the external network is the Internet and what is in the DMZ is the web server but this isn’t the only possible configuration. The most secure network configuration for a DMZ is to separate your external network, your demilitarized zone, and your internal network by putting them all on different subnets. A firewall separates the external Internet to the DMZ.



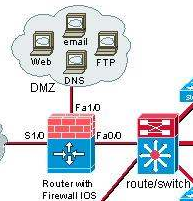
1. DMZ services (Web proxy, VPN)

These are services that are especially subject to attack and are isolated into a boundary network referred to as the DMZ. These also include a firewall at both the input to the DMZ and the output to the sub-networks. These firewalls are different in that they apply different rules and filters to allow the traffic beyond the firewall in both directions. The DMZ also

includes an Intrusion Detection System and a Honeypot which work in tandem to identify

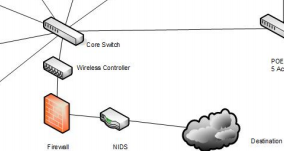
traffic and attack conditions on the boundary. The focus of this boundary network is to isolate more sensitive domains from direct attacks and to place more outside facing servers away from sensitive networks.

1. DMZ to the internal network



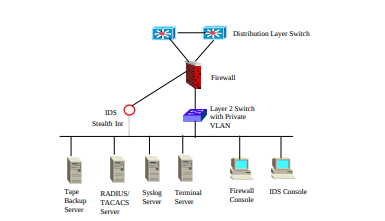
In this step, a DMZ is created and devices such as web servers, FTP servers, email servers and DNS servers are moved into this zone. These servers will reside in a secure area that is access controlled for only authorized personnel.

1. Guest WiFi network

Control of guest network access is by Web Authentication (Web-Auth). Guests receive a Username, and password that expires after a 24-hour period. When connecting to the Guest Service Set Identifier (SSID), all users are forced into a web portal that requires them to provide their credentials.

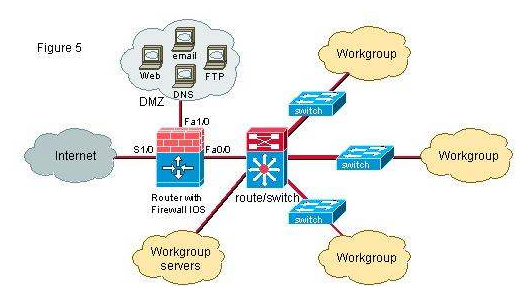
Sensitive financial database servers in the data centre

The data center is equipped with video surveillance camera, on-site security officers, backup generators, biometrics sensors, fire suppression system and on-site management. Typically, an Internet Data Center provides the following services: i) Shared Web Hosting – In this service, the customer typically uses a portion of a server ii) Dedicated Server hosting – the customer uses the whole server and is normally a fully functional e-commerce software. iii) Co-location hosting – The customer has dedicated racking space to house their servers iv) Application hosting – The customer application is hosted at the IDC



Internet Data Center provides the following services: i) Shared Web Hosting – In this service, the customer typically uses a portion of a server ii) Dedicated Server hosting – the customer uses the whole server and is normally a fully functional e-commerce software. iii) Co-location hosting – The customer has dedicated racking space to house their servers iv) Application hosting – The customer application is hosted at the IDC

1. Network switches



This design is called a tri-homed DMZ and we will take one subnet from the internal class B and use it for this network in order for the devices in the DMZ to have public addresses.

1. Computers

User Awareness - Employees need to be made aware that strangers cannot be in the office without an escort. Awareness programs should encourage all employees to confront and ask an unidentified individual if they need any assistance.

Laptop Locks - These cables are physically connected to the laptop, which are then connected to a desk. A key is required to unlock the cable and, although these cables can be cut, implementing them on easily removable devices such as laptops may deter an attacker from actually making the effort.

OS Hardening - USB ports for drives and CD-R/DVD-R drives should be disabled on all laptops/desktops so that files cannot be easily copied and stolen by a malicious user wandering around in the office. NOTE: there is still the problem of USB devices that are programmable keyboards.