



REQUEST FOR PROPOSAL NUMBER: AF/NTW/RFP26O1O/2026

Date: October 08, 2026

RFP Deadline: November 03, 2026

REQUEST FOR PROPOSAL

NAME: RFP for Centralized Firewall Solution

CONFIDENTIALITY

No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of ATOMA. This document, its associated appendices and any attachments remain the property of ATOMA and shall be returned upon request

Background ATOMA:

A telecommunication company incorporated and existing under the Laws of Islamic Emirate of Afghanistan and having its office at Park Plaza opposed of Shar-e Naw Park Kabul Afghanistan PO Box # 100208-07-O54, Kabul. ATOMA is a leading telecom company in Afghanistan, having the highest customer base and operates a large network of sites across Afghanistan. ATOMA played a significant role in the development and expansion of telecommunications services in Afghanistan, particularly in the areas of mobile voice and data services. Offering a wide range of mobile communication services, including voice calls, SMS, mobile internet, and value-added services. We introduced various innovative products and packages tailored to the needs of Afghan consumers. Also serves the business sector, offering solutions such as mobile banking, enterprise connectivity, and other services to support businesses' communication needs.

TENDERER'S ACKNOWLEDGEMENT / PRELIMINARY NON-DISCLOSURE AGREEMENT.

Tender's Acknowledgment: Please mark as appropriate:

We acknowledge receipt and acceptance of the RFP and intend to submit a tender as required ☐

We acknowledge receipt of the RFP but decline to tender for the following reasons: ☐

Please write your reason here:

- We undertake to return to ATOMA within the below-mentioned deadline from receipt of the complete RFP package with all attachments, information and documents related thereto as provided by ATOMA and any copies made thereof.
- The complete tender documents along with the Proposal to be submitted in a SEALED envelope addressed to the Supply Chain Department of ATOMA and to be physically submitted in the tender box located in ATOMA Head Office, Reception, located in Shar-E-Naw Kabul not later than Date November 03, 2026
- Bidders are requested to do the registration at ATOMA at the time of obtaining the RFP from ATOMA reception.
- Bidders should ensure that they provide accurate email addresses and contact numbers at the time of registration.
- Bids are invited from reputable companies for **"Request for Proposal for Centralized Firewall Solution"** according to ATOMA requirements and Technical Specifications as per RFP.
- Bid received after the mentioned deadline shall not be accepted.
- ATOMA reserves the right to accept or reject any or all bids and to annul the bidding at any time, without thereby incurring any liability to the affected supplier(s) or any obligations to inform the affected supplier(s) on the grounds of ATOMA's action.

12: Preliminary Non-Disclosure Agreement:

We agree that all information and documents contained in or related to this RFP as provided by ATOMA is proprietary information and shall be treated as confidential. We undertake that all such information and documents, as described above, shall not be divulged to any other party (such prohibition applies to any further release of information regarding this RFP by ATOMA) without the prior written permission from ATOMA to do so. We agree that this RFP and all information and documents relating to it and provided hereunder by ATOMA are not to be used for any purpose other than for the preparation of our tender submission. This undertaking will also apply to any subsequent contract resulting from this RFP.

Name: _____

Designation: _____

Signed / Date / Stamped: _____

Project Introduction

The goal of the project is to implement a centralized Firewall solution on to of the network. The purpose is to combat deficiencies and vulnerabilities in Voice, SS7/Diameter, SMS and Roaming protocols and to protect the ATOMA network and subscribers from the fraudulent cases mentioned in the scope of work.

Protection means monitoring, detection and blocking of fraudulent traffic based on criteria defined together with the ATOMA.

This document represents a high-level requirement; detailed discussion and clarifications will be provided after the supplier's alignment on this high-level scope.

All details have to be agreed upon prior to any work in order to avoid delays & last-minute blocking issues.

Scope of Work:

The proposal should comply with the requirements below and include the listed specifications, features and documents.

- 1 On-net, off-net and international Voice, SS7/Diameter, SMS (A2P, P2P, P2A) & Roaming traffic analysis for anomalies, helping to identify fraudulent traffic, apply filtration and real-time or near-real-time blocking, including:
 - 1.1 International to international & International to local CLI manipulation / Number masking.
 - 1.2 OTP through flash call.
 - 1.3 SMS bypass:
 - 1.3.1 UDT/XUDT based bypass
 - 1.3.2 Unauthorized GT
 - 1.3.3 unauthorized signaling route
 - 1.3.4 Spam/Spoofing GT
 - 1.3.5 Spoofed SCCP addresses
 - 1.3.6 International SMS bypass
 - 1.3.7 Grey routes
 - 1.3.8 SMS sent through unauthorized signaling partners
 - 1.3.9 Unauthorized direct MAP access to the SMSC
 - 1.3.10 SMS routing manipulation
 - 1.4 OTT bypass, detection of SMS traffic bypassing approved SMSC/interconnect routes through unauthorized SS7 signaling paths.
 - 1.5 Artificially Generated Traffic (AGT) / Robocalls and spam traffic.
 - 1.6 IRSF and WANGIRI.
 - 1.7 SIM-box related traffic.
 - 1.8 Abnormal and anomalous traffic patterns.
- 2 SMS spam / bulk SMS detection
 - 2.1 High-volume SMS from one source
 - 2.2 Same OA → multiple DAs
 - 2.3 Multiple Oas → same DA
 - 2.4 Short-time SMS bursts
 - 2.5 Repeated failed deliveries
 - 2.6 Abnormal destination distribution
 - 2.7 Abnormal originating-number patterns
 - 2.8 Sudden change in normal traffic profile

