TrustIoT Framework for Industry 4.0

"Firewall Policies: Configuration best practices"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc176333194)

[2. Purpose 4](#_Toc176333195)

[3. Scope 4](#_Toc176333196)

[4. Policy Statement 4](#_Toc176333197)

[4.1. Rule Design and Implementation 4](#_Toc176333198)

[4.2. Default Deny Principle 4](#_Toc176333199)

[4.3. Network Segmentation 4](#_Toc176333200)

[4.4. Logging and Monitoring 5](#_Toc176333201)

[4.5. Regular Reviews and Updates 5](#_Toc176333202)

[5. Responsibilities 5](#_Toc176333203)

[6. Breaches of Policy 5](#_Toc176333204)

[7. Document Management 5](#_Toc176333205)

# Introduction

Firewalls serve as critical security components in protecting networks from unauthorised access and malicious activity. In the context of the Internet of Things (IoT), where numerous devices with varying security postures are connected, the proper configuration and management of firewalls become even more crucial. This policy outlines best practices for configuring firewalls to safeguard the organisation's IoT infrastructure.

# Purpose

The purpose of this policy is to establish guidelines and configuration best practices for firewalls deployed within the organisation's IoT environment. This policy aims to:

* Control and monitor network traffic to and from IoT devices.
* Prevent unauthorised access and malicious activity from reaching IoT devices.
* Protect the confidentiality, integrity, and availability of data and systems connected to the IoT network.
* Ensure that firewall configurations align with industry best practices and security standards.

# Scope

This policy applies to all firewalls deployed within the organisation's network, including those specifically dedicated to protecting IoT devices and segments.

# Policy Statement

## Rule Design and Implementation

* **Least Privilege:** Firewall rules shall adhere to the principle of least privilege, allowing only the minimum necessary traffic required for legitimate IoT device operation.
* **Explicit Permit/Deny:** Firewall rules shall be explicit, clearly defining permitted and denied traffic based on source/destination IP addresses, ports, protocols, and other relevant criteria.
* **Stateful Inspection:** Stateful inspection shall be enabled on firewalls to track the state of network connections and prevent unauthorised packets from bypassing the firewall.
* **Application-Layer Filtering:** Where applicable, application-layer filtering shall be implemented to inspect and control traffic based on specific application protocols or behaviours.

## Default Deny Principle

* **Implicit Deny:** A default deny policy shall be implemented, meaning that all traffic not explicitly permitted by firewall rules shall be blocked.
* **Exception Management:** Exceptions to the default deny policy shall be granted only with proper justification and approval, and shall be documented and reviewed regularly.

## Network Segmentation

* **IoT Segmentation:** IoT devices shall be segmented from other parts of the network using firewalls to create isolated zones based on security requirements and device types.
* **Critical Asset Protection:** Critical systems and sensitive data shall be placed in highly restricted network segments with limited access.
* **Guest and External Networks:** Guest and external networks shall be isolated from the internal network using firewalls to prevent unauthorised access.

## Logging and Monitoring

* **Log Collection:** Firewall logs shall be collected and stored securely for analysis and incident response.
* **Real-time Monitoring:** Security information and event management (SIEM) systems or equivalent tools shall be utilised to monitor firewall logs in real-time, enabling the detection and response to security events.
* **Alerting:** Automated alerts shall be generated for suspicious activity or policy violations, triggering timely investigation and remediation.

## Regular Reviews and Updates

* **Periodic Reviews:** Firewall configurations and rules shall be reviewed periodically to ensure their continued effectiveness and alignment with security requirements.
* **Change Management:** Changes to firewall configurations shall be subject to a formal change management process to ensure proper authorisation, testing, and documentation.
* **Firmware Updates:** Firewall firmware shall be kept up-to-date to address security vulnerabilities and ensure optimal performance.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Network Administrators:** Responsible for configuring and managing firewalls in accordance with this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring firewall logs, analysing security events, and responding to incidents.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager