**مواصفات العطاء (7/2022)**

**توريد وتركيب وتشغيل نظام حماية شبكة الجامعة-الجدار الناري عالي التوافر**

 **(High Availability Next Generation Firewall Infrastructure)**

**Part 1**

1. **Overview**

Al Albayt University would like to refresh its existing firewalling infrastructure, where the existing infrastructure contains only one appliance, and the university wants to update this infrastructure to be **high availability firewalling infrastructure (HA) by installing two NGFW appliances,** this will help the university in setting high standard policies, improve the overall security of the university infrastructure.

This document is an invitation to qualified bidders to offer their solutions and ideas to design, deliver, install, accommodate and test a **turnkey** project based on the latest technology in this field, all technical details are clarified in the technical specifications section.

1. **General Terms and Conditions**

The following terms and conditions must be read carefully and understood by bidders:

* 1. **The bidder must meet the qualifications that listed below in item (4).**
	2. It is the bidder's sole responsibility and on his own expenses to understand the site nature and environment and all requirements that are related to the tender or that may influence its pricing. Where the bidder must provide all necessary requirements to make the solution ready to work.
	3. The bidders must provide any additional equipment or licenses or subscriptions that is not specified in this RFP but necessary to meet AABU’s requirement for the whole project, the specifications and costs of such equipment or licenses or subscriptions must be presented in detail in the bidder’s offer.
	4. **Extra hardware/software Must be provided and included in the proposals if it is required to comply with this RFP.**
	5. If any item is needed during the installation or operation and was not stated in the offer; then it is the bidder's responsibility to provide it at no extra cost.
	6. **Compliance Sheet is required and must be filled.**
	7. **Three years of licenses, subscriptions, warranty, and support.**
	8. **On-site warranty with labor and spare parts is required.** the warranty period must be also covered from the mother company.
	9. **Vendor support and partner support is required.**
	10. **All necessary licenses and subscriptions that needed to activate the required security features must be covered.**
	11. The bidder should explain the delivery and implementation time frame.
	12. Proposal Documents should be provided in separate financial and technical envelopes.
	13. Electronic format version of the offers must be handed alongside the hard copies' documents mentioned above.
	14. The software & hardware quoted by bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of Purchase order/contract period. In the event of the supplied equipment being declared End of support/End of Life during the contract period of 5 years, the bidder has to replace the equipment with equipment having equivalent or higher configurations.
	15. **The technical specifications in section (5) are the minimum requirements, bidders can offer products that can achieve the goal with modified specifications and AABU has the right to consider whatever it deems appropriate.**
	16. Bidders requiring further information or clarification may notify AABU in writing at Central Tendering Department, AABU will respond in writing to any request for information or clarification of the bid.
	17. Bidders are required to supply original commercial product brochures or PDF files for the equipment and software that they are proposing.
	18. The bidder who’s won the tender will comply the maintenance SLA with the university.
1. **Evaluation Criteria**
* Bids will be evaluated on the basis of compliance with the instructions to the bidders, the specifications, and the price. There is no obligation on AABU to accept the lowest price.
1. **Bidder Qualifications**

Al Albayt University (AABU) is inviting **qualified bidders only** to provide the requirements of mentioned RFP. AABU have defined the followings as mandatory qualifications requirements, any bidder does not comply to any of them will be disqualified:

1. Bidder must be in business and a registered company in Jordan for at least 5 years.
2. Bidder should have enough experience and certified technical staff to do the installation and support, where it must have at least (2) local qualified and certified engineers to install and support the offered solution. Name, experience, certificates and CVs of the staff who will do the installation and support should be included.
3. Bidder should **have a reference projects with similar scope in Jordan during the latest two years**, and must be stated in the following: Company name, contact person, phone number, Scope of work implemented (must be stated clearly all Services and Device model), and Project Start and end dates.
4. Bidders should have **valid partnership** with the vendor of the offered devices and solutions, original **authorization letter** from the mother company must be provided.
5. **Technical Specifications for the NGFW appliances (QTY: 2)**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Specification** | **Comply** | **Reference(page/line)** |
| **Yes** | **No** |  |
| 1. **General Requirements**
 |
|  | The solution should be based on modern next generation firewall architecture. Allowing the university to benefit from the design in improving network security by supporting (activated) the following functions: |
|  | Application Control |  |  |  |
|  | SSL traffic inspection |  |  |  |
|  | User Identification and control |  |  |  |
|  | Content Protection against (network attacks, spyware, viruses, modern malware …etc). |  |  |  |
|  | NAT (Static, Source, Destination ..etc) |  |  |  |
|  | URL filtering |  |  |  |
|  | The application policy controls, firewall policy controls, and threat prevention features all be enabled in a single rule (Policy) in the solution. |  |  |  |
|  | The device should have an internet traffic shaping feature based on traffic type, category and application (Facebook, YouTube…etc.). |  |  |  |
|  | The traffic shaping feature should be able to control bandwidth per group of users as sources and per destination (URL, IP address, and application). |  |  |  |
|  | The vendor must be achieved as Rating **AAA of Security Effectiveness** tests in *CyberRatings Enterprise Firewall Test Report 2021* report.**\*latest CyberRatings report should be attached with the offer.** |  |  |  |
|  | The proposed product should not be announced End of Sale or End of Life. |  |  |  |
|  | Vendor warranty and support with required licenses included. |  |  |  |
| 1. **Hardware Requirements**
 |
|  | The proposed systems must be able to have minimum support of (per appliance) **without Management I/O or HA ports**: |
|  | 6 x UTP (1 Gbps), **or** 6 x 1 Gbps SFP (provided with RJ45 transceivers) |  |  |  |
|  | 4 x SFP (1 Gbps) Fiber connection (must provide with SFP SX transceivers) |  |  |  |
|  | 8x SFP+ (10 Gbps) Fiber connection (must provide with SFP+ SR transceivers)  |  |  |  |
|  | The proposed appliances from factory shall be Rack Mountable |  |  |  |
|  | The proposed systems must use dual hot swappable power supplies. |  |  |  |
| 1. **Systems Requirements**
 |
|  | The device shall s minimally (4) functioning virtual domains. |  |  |  |
|  | The Systems must be able to support profiling of the following feature components for each virtual domain: |
|  | Firewall |  |  |  |
|  | Application Firewall |  |  |  |
|  | IPS |  |  |  |
|  | Antivirus |  |  |  |
|  | Web Filtering Settings |  |  |  |
|  | Routing & NAT |  |  |  |
|  | Log & report Configurations |  |  |  |
|  | The proposed Systems shall be able to operate on either Transparent (Bridge \_ Layer2) mode, Route (Layer3) mode or span mode.  |  |  |  |
|  | Must support VPN with at least the below protocols: MD5, SHA-1, SHA-256 authentication, Diffie-Hellman Group 1, Group 2, Group5, Group 14 .etc. . Internet Key Exchange IKE v1, IKE v2 algorithm …etc. , encryption standard 3DES, AES (128, 192 & 256) … etc. |  |  |  |
|  | Supports site-to-site IPSec VPN |  |  |  |