-
- 3 Inspects protocols (e.g., SS7, SIP/RTP (VoIP), MAP, CAP, Diameter, SMPP, HTTP, SMTP, TCP and more) to detect and block malicious activity and fraudulent traffic, including automatic alert-to-block capability.
 - 4 Support for ANSI and ITU-T variants, national variants and network-specific profiles.
 - 5 Signalling-link and signalling-association protection.
 - 6 Message normalization, malformed-message rejection and protocol-conformance checks.
 - 7 Protection against unauthorized or unexpected signalling routes and point codes.
 - 8 Protects against unauthorized port usage, preventing toll fraud and other malicious activities.
 - 9 Blacklist/Whitelist management to block or allow specific traffic and allow/deny by:
 - 9.1 Originating and destination point codes.
 - 9.2 Global titles and global-title ranges.
 - 9.3 SCCP calling/called party addresses.
 - 9.4 Network, operator, country and roaming partner.
 - 9.5 Message type, service and transaction context.
 - 10 Partner and route-specific security policies.
 - 11 Trusted/untrusted peer classification.
 - 12 Validation of originating network and signalling relationship.
 - 13 Controls for international, domestic, roaming and interconnect traffic.
 - 14 Validate message structure, mandatory fields, parameter lengths and encoding.
 - 15 Validate operation codes against peer permissions and service profiles.
 - 16 Enforce valid source/destination combinations and routing rules.
 - 17 Intercept / man-in-the-middle attacks to eavesdrop on voice calls and SMS. Route calls via attacker infrastructure. Denial of Service / prevent victim from using network service (Voice / Data / SMS).
 - 18 Denial of Service / prevent victim from using network service (Voice / Data / SMS).
 - 18.1 SMSC Flooding and Overload Protection: The solution shall provide dedicated protection against SMSC flooding, signaling overload and SMS resource-exhaustion attacks, including:
 - 18.1.1 MT-ForwardSM flooding.
 - 18.1.2 MO-ForwardSM flooding.
 - 18.1.3 SendRoutingInfoForSM flooding.
 - 18.1.4 ReportSM-DeliveryStatus flooding.
 - 18.1.5 TCAP transaction flooding.
 - 18.1.6 SCCP signaling flooding.
 - 18.1.7 SMS submission bursts and repeated SMS delivery attempts.
 - 18.1.8 Slow-rate / low-volume attacks intended to exhaust SMSC or signaling resources.
 - 18.2 SMS Rate-Limiting and Traffic Control: The solution shall support configurable SMS traffic rate limiting and overload controls based on:

-
- 18.2.1 Global SMS TPS thresholds.
 - 18.2.2 Per GT rate limiting.
 - 18.2.3 Per point-code rate limiting.
 - 18.2.4 Per-partner/interconnect rate limiting.
 - 18.2.5 Per-MAP-operation rate limiting.
 - 18.2.6 Per-subscriber/MSISDN or IMSI-range rate limiting.
 - 18.2.7 Configurable burst thresholds.
 - 18.2.8 Automatic alerting, throttling and blocking when configured thresholds are exceeded.
 - 18.2.9 Automatic update of malicious GTs, point codes, IPs and attack indicators and blocking of emerging global attacks.
 - 18.2.10 Separate thresholds and policies for legitimate high-volume A2P traffic and P2P/P2A traffic, where applicable.
- 19 SMSC-originated vs network-originated traffic: The solution should distinguish between:
 - 19.1 SMS generated by the SMSC
 - 19.2 SMS received by the SMSC SMS originated from legitimate network elements
 - 19.3 SMS originated from roaming partners
 - 19.4 International SMS traffic
 - 19.5 Domestic interconnect traffic
 - 19.6 A2P SMS traffic
 - 19.7 P2P SMS traffic
 - 19.8 P2A traffic.
 - 20 Policies to cover sensitive operations and prevention of attack vectors, including:
 - 20.1 SendRoutingInfo, ProvideSubscriberInfo, ProvideRoamingNumber, SendIdentification, CheckIMEI, UpdateLocation, CancelLocation, PurgeMS, SendRoutingInfoForSM, ForwardShortMessage, ReportSM-DeliveryStatus, AnyTimeInterrogation, RegisterSS, InsertSubscriberData, InitialDetectionPoint, SendIMSI, MTForwardSM.
 - 21 Restricting operations by peer, direction, subscriber range and roaming status.
 - 22 Detecting repeated, bulk or geographically anomalous queries.
 - 23 Detect SMS (A2P, P2P and P2A) interception, redirection or routing manipulation attempts.
 - 24 Detect call-forwarding and supplementary-service abuse.
 - 25 Detect abnormal roaming, registration and subscriber-profile activity. Roaming Risk Scoring, Dynamic reputation score for roaming partners and peer networks, identify compromised or high-risk partners.
 - 26 Detect signalling storms, floods and resource-exhaustion attempts.
 - 27 Detect suspicious message bursts, low-and-slow activity and coordinated campaigns.
 - 28 Detection of blocked legitimate traffic.
 - 29 Performance alarms and degradation reporting.
 - 30 **Correlate activity across point codes, global titles, partners and time windows.**

