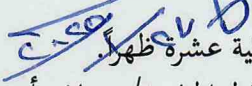


عطاء رقم 8/ل ر/2025

توريد وتركيب وتشغيل أجهزة لشبكة الجامعة والداتا سنتر

السادة يرجى موافاتنا بأسعار المواد المبين تفصيلها بالكشف المرفق المكون من (١٢) صفحة، وتسليمها الى وحدة اللوازم/ دائرة المشتريات في موقع جامعة مؤتة/ الكرك-المجمع الإداري بالظرف المختوم مكتوب عليه اسم المناقصة ورقمها واسم المتعهد ورقم التلفون والفاكس الخاص بالمتعهد على أن يلتزم المتعهد بما يلي:

توقيع رئيس اللجنة:



- ١- آخر موعد لتسليم العروض يوم الاحد تاريخ ٢٣/٢/٢٠٢٥، قبل الساعة الثانية عشرة ظهراً.
- ٢- ثمن نسخة المناقصة (١٢٥) دينار غير مستردة وتشتري عن طريق مكتب ارتباط الجامعة/ عمان، أو عن طريق وحدة اللوازم/ جامعة مؤتة - المجمع الإداري، ويكون اخر موعد لبيع النسخ يوم الاحد تاريخ ٢٣/٢/٢٠٢٥ لغاية الساعة الحادية عشرة صباحاً.
- ٣- ارفاق رخصة المهن وشهادة التسجيل ووصل ثمن النسخة الخاصة بالمتعهد بالعرض.
- ٤- تقديم العرض (نسخة أصلية، نسخة إلكترونية "Excel أو Word").
- ٥- تقديم كفالة دخول للمناقصة بنسبة ٣% من قيمة العرض، وشيك مصدق كحسن تنفيذ بنسبة ١٠% من قيمة الإحالة في حالة تمت الإحالة.
- ٦- تدفع الطوابع القانونية وأية رسوم تترتب على قرار الإحالة خلال ١٠ أيام من تاريخ التبليغ بالإحالة.
- ٧- تقديم الأسعار شامله الضريبة العامة على المبيعات وشاملة الرسوم الجمركية.
- ٨- تفرض غرامة تأخير كما يلي:
 - ١.٠٠٠١ واحد بالآلاف من قيمة اللوازم عن كل يوم تأخير للفترة من ١ يوم إلى ٤٥ يوم.
 - ٢.٠٠٠٢ اثنان بالآلاف من قيمة اللوازم عن كل يوم تأخير للفترة من ٤٦ يوم إلى ٦٠ يوم.
 - ٣.٠٠٠٣ ثلاثة بالآلاف من قيمة اللوازم عن كل يوم تأخير للفترة من ٦٠ فما فوق.
 على أن لا تتجاوز قيمة مجموع الغرامات نسبة ال ١٥% من قيمة اللوازم في قرار الإحالة.
- ٩- عرض الأسعار المقدم من المناقص جزء لا يتجزأ من قرار الإحالة.
- ١٠- المواد المطلوبة قابلة للزيادة أو النقصان بنسبة ٢٥%.
- ١١- صلاحية العرض (٩٠) يوم على الأقل.
- ١٢- يتم فتح العروض المقدمة بعد ربع ساعة من وقت الاغلاق المبين أعلاه.
- ١٣- للجامعة الحق بإلغاء المناقصة دون ذكر الأسباب.
- ١٤- تعتبر شروط نظام المشتريات الحكومية رقم ٨ لعام ٢٠٢٢ وملحقاته والتعليمات الصادرة بموجبه جزء لا يتجزأ من شروط المناقصة وتكون شروطه هي المرجحة إذا تعارض أي منها مع الشروط الواردة أعلاه (علماً بأن شروط النظام المشار اليه أعلاه على موقع الجامعة (العطاءات).