|  | Must support client SSL-VPN remote access for multiple operating systems (Windows, Mac, and Linux) for at least 1000 concurrent remote VPN users. \* required licenses must be included if needed. |  |  |  |
|  | Must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management and SNMPv3 support. |  |  |  |
|  | The device shall be capable of creating at least (10) security interface zones. |  |  |  |
|  | The physical interface shall be capable of link aggregation, otherwise known as the IEEE 802.3ad standard. |  |  |  |
| 1. **Routing**
 |
| **4.1** | The Systems must be able to support routing protocols including (OSPF, static routes, policy based routes ... etc.) |  |  |  |
| 1. **Firewall Requirements**
 |
|  | **The appliance must be able to handle a traffic of at least (10) Gbps of Threat Prevention/Protection Throughput** when all security features enabled (NGFW, Application Control, and IPS ...etc.) |  |  |  |
|  | **The appliance shall be capable of handling at least (2,500,000) concurrent sessions.** |  |  |  |
|  | **The appliance shall be capable of handling at least (180,000) of new sessions per second** |  |  |  |
|  | The definition of a Firewall policy should include Address Object(s) (IP, IP range, Subnet, user) and Service Object(s). |  |  |  |
|  | The firewall policy table shall support both IPv4 and IPV6 for unlimited IP addresses.  |  |  |  |
|  | The proposed Systems shall support the predefined and Customs Service Objects (services/app) |  |  |  |
|  | The proposed NGFW should include: |
|  | Policy based Network Address Translation (dynamic and static NAT) |  |  |  |
|  | Static NAT; one to one address mapping and static NAT groups |  |  |  |
|  | Port Forwarding |  |  |  |
| 1. **User / Device Authentication Requirements**
 |
|  | The proposed Firewall shall be able to support various form of user Authentication methods simultaneously, including: |
|  | Local Database entries |  |  |  |
|  | LDAP server entries |  |  |  |
|  | RADIUS server entries |  |  |  |
|  | Windows AD |  |  |  |
|  | The administrators shall be able to create user groups which are lists of user identities. An identity can be:  |
|  | A local user account (user name and password) stored on the unit |  |  |  |
|  | A user, users group & (OU) defined on a Microsoft Active Directory server |  |  |  |
| 1. **IPS Requirements**
 |
|  | The IPS detection methodologies shall consist of (**Signature** based detection using updated database and **Anomaly** based detection that is based on thresholds). |  |  |  |
|  | Must be Able to prevent DOS and DDOS attacks. |  |  |  |
|  | The proposed Systems shall identify, set threshold and act on network traffic anomalies of statistical anomaly types (Flooding, Scan, Source session limit, Destination session limit) for the TCP, UDP, and ICMP … etc.  |  |  |  |
|  | When a signature is matched, the following configurable actions can be automatically taken: |
|  | Detailed attack logging |  |  |  |
|  | Email alerts |  |  |  |
|  | SNMP traps |  |  |  |
|  | Packet logging |  |  |  |
|  | Pass, block or reset sessions |  |  |  |
|  | Syslog messages  |  |  |  |
| 1. **Threat Protection**
 |
|  | Must support embedded Antivirus, include advanced Malware Prevention, with real time detection. |  |  |  |
|  | Threat Signatures must be updated automatically. |  |  |  |
|  | Support Cloud Sandbox  |  |  |  |
|  | The proposed Systems must able to detect Gray-ware includes adware, downloader, hacker tool, key-logger, RAT and spyware ….etc. . |  |  |  |
|  | The proposed solution should provide malicious DNS signature blocking (ability to alert, and drop) malicious DNS requests. |  |  |  |
|  | Blocks the DNS request for the known botnet C&C domains. |  |  |  |
|  | Inline malware prevention. |  |  |  |
|  | Vulnerability-based protections against exploits and evasive techniques on network and application layers, including port scans, buffer overflows, packet fragmentation, and obfuscation |  |  |  |
| 1. **Web Content Filter Requirements**
 |
|  | The proposed Systems should have integrated Web Content Filtering solution. |  |  |  |
|  | Must contain URL filtering capability based on updatable database that has different categories. |  |  |  |
