*Note: In all cases check against online version for the latest revision prior to use*

# STATEMENT OF WORK

## For: Web Application Firewall for five (5) years

Project Name: Trans-WAF-01
Project Number:

Revision Number: Trans-WAF-05Y
Approved by:

Release Date:
Print Date: 15/09/2026
Template Date: 09/09/2026

| Distribution | |
|---|---|
| Name | Location |
| | |

# Statement of Work

| | |
|---|---|
| **Planned start:** | **01st September 2026** |
| **Planned finish:** | **30 September 2026** |
| **Key contact name:** | **Nhlanhla Shongwe** |

## Background

As part of its cybersecurity strategy and risk mitigation programme, Transnet continues to strengthen the protection of its online business applications against application-layer threats such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Web application attacks remain a primary vector for data breaches, often providing unauthorised access to sensitive organisational data.

In response to this risk, Transnet seeks to appoint a service provider to deliver a fully managed, turnkey Web Application Firewall (WAF) solution for a period of five (5) years. The solution will be deployed to protect customer-facing web applications and mitigate cyber threats that could lead to the compromise or exfiltration of sensitive data.

## Responsibility of parties

The WAF solution is managed under a co-managed operating model, where Transnet Group ICT retains full control and accountability for policy management, configuration, monitoring, and incident response, while the service provider provides platform support, threat intelligence updates, and advanced tuning services.

## Mandatory deliverables

The service provider shall deliver, but not be limited to, the following:

- Design and implementation of a WAF architecture aligned to Transnet's application and network environment.
- Deployment and configuration of WAF controls for all identified customer-facing web applications.



TRANSNET CONFIDENTIAL INFORMATION

- Development and application of baseline security policies (including OWASP Top 10 protections).
- Integration with existing security infrastructure (e.g., SIEM, SOC monitoring tools, and logging platforms).
- Real-time traffic inspection, monitoring, and blocking of malicious web application requests.
- Threat intelligence integration with continuous updates to detection and protection rules.
- Centralized management console providing visibility, reporting, and policy administration.
- Comprehensive logging, alerting, and audit trail capabilities for security and compliance reporting.
- Incident detection, response support, and escalation procedures aligned to Transnet's operational requirements.
- Performance tuning and optimisation to ensure minimal impact on application availability and user experience.
- Training and knowledge transfer to Transnet technical and security teams.
- Detailed documentation including architecture design, configuration standards, operating procedures, and as-built documentation.
- Ongoing managed service support, including patching, upgrades, and 24/7 technical support for the full five-year period.

---

**WAF Technical Deployment Architectures**

- **Reverse Proxy (Inline):**
    - Traffic flows through the WAF before reaching the application; provides full inspection and strongest protection but may introduce latency.
- **Transparent / Bridge Mode:**
    - Deployed inline without changing IP addressing; easier integration but still requires high availability design.
- **Out-of-Band (Monitoring Mode):**
    - Inspects mirrored traffic only; used for detection and tuning but cannot block attacks in real time.
- **Cloud / CDN-Based WAF:**
    - Delivered as a managed service at the network edge; highly scalable with reduced infrastructure overhead, but dependent on provider.
- **Hybrid Model:**



TRANSNET CONFIDENTIAL INFORMATION

- Combination of on-premise and cloud WAF deployment to balance control, scalability, and resilience.

---

**Preferred WAF Technical deployment Architecture**

- **Cloud / CDN-Based WAF:**
  - Delivered as a managed service at the network edge; highly scalable with reduced infrastructure overhead, but dependent on provider.

**WAF Operational Deployment Models:**

- **Fully Managed WAF (Managed Service):**
  - The service provider manages the entire WAF environment, including deployment, policy configuration, monitoring, incident response, and reporting. Transnet consumes the service with minimal operational involvement.
- **Self-Managed Cloud WAF:**
  - Transnet retains full control of the WAF, including policy management, configuration, monitoring, and response activities, using a cloud-based platform.
- **Co-Managed WAF:**
  - A shared responsibility model where the provider manages the platform and provides expertise, while Transnet retains control over policies, approvals, and oversight (typically via the SOC).
- **Auto-Provisioned WAF:**
  - A largely automated model where applications are onboarded using predefined templates and baseline policies, enabling rapid deployment with minimal manual configuration.
- **Hybrid Operational Model:**
  - A mixed approach where different applications use different operational models (e.g., critical systems co-managed, standard apps fully managed, and new apps auto-provisioned) based on risk and complexity.

