Tender Reference: UHS/IT/EQP/TENDER/0001/2021 25.01.2021
Tender Expiry Date: 11.02.2021

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 (RFP) for Perimeter Firewalls Upgrade Project

1. REQUEST FOR PROPOSAL

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

- Perimeter Firewalls Upgrade 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.

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 and its addendums (Appendix A).

3. PROJECT BACKGROUND

University Hospital Sharjah (UHS) is looking forward to replace the existing Network perimeter Fortigate 200D Internet firewalls, in alignment with business drives for improvement, architectural and product road map.

The Perimeter firewall solution the hospital chooses through this RFP will be deployed at the hospital infrastructure edge to provide complete control and protection from and to the internet.

Therefore, the proposed systems must be scalable to the enterprise level with commensurate reliability.

Current Environment

The IT core infrastructure is located in UHS Main site, the Network consists of two (2) core switches with a failover technology, and 45 edge switches in the Network (the infrastructure is currently divided based on the departments, VLAN's and its locations).

In the current setup the 300 Mbps ADSL and 16 Mbps leased lines are connected to the Firewall for browsing, email and VPN service in the main campus to monitor & control the Internet traffic that are flowing to UHS Network.

In addition the firewall is basically used to publish OWA/Intranet services to outside world.

3.1. Technical Requirements

The proposed firewall solution should support but not limited to the following requirements:

- Solution must be Appliance based enterprise class security solution.
- Solution must be based on dedicated ASIC-based appliance empowered by dedicated ASICs/Processors to accelerate the performance of UTM, Application Control, Stateful packet inspection, VPN encryption/decryption, protocol anomaly offloading, QoS enforcement etc.
- Proposed solution must offer IPS & Next-Generation firewall real-world throughput of at least 5 Gbps (with complete threat prevention and security features enabled).
- 16 x 1 GE fixed RJ45 Ports and at-least 4 x 10GE SFP+ / GE SFP slots per firewall.
- Dedicated management & Console port.
- HA Ports for High Availability. Proposed solution should support more than two (2) heartbeat links, any of the interface must be configurable as heartbeat interface.
- Support for SD-WAN with no extra license or module.
- IPsec & SSL VPN out of the box support without any need for additional licenses.
- Solution must provide full-fledged bandwidth and traffic management capabilities.
- Solution should provide full support for IPv6 (which includes IPv6 routing protocols, IPv6 tunneling, IPv6 firewalling, UTM, NAT46, NAT64 and IPv6 IPSec VPN).
- Solution must provide ease of use administration and management.
- Sensitive configuration items, such as passwords known to the appliance or RSA keys, should either be encrypted or hashed when stored on disk.
- Solution must support multiple administrators to access the appliance simultaneously for monitoring and managing.
- Centralized management with configuring, monitoring, logging & reporting.
- Solution must provide an out of band Ethernet interface for management that supports SSHv2 and SCP.

- Solution should provide an Intuitive Web-based administrator interface with Graphical Dashboards with drill-down capability and detailed log-data. Incase if the management is client-based, it should not reflect financial figures.

- Solution should provide Single Pane of Glass with Network Operations Center (NOC) view to provide 360° visibility to identify issues quickly and intuitively.

- Solution must provide reports for presentation, investigation and real time reports. Logging and Reporting should be inbuilt into the solution.

- Support for trending and metrics reporting of user, usage, and traffic activities.

- Support for exporting of report information to HTML, PDF, and text/csv formats.

- Solution must provide Log data to be filtered comprehensively at the gathering stage.

- Authentication and activity reports alerting and logging.

- Solution must provide reporting capabilities for the following: user, group, IP statistics, bandwidth & traffic management, caching statistics, malware, content, URL triggers and events, system performance and errors.

- Sending logging transactions to remote collection devices and for transferring via the network raw or customized log file data or data via syslog methods.

- Solution should provide Real-time viewing of logging on usage, session, traffic and threats with built-in log searching and filtering capabilities.

- Support for mechanism to archive or retire old logs data from the repository.

- Solution should support Next Generation Firewalling capabilities.

- Support Stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.

- Solution should support High availability clustering (Active/Passive and Active/Active support) with Failure detection (path and interface monitoring).

- Must maintain user and application sessions including VPN sessions when one of the high availability pairs (firewall devices) fails.

- The HA solutions should support automated firmware upgrade process that provides minimum downtime.

- Proposed solution must support modular hot swappable (1+1 redundant) dual power supply.

- The proposed firewall solution should provide fast (SSD), sufficient internal storage to retain the operational data on the device.

- Solution must support Full IPS capabilities with decryption.

- IPS device should perform Stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.

- The proposed IPS must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.

- Proposed solution must provide integrated intrusion detection and prevention (IPS) function that offers advanced detection capabilities such as exploit signatures, protocol anomalies, application controls and behavior based detection.

- IPS must be able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures.

- SSL Inspection should be supported within the same appliance with no additional hardware required.

- Solution should provide industry's best threat protection performance and ultra-low latency.

- Provide advanced application identification, visibility and control. Should also support building Custom Applications.

- Provide granular application function control to identify, allow, block or limit usage of applications and features within them.

- Proposed solution must support to be integrated with On-Premise Sandbox technology to detect and block 0-day and advanced threats (optional - for future).