|  | Must have Blocking/allowing feature based on user, subnet, IP, and time-based Policies. |  |  |  |
|  | Must have force safe search option for all known search sites including Google, Yahoo, and Bing and for both HTTP/HTTPS. |  |  |  |
|  | Must have WEB2 control feature for all known social networks like Facebook, Twitter, google+, etc. |  |  |  |
| 1. **Application Control Requirements**
 |
|  | Must have Application Control feature for popular applications such as Facebook, YouTube, Twitter, Google Play, iTunes, skype, WhatsApp, TeamViewer…etc. and for P2P applications regardless of port/protocol. |  |  |  |
|  | Must be able to classify traffic according to the application based on port number, application signature and behavior. |  |  |  |
|  | Must provide full control for all known proxy avoidance tools (Ultra Surf, Spot Flux, TOR …. etc.). |  |  |  |
|  | The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions. |  |  |  |
| 1. **SSL content scanning and inspection Requirements**
 |
|  | The proposed systems must have the ability to perform SSL Inspection.  |  |  |  |
|  | The proposed Systems shall support SSL and TLS releases such as : SSL 3.0, TLS 1.0, and TLS 1.2 ..etc. . |  |  |  |
|  | The proposed Systems shall support certificate key size of 1024, 2048 bits …etc. . |  |  |  |
|  | The proposed Systems must support Inbound and outbound inspection |  |  |  |
|  | The proposed Systems must be able to perform the following tasks over SSL encrypted traffic: |
| **11.6.1.** |  AV Scanning |  |  |  |
| **11.6.2.** | Web content Filtering |  |  |  |
| **11.6.3.** | IPS |  |  |  |
| 1. **High Availability Requirements**
 |
|  | The proposed Systems must support high availability architecture (Active-Active, Active-Passive) with full synchronization. **\* Active- Passive will be implemented** |  |  |  |
|  | The devices shall support state full session maintenance in the event of a fail-over to a standby unit. |  |  |  |
|  | The devices shall event log, send SNMP traps and send alert email when fail-over occurs. |  |  |  |
|  | High Availability feature must be supported for either Transparent (bridge) mode, Route mode or span mode. |  |  |  |
|  | The proposed Systems shall support interface link monitoring failover (**multiple heartbeat links**). |  |  |  |
|  | The HA solutions should support automated firmware upgrade process that provides minimum downtime. |  |  |  |
| 1. **Dedicated Logging & Reporting Solution Requirements**
 |
| Powerful logging and reporting solution that provides consistent rules in an ever-changing network and threat landscape is required. |
|  | Real time log management, analytics and reporting platform. |  |  |  |
|  | Complete visibility of the entire attack surface and systems status. |  |  |  |
|  | Predefined reports and **custom** generated reports which are manually/automatically generated. |  |  |  |
|  | Support to generate customized reports based on traffic bandwidth, number of sessions per user, URLs, destination, application, specified user, top sources, and top destinations …etc. |  |  |  |
|  | Must have the ability to identify port, protocol (TCP /UDP, source/destination IP address) for all unknown traffic. |  |  |  |
|  | Define output profiles for notifications and deliver reports in flexible viewing formats including PDF, HTML, and CSV..etc. |  |  |  |
|  | Must monitor network, traffic and user's events in **real-time or browse historical logging** for specific events, provides powerful insight into network security threats, performance and user behavior. |  |  |  |
|  | Correlate attacks logs and display top attacks information on various periods of time |  |  |  |
|  | **Hardware Specifications:** |  |  |  |
|  |  | The Required System must Appliance deployment **not** VM or Cloud deployment. |  |  |  |
|  |  | Rack Mountable |  |  |  |
|  |  | Minimum 100 GB/Day of Logs |  |  |  |
|  |  | Capable to store logs for 30 days with **3TB of minimum storage .** |  |  |  |
|  |  | 4x RJ45 GE, **or** 4 x SFP GE Interfaces |  |  |  |