التوقيع:

رقم الهاتف:

اسم المناقص:

التاريخ:

الخلوي:

الختم:

مناقصة رقم ٨/ل/ر/٢٥٠٢٥
توريد وتركيب وتشغيل أجهزة لشبكة الجامعة والداثا سنتر
(Data Center Firewall, Internet Firewall & DDI)

شروط العطاء العامة:-

- جميع البنود في هذا العطاء سيتم توريدها وتركيبها وتشغيلها في حرم جامعة مؤتة الرئيسي.
- يجب توريد جميع الأجهزة المشمولة في هذا العطاء ضمن صناديق مغلقة (Sealed) من الشركة المصنعة.
- على المشاركين في هذا العطاء إرفاق ما يثبت تنفيذهم عدداً من المشاريع المشابهة لهذا العطاء.
- على المشاركين إرفاق السير الفنية للفريق الذي سيتولى عملية تركيب وتشغيل هذا العطاء مع الالتزام بكون الفريق المشارك في تنفيذ العطاء يعمل في المجال التقني وليس الاداري او الاشرافي او المبيعات مع التقيد التام بتقديم عدداً كاف من المهندسين وضمن الشروط العامة الواردة في هذا العطاء.
- من يقع عليه الاختيار يجب عليه القيام بـ التركيب والتشغيل على أتم وجه وبافضل الاساليب التقنية وعلى وجه الخصوص عملية الـ (Configuration) كما يلزمه تقديم الدعم النوعي الكافي و السريع بعد فترة التشغيل واثناء فترة الصيانة والدعم المطلوب على أن الجامعة تحتفظ بحقوقها الكاملة في هذا الجانب ضد أي تقصير يظهر أثناء عمليات (التوريد والتركيب والتشغيل) ولاحقا وبشكل خاص أثناء تقديم الدعم الفني بعد التشغيل.
- يجب على المشاركين في العطاء ذكر فترة التوريد للبنود موضوع العطاء بشكل واضح ودقيق على أن الجامعة تحتفظ بحقوقها في إستثناء العروض التي تحتل فترات توريد طويلة الأمد وإن كانت مطابقة للمواصفات.
- جميع المتقدمين للعطاء مرحب بهم لعمل زيارة ميدانية للاطلاع على واقع الحال، على أنه وفي حال تعارضت أي معلومة وردت في هذا العطاء مع ما قد يحصل عليها من الزيارة الميدانية بشكل مباشر أو غير مباشر؛ فتعتبر المعلومة الواردة في هذا العطاء هي المعلومة المرجعية والمقبولة بشكل رسمي.
- العطاء قابل للتجزئة حسبما ترثنيه اللجنة الفنية وبما يحقق مصلحة الجامعة.

General Information's: -

- The bidder must ensure a successful failover test scenario for the Core, Server and WAN Switches, based on a test checklist of services provided by Mutah.
- All proposed products should be USA, Japan or European-based. A country-of-Brand certificate must be provided.
- The local partner (Bidder) should provide Project team CVs to handle the implementation. Those teams should have *Security Certifications* for the technology proposed in their proposal, with a minimum of *5 certified engineers*.
- Mutah university has the right to interview the *implementation team*.
- The bidder must be:
 - The bidder must be a company that has been registered with the Jordanian Ministry of Industry and Trade for at least **(10) years**, and its registration should be current
 - Authorized certified partner by vendors for all components included in the project.
 - The bidder must have international ISO Certificates. Evidence must be submitted (preferred).
 - An official document of authorization or partnership must be included within the proposal. Otherwise, the offer will be excluded.
 - Familiar with similar projects and have a reference list for similar projects.
- At least one of Mutah University staff must participate in the installation and configuration process.
- Training for Mutah should be provided *during and after* the implementation process.
- Five years warranty and support services on hardware, software, licenses and subscriptions, With NBD replacement.
Optional (3 years).
- The provider of items must be:
 - Authorized reseller for all Components.
 - Familiar with the same projects and have reference list for similar big projects.
- Subcontractors are not accepted without University Approval (*Official letter*).
- All solutions should be built with drawing and documentation.