- Proposed solution must include Cloud based Sandboxing service.

- LACP (802.3ad) support on the interfaces.

- Support for PPPOE (Point-to-Point Protocol over Ethernet).

- Solution should support Static and dynamic routing protocols (RIP, OSPF, ISIS, BGP).

- Policy based routing (PBR) must be supported.

- Solution should be able to provide outbound WAN link load-balancing capabilities.

- Support for Network Address Translation (NAT) types such as Interface-NAT, Source & Destination NAT, Static NAT, Network address and port address translation (NAPT).

- Proposed solution must WCCP and ICAP.

- SSL Inspection should be supported within the same appliance with no additional hardware required.

- The proposed solution must support Botnet server IP blocking based on a global IP reputation database.

- Solution must support Accelerated Encrypted inspection.

- Solution must provide Anti-Bot Protection.

- Solution must provide Anti-Virus and Anti-Malware Protection.

- Solution must provide protection against DoS, DDoS, Anti-Replay & DNS based attacks.

- Solution must not just be signature based security but should also be able to protect against unknown attacks and should provide proactive defenses.

- Solution must support Active Directory (AD) Integration without any agent.

- Solution must support Multi-AD environment and automatic synchronization with directory service, to simplify policy, user and group management.

- Solution must be able to provide advanced security dashboard with classification of threats in different levels.
- Anti-Evasion defenses. Should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.
- Exploit detection.
- File scanning (content filtering).
- Solution should identify the application reputations and should have the functionality to modify the reputation for certain internal applications.
- Must offer adaptive real-time threat intelligence to improve firewall functions.
- Real-time monitoring (customizable Dashboard view).
- Should support CLI & GUI based access to the firewall nodes (CLI access for advanced debugging and troubleshooting).
- Any additional security feature (other than the requested) that comes with the solution should not reflect financial proposal.
- Varied offering with model selection to cover the desired performance and deployment location scenarios.
- The System should be a hardware appliance.
- Support for SNMP versions 1, 2c, and 3.
- Solution must offer perpetual licensing as applicable.
- Solution must support Port Aggregation (LACP) and must be compatible with our existing Cisco Switches.
- Must support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions (if required to migrate to IPv6 in future).
- The proposed firewall solution must be extensible to accommodate the hospital’s growing needs and keep up with higher throughput requirements.
- Must integrate with the hospital’s SIEM solution.
- Must seamlessly integrate with Active Directory to provide complete user identification and enable application based policy definition per user and/or group.
- There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.
- Solution should be an Enterprise-level market leader in NGFW for last consecutive 3 years.
- Free-of-cost instructor-led training from authorized training partner must be provided on all aspects of the solution.
- Complete set of volumes for the Configuration and Management Guides should be provided.
- Clear Support Escalation Process with Points of Contact with Local Support office in same time zone.

- The vendor must provide a three year product road map and all proposed systems and sub-components must be guaranteed not to be End-of-Life for at least five years.

- The vendor must ensure that the proposed firewall solution is the latest and must provide proof documents for product End-of-sale, End-of-life and End-of-support.

- Hardware maintenance for the proposed solutions must be 24x7xNBD shipment. Software maintenance must be 24x7x4h.

- The proposed solution(s) must address the technical requirements and design objectives delineated herein. The vendor is solely responsible to deliver a fully functional solution meeting the specifications described herein. After the award of the contract, the awarded vendor is responsible for any necessary item not brought to the attention of UHS before the award in order to complete the project by the specifications & design objectives.

The proposed solution should fulfil complete technical requirements mentioned in this RFP and at **Appendix A: "*UHS_PERIMETER_FW_TECHREQ_COMPLIANCE (APPENDIX A)*"**.

3.2. Security and Audit

The solution should not cause any security vulnerabilities.

3.3. Training and Support

3.3.1. Training

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

3.3.2. Support

a) Proposal must include 24 x 7 support (Manufacturer Support) as an option for 3 years.

b) Vendor should provide mandatory 3 Months support after go-live (remote or on-site support).

c) Need to specify what will be on-going maintenance & subscription cost for 4th & 5th year.

4. INSTRUCTIONS TO VENDORS

- Vendor must provide a brief presentation of the proposed firewall solution including the diagrams according to UHS campus architecture.
- Proposed solution should include the part numbers and its description of all relevant components.
- Solution must include Intelligent and controllable security infrastructure with monitoring solutions to support UHS requirements.
- Vendor must include Installation, maintenance & support including the migration of the new firewall solution with minimum downtime in the Network.
- Complete documentation and handover with diagrams.
- Project signoff document at completion.
- Vendor to clearly specify the structure of Licensing whether it is Annual or Perpetual.
- Vendor to provide initial warranty and subscription (software / hardware) for the Solution for minimum 3 Years (24/7 support).
- **End-of-Sale, End-Of-Support, End-Of-Life for each individual component - Proof documents from the manufacturer to be attached with the proposal. Proposals without this requested information will strictly be REJECTED.**
- Vendor should provide reference sites where each components/module of your proposed system 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 IT Dept. before submission.

4.1. *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 whatever be the response. Provide the explanation in the COMMENTS column or on a separate page, if necessary, with reference to the requirement number.**