Tender Reference: UHS/IT/TENDER/0002/2022 **07.03.2022**
Tender Expiry Date: 22.03.2022

Title: Web Application Firewall (WAF) Project

Dear Valued Vendors

The Hospital Management has decided to invite vendors for a Tender. You, as a vendor are requested to participate in the tender process by submitting your offer for one or more of the items described in attached document.

The Tenderer should comply with the following terms & conditions:

1. All the prices should be presented in UAE Dirham.

2. Only platinum or Gold or equivalent partnership level of vendors are requested to submit the proposal.

3. The Specification of the proposed product should be clear, informative & include Brand, Origin, Unit of Measure, Qty and Delivery Period.

4. The price quoted is inclusive of the delivery/ installation or as mentioned in the technical requirement (specified in the attached document) to **University Hospital Sharjah**.

5. Warranty and support services from manufacturer should be for 3 years. Support should be 3 years premium. Vendor should provide 3 months post support.

6. Vendors have to submit their partnership level certificate of the proposed products.

7. Vendors have to submit the end of marketing, end of life and end of support documents regarding the proposed products. Failed to submit the documents will eliminate the vendors from the evaluation.

8. Vendors have to provide the customer references on similar projects.

9. Vendors have to provide the technical team details and their level of certifications on the proposed project.

10. Technical BOQ should be discussed with IT department before submitting.

11. The financial offer should be on you company letter head containing authorized signatory and may please be sent to the attention of Director of Finance and Administration, **University Hospital Sharjah, PO Box 72772, Sharjah in a sealed document**.

12. All deliveries should be made for ordered quantity in full to our Main Warehouse, located in the Hospital vicinity or as specified on the Purchase Order/ Contract.

13. As a part of the Tender document, the Vendors are requested to provide their valid Trade License, Name and Designation of the Managing Director/General Manager/Sr. Manager who has authority to bind their company for business relationship. Also is required the authorization letter/Agency certificate providing the confirmation that the vendor is legalized to supply the items on behalf of the manufacturer/principal company.

14. Standard payment terms are 90 days from the date of completion of delivery of all the items ordered or as specifically agreed in writing by the Materials Management Department of the University Hospital Sharjah.

15. Any delays or short supply or non-conformance may result in the termination of Purchase contract and/or imposition of penalty for delayed supplies as per the discretion of the Hospital Management.

16. The proposed items should be evaluated & approved by our Hospital Technical team before confirmation. Once the agreement is signed off, the supplies will have to correspond to the same quality, specification and source as originally agreed and any deviations will be considered as non-compliance with agreed terms.

17. The brand/manufacturer mentioned should be maintained during the Purchase contract period.

18. Any defective products should immediately be replaced with new ones, as and when notified within a maximum period of one month of date of notification.

19. University Hospital Sharjah will be constantly evaluating the compliance of Contracted Terms and consistency in supplies throughout the duration of the Purchase contract. Should Vendors not be meeting the requirements of University Hospital Sharjah, we reserve the right to cancel the contract giving 1 month notice.

20. Purchase Contact details (landline, mobile, emails) of the responsible person/s should be mentioned.

21. **Tenders should be submitted in two sealed envelope and submitted to Administration Office Finance Department- UHS:**

    a. **The Technical Specification details (PLEASE DO NOT INDICATE ANY FINANCIAL VALUE IN THIS).** If requested for additional clarifications and details these needs to be submitted to University Hospital Sharjah- **(Materials Management Department).**
        i. The technical offer should conform to the Indicative specification as per attachment.

ii. Completed indicative specification document to submit along with the technical offer (hard copy).
iii. Reference hospital where the equipment is currently installed.
iv. Authorization letter from the Principal Company indicating.
v. Soft Copy (CD or USB)

b. **The Financial Offer** address to Director of Finance and Administration, University Hospital Sharjah with **tender reference**.

All above document should be submitted before the tender expiry date, all documents submitted after the expiry date will not be accepted.

22. University Hospital Sharjah reserves the right to accept / reject the tenders without assigning any reason thereof.

23. Tender will be awarded project wise as per the Purchase contract.

24. Quality, Price, after sale services are combined parameters for tender evaluation.

The list of Equipment's/ Service/ Medical Disposables for which Tender is being invited are listed as per Annexure I which is an integral part of this Tender Invitation. The vendors are advised to strictly mention the Item Code, the Group Code mentioned therein.

For University Hospital Sharjah

Materials Department

Request for Proposal for Web Application Firewall (WAF) Project

1. REQUEST FOR PROPOSAL

The University Hospital Sharjah (UHS) herewith invites proposals from interested service providers to submit responses to this Request for Proposal (RFP) for the:

- Web Application Firewall (WAF) Project

2. PURPOSE

The purpose of this Request for Proposal (RFP) is to provide broad details relevant to the services required and is not intended to provide a detailed overview of every action required.