-
- 30.1 The firewall shall support stateful SMS transaction correlation across SCCP, TCAP and MAP layers to identify abnormal, incomplete or unexpected SMS transactions.
 - 30.2 The solution shall support correlation of SMS transaction sequences, including:
SendRoutingInfoForSM → MT-ForwardSM → ReportSM-DeliveryStatus.
 - 30.3 The solution shall identify where applicable:
 - 30.3.1 MT-ForwardSM without a preceding legitimate SendRoutingInfoForSM.
 - 30.3.2 Excessive SendRoutingInfoForSM requests without corresponding MT-ForwardSM activity.
 - 30.3.3 Excessive MT-ForwardSM transactions without expected transaction behaviour.
 - 30.3.4 Repeated SendRoutingInfoForSM requests for the same subscriber.
 - 30.3.5 Repeated SMS delivery attempts.
 - 30.3.6 Abnormally long SMS transaction duration/timeouts.
 - 30.3.7 Unexpected or invalid MAP operation sequences.
 - 30.3.8 Incomplete or abandoned TCAP/MAP transactions.
 - 31 Support operator-defined fraud rules and threat indicators.
 - 32 SMS subscriber/MSISDN-based controls: The ability to define policies based on:
 - 32.1 MSISDN
 - 32.2 IMSI
 - 32.3 MSISDN ranges
 - 32.4 IMSI ranges
 - 32.5 MCC/MNC
 - 32.6 Roaming status
 - 32.7 Subscriber location where available
 - 32.8 Home/visited network.
 - 33 Filtering and enforcement actions:
 - 33.1 Drop or reject messages.
 - 33.2 Allow, monitor, or rate-limit messages.
 - 33.3 Redirect or quarantine traffic where supported.
 - 33.4 Return protocol-appropriate error responses where it's safe.
 - 33.5 Apply selective controls by peer, service, subscriber range, or operation.
 - 33.6 Use gradual enforcement, alert, monitor, throttle, then block.
 - 33.7 Support emergency bypass.
 - 33.8 Prevent policy actions from disrupting legitimate emergency or critical services.
 - 34 Support custom rules, signatures and behavioural policies.
 - 35 Provide policy simulation or shadow mode before enforcement.
 - 36 Integration with AI and machine learning algorithms for improved detection. Support Northbound APIs capability.
 - 37 Advanced analytics for identifying and mitigating new threats.
 - 38 A comprehensive Firewall that counters all threats & provide full visibility and control over all signalling and support GSMA identified and suggested countermeasures:

- 38.1 FS.O7, IR.82, FS.11, IR.88, FS.19, IR.70, IR.71.
- 39 Provide solution design, architecture and connectivity requirements.
- 40 Provide Interfaces/Signalling/Protocol and Integrations document.
- 41 Provide security at the network, application and database levels.
- 42 Solution needs to be using robust and proven software and hardware technologies.
- 43 Solution architecture should be built on sound architectural principles enabling fault- tolerance, high-performance, high availability and scalability both on the software and hardware levels, including:
- 43.1 Protection against signalling overload and resource exhaustion.
- 43.2 Traffic shaping, queue management and overload controls.
- 43.3 Health checks, alarms and automated recovery.
- 43.4 Capacity monitoring and horizontal or chassis-based scaling.
- 43.5 Redundant network interfaces, links, power and management paths.
- 44 Interoperability and standards:
- 44.1 Interworking with STPs, signalling gateways, roaming hubs, SMS hubs and SMSCs/GMSCs.
- 44.2 Compatibility with multi-vendor SS7 networks and national variants.
- 44.3 Support for operator-defined numbering, point-code and global-title plans.
- 44.4 Standards-based protocol handling and configurable conformance profiles.
- 44.5 Interworking with SS7 (MAP/CAP), Diameter, SIP/RTP, 2G, 3G, 4G, VoLTE and 5G.
- 44.6 Support for mixed SS7, SIGTRAN.
- 45 System design should be highly adaptable and should be modified if required.
- 46 Backup, log capabilities and Integration with Splunk, QRadar, ArcSight, Elastic and Syslog.
- 47 Support for design, development, implementation, integration, adaptation, activation, migrations.
- 48 Responsibility Matrix, SLA, escalation matrix and issue resolution timelines etc.
- 49 Operation support L1, L2, L3.
- 50 Real-time dashboards for reporting and monitoring traffic volume, message types, peers, alerts, AI and non-AI anomalies. Including, Reports for roaming partners, interconnects and internal services. User-defined dashboards and report generation capability.
- 51 Abide to ATOMA security policy.
- 52 Grant system access to ATOMA team.
- 53 Total cost breakdown (Hardware, software, licenses, Support, any annual fee etc).
- 54 Implementation timeline.
- 55 Provide training to ATOMA team.

