

## إعلان صادر عن وزارة العمل

تعلن وزارة العمل/ لجنة الشراء الرئيسية عن طرح العطاء التالي :-

الرقم المتسلسل	رقم العطاء	اللوازم المطلوبة	كفالة دخول العطاء	ثمن النسخة غير مستردة	آخر موعد لبيع دعوة العطاء الساعة 2:30 من تاريخ	آخر موعد لايداع العروض الساعة 12:00 من تاريخ
1	2023/15	Firewall	3% من قيمة العرض المقدم	50 دينار	2023/8/31	2023/9/3

على الراغبين بالمشاركة بدخول العطاء وشراء نسخة العطاء مراجعة وزارة العمل- الدوار السابع بجانب كوزمو خلال ساعات الدوام الرسمي مصطحبين معهم رخصة مهن سارية المفعول ، واحضار وصل شراء دعوة العطاء إلى مبنى الوزارة (2) - شارع عبدالله غوشة لإستلام النسخة.

ملاحظة: \* أجور نشر الإعلان على من يرسو عليه العطاء .

\* يحق للوزارة إلغاء العطاء دون إبداء الأسباب

\* يمكن الإطلاع على الإعلان والمواصفات الفنية على موقع الوزارة الإلكتروني [www.mol.gov.jo](http://www.mol.gov.jo)

# **Request for Proposal (RFP)**

## **Next Generation Firewall (NGFW)**

Ministry of Labor

AUG 2023

## 1. Introduction

Ministry Of Labor (MOL) is seeking proposals from qualified bidders for the supply, configuration and final commissioning of Next Generation Firewall (NGFW)

MOL is issuing this RFP for selecting a qualified bidder to supply, configuring, testing the NGFW, documenting the final configuration, placing the solution into production, and providing ongoing training and technical support.

The selection of the firm will be based on factors such as: qualifications and experience of performing the aforementioned tasks and proposed price.

## 2. General Terms and Conditions

- 2.1 The bidder's sole responsibility and on his own expenses to understand the environment and all requirements that are related to the tender or that may influence its pricing.
- 2.2 Bidders are expected to prepare and examine all instructions, terms, specifications, and other information in the bidding documents. Failure to furnish all information required by the bidding documents or to submit a bid not substantially responsive to the bidding documents in every respect will be at the bidder's risk and may result in the rejection of its bid.
- 2.3 The bidder should supply all necessary licenses to allow MOL to have it full features and without any additional cost.
- 2.4 The bidder should compare and evaluate MOL specification and current configuration to confirm that are comply with MOL environment and the new configuration will be comply with our existing systems and in case any missing requirement (not mentioned in RFP) or will not work with our existing environment, new requirement supplying, installing and configuring (after taking approval of MOL) will be the bidder responsibility and without any additional cost.
- 2.5 The bidder should mention clearly any annual licenses renewal needed and the cost of the annual fees. When needed, MOL will use these costs to purchase additional licenses during the warranty period.
- 2.6 MOL reserves the right to contact the technology vendor to acquire information and details concerning offered items by the bidder.
- 2.7 MOL will only accept to sign original software licenses with the technology vendors (each relevant original software package with its technology vendor). All relevant software should be signed to MOL

- 2.8 The bidder should propose a complete solution that will meet all requirements indicated in this RFP document.

### 3. Validity Period

- 3.1 Proposal shall remain valid, at a minimum, for the period of 90 days

### 4. Bidder Qualifications

The bidder shall be required to furnish information sufficient to enable MOL to assess their capability for performing the complete configuration and commissioning. The information that all bidders are requested to have the minimum capabilities:

- 4.1 The bidder must be well established and have efficient and reliable resources for providing the required services and providing support that caters for required services.
- 4.2 The bidder is responsible to handover the new setup to MOL staff and handover the setup documentations.
- 4.3 The bidder must have a partner certificate from technology vendor on the proposed NGFW solution. The partnership must be active during the period of the proposal validity period.
- 4.4 The bidder is responsible for performing all scope as detailed in Scope and Deliverables section.
- 4.5 The personnel once assigned should not be removed / replaced except when they resign or for other force majeure reasons. If such a case occurs then the Bidder is required to replace personnel with another of the same caliber, qualification, and experience subject to MOL's approval.
- 4.6 An official letter from the technology vendor of the proposed solution indicating that the local bidder is authorized to perform the services assigned to it by the technology vendor along with any certification.
- 4.7 Bidder can hire a subcontractor to carry together the capabilities, but the Bidder will be the sole responsible for all deliverables in front of MOL

### 5. Scope Of WORK

- 5.1 MOL is soliciting proposals from Bidders qualified to provide a bid to implement a scalable NGFW Solution for the Datacenter enabling MOL to have efficient Security

solution with enhanced capabilities. The Solution shall be implemented at MOL headquarter.

