Request for Proposal for Secure Web Gateway (Web Proxy) 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:

- Secure Web Gateway (Web Proxy) 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 Secure Web Gateway solution to provide comprehensive web protection and application control technologies to defend users from internet-borne threats and help in enforcing internet security policy compliance.

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 secure web gateway solution.

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

The Secure Web Gateway solution the hospital chooses through this RFP will be deployed at the hospital Core infrastructure to provide comprehensive web protection against multiple web threats including malicious lures, phishing, evasive malwares, bot networks etc. and application control technologies to defend users from internet-borne threats and help in enforcing internet policy compliance.

The proposed solution must be scalable to the enterprise level with commensurate reliability.

Hospital invites technically complete and commercially competitive bids from reputed vendors/OEM for Supply, Installation, Configuration, Testing and Implementation of Secure Web Gateway solution.

3.1. Current Environment

Hospital operations and user base is currently at the main site having around 1200 users. Current web security solution at the hospital is from Cisco (WSAs) centrally managed by Cisco (SMA) with proxy deployment in transparent mode (using WCCP redirection).

Hospital is planning to replace the existing web security solution with a solution that has full functionality support mentioned in this RFP and attached compliance sheet (Appendix A).

3.2. Project Scope

The proposed secure web gateway (web proxy) 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 Security Gateway solution:

1. Supply, Installation, Testing, and Commissioning of Secure Web Gateway and its associated components in High Availability (HA) mode.
2. Any other software/hardware component required to satisfy the requirements must be supplied and installed.
3. Secure web gateways integration with the existing infrastructure.
4. Importing or implementing current web Gateway policies into the new Web Gateway solution.
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.

3.3. 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.

3.3.1. General

- The secure web gateway solution must be dedicated appliance based and it must provide features like Web Proxy with Caching, Web Content based/ Web Reputation based filtering, URL filtering, Antivirus, Antimalware, Application Visibility & control, SSL inspection, Protocol filtering, Detailed Reporting and Management etc. and all the functionality should be available from day one. All required licenses, hardware, software should be provided in the RFP.
- The solution should be appliance based, Reliable, purpose-built security appliance with hardened operating system supporting Stateful policy inspection technology.

- Appliance should support a total of 1500 concurrent users. The same appliance system should be 100 % scalable over the next 5 years.
- The solution should support NTP time synchronization.
- The proposed system should have support for both transparent mode and explicit proxy mode.

3.3.2. Web Content Filtering & Application Control Features

- The solution should have an inbuilt URL filtering functionality with multiple pre-defined categories. It must support the creation of custom URL categories for allowing/blocking specific domains/destinations as required by the organization.
- Solution should have strong Content filtering database with URLs segregated into different groups/categories, which should be automatically updated with latest changes on a regular basis from the appliance manufacturer's web sites.
- The solution should have the option to enforce content based, application wise, hash value based, key word and protocol based blocking. Also it should be able to provide safe search, URL re-categorization option.
- Solution should have web protection mechanism to identify and block web pages having malicious java script, VB script, executable, malicious or unauthorized ActiveX applications, potentially harmful programs or software's download and shareware.
- It should be possible in the solution to create policies with administrator having the provision to allow or deny any group/category as per the appliance's/solution's URL database (including custom created groups) and to assign it to a particular user, IP address or group etc. for permanently or for a specific time period.
- Solution should have own Global Threat Intelligent Network to protect from Zero day attack, blended threats, Botnet, Trojan, Malwares communication, Spywares, Pharming attack and traffic includes compressed files.
- Also the solution must have the option to allow or deny a particular domain or destination for a user or IP group permanently or for a specific time period. Solution should be able to block domains which are containing alpha numeric and special characters.
- The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. Should support detection of threat attempts occurring from the entire inside and outside Network by tracking all network ports and all protocols.
- The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed/updated from OEM different domains to assign a web based score to determine the likelihood that it contains URL-based malware.

