# 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.

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Changes** | **Reviewer Name** | **Approver** |
| 6th Oct’2020 | FW Rule Review | Archit Dureja | Deepak Kumar |

*Genpact Firewall review report*

Athena Health- PHP 5132, Eton

*Review Date:* 6th Oct, 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 PCI data in **PHP-ETO-GSD-INT-FW**, **PHP-513-GSD-BUS-FW & PHP-513-GSD-INT-FW**

**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**

**Observations:**

* No Observations.

**Summary**

|  |  |  |
| --- | --- | --- |
| **Firewall Name** | **Standard Configuration** | **ACLs** |
| **PHP-ETO-GSD-INT-FW** | Reviewed | Reviewed |
| **PHP-513-GSD-BUS-FW** | Reviewed | Reviewed |
| **PHP-513-GSD-INT-FW** | Reviewed | Reviewed |

**Observations:**

* Port TCP 3389 allowed
* Bidirectional communication allowed for port UDP 53
* Unused rules available.

**Result or Action required**

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

* **Observation 1:** Port TCP 3389 allowed

**Recommendation:** Being a management port 3389 Verify the port requirement & remove in-case not required.

* **Observation 2:** Bidirectional communication allowed for port UDP 53

**Recommendation:** Being a DNS service port 53 Verify the port requirement & remove as bidirectional communication would not be required.

* **Observation 3:** Bidirectional communication allowed for port UDP 53

**Recommendation:** Remove 0 hit rules.

**Complete Configuration**

***Firewall Ruleset configuration for* Athena Health**







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