PROPOSAL REQUIRED DOCUMENTS

The following documents are required to be submitted along with Sealed Proposal to be submitted in Tender Box Located in reception of ATOMA-Head Office.

- **Technical Proposal** Detailed technical approach and demonstrating compliance with the RFP requirements.

- **Commercial Proposal** Detailed financial proposal and breakdown, which cover all associated costs to this project.
- **Company Profile** (Company Background, Staff Availability, Office location, Tangible Assets)
- **Valid License from Government of Afghanistan** (Relevant License duration should be not less than three years), Business license and the TTSP Grade B required license)
(In case any supplier doesn't provide the TTSP license during the initial proposal submission, this will not impact their eligibility but, they will obtain the TTSP Grade B license prior to the contract award).
- **International Supplier Licensing Compliance:** The International Supplier shall comply with all applicable Afghan laws and regulatory requirements. Where the nature of the Services requires a local license, permit, registration, or authorization, the Supplier shall obtain the required authorization or, where permitted, engage an appropriately licensed local partner, subject to ATOMA's prior approval. All related compliance requirements and costs shall be the Supplier's responsibility.
The applicants or local partner require TTSP Grade B license. (In case any supplier doesn't provide the TTSP license during the initial proposal submission, this will not impact their eligibility but, they will obtain the TTSP Grade B license prior to the contract award).
-
- **At least 3 references** of reputable and well-known organizations along with their names and contact numbers where the company has provided or providing the same services to.
- **Experience in relevant field** minimum 3 years and (Relevant Experience, Client References, Projects Values and Turners)
- **Financial Stability** (Bank Statement for last Six Months, (All bank accounts should be in the name of the company stamped by Authorized Bank.)
- **Audited Financial Statement:** Latest audited financial statement
- **Team Composition** Details of the proposed team, including key personnel, qualifications, roles, responsibilities, and relevant experience.

Evaluation Criteria:

- Technical capabilities and experience
- Project implementation methodology
- Price and commercial terms for entire project implementation
- Financial stability and references
- Compliance with Documentation Requirements (Pass/Fail)

The Evaluation Committee shall assign the percentage weight for each evaluation criterion prior to the opening and evaluation of proposals. The weighting shall reflect the importance of each criterion in achieving the objectives of this procurement and shall remain unchanged throughout the evaluation process.

Only proposals that satisfy the mandatory compliance requirements shall be considered for detailed technical and commercial evaluation.

Submission Instructions:

- All proposals must be submitted electronically to:
Temp_ismail.safil@atoma.com.af, sadeequllah@atoma.com.af
- All commercial proposal which are submitted electronically must be **password protected**. Unprotected proposal will not be considered for further evaluation.
- The sealed envelope should be submitted at:
ATOMA Head Office, Reception Shar-E Naw Kabul, Afghanistan.
- The sealed envelope must be placed in ATOMA tender box, located in ATOMA main office reception.
- All questions regarding this RFP must be submitted in writing.
- Responses will be provided to all potential bidders.
- Bids must remain valid for 120 days from the submission deadline.
- The bid must be submitted in English.
- ATOMA reserves the right to reject any or all proposals.

General Requirements and Compliance

- The supplier must have and always maintain and all the time, at its own cost and expense, all permits, licenses, authorization, and approval from relevant government entities necessary for the service provided under this RFP/Agreement.
- The top three suppliers shall present slide presentations to the cross-functional team comprised of technical IT and Network, Carrier and Roaming, legal and compliance and procurement).

Queries and Submissions:

All queries related to this document should be addressed to:

Procurement department of ATOMA

Email: Temp_ismail.safil@atoma.com.af, sadeequllah@atoma.com.af.

Phone# 0772227050, 0772222021