- Solution should have capabilities to detect and prevent accessing domains like Domain Fluxing (Fast Flux / Dynamic Reputation/ Domain Generation Algorithms).
- The solution should support following actions for websites/Applications like allow, monitor, block, time-based access.
- Solution should be able to restrict User to access internet/specific set of URLs/URL groups/Categories, during specified hours / time (Time based revocation) or based on bandwidth quota (for example in 30 days user can access mentioned sites for 30 hours).
- Solution should have capabilities to configure User, IPs, URLs and Domains to Black list or white list/ exceptions for detections. Also it should have the option to bypass some of the IP addresses/URLs completely.
- The solution should have visibility for cloud applications and shadow IT application usage.
- The solution should perform HTTPS traffic deep packet inspection (SSL/TLS based).
- The solution should have facility for End User to report Mis-categorization in URL Category. OEM should provide feeds on a regular basis to categorize URLs which can be fed in the appliance manually or automatically.
- The solution should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.
- Should be able to scan real time downloads and show the status page to end user. In case infection found, should restrict user to download the file.
- The proposed solution should support to provide real time data identifiers to detect and prevent sensitive information getting stolen by malware through web channel. Solution should have pre-built signatures to detect information leaks through malware.
- The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents.
- The solution should filter out embedded objectionable or unproductive content, this includes examination of the source server, URL, page content, and active content.
- The proposed system should have integrated Web Content Filtering functionality.
- The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.
- The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet, CIDR basis and user & user group wise (Active Directory user or similar authentication mechanisms)
- The proposed solution should be able to enable or disable Web Filtering per policy or based on authenticated user groups for both HTTP and HTTPS traffic.
- Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
- Should include Web URL block
- Should include Web Exempt List

- The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.
- The proposed solution shall be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google.
- The solution shall allow administrators to create multiple new local URL filtering categories besides dynamic categories.
- Should have the intelligence to identify & control of popular IM & P2P applications like BitTorrent, KaZaa, Skype, Youtube, Facebook, LinkedIn etc.
- Appliance must have proxy and caching functionalities.
- Solution should be able to restrict User to access internet, during specified hours / time. (Time based revocation).
- Solution should be able to restrict User to access internet for given limited time period, for example in 30days user can access internet for 30 hours (surfing Quota).
- Solution should have capabilities to configure User, IPs, URLs and Domains to Black list or white list/ exceptions for detections
- Solution should be able to restrict Users to download certain amount of data, for example a user can be restricted to use not more than 1 GB data during a time interval.
- The appliance should have Quota restrictions based on Users and URLs.
- The appliance should provide Website categorization and the website categorization needs to be updated regularly by the vendor.
- The appliance should have provisions for granular access control like allowing access to Facebook but not Facebook messenger.
- The appliance should have provisions to restrict bandwidth per User.
- The appliance should have provisions for IP blacklisting and URL blacklisting.
- The appliance should have provisions for allowing Category based access and port based access.
- The solution should have a provision for SSL bypass based on URLs and Domains.

3.3.3. Anti-virus, Anti-bot and Anti-Malware

- Solution should be able to block, allow or monitor only using AV signatures and file blocking based on policy or based on authenticated user groups for HTTP, HTTPS, FTP services.
- The solution should have Anti-APT features and should be able to integrate with Sandbox to detect and mitigate unknown threats and advanced threats.
- Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack.
- Appliance should provide inline Anti-Virus and Anti-Malware inspection and prevention.

- The appliance should have support for at least 2 industry known Anti Malware/Anti-Virus engines (Signature and Heuristics based) that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors, Key loggers and as additionally defined by the organizations policy. The bidder has to mention the antimalware engines used in the solution.
- The appliance should protect itself against any attacks from Internet.
- The solution must support different types of compression algorithms and scan nested compressed files and it should also have capabilities to inspect malware embedded in all types of files
- Solution should be able to restrict Users to download certain files based on file types, size, extensions etc. Also the solution should be capable of blocking specific set of files downloads for specific user groups. Even if the file types are blocked globally, exception based on URLs, IPs, domains should be allowed.
- The appliance should be capable of nullifying the malware/virus and should be able to stop the spreading of the same to other endpoints in the network. Solution should be able to identify the origin of the event and must take remedy for the issue immediately.
- The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.
- The appliance should catch malware that attempts to bypass known ports including port 80.
- The appliance should have virus signature database which should update automatically from OEM websites, with new signatures and act as anti-virus gateway to scan all the data passing through the appliance using protocols like FTP & HTTP/ HTTPS etc.
- The solution should be capable of integrating with Sandboxing solution of the same OEM.
- The appliance should alert the user if the content being downloaded is found to contain virus.
- Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack.