- 5.2 Bidders shall state other related services that can be provided, such as service agreements, warranties, training, etc. that offers the most attractive and beneficial proposal that will enable MOL to offer the best services to its employees.
- 5.3 Bidder shall be responsible for the complete scope of work related to the This Project and to allocate all the necessary recourses to implement/integrate the proposed NGFW solution with existing MOL infrastructure HW & application.
- 5.4 Bidder MUST comply with HW & SW solution specification
- 5.5 The Bidder is required to provide Technical Support Services with three years support from Mother Company & Partner.
- 5.6 Provide Mother Company training for three related engineers for the solution.
- 5.7 Delivery and implementation within 8 weeks
- 5.8 During implementation and configuration, a knowledge transfer, and a detailed elucidation for every step of work must take place by the company team for MOL technical staff.

## 6. Scope and Deliverables

- 6.1 Planning, supply, building, and configuring NGFW Solution
- 6.2 All licenses should be for period of one year related to any license including support, subscription and update. Software policy (if any) and licensing price related to the supplied system should also be clearly mentioned.
- 6.3 The bidder must take total responsibility of commissioning, configuration and integration of NGFW Solution and its relevant software and configuration without any extra cost.
- 6.4 The bidder will be challenged and evaluated to provide smooth, silent and swift configuration and implementation. A minimum downtime and wise management may achieve Zero downtime during the configuration and implementation.
- 6.5 The bidder should do knowledge transfer during the implementation, explaining the configurations that is done during the implementation process.
- 6.6 In the event of any difficulties or delinquency by the bidder in this agreement, MOL has the right to carry the maintenance by another certified partner and MOL must be credited the cost of that maintenance.

- 6.7 The bidder should provide local specialized technical personnel to assist in the future connection and operation of the NGFW and wherever applicable its relevant software.
- 6.8 During the warranty period, the Bidder shall be responsible for all repair costs associated with the NGFW
- 6.9 Bidder will be responsible to work hand by hand with MINISTRY OF LABOR (MOL) team to prepare any configuration.
- 6.10 Bidder should support MOL team to enhance the NGFW policy and tasks to achieve the best performance for endpoints and to achieve premium protection against viruses, worms, trojans ...etc. This include create or update existing policies and tasks to implement and maintain MOL Policy
- 6.11 NGFW best practice should be applied on any configuration implemented. The supplier must proof that by NGFW documentation.

## 7. Technical Support & Maintenance

- 7.1 The NGFW solution associated with this contract shall have 24/7 support from technology vendor through the bidder, for three years starting from the date of final acceptance letter
- 7.2 The bidder should be responsible to manage all support issues either by himself or to follow it with the mother company
- 7.3 The bidder shall provide 24/7 onsite, phone and web technical support for NGFW and utilities. The warranty shall provide higher levels of service.
- 7.4 Apply any needed configuration related to any audit result or vulnerabilities discovery

## 8. Technical Specs

The bidder must deliver the solution as a **turnkey solution**, any missing items or components it's the bidder responsibility to mention and to include in his proposal.

- Support the following security services: Enterprise Firewall Intrusion Prevention Systems (IPS) URL Filtering (URLF) Advanced Malware Protection (AMP)
- **VPN connection for minimum 50 user with double factor authentication feature**
- The vender shall apply and insure the latest firewall security and maintain MOL system working in proper way, so the vender shall make site survey, and its responsibility to copy all settings of existing firewall and deploy on the new one.

**Licensed subscriptions:** Extreme value and protection for network. Includes essential network, web, and zero-day protection, VPN (site-to-site and remote access) with advanced Central Firewall Reporting. Moreover, any other subscriptions needed to get the full secure features like:

- **Base Firewall ( Stateful Firewall, VPN)**
- **Network Protection(IPS, ATP, Device Management)**
- **Web Protection (Web Security and Control, Application Control, Web Malware Protection - Antimalware)**
- **Zero-Day Protection (Machine Learning, Sandboxing File Analysis, Threat Intelligence)**
- **Central management (SD-WAN VPN , CFR Advanced)**
- **Email Protection(Anti-spam, Antivirus, Email Malware Protection)**
- **Web Server Protection(Web Application Firewall)**

- على الشركة العمل على تفعيل اعلى معايير الامن السيبراني من خلال الجدار الناري على عموم شبكة الوزارة وبحيث تضمن عدم انقطاع اي من الخدمات العاملة وتقع مسؤولية ذلك على الشركة المنفذة للعطاء وبالتنسيق مع كادر الوزارة
- كفالة ورخص لمدة 3 سنوات من تاريخ الاستلام
- توريد و تركيب وتشغيل الحل بشكل كامل يقع على مسؤولية الشركة المنفذة . بالاضافة لنقل جميع الاعدادات والضبط للجهاز الناري القديم وتفعيل ذلك