UHS is currently planning procure Web Application Firewall and DDOS protection to secure and protect its public facing applications like EMAIL, health and ERP applications etc.

The purpose of this RFP is to:

(a) Select a competent Proponent who has sufficient experience supplying, installing, training and supporting the solution deployment that satisfies requirements equivalent to the UHS's requirements;

(b) Acquire hardware, software, maintenance, support and Implementation services required to deploy the wireless system.

The RFP contains sufficient information and instructions to enable qualified bidders to prepare and submit proposals and supporting material. To be considered responsive, vendors must submit a complete bid that satisfies all requirements as stated in this RFP.

3. PROJECT BACKGROUND

UHS is planning procure Web Application Firewall (WAF) solution with built-in application DDOS and load balancing functionality to secure and protect its public facing web based applications like health, ERP, OWA applications etc. and to balance the load balance applications across multiple DMZ servers hosted on premise behind the network firewalls. The application environment is a heterogeneous mix of Linux and Windows platforms. The application environment is a heterogeneous mix of Linux and Windows platforms.

3.1. Project Scope

The proposed web application firewall (WAF) solution must meet the technical & functional requirements delineated in this RFP. The Successful vendor should initially supply, install and operationalize the whole of the proposed system (hardware, software, HA etc.) based on the requirements mentioned in this RFP.

The proposed solution/model should be a comprehensive and complete Web Application Firewall Security solution:

1. Supply, Installation, Testing, and Commissioning of Web Application Firewall and its associated components in High Availability mode.
2. Any other software/hardware component required to satisfy the requirement must be supplied and installed.
3. Applications integration with WAF.
4. Application Load balance configuration for the DMZ servers.
5. Upgrade all the solution equipment's to the latest firmware prior to deployment.
6. Configure and harden all solution equipment's as per the best security practices.

3.2. Requirements

The proposed solution(s) must meet the below mentioned Technical & Functional requirements and design objectives mentioned in this RFP. These features will be part of the scope of work.

3.2.1. General and Architecture

- Solution must be a market leader for Web Application Firewalls (WAF).
- The solution must be hardware appliance-based and must be in HA (Active-Active).
- Solution must support load balancing functionality.
- The entire solution must be centrally manageable for day to day operations. Reporting, policy creation, alerts management, web application protection configuration etc. must be managed from a central management server. The management server must centrally manage WAF using a standard web browser to access the management UI.
- The solution must provide Role-Based Access Control (RBAC) or multiple user roles that facilitate separation of duties.

3.2.2. WAF

- The solution must support both positive security model and negative security model approaches. (A positive security model 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. A negative security model states explicitly defined known attack signatures).
- The solution should include Botnet protection & DDOS protection on the application level.
- Solution should be able to detect and mitigate DOS attacks.
- Solution should intelligently manage bot traffic to your application in order to prevent credential stuffing, inventory hoarding, content scraping and other types of fraud.
- Advanced Bot Management with custom CAPTCHAs & threat response, advanced bot analytics.
- 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.
- Should have a vulnerability proactive protection from newly discovered or new zero days threats.
- Solution must support AI/ML analysis of traffic patterns to identify attacks even if they do not match a known malicious pattern.
- Solution must support In-Browser Data Encryption which can encrypts data at the app layer to protect against data-extracting malware and man-in-the-browser attacks.
- Solution must support App-level field encryption that protects data and credentials as they pass between the user and server.

- Should have rate limiting protects against denial-of-service attacks, brute-force login attempts, API traffic flows and applications. Must offer protection against brute-force attacks that use stolen credentials.
- The solution must be able to support both inline and non-inline monitoring-only and active enforcement mode. In monitoring-only mode, the administrator must be able to view alerts, attacks, server errors, and other unauthorized activity. In active enforcement mode, the solution must perform everything that is done in monitoring-only mode and additionally be able to block attacks.
- The solution must be able to protect SSL (HTTPS) web applications.
- The solution must enhance web application performance by bringing content closer to your users, caching static content on its network, optimizing image files, compressing dynamic content.
- The solution must allow administrators to add and modify signatures.
- The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats.
- The solution must have an in-built correlation engine which can address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic.
- The solution must be able to inspect HTTP requests and responses.
- Solution must offer API protocol security that can deploys tools to secure REST/JSON, XML, and GWT APIs.
- The solution must automatically build/ learn the web application profiles and use them to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.
- The solution must be able to learn and create profile and in parallel should protect applications by blocking malicious requests.
- The solution must allow profiles to be manually changed and information can be added and removed to fine tune the profiles.
- The solution must be able to perform profiling of web applications in an environment where there is a mixture of good and bad traffic. The solution must be able to automatically differentiate good and bad traffic when learning the profile. Bad traffic should not be learnt.
- The solution must support custom security rules. This should be possible without need to write any script/code.
- The solution must address and mitigate the OWASP Top Ten web application security vulnerabilities.
- The solution must support the capability to define security policies based on the threat intelligence feeds to perform the following functions: -

  - Alert
  - Block IP
  - Block Session
  - Block User
- The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.

