# Firewall Rule Set Review Document

# NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by GENPACT, nor is this document (in whole or in part) to be reproduced or furnished to third parties or made public without the prior express written permission of GENPACT.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Review Start Date** | **Review End Date** | **Changes** | **Reviewer Name** | **Approver** |
| 25 Nov 2020 | 25 Nov 2020 | FW Rule Review | Gaurav Agrawal | Ranadheer |

*Genpact Firewall review report*

*MHE - Hyderabad (RITP)*

*Review Date: 25 Nov 2020*



**Table of Contents**

1. **Objective & Scope**
2. **Methodology**
3. **Results**

**Objective & Scope**

The objective of this review on Genpact firewall devices was to detect any configuration vulnerability and/or deviations in the firewall devices which can be exploited to get unauthorized access and information.

The scope of review is limited to firewalls implemented in networks supporting/handling customer data.

**Methodology**

The running configuration on the firewall in scope is pulled out from the device. The configuration is then assessed against the standard configuration guidelines and the standard ports allowed in environment. The ACLs are reviewed to validate against any deviations from the allowed communication.

The activity is carried out to identify any configuration vulnerabilities and deviations from allowed communication. The goal of the activity is to determine whether unauthorized changes are done on the firewalls or deviations exist that can result in unauthorized access to information.

Further to break this process the outcome in a stage view will be….

* **Collection** – Pull out the current running configuration on the firewalls in scope. The raw configuration is captured in text file.
* **Review** – Compare the configuration of the firewall with the standard configuration guidelines to identify if there are any deviations from the standard configuration.
* **Validation** - Analysis of the ACLs with the allowed communication on the network. This effort compares ACLs configured on the firewall.
* **Reporting** - provides an overview of the assessment methodology, vulnerability and threat assessment findings, recommendations and corrective actions and a copy of all data collected.

**Test Results**

* Unused rules available on firewall

**Summary**

|  |  |  |
| --- | --- | --- |
| **Firewall Name** | **Standard Configuration** | **ACLs** |
| IND-COS-GSD-VPN-FW-01  IND-COS-GSD-INT-FW-01  IND-DLF-GSD-BUS-FW-01  IND-DLF-GSD-INT-PA-01 | Reviewed | Reviewed |

**Observations:**

Below are the annotations that were identified the same has been confirmed after the comparison of the configuration.

* Unused or zero hits rules available on FWs

**Result or Action required**

As there are few work areas identified hence, below are the recommended actions which are required on the firewall configuration.

**Recommendation:**

* Rules With 0 hit-counts to be removed

***Firewall Rules***



***Double click the above icon to open the configuration***