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

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

# Instructions

Prepare an internal security audit on a DMZ firewall to ensure it complies with the company’s security standard.

Audit the firewall ruleset below and report any discrepancy between the company’s security standard and the firewall ruleset. You must also provide recommendations to address the issues.

# Security Standard Defined by Company for Firewall Ruleset

* Block by default – All traffic should be blocked by default, with an explicit deny rule at the bottom of the ruleset
* Explicit allow – All required and approved network communication must be explicitly allowed in the firewall rule
* Specific traffic – Source IP, Destination IP and Destination port must be as specific as possible to enforce the least privilege principle
* Do not use ANY in all three fields – Source IP, Destination IP and Destination port cannot be ANY, unless it is a default block rule
* Rule position – more specific rules should be positioned higher in the ruleset than general rules
* Logging – all firewall rules should be logged
* Comment – the Comment field must include the approval ticket number, the reason for the rule and the last modified date of the rule
* Network address – the company’s internal network uses a class b network   
  address – 192.168.0.0/16

# Firewall Ruleset to Audit

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No** | **Source IP** | **Dest IP** | **Dest Port** | **Action** | **Logging** | **Comment** |
| 1 | ANY | 8.8.8.8 | UDP 53 | Allow | Yes |  |
| 2 | 192.168.1.45 | 207.67.22.103 | TCP 80 | Allow | No | Temp internet access for CEO |
| 3 | ANY | ANY | TCP 80, TCP 443 | Allow | No | Company web access |
| 4 | ANY | 192.168.9.254 | TCP 80 | Allow | Yes | Ticket# 0568392 – inbound traffic to company web server – 05/31/16 |
| 5 | 192.168.0.0/16 | ANY | PING | Allow | No | Allow company internal network to ping hosts on internet |