3.2.3. Alerting and Blocking Capabilities

- Solution must provide automated, real-time event alert mechanism.
- Solution must be able to monitor and block users when required.
- Solution must support masking of sensitive data in alerts.
- Solution must support sending alerts to external syslog servers.

3.2.4. Reporting

- The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration.
- Solution must support creating custom report templates based on the existing out-of-the-box reports.
- Solution must support generation of reports with both tabular views and data analysis graphical views.
- Solution must support automatic generation of reports based on defined schedule.
- Report must support distribution via email on demand and automatically (on schedule) with PDF and CSV formats.
- Solution must include a single & dedicated centralized management hardware/virtual appliance to manage WAF.
- Solution must come with a web based administration interface and GUI.
- Solution must have an out-of-band management port.

3.2.5. ***High Availability and Performance***

- Solution must support high availability (Active-Active).
- The WAF solution appliance must support dual hot-swap power supplies for high availability.
- Each WAF solution appliance must have 2 x 10G Fiber Multimode NICs with compatible SFP transceivers and Fiber Patch Chords (LC-LC) for these 10G connections.
- The WAF solution must be able to support at least 5 Gbps of HTTP throughput with single appliance.
- The WAF solution must include the SSL hardware acceleration module.

The proposed solution should fulfil complete technical requirements mentioned in this RFP and at **Appendix A: "*Appendix A - UHS WAF Tech Req Compliance*"**.

4. Security and Audit

The solution should not cause any security vulnerabilities.

5. Training and Support

5.1. Training

- Vendor must provide free-of-cost certified (authorized) professional training from an authorized training partner for two (2) UHS IT Administrators.

5.2. Support

- Proposal must include 24 x 7 support of 3 years for all proposed solution components.
- Vendor should provide mandatory 3 Months support after go-live (remote and on-site support).
- **Need to specify what will be on-going maintenance & subscription cost (HW/SW/Licenses) in figures for 4th & 5th year.**

6. INSTRUCTIONS TO VENDORS

- Vendor must have a highest level of partnership with the proposed product.
- Vendors must address all information specified by this RFP.
- Vendor to clearly specify the structure of Licensing whether it is Annual or Perpetual.
- It is mandatory for the Vendor to provide item-vised and with sub-total prices in Commercial Proposal.
- Technical and Financial proposals should be submitted to Director of Finance Office in separated shield envelops.

- Partial proposals will not be considered/accepted.
- **It is mandatory for the Vendor to submit End-of-Sale, End-Of-Support, and End-Of-Life for each individual hardware component - Proof documents from the manufacturer to be attached with the proposal. Note: Proposals submitted without these documents will not be considered.**
- Vendor should provide reference sites where each components/module of your proposed solution has been installed. UHS may contact these users to obtain any information on the solution and implementation. Vendors will co-ordinate with the reference sites and arrange the visit on request from UHS if required.
- Vendor is required to share the manufacturer's vision and road map to look for indicators of an advanced technology strategy (Proof documents need to be provided).
- Vendor should commit the Hardware and required software's Delivery within 4 weeks' period
    - (Note: UHS is exempted from Sharjah Customs).
- **Vendor should discuss the final technical proposal with the technical team before submission.**
- Proposal should include ongoing hardware warranty, support and license subscription for 4th and 5th each year.

6.1. Completing the Technical Requirement (Compliance Sheet) Specification

The Requirement Specification contains a list of requirements of the service. The vendor should respond as follows in the level of compliance column:

Response	Meaning
Compliant	Requirements are met without Customization.
Customize	Basic functionality exists in solution, but it must be customized to meet requirements.
Not Compliant	Solution can't meet the requirements.

a) Vendor must share the filled Compliance sheet and should discuss it with the IT dept. before submitting the proposal.

b) The response should be given by stating the response that applies to the requirement from the table above**. Please provide an explanation/justification whatever be the response. Provide the explanation in the COMMENTS column or on a separate page, if necessary, with reference to the requirement number.**