**Security and Support in IT G (6689) – Assignment 2**

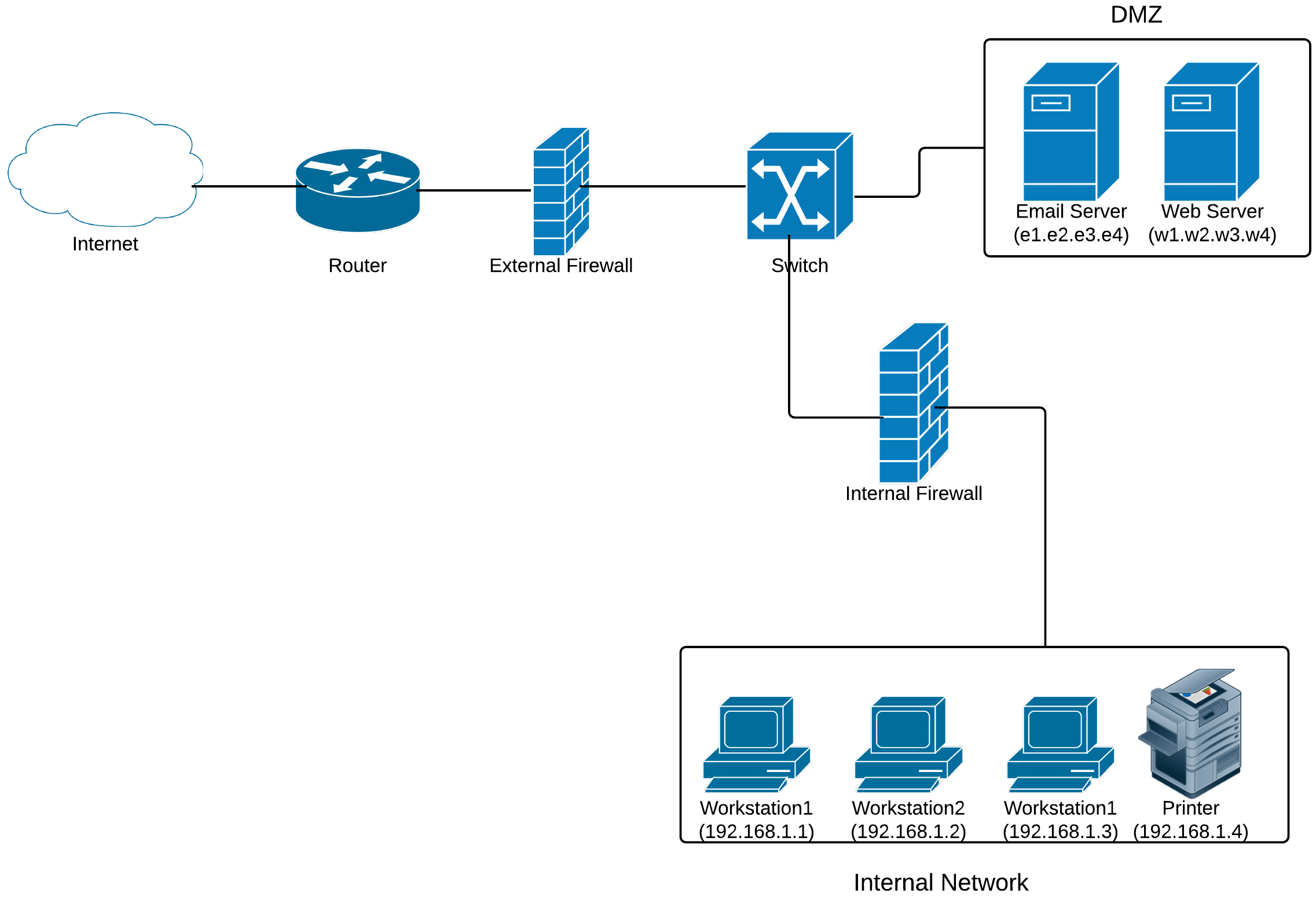
**Submitted by:**

**Name: Tenzin Dendup**

**Student ID: u3149399**

**Answers to Question 1**

Organization’s Network:



*Fig 1: Organization’s Network Diagram*

The organizations network is connected to the internet through their main router behind which sits the external firewall. A switch then divides the network into two, namely, the DMZ which has the webserver and the email server and the internal network.

The two servers (email and web) are provided with global IP address and are put in the DMZ since they need to allow connection from the internet. The workstations and printer are in the internal network and given private IP addresses under the same subnet. The internal network sits behind internal firewall which provides additional security. Hosts on internal network can access services on the internet and DMZ but are protected from the malicious connection requests and other threats from the internet. We also assume that the internal firewall acts as Network Address Translation (NAT) for internal network.

Firewall rules for External Firewall:

* Allow access to email server from the internet (SMTP & IMAP)
* Allow access to webserver from the internet (both http and https)
* Block any other connection request from outside
* Allow access to all services on internet from the organization’s network (Assuming the global IP addresses of the organization is in the range **x1.x2.0.0/24**, which includes IP addresses of the servers)

Chain INPUT (Policy ACCEPT)

target prot opt source destination

*ACCEPT tcp -- anywhere e1.e2.e3.e4 tcp:dpt:smtp state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere e1.e2.e3.e4 tcp:dpt:imap state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere w1.w2.w3.w4 tcp:dpt:https state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere w1.w2.w3.w4 tcp:dpt:http state RELATED, ESTABLISHED*

*REJECT all -- anywhere anywhere reject-with-icmp-port-unreachable*

Chain OUTPUT (Policy ACCEPT)

*ACCEPT any -- x1.x2.0.0/24 anywhere any*

Firewall rules for Internal Firewall:

* Allow connection from DMZ servers to internal network workstations
* Block all connection request from internet to internal network
* Allow access from internal network to all internet services

Chain INPUT (Policy ACCEPT)

target prot opt source destination

*ACCEPT tcp -- w1.w2.w3.w4 192.168.1.0/24 any*

*ACCEPT tcp -- e1.e2.e3.e4 192.168.1.0/24 any*

*REJECT all -- anywhere 192.168.1.0/24 reject-with-icmp-port-unreachable*

Chain OUTPUT (Policy ACCEPT)

*ACCEPT any -- 192.168.0.0/24 anywhere any*

**Answer to Question 2**

Buffer Overflow

Buffer overflow is a condition that occurs in software programs where more input can be placed into a buffer or data holding area compared to the actual capacity allocated, which results in overwriting other information in adjacent memory locations. This mainly happens due to use of unsafe function calls and careless programming. Attackers exploit buffer overflow vulnerabilities to crash a system or to insert especially crafted code, called shellcode, to gain control of the system. The consequences of buffer overflow problem could cause corruption of data, unexpected transfer of program execution, memory access violations and program termination. If the program being affected us used to provide service to users, its termination may result is Denial of Service.

Programming techniques a software development team should adopt to avoid buffer overflow problems include:

* Choosing a modern high level programming language, like Java, that does not permit buffer overflow
* Making use of safe standard library functions
* Using safe coding standards like ensuring any code that writes to a buffer must check size of buffer for available space
* Including additional code that detects stack frame corruption
* Using Defensive and Secure Programming techniques

Nessus Report