المحلق (أ) : المواصفات الفنية والشروط الخاص بالعطاء رقم م ش 5/65/2022 (شراء حلول من التهديدات السيبرانية (WAF+NGFW)

|  |  |
| --- | --- |
| Document Type | Request for Proposal |
| Project / Initiative | **حلول حماية من التهديدات السيبرانية (WAF+NGFW)** |
| Issued by | Military Credit Fund |

|  |  |
| --- | --- |
| وثيقة دعوة عطاء | نوع الوثيقة  |
| **حلول حماية من التهديدات السيبرانية (WAF+NGFW)** | اسم المشروع |

Table of Contents

[**1.** **About Military Credit Fund (‘MCF’).** 3](#_Toc62065453)

[**2.** **Introduction & Background** 4](#_Toc62065454)

[**3.** **Submission Guidelines & General Terms/Conditions.** 5](#_Toc62065457)

[**4.** **Technical & Functional Requirements** 7](#_Toc62065480)

[4.1. Part One:Web Application Firewall (WAF) 7](#_Toc62065481)

[4.2. Part Two: Next Generation Firewall 10](#_Toc62065495)

# **About Military Credit Fund (‘MCF’).**

The Military Credit Fund was established in 2010 under the directives of His Majesty King Abdullah II, Chief Commander of the Jordanian Armed Forces, under paragraph (f) of Articles 17 and 20 of the Jordanian Armed Forces Law no 3 of 2007.

MCF is regulated by a special by-law issued by the Jordanian Government under No. 60 of the Year 2010. This by-law stipulates in article 3 that “A fund to be called the ‘Military Credit Fund’ shall be established in the Armed Forces, with legal persona, and financial and administrative independence, and as such may own transferrable and non-transferable funds, as well as to conduct all legal transactions necessary to achieve its goals. It shall be headquartered in Amman”.

This MCF initiative was established to serve Jordanians affiliated with the Jordanian Armed Forces and security agencies.

The Fund is a testament to the firm belief held by His Majesty that these public servants are entitled to financial security and dignified livelihood.

 For more information and browsing the full legislation, visit the Legislation and Opinion Bureau at <http://www.lob.jo/>

 Direct Link to the Bylaw:

<http://www.lob.gov.jo/?v=1.6&url=ar/LegislationDetails?LegislationID:6515,LegislationType:3,isMod:false>

**MCF Vision**

 We strive to be the leading provider of banking services and financial products, based on the Islamic Banking principles that fulfill all the needs of members of the Jordanian Armed Forces and Security Agencies. Contributing to actual and sustainable improvements in their financial standings.

**MCF Mission**

 To offer comprehensive and specialized financial services, ensuring modern and innovative banking operations, to all members of the Jordanian Armed Forces and Security Agencies, allowing them to safely and securely realize their financial objectives. We are committed to the continued development of our products and services, and the ideal employment of our resources.

**MCF Objectives**

 The Fund aims to anchor a not-for-profit organization, with a goal to encourage the Armed Forces and Security Agencies personnel to save money and help them to achieve their diverse financial goals and meet their living needs and future hopes, by providing them with financial solutions at relaxed terms. In addition to offering different types of banking services and finances, the fund seeks to educate its customers on the available investment opportunities and help them to take deliberate decisions regarding their options and practical aspirations, therefore, the mutual benefit between the fund and beneficiaries is taking precedence over the Fund priorities.

In order to achieve it’s intended mission, MCF is authorized to:

1. Offer financing products and services based on Islamic Banking principles.
2. Extend financings products and services to the martyr’s families
3. Accept of restricted deposits according to the fund’s bylaws
4. Invest own and depositors’ funds in various investment venues
5. Offer salary transfer services
6. Offer payment and collection services
7. Issue debit and credit cards
8. Offer Financial Lease products according to the Financial Lease law.

# **Introduction**

MCF invites qualified bidders to submit a proposal to provide, install, deploy, configure, and maintain a (As per the requirements defined within this Request for Proposal “RFP” or “Document”):

1. Web Application Firewall.
2. Next Generation Firewall.

The proposed solutions will have to adhere to a set of technical and functional rules and requirements, detailed in the **Technical & Functional Requirements** of this Request for Proposal hereunder.

1.
2.

# **Submission Guidelines & General Terms/Conditions.**

The following submission guidelines & requirements apply to this Request for Proposal (‘RFP’):

1. Only qualified bidders with prior experience on projects such as this should submit proposals in response to this RFP.
2. Bidders must list at least two projects that are similar to this project as part of their response, including references for each.
3. A technical proposal must be provided. This technical proposal must provide an overview of the proposed solution.
4. A financial proposal must be provided. This price proposal should indicate the overall fixed price for the project as well as the running, recurring, and/or exceptional costs.
5. Proposals must be signed by a representative that is authorized to commit bidder’s company.
6. If you have a standard set of terms and conditions, please submit them with your proposal. All terms and conditions will be subject to negotiation.
7. Proposals must remain valid for a minimum period of 90 days.
8. Bidders wishing to respond to this tender should note that they do so at their own cost.
9. MCF has the right to source the components of the solution from one or multiple bidders to achieve MCF desired target results as best fit MCF needs at MCF sole discretion.

**Bidders Responses Structure:**

Bidders are advised to adhere to the following response structure and rules.

1. Responses should be separated into two sets; **Set-A**: The Technical Proposal and **Set-B**: The Financial Proposal. Both of which are clearly marked in sealed envelopes.
2. Each envelope should also carry the bidder's name, contact person details.
3. All Tender and supplement documents should be page numbered.
4. Prices must be quoted in terms of Jordanian Dinar without sales tax, and must be itemized.
5. MCF purchases are exempt from all customs duties, sales taxes, and any other fees or governmental returns.
6. The bidder is committed to provide datasheets for the proposed solutions.
7. The bidder must provide proof of its ability to perform after-sales maintenance and provide MCF with the qualifications of the technical staff to maintain the system and their experience in implementing such projects.
8. Bidders seeking clarifications, or more information might do so in writing. All such requests to be sent by email, MCF will timely respond to the clarifications, however, lack of response does not qualify the bidder for more time in responding to the bid.
9. The Bidder shall provide a single point of support for the solution provided. All deployed system configurations shall be fully supported to accelerate problem resolution. This service support shall be 24 hours a day, 365 days a year.
10. The Bidder should provide compliance sheets for all RFP Requirements **(marked on submitted datasheets)**.
11. Installation, implementation, and configuration for (hardware and Software) in the MCF designated location(s) and according to MCF requirements & design.
12. Warranty and Support for 3 years.
13. The latest software images should be installed by the delivery date and any future software update should be installed during the warranty period without any additional cost.
14. The bidder must handle all Project Management tasks and provide a detailed project plan that shall address clearly the following main subjects: - Tasks, duration, milestones, dependencies, recourses, design, delivery, installation of items, transition, implementation, as-built document, and testing procedure.
15. Installation & Support should be carried out by certified Engineers.
16. Hands-on and (OJT) On Job Training on the new system by Qualified & Certified Engineers.
17. The Bidder should be at a high level of Partnership status (proven by a current certificate from the main vendors).
18. The bidders are committed to providing MCF with spare parts for a period of ten years in return for the price according to the prevailing market rates at the time.
19. The Bidders shall warrant that the supplies are new, unused, of the most recent models and incorporate all recent improvements in design and materials. The bidders shall further warrant that none of the supplies have any defect arising from design, materials, or workmanship. This warranty or license activation starts from the date of provisional acceptance and shall remain valid for 3 Years for part one, two and three, and one year for part four.
20. All the needed proofing documents should be attached to the technical proposal.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.

# **Technical & Functional Requirements**

## **Part One: Web Application Firewall (WAF).**

|  |
| --- |
| 1. General:
* The WAF will be used to secure and protect public facing applications like EMAIL, mobile App service.
* Capability to support load-balancing, compression.
* The solution must be hardware appliance-based and must be in HA (Active – Active).
* The solution should support Reverse Proxy deployment mode.
 |
| 1. . Performance Requirements:
* The WAF should support 10Gbps L4/L7 throughput.
* Interfaces: 4x GE RJ45 4x 10GE SFP
* The form factor is Rack mounted and all accessories needed to install in the cabinet must be provided.
* All Required cables and transceivers should be provided.
 |
| 1. The solutions should support REST full API management.
 |
| 1. The solution must support positive security model that states what are the expected inputs and behavior that is allowed and everything else that deviates from the positive security model is alerted and/or blocked.
 |
| 1. The solution must support negative security model that model states explicitly defined known attack signatures
 |
| 1. The solution should be capable and configured to protect against the following:
* Invalidated Input.
* Injection Flows
* SQL Injection
* OS Injection
* Parameter tampering
* Cookie Security and Poisoning
* Hidden Field Manipulation.
* Cross site scripting flaws
* Buffer overflows
* Broken access control
* Broken authentication and session management
* Brute force attack
 |
| 1. The solution must identify and mitigate the OWASP web application security vulnerabilities.
 |
| 1. The solution should support LDAP, Radius and Kerberos authentication.
 |
| 1. The solution must offer API protocol security that can deploys tools to secure REST/JSON, XML, and GWT APIs.
 |
| 1. The solution must protect both HTTP Web applications and SSL (HTTPS) Web applications.
 |
| 1. Solution should provide XML filtering and validation.
 |
| 1. Anti-DoS Capabilities
	* + The solution should be able to detect, prevent and log layer 7 (application layer) attacks with lowest false-positive rates to secure MCF services.
		+ The solution should include DDOS protection on the application level.
		+ The solution shall be able to detect of anomalous traffic patterns that stem from a specific unique geo-location.
		+ Server-side stress-based detection and protection
		+ The solution shall be able to monitor latency of Layer 7 (application layer) traffic to detect the spikes and anomalies in the typical traffic pattern to detect, report on, and prevent layer 7 DOS attacks
		+ The solution shall utilize different techniques to generate confusing responses to attacker request.
 |
| 1. Bot and Bad-IP detection & protection Capabilities
	* + The Solution should be capable of detecting and distinguishing two sets of Bots from the Internet
		+ The solutions should have a historical view on Botnets and search engines
		+ The solution should have a view of all blocked IP addresses and the blocked time period.
		+ The solution should have integration search engines, Bad robots (scanners, crawlers, spiders), Solution should have a dashboard to show event statistics from the robot-based and normal clients,
		+ The Solution should protect against low reputation sourced from Botnets, Anonymous proxy, Scanners, Spammers, Tor networks, Phishing hosts.
		+ Mitigating Bots via CAPTCHA, it will only be sent to intruders and not to legitimate users.
 |
| 1. The Solution should be able to track, correlate and report traffic per IP-address, User, Device
 |
| 1. The solution should capable of Full/Partial Masking of sensitive information or credit card numbers in logs or payloads. For example, exposing only the last 4 digits of a credit card number.
 |
| 1. Solution must provide Anti-Bot Mobile SDK Protection to protect mobile apps via an allow list, behavioral analysis, secure cookie validation, and advanced app hardening.
 |
| 1. Protocol Load balancing
	* + The following load balancing Mechanisms should be supported

Round Robin, Weighted Round Robin, Source IP. |
| 1. Monitoring and Reporting
	* + The solution should have a dashboard showing real time Traffic Throughput, Connection, Attack and Request information
		+ The solution should have a dashboard showing web service and back-end server status.
 |
| 1. Logging and Reporting
	* + The solution should be capable to store event (audit) information, locally store alert information, be able to locally store traffic information, or send all these log types above to a centralized logging system supplied by the vendor.
		+ The solution should be able to send all log types above to an external syslog server.
		+ The WAF shall have ability to customize logging for reporting
 |
| 1. The warranty should be 3 years of 24x7 Hardware and Software support.
 |
| 1. Training.

Certified professional training on how to deploy, tune, and operate Web Application Firewall from an authorized training center for two (2) persons must be provided. |

## **Part Two: Next Generation Firewall**

|  |  |
| --- | --- |
| **Item** | **Description** |
| Appliance Brand | Country of origin: America's /Europe. |
| Global Recognition | The vender should be listed in the latest LEADERS Magic Quadrant for Next Generation Firewall.  |
| Subscriptions | Full license include (IPS, Threat Prevention, URL Filtering,….) |
| Minimum Throughput | Combined inspection throughput must be capable of maintaining a minimumof **5 Gbps** NGFW throughput with all features configured. |
| Interfaces (Minimum) | 4x 10 GE SFP+ / SFP.12x GE RJ45 Ports.1x Console1x HA Port1x Management. |
| Local storage | 480GB |
| Power Supply | Redundant Power supply. |
| Form Factor  | Rack mounted with and all accessories needed to install in the cabinet. |
| Cables | All Required cables and transceivers should be provided. |
| Warranty & Support | 3 years of 24x7 Hardware and Software support. |
| Training | Certified professional training on how to deploy, configure, and troubleshoot NGFW from an authorized training center for two (2) persons must be provided. |