UHS | UNIVERSITY HOSPITAL SHARJAH
مستشفى الجامعة بالشارقة

Data Center Firewall Project Technical Requirements

1. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified vendors for the procurement of enterprise data center firewalls that natively provide next generation high throughput intrusion detection & prevention (IDS/IPS), application control, next generation firewalling capabilities with integration of cloud sandboxing for advanced threat prevention and acquisition of professional services to install, configure, and integrate these solutions into the hospital network for the University Hospital Sharjah.

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).

2. Project Background

The Data Center firewall solutions the hospital chooses through this RFP will be deployed at the hospital Core infrastructure to provide complete protection to the Main data center/server farm.

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

2.1. Current Environment

The hospital is currently utilizing Forcepoint NGFW for datacenter/core level security.

The hospital currently has approximately 750 managed computers (desktop & laptops), around 100-150 servers (physical and virtual) and around 100 network devices distributed across the campus.

The majority of these desktop computers and servers are running Microsoft's Windows operating systems. However, there are also some Linux based servers, and some operational technology equipment (building management systems, etc.).

The following are the services running in the datacenter/server farm.

1) TrakCare (HIS) – Web based Application
2) SAP – Web based Application
3) Windows File Services
4) Print Services
5) Radiology Imaging System (PACS – Picture Archiving and Communication Systems)
6) Exchange Servers
7) VMWare Environment
8) Citrix & Nutanix based VDI platform
9) AD, DNS & DHCP Services

2.2. Firewall Requirements

The hospital’s firewall security practice is to implicitly deny communications unless explicitly permitted. The data center firewall solution implemented should secure all the systems from unauthorized and malicious activities. An Active/Active solution is mandatory for high availability. And solution should maintain 100% availability. The following requirements are mandatory.

The data center firewall solution must:

- Solution must be Appliance based enterprise class security solution
- 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
- Solution should provide centralized management console for management and configuration of the data center firewalls providing a single point for monitoring, configuring and 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) and Security Operations Center (SOC) 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 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 and traffic
- Support for mechanism to archive or retire old proxy 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.
- Support Active/Active configuration modes for high availability. High Availability between the two Firewalls should use the existing connections/links between the two Core Switches. The two core switches are deployed in two different MDF communication rooms with a separation distance of approx. 100m between them.
- Must maintain user and application sessions when one of the high availability pairs (firewall devices) fails.
- 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.
- Overall security/inspection throughput (real-world) for each appliance should be 10 Gbps. (Note: Vendor should prove that these are real world specs and not test bed values). Required Proof document needs to be submitted.
- Provide multiple security zones and interfaces to partition the data center networks into more manageable highly controlled network segments.
- Ability to create granular security policy definitions per Microsoft Active Directory user and security groups to identify, block or limit usage of applications.
- Solution must support Full IPS capabilities with decryption
- Solution must support application based firewall policies specific to applications (pre-defines and custom-defined).
- 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.
- Solution must be able to block known as well as unknown attacks (ex. Zero day attacks).
- Solution must offer comprehensive vulnerability protection (using signatures & behavior for both known and unknown attacks).
- 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.
- Solution must enable administrator to create detailed firewall security policies that is based on combination of multiple characteristics such as user's identity, computer name (NetBIOS name of the system is being used by the user) and specific aspects of an application.
- Solution must support Accelerated Encrypted inspection
- Solution must provide Anti-Bot Protection
- Solution must provide Anti-Virus Protection
- Solution must provide Anti-Malware Protection
- Solution must provide protection against DoS, DDoS, Anti-Replay 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 also have a capability to offload decrypted SSL traffic to third party device for further malware and security analysis (optional - to meet future requirement)
- 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
- Advanced Malware Detection & Protection. Proposed solution must include a cloud sandbox and the proposed firewalls must integrate with the cloud sandbox for advanced threat prevention.
- Anti-Evasion defenses. Should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.
- File scanning (content filtering)
- Firewall should support file, application based (pre-defined and custom-defined) whitelisting/exclusions.
- Exploit detection

- 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)
- Per firewall, Include a minimum of two (2) 10 Gbps multi-mode fiber (SFP+) optical interfaces, a minimum eight 100/1000 Mbps copper Ethernet interfaces. All ports must be compatible and work with the existing network equipment.
- Solution must include required Four (4) 10G SFP+ SR transceiver modules and Four (4) LC-LC OM3 MM Fiber optical cables as part of the proposed system.
- Support all the latest web browsers (MS Internet Explorer, Edge, Mozilla Firefox, Google Chrome and Apple Safari)
- 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 9407 Core Switches
- Must support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions (if required to migrate to IPv6 in future).
- Solution should be a Market leader for the past three years.
- Free-of-cost instructor-led training from authorized training partner must be provided on all aspects of the solution for 2 seats. Training should be a comprehensive administrative training and not basic.
- 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 years 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 and software maintenance for each of the proposed solutions will be submitted for 24x7xNBD
- 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.
- 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_DCFW_TechReq_Compliance*"**.

2.3. Security and Audit

The solution should not cause any security vulnerabilities.

2.4. Training and Support

2.4.1. Training

- ➢ Vendor must provide free-of-cost certified (authorized) training from an authorized training partner for two UHS IT staff. Training should be a comprehensive administrative training and should not be basic.

2.4.2. Support

- ➢ Proposal must include 24 x 7 support (Manufacturer Support) for 3 years
- ➢ Vendor should provide mandatory 3 Months support after go-live (remote or on-site support).
- ➢ Need to specify what will be on-going maintenance cost in percentage for 4th & 5th year.

3. 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.

3.1. 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.

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