Active / passive Qty (2)	Comply			Notes
	Yes	Partially	No	
<b>Firewall Specifications (Minimum specification)</b>				
Firewall throughput 20 Gbps				
NGFW throughput 6 Gbps				
Threat Protection 3 Gbps				
IPS throughput 7.8 Gbps				
IPsec VPN Throughput 6 Gbps				
Concurrent connections 4 million				
New sessions /sec 120,000				
2 x USB 3.0				
1 x Console Port, 1 x MGT Port (RJ45), 1 x HA Port (RJ45)				
8 GbE RJ45 port				
4 X 1 GbE SFP				
2 X 10 GbE SFP+				
Storage at least 240GB				
Dual AC Power Supply				
<b>General Management</b>				
Purpose-built streamlined user interface				
Self-documenting menu system				
Advanced trouble-shooting tools in GUI (e.g. Packet Capture)				
Full command-line-interface (CLI) accessible from GUI				
Self-service user portal				
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly				
<b>Firewall, Networking &amp; Routing</b>				
Unified policy model enabling policies to be managed on a single screen				
deep packet inspection firewall				
User, group, time, or network based policies				
Access time polices per user/group				
Enforce policy across zones, networks, or by service type				



Custom zones on LAN or DMZ				
Upstream proxy support				
Flood protection: DoS, DDoS and portscan blocking				
VLAN DHCP support and tagging				
Blocking by IP addresses				
Full configuration of DNS, DHCP and NTP				
<b>Multiple Firewall Management</b>				
Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group				
Task Manager provides a full historical audit trail and status monitoring of group policy changes				
Backup firmware management				
<b>SD-WAN</b>				
Support for multiple WAN link options including cable,static IP, and 3G/4G/DHCP with essential monitoring, balancing, failover and fail-back				
Enhanced SD-WAN, a Security feature which leverages the added clarity and reliability of application identification that comes with the sharing of Application Control information between managed endpoints and Firewall.				
<b>Traffic Shaping &amp; Quotas</b>				
Network or user-based traffic shaping (QoS) ( <i>Web and App based traffic shaping are included with the Web Protection Subscription</i> )				
Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical				
Real-time VoIP optimization				
<b>User Self-Service Portal</b>				
Download the Authentication Client				
Download SSL remote access client (Windows) and configuration files (other OS)				
Change user name and password				
View personal internet usage				
<b>Authentication</b>				

Transparent, proxy authentication (NTLM/ Kerberos) or client authentication				
Authentication via: Active Directory, RADIUS, LDAP and TACACS+				
Authentication services for IPSec, L2TP, SSL				
Captive Portal				
<b>Base VPN Options</b>				
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key				
SSL client for Windows & configuration download via user portal				
<b>VPN Client</b>				
IPSec and SSL support				
Send device security status to the firewall				
<b>Support SSLVPN Double Factors Authentication with 50 connections Concurrent</b>				
<b>Cloud Sandbox Protection</b>				
Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis				
Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)				
<b>Intrusion Prevention Systems (IPS)</b>				
High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection				
Support for custom IPS signatures				
IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added				
<b>Advance Threat Protection and Coordinated Security</b>				
Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)				
Provides visibility into top risk users, unknown applications, advanced threats and suspicious payloads				
Limit access to network resources or completely isolate compromised systems until they are cleaned up				
<b>Application Protection and Control</b>				

Enhanced application control with signatures and Layer 7 patterns for thousands of applications				
Application Risk Meter provides and overall risk factor based on the risk level of applications on the network				
Per-user or network rule application control policy enforcement				
<b>Web &amp; App Traffic Shaping</b>				
Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared				
Dashboards (Traffic, Security, and User Threat Quotient),				
Applications Report (App Risk, Blocked Apps, Web Uses, Search Engines, Web Servers, FTP),				
Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, quarantine, and DoS attacks				
<b>Reporting</b>				
No extra charge				
Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)				
Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks				
Export reports as HTML, PDF				
Log retention customization by category				
Full-featured Live Log Viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization				
Hardware warranty & RMA with Advanced Exchange				
24x7 Enhanced Plus Support via Telephone & Email with Remote Consultation				
FREE Security Updates & Patches				
FREE Software Features Updates & Upgrades				
<b>Standard Protection Bundle Includes:</b>				
Enhanced Support: 24/7 support, feature updates, advanced replacement hardware warranty for term				

Email Protection: On-box antispam, AV				
Web Server Protection: Web Application Firewall				
<b>36 months License and Warranty Includes:</b>				
Licenses & subscription for NGFW Antivirus, Antispyware, Antispam, Sandbox Advanced Threat prevention, IPS, Web/URL Filtering, content and application filtering.				