



11th Floor, The Marine Building,
22 Dorothy Nyembe (Gardiner) Street, Durban, 4001
Private Bag X54322, Durban, 4000
Tel: 031 365 7800 Fax: 031 365 7858
Website: <http://www.portsregulator.org>

REQUEST FOR QUOTATION (RFQ)

SUPPLY, DELIVERY, INSTALLATION AND MAINTENANCE FOR FIREWALL HARDWARE

RFQ	RFQ2025/26/43
RFQ ISSUE DATE	07 November 2025
BRIEFING SESSION	N/A
RFQ DESCRIPTION	SUPPLY, DELIVERY, INSTALLATION AND MAINTENANCE FOR FIREWALL HARDWARE
CLOSING DATE & TIME	10 November 2025 @16H00
LOCATION FOR SUBMISSIONS	quotations@portsregulator.org

Service providers must submit their responses via e-mail at: quotations@portsregulator.org before or on the stipulated date and time. For any queries or questions, please use above mentioned email address.

Ports Regulator of South Africa requests your quotation on the services listed above. Please furnish us with all the information as requested and return your RFQ on or before the date and time stipulated above.

SUPPLIER NAME: _____

POSTAL ADDRESS: _____

MAAA NUMBER (CSD NO): _____

TELEPHONE NO: _____

FAX NO: _____

E MAIL ADDRESS: _____

CONTACT PERSON: _____

CELL NO: _____

SIGNATURE OF SERVICE PROVIDER: _____

DETAILED RFQ

SUPPLY, DELIVERY, INSTALLATION AND MAINTENANCE FOR FIREWALL HARDWARE

1. BACKGROUND

- 1.1** Ports Regulator of South Africa (“the Ports Regulator”) is a Schedule 3A public entity in terms of the Public Finance Management Act, Act No.1 of 1999, as amended (PFMA). The Port Regulator must fully comply with all the requirements of the PFMA and all other relevant and applicable legislation.
- 1.2** The Ports Regulator is an independent ports regulatory body, governed by the National Ports Act, Act No. 12 of 2005, (“the Act”).

In terms of section 30 (1) and (2) of the National Ports Act, the main functions of the Regulator are to:

- Exercise economic regulation for the ports system in line with government’s strategic objectives.
- Promote equity of access of ports and facilities and service provider by ports.
- Monitor the activities of the National Ports Authority to ensure that it performs its functions in accordance with the Act; and
- Hear appeals and complaints contemplated in terms of Sections 46 and 47 of the Act, respectively.

2. PURPOSE

Ports Regulator of South Africa requires a suitable service provider to supply, delivery, installation and maintenance for Firewall hardware.

SCOPE OF WORK

Overview

The firewall solution must provide enterprise-grade, next-generation security capabilities to protect the Ports Regulator’s network infrastructure, endpoints, and users from both internal and external cyber threats. The system must integrate intrusion prevention, web and email security, endpoint protection, and secure remote access (VPN), with centralized management and reporting.

Functional Requirements

Firewall and Intrusion Protection

Next-Generation Firewall (NGFW) with Layer 3–7 inspection.
Stateful inspection and application-aware traffic filtering.
Intrusion Prevention System (IPS) with real-time threat signature updates.
Deep packet inspection (DPI) for malware and exploit detection.
Advanced Threat Protection (ATP) and sandboxing capabilities.
Protection against DoS/DDoS attacks, port scans, and brute-force attempts.
Geo-IP blocking and IP reputation-based filtering.

VPN and Remote Access

Support for both Site-to-Site VPN and Remote Access VPN (SSL/IPSec).
Two-factor authentication (2FA) integration (via LDAP, RADIUS, or Active Directory).
Secure VPN client compatible with Windows, macOS, and mobile devices.
Always-on VPN capability for remote staff.
Bandwidth management and QoS for VPN traffic.

Endpoint and Phishing Protection

Endpoint integration for malware detection and response (EDR/XDR).
Web filtering with category-based access control (e.g., blocking malicious or phishing sites).
Anti-phishing engine that scans and blocks malicious URLs and domains.
DNS-layer protection for outbound connections.
Email security filtering to detect spoofing, phishing, and spam attempts.

Penetration Testing and Security Monitoring

Built-in vulnerability scanning and compliance reporting tools.
Integration with third-party penetration testing and SIEM systems.
Automated alerts for anomalous activities or intrusion attempts.
Logging and audit trail for all security events.
Role-based access control for administrative functions.