**Part 2**

**Training**

**The cost of the required training in sections (A, B, C) must be presented in detail in the bidder’s offer.**

1. **Site Training:**
	* The offer should include site training for the technical staff of Computer Center.
	* Training must focus on Operation, installation, troubleshooting, Configuration, Management, and Reporting.
2. **Certified Training:**
	* Official Training Program Consists of **Essential (Associate) level**, **Advanced (Professional) level**, **Management and Reporting** Courses for proffered solution.

**Training Conditions for item (B):**

* + **The training programs must contain and focus on the following required topics (configure, install, monitor, management, troubleshooting, analysis, logging and reporting) for the proffered solution.**
	+ The Bidder should provide a training courses that covered required topics. courses description, guidelines, prerequisites and number of days must be included in the offer.
	+ **The trainings programs should be delivered by a vendor authorized training center.**
	+ **Labs access, courses materials and exams vouchers must be covered and must be included in the offer.**
	+ **Bidder must specify the training cost per person, AABU has the right to identify the number of trainees.**
	+ AABU has the right to send trainees individually.
	+ Training schedule must be delivered one month before starting training.
	+ The training programs must cover all training expenses related to course registration fees, original documents, and any other required expenses that may include travelling and transportation expenses, accommodation and living expenses.
1. The bidder most provide **two** subscriptions for the following **eLearnSecurity** courses **ELITE** version:
2. Web Application Penetration Testing (WAPT v3) with eWPTv1 Infinity (No Expiry) exam Voucher.
3. Practical Web Defense (PWD) with eWDP Infinity (No Expiry) exam Voucher.
4. Penetration Testing Professional (PTP V5) with eCPPTv2 Infinity (No Expiry) exam Voucher.

**الشروط الخاصة:**

1. تقدم الأسعار بالدینار الأردني شاملة جمیع أنواع الضرائب وشاملة ضریبة المبیعات ومعفاة من الرسوم الجمركیة.
2. الأسعار تشمل التورید في المواقع التي تحددھا الجامعة
3. الجامعة غیر مقیدة بأقل الأسعار، ولھا الحق في تجزئة العطاء أو إلغائھ كلیاً أو جزئیاً إذا اقتضت مصلحة الجامعة ذلك وفي أي مرحلة من مراحل العطاء، دون أن یكون للمناقصین الحق في المطالبة بأیة خسارة أو ضرر ناتج عن ذلك.
4. تحدید الماركة والمنشأ والصناعة بشكل واضح ودقیق.
5. ضرورة تحدید مدة التسلیم من تاریخ التوقیع على قرار الإحالة، ویفضل أن یكون بأقرب مدة ممكنة
6. یحق للجامعة إلغاء العطاء في أي وقت ودون إبداء الأسباب.
7. تعتبر الشروط العامة للعطاءات لجامعة آل البیت جزء لا یتجزأ من ھذه الشروط.
8. تلتزم الشركة التي یحال علیھا العطاء بتقدیم كفالة حسن تنفیذ بقیمة( 10%) من القیمة الاجمالیة للأحالة.
9. تسري أحكام نظام المشتریات الحكومیة رقم(8) لسنة( 2022) وتعلیمات تنظيم اجراءات المشتريات الحكومية لسنة 2022على ھذا العطاء ولھا صفة الاولویة.
10. مدة التورید ستؤخذ بعین الاعتبار عند الاحالة.
11. أن یكون المتقدم مؤھلاً تجاریاً، ویحمل رخصة مھن وشھادة تسجیل ساریتي المفعول ضمن المجال ویحمل رقما ضریبیا للمنشأة / صاحب المنشأه.
12. الاسعار تشمل التركیب والتشغیل والتدریب وبالتنسیق مع الجھة المعنیة بالجامعة.
13. الأسعار تشمل التورید في الموقع - المفرق / جامعة ال البیت / مركز الحاسوب.
14. الاسعار تشمل تقدیم كتیبات التشغیل لجمیع الاجھزة المحالة وتدریب المھندسین في الجامعة.
15. المواصفات الفنیة للأجھزة والأنظمة تمثل الحد الادنى للمواصفات المطلوبة.

**ضرورة إرفاق ( C.D.) یشتمل على عرض الأسعار، بحیث یتم تعبئة الأسعار على نفس دعوة العطاء إلكترونیاً (موجودة على برنامج word + Excel (نسختین) ضمن صفحة الجامعة الإلكترونیة) والمواصفات الفنیة لكل بند إلكترونیا ً.**