General terms & conditions: -

- The proposal should include the following:
 - Contract Drafts for support including:
 - Response time for problem call.
 - Response time for problem solving.
 - Response time for solving software/configuration support call.
 - Response time for (hardware/software) failure.
 - Actions that will be taken during (hardware/software) failure.
 - Response time for failed hardware
 - Preventive Maintenance
- BoQ, Prices and comply sheet must be provided, considering the following:
 - Unit prices must **NOT** include any tax, The tax must be added to the total of *each item*.
 - Detailed BoQ for all Items must be part of the technical proposal.
 - A detailed *compliance sheet* must be part of the technical proposal.
 - Prices for training and installation should be separated and clear.
 - All required licenses during warranty time must be included.
- All item's warranty must be supported by the vendor for the required support period, including licenses and warranty for all devices, hardware and software components including any software upgrade, update, security patches and fixes and must support hardware replacement within the next business day.
- During the warranty period, the company should provide all required spare parts free of charge.
- *All connectivity between new devices and all connected devices are bidder responsibility.*
- *Installation, Configuration, labelling, Testing and all needed cabling should be included.*
- Products and all their components (Hardware, Software and Licenses) must **NOT** be *end-of-life, end-of-sale or end of support*.
- Dates of (end-of-life, end-of-sale and end-of-support) for each proposed product and all its components (Hardware, Software and Licenses) must ***NOT be announced yet.***
- The bidder must provide reference sites where similar devices were installed; the reference information must include the device model, date of installation and contact person details.

Lot #1: - (Firewalls)

➤ **Technical Specifications for Data Center Firewalls - Hardware Appliance:**

- The vendor should be recognized as a leader or challenger in the latest Gartner Magic Quadrant report for Network Firewalls.

Part #1: - Data Center Firewalls QTY (2):

Firewall Throughput when (Firewall, App-ID and IPS Services are enabled)	Min 16 Gbps
IPsec VPN throughput for TCP	Min 8 Gbps
Concurrent sessions with App-ID	Min 2.2 million
New sessions per second	Min 150,000
LAN interfaces	<ul style="list-style-type: none"> • Min 8 x 10G SFP+ • Min 8 x 1G Base-T RJ-45
Power & Cooling	<ul style="list-style-type: none"> - Hot-swappable Redundant AC power supplies. - Hot-swappable Redundant fans
High Availability	<ul style="list-style-type: none"> • The Proposed solution Shall Support Active/Passive (Standby), Active/Active (load sharing)
Networking	<ul style="list-style-type: none"> • The Proposed solution Should support both static routing and the following dynamic routing (OSPF, BGP, RIP). • The Proposed solution should support dual IPv4 and IPv6 stacks including application control and inspection. • The Proposed solution should support aggregation of links on all interface ports based on IEEE 802.3ad. • The Proposed solution must support policy-based routing. • The Proposed solution shall support QoS.
Application security	<ul style="list-style-type: none"> • The Proposed solution shall support Application visibility and control.

Firewall Features	<ul style="list-style-type: none"> • The proposed solution should be Data Center firewall with full L7 capabilities. • The Proposed solution shall be able to selectively apply Deep Inspection and IPS. • The Proposed solution shall support integration with Radius and LDAP to enable identity-based rule • Network address translation (NAT) using static IP, dynamic IP, dynamic IP and port (PAT) • Command Line Interface (CLI) • Built-in web interface (GUI)
Intrusion Prevention System	<ul style="list-style-type: none"> • The proposed solution must support SSL traffic inspection to protect from encrypted attacks. • The proposed solution must support the creation of custom attack signatures.
Transceivers	<ul style="list-style-type: none"> • 6 x 10G SR SFP+ Transceivers with 6 x <u>MM Patch cords</u>
Alerting and Reporting	<ul style="list-style-type: none"> • DC FW should have an on-box reporting and logging facility. If the vendor doesn't have it, then they should propose an external reporting/log analysis engine. • The proposed firewall shall support logging and reporting mechanism to generate reports • The DC FW must be able to send alerts to external targets Syslog Server. • The system must support SNMP & SNMP Traps. • 900 GB SSD Storage (built-in on-box or through external server).
Required Licenses	<ul style="list-style-type: none"> • <u>Five years</u> warranty and support services 24x7 with IPS and Application Control subscription. With NBD replacement (Optional Three Years).

➤ **Technical Specifications for Internet Firewalls - Hardware Appliance:**

- The vendor should be recognized as a **leader or challenger** in the latest Gartner Magic Quadrant report for Enterprise Firewalls

Part #2: -Internet Firewalls QTY (2):

<p>LAN interfaces</p>	<ul style="list-style-type: none"> • Min 8 x 1G Base-T RJ-45 • 8