3.3.4. User Authentication

- The appliance should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). The solution should have the option to exclude the authentication for user groups/IP addresses/ Subnet based.
- The proposed solution shall be able to support various form of user Authentication methods simultaneously, including:
  1. Local Database entries
  2. LDAP server entries

3. Native Windows AD (Single sign on capability)
4. Industry leading Single Sign On Agent support

- The solution shall be capable of providing Windows AD single sign-on when they log on to the AD domain and the device.
- The authentication should be done every time a user access web through the appliance after defined idle time. The appliance should timeout user if the connection is left idle for a certain amount of time. The solution should provide option to exclude the idle time for selected users or IP address groups and to set different range of idle time out period for different groups.
- The appliance should have the option to exclude some of the user groups completely exempted from authentication.
- The appliance when deployed in in-line mode should support bypass mode in case of appliance failure i.e. traffic flow should not break. Also there should be some indication to know whether bypass mode is active or not.
- The appliance should not create any unnecessary load in the network and the user request processing should be completed and the outcome should be reflected to user without any delay.

3.3.5. Data Leakage Prevention features in Web Gateway Solution (Web DLP)

- System should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.
- Solution should have web DLP functionality. Data Leakage prevention should prevent critical, sensitive and proprietary data from being leaked outside Hospital's secured network using web as channel.
- The proposed web security solution should have the option to integrate with the DLP solutions of same OEM or third parties.
- The solution should be able to detect data theft even if the malware sends the data through image files.

3.3.6. High Availability

- The appliance must be capable of deploying it in active –active mode or in active standby mode with auto fail over option under both modes.
- The policy synchronization must happen in real time between the devices deployed in HA mode.
- High Availability feature must be supported for either explicit proxy mode or transparent proxy mode.

- The appliance should have provision to back up the system data, configuration data, and policy data to an external storage medium/server.
- The solution should support explicit forward proxy mode deployment and transparent mode deployment. The method through which explicit and transparent mode deployments are achieved should be mentioned clearly.
- The solution should provide load balancing, with the support of PAC file or DNS round robin technique or with built in load balancer.
- Appliance shall work in Active-Active mode, with a condition that each appliance can handle 1500 concurrent users with auto failover.

3.3.7. Logging and Reporting

- Proposed central management appliance must have support for built-in logs and reporting.
- Appliance to be built in such a way that it should be capable of storing logs for atleast 6 months.
- Solution should show real-time traffic details.
- Solution should be capable of being integrated with on-prem industry leading SIEM solutions.
- Appliance should provide advanced threat dashboard to track the infection or threat history for User/IP
- Appliance should have built in various reports and can create custom reports like Executive report, Infection life cycle report, Top 10 reports for various category and Health reports etc.
- Appliance should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time).
- The Appliance should support real time graphical and chart based dashboard for the summary of activities over Web.
- Appliance shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access user
- Appliance should provide advanced threat dashboard to track the infection or threat history for User/IP addresses
- The Appliance should support real time graphical and chart based dashboard for the summary of web filtering activities. The solution should have pre-built report templates which the administrator can use for generating reports.
- The Appliance should be able to consolidate reports from multiple boxes for centralized logging and reporting.
- The appliance should generate reports showing the full details of access user-wise, time-wise, destination-wise, application-wise etc.
- Appliance should support a web interface that includes a tool that traces & can simulate client requests as if they were made by the end users. It should describe how Web Proxy

processes the request and can be used for troubleshooting purpose. It should also support policy simulating functionality.

