ITSC 308 M09

Firewall Security Audit Assignment

Submitted to Ritika on July 29th 2022

Jack Chen & Coleton Sanheim

# 

# 

# **Table of Contents**

# 

[**Introduction**](#_eqxact1c9ar9) **3**

[**Current Network Design**](#_xbujhw27i5f6) **3**

[**Security Standard**](#_4iqxfmxkylim) **4**

[**Firewall Ruleset to Audit**](#_tzve8yx7qf1h) **4**

[**Rule Violations and Recommendations**](#_utigw3k9conx) **5**

# 

# **Introduction**

In this report we are performing an audit on a company’s DMZ firewall to ensure it complies with the security standard that has been defined by the company for the firewall ruleset. We will describe what rules in the security standard it breaks and what it needs to change in order to comply.

# **Current Network Design**

# 

# 

# 

# 

# Security Standard

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** |

# Rule Violations and Recommendations

The first major rule violation present in this ruleset is that all traffic is not blocked by default, an explicit deny rule needs to be added to the bottom of the ruleset.

None of these rules are very specific, and need to include more specificity to adhere to the Security Standard. For example, the source IP should always include the company’s internal network IP range, only allowing employees to access the network. From there you can then only allow specific ranges to only allow certain employees to do certain things.

All five current rules all use ANY in either Source IP, Destination IP, and/or Destination Port, this is a rule violation, none of these fields can be ANY (unless it is the default block rule) and as such need to be changed, including what IP’s are allowed as sources and what IP’s/Ports are allowed as destinations.

Only rules 1 and 4 include logging, rules 2, 3, and 5 do not. every rule should have logging enabled.

Only rule 4 adheres to the comment standard, rules 1, 2 ,3, and 5 do not. Every comment should include the ticket number, description of rule and time it was last modified. The first rule doesn't even have a description of itself at all.