**Preferred WAF Operational Deployment Model**

- **Co-Managed WAF:**
  - A shared responsibility model where the provider manages the platform and provides expertise, while Transnet retains control over policies, approvals, and oversight (typically via the SOC).

**Target WAF Architecture and Operating Model**

Transnet requires a Cloud / CDN-based Web Application Firewall (WAF) deployed at the network edge to provide scalable protection for customer-facing web applications. The solution must



TRANSNET CONFIDENTIAL INFORMATION

deliver application-layer (Layer 7) security controls, including protection against SQL injection, cross-site scripting (XSS), bot attacks, and API abuse, while leveraging the scalability, resilience, and availability of a cloud delivery network.

The solution will be delivered under a co-managed operating model, with Transnet retaining full control over WAF policy management, configuration, monitoring, and incident response through a centralised cloud management platform integrated with SOC operations. The service provider will provide platform management, threat intelligence updates, and advanced security tuning support.

**Rationale**

- Cloud/CDN-based architecture: Enables edge-based protection, DDoS mitigation, and scalable Layer 7 security for internet-facing applications.
- Co-managed operating model: Ensures Transnet retains full operational and governance control over WAF security decisions while benefiting from specialist provider expertise, continuous threat intelligence, and platform support.

**Artificial Intelligence and Automated Capabilities**

**Where the proposed WAF solution uses artificial intelligence, machine learning, behavioural analytics, automated policy generation, automated tuning, bot classification, threat scoring or similar automated decision-support capabilities, the Service Provider shall:**

- identify and describe each AI-enabled or automated capability offered as part of the solution;
- state whether the capability is mandatory, optional or configurable.
- explain the purpose of the capability, the information processed and the resulting action or recommendation;
- ensure that AI-enabled functionality is implemented and operated in accordance with the current Transnet Artificial Intelligence Policy, information-security requirements, privacy requirements and governance controls;
- ensure that automated recommendations or policy changes affecting Transnet services remain subject to authorised human oversight and Transnet's approval and change-management processes;
- provide an audit trail of material AI-generated recommendations, automated policy changes and security actions;
- not use Transnet information to train, improve or validate any shared or public AI model without Transnet's prior written approval;
- implement appropriate access control, data segregation, retention, integrity, confidentiality and incident-management controls for information processed by AI-enabled capabilities; and
- provide sufficient information to Transnet to assess the risks, limitations, accuracy, explainability and security implications of the AI-enabled capabilities.

**The inclusion of an AI-enabled capability shall not reduce or transfer the Service Provider's accountability for compliance with the Agreement, achievement of the Service Levels, accuracy of configuration, protection of Transnet information or the performance of the WAF service.**
**If the solution does not use AI or machine-learning capabilities, the bidder shall expressly state this in its response.**



TRANSNET CONFIDENTIAL INFORMATION

**WAF – ERT per Application for the duration of contract**

| Qty | Component Description |
|---|---|
| 1 | Volumetric Cloud DDoS Protection Add On For Cloud Web Application Firewall (WAF) |
| 250 | Cloud Waf Applications Add On as per contract |
| 1 | Cloud Waf Enterprise 1 Application Managed Service for the duration of contract |
| 1 | Cloud Waf Enterprise Ert Premium Add On |
| 1 | Cloud Waf Enterprise Ert Premium Per Application as |
| 1 | Cloud Waf Enterprise Ert Active Attackers feed for the duration of contract |
| 1 | Bot Manager Services |
| 1 | Volumetric Cloud DDoS Protection Add On For Cloud Web Application Firewall (WAF) |
| 20 Engineers | Instructor led-training ( OEM Certification and exam vouchers) |
| 1 | Installation and commissioning of system within Transnet Environment |
| 1 | Support package also includes 24 X 7 Telephone support for the duration of contract |
| 1 | Cloud real-time monitoring for the duration of contract |

**Standards of Acceptability**

- Vendor must be ISO27001 certified.
- Application should be in the market for more than 5 years.
- POPIA or GDPR compliant
- Implementation Track Record in large organizations.



TRANSNET CONFIDENTIAL INFORMATION