- Appliance should have built in various reports and can create custom reports like Executive report, Infection life cycle report, Bandwidth usage reports, Top 10 reports for various category and Health reports etc.
- Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat, Bandwidth based reports).
- Appliance should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time).
- The auto generated reports should be forwarded to the email ids configured in the appliance.
- The appliance should have the provision to integrate with third-party SIEM applications and custom monitoring tools
- The appliance should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.
- The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and packet capture.
- Appliance should support automatic “rollover” & archive the log file when it reaches admin defined maximum file-size or time interval like daily/weekly rollover of logs.
- The appliance should support the retrieval of logs through FTP/SCP protocol and require option to retrieve the logs as per scheduled.
- Appliance should also support centralized reporting. Product to maintain detailed web security solution access logs that can be searched via filters, for identifying any desired access of the user and to see how the product dealt with it.
- Appliance should support generating a printer-friendly reports in PDF, Excel/ CSV files and other standard formats.
- Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.
- The appliance should report incident with URL category information along with user, IP, content violating policy etc.
- The appliance should send an alert message to the user, if he/she is trying to access a blocked website. The Message should be configurable by administrator.
- The appliance should provide detailed information on security incidents to comprehensively investigate individual threat events.
- The system should have facility to log all activities within the appliance. The appliance should be able to send logs to an external syslog servers.
- Even if the appliance are functioning in active-passive mode all the reports and logs should be available in the central console.

- Appliance should have the provision to archive/retrieve old web security solution logs data from the repository.

3.3.8. Appliance capability and administration

- Appliance should have sufficient storage space to store device logs in the appliance itself or pushed to a reporting server as part of the solution
- The appliances must have RAID redundancy (for hard drives), network redundancy (for management network interfaces) and Power-Supply and Fan module redundancy
- The appliance should have hardened Operating System for handling web objects. The OS should be secure from vulnerabilities.
- The appliance should be rack mountable, preferable with 1 U or 2 U size for each appliance.
- Each appliance should have redundant power supplies.
- Appliance should have centralized architecture with web or GUI based dashboard console to monitor, reporting, notification, delegated administration, maintaining and policy management for the registered users centrally for multiple boxes/appliances.
- All the appliances deployed in the solution should be in sync in all policy and other the parameters.
- The centralized management should be provided without the support of additional hardware/server (preferably) and if any additional devices required for the management of solution, it should be mentioned clearly.
- Appliance shall support role-based administration.
- All the user including the administrator activity should have logged and available for auditing or troubleshooting.
- The solution should support real time graphical and chart based dashboard for the summary of activities over Web.
- The appliance should be able to export all the solution policies and configurations to a server/ local machine or even to the appliance itself. The exported file can be directly loaded to the appliances/solution for restoration purpose.
- Appliance shall support the following remote access capabilities on its management interface via HTTP, HTTPS, SSH access. Also there should be provision for serial console and separate Ethernet management port for managing the appliances.
- GUI/Web based console should be accessible in all browsers.

3.3.9. License

- The appliance should have complete and perpetual license for all the features required Web security solution, like Web filtering, content inspection & control, Antivirus, reporting etc.
- The Web Security Solution licensing criteria could be User or Concurrent session based.

3.3.10. General Features

- Appliance should have the provision to integrate it cloud sandboxing solution.
- Multiple accesses provisioning for same user using single policy instead of creating multiple policies or multiple access control
- Appliance should support all browsers for accessing websites for the end user. (MS Edge, IE , Mozilla Firefox, Chrome etc.)
- The proposed solution should support SNMP V1, V2, and V3. And should have capabilities of hardware & software monitoring via both enterprise grade MIBS as well as alerts via SNMP traps.
- All the regulatory compliance regarding web security solution should be adhered in the proposed solution.
- Solution should be a Gartner Leader for at-least last three years (from 2020-2022).
- 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.
- Clear Support Escalation Process with Points of Contact with Local Support office in same time zone.
- Vendor should submit the End-of-sale, End-of-life, End-of-support documents of the proposed solution from the manufacturer.

The proposed solution should fulfil complete technical & functional requirements specified at **Appendix A: "*UHS_SWG_TechReq_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 which includes hardware, licenses and subscriptions.
- 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.