

Web Application Firewall (WAF) Rules & Policy

Document Title: Web Application Firewall (WAF) Policy

Version: 1.0

Prepared by: Muneer Shaukath

Designation: Network Engineer

1. Purpose

To define rules and configuration standards for the Web Application Firewall (WAF) to protect web applications from common threats and vulnerabilities, ensure compliance with security standards, and support continuous monitoring and improvement.

2. Scope

This policy applies to:

- All web-facing applications and services owned or managed by the organization.
- All employees, contractors, and vendors responsible for deploying, maintaining, or managing web applications.

3. Policy Requirements

3.1 WAF Deployment

- A WAF must be deployed in front of all internet-facing web applications.
- The WAF must operate in **blocking mode** (not just monitoring) for production environments.
- WAF policies must be reviewed and tuned regularly to reduce false positives and negatives.

3.2 Minimum Rule Set

The WAF must enforce rules that protect against:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)

- Directory Traversal
- HTTP Protocol Violations
- Known OWASP Top 10 threats

3.3 Custom Rules

- Custom application-specific rules must be created based on application logic, known vulnerabilities, or pentest results.
- Rules should be tested in staging before deployment to production.

3.4 Logging & Monitoring

- All WAF events and rule triggers must be logged and monitored.
- Logs must be retained according to the Log Management Policy (e.g., minimum 90 days).
- Critical alerts must be integrated with the SIEM/SOC for real-time monitoring and response.

3.5 Updates and Tuning

- WAF signature updates must be applied promptly.
- Rule sets must be reviewed at least quarterly or when significant changes to applications occur.

3.6 Exception Management

- Any request to bypass or disable a WAF rule must be documented, risk assessed, approved by the IT Security Manager, and compensated with alternative controls where possible.

4. Non-Compliance

Non-compliance with this policy may result in disciplinary action and could expose the organization to increased risk of attacks, data breaches, or legal liability.

5. Roles and Responsibilities

Role	Responsibility
IT Security Manager	Approve and oversee WAF configuration, tuning, and compliance.
System Administrators	Implement, update, and monitor WAF rules and logs.
SOC / Incident Response Team	Monitor WAF alerts and respond to incidents as needed.

6. Review and Maintenance

This policy and WAF rule sets must be reviewed at least annually or when major changes to applications or threat landscapes occur.

For Office Use Only:

Approved By: Sherry George	
Designation: Technical Director	
Reviewed By: Rixon Thomas	
Designation: Sr. Infrastructure Engineer	
Signature Of Approver:	Date:

--End of Document--