Machine and Network Security

Network segmentation with VLAN and micro-segmentation support.
Device profiling to identify and control access of IoT or unmanaged devices.
Integration with antivirus, patch management, and device control solutions.
Real-time monitoring and reporting dashboard.
Secure configuration and backup of firewall policies.

Performance Requirements

Minimum throughput: 5 Gbps firewall throughput (NGFW enabled).
VPN throughput: 1 Gbps or higher.
Concurrent sessions: Minimum 500,000.
SSL inspection performance: Minimum 2 Gbps.
Redundant power supply and high-availability (HA) capability.

Management and Reporting

Centralized, web-based management console.
Real-time monitoring and analytics dashboard.
Automated policy enforcement and configuration backup.
Role-based access with MFA for administrators.
Integration with syslog/SIEM (e.g., Splunk, Microsoft Sentinel).
Scheduled and on-demand reporting (traffic, threats, users, VPN usage, etc.).

Compliance and Standards

The firewall solution must comply with:
ISO/IEC 27001: Information Security Management.
NIST Cybersecurity Framework.
POPIA (Protection of Personal Information Act).
GDPR (for data protection best practices).

Recommended Features (Optional Enhancements)

Cloud sandboxing for advanced malware detection.
AI/ML-based threat intelligence updates.
Zero Trust Network Access (ZTNA) integration.
Automated endpoint quarantine and remediation workflows.
Security orchestration and automated response (SOAR) support.

Vendor and Support Requirements

Minimum 3-year hardware warranty and software subscription.
24/7 vendor technical support (with SLA).
Local partner support within South Africa.
Regular firmware and signature updates.
Compatibility with existing IT infrastructure and VLANs.

Preferred Brands / Models (Examples)

Fortinet FortiGate 200F or 400F series
Sophos XGS 4500 series
Palo Alto Networks PA-3430 or PA-3410
Cisco Firepower 2110
Check Point Quantum 26000 series

4 EVALUATION CRITERIA

4.1 SCM Administrative (Phase 1)

- 4.1.1 The SBD4 must be completed and signed by the authorised company representative.
- 4.1.2 The bidder must submit proof of registration on CSD (Central Supplier Database).
- 4.1.3 The POPIA consent form must be completed and signed by the authorised company representative.
- 4.1.4 The SBD 6.1 must be completed and signed by the authorised company representative.

4.2 Mandatory Requirement (Phase 2)

- 4.2.1 The service provider must submit a certificate / accreditation to render this service
- 4.2.2 Submit written confirmation of the hardware warranty and must provide maintenance for a period of three (3) years.

4.3 Pricing Considerations and Specific Goals (Phase 3)

- 4.3.1 Bidders' price quotations must be inclusive of all applicable taxes (**including VAT**)
- 4.3.2 Service providers are required to detail their rates / itemized pricing schedule.
- 4.3.3 Bidders total price proposal weighs 80 points.

4.4 BBBEE

- 4.4.1 The bidder must submit SBD 6.1 preference points claim form.
- 4.4.2 The bidder must submit a BBBEE certificate/ Sworn affidavit.
- 4.4.3 Specific goal: BBBEE Level 1 Companies as per SBD 6.1. Weighs 20 Points

NB: Tax status for the recommended bidder will be verified on Central Supplier Database (CSD) or SARS E-Filing prior to awarding. If the bidders' tax matters are non-compliant the Regulator will apply clause 4.2 of the National Treasury Instruction No. 09 of 2017/2018, if the bidder is still not compliant then the Regulator will exercise clause 4.3 of the said instruction note.

5. CONDITIONS TO BE OBSERVED

No RFQ shall be deemed to have been accepted unless and until a formal contract / letter of award / order form is prepared and executed. Quotation shall remain open for acceptance by the Ports Regulator for a period of ninety (90) days from the closing date of the RFQ Enquiry.

6. COMMUNICATION

All enquiries relating to this RFQ should be sent via email quotations@portsregulator.org

7. COST OF PROVIDING WITH RFQ

The service provider shall bear all costs and expenses associated with preparation and submission of its RFQ, and the Ports Regulator of South Africa shall under no circumstances be responsible or liable for any such costs, regardless of, without limitation, the conduct or outcome of the bidding, evaluation, and selection process.

END OF RFQ DOCUMENT

Annexed to this document for completion and return with the document:

- Quotation on a letterhead
- Declaration of Interest (SBD 4)
- Copy of CSD Report or MAAA Number (National Treasury)
- B-BBEE Certificate
- Preference points claim form SBD 6.1
- POPIA consent form
- Certificate / accreditation to render this service
- written confirmation of the hardware warranty and must provide maintenance for a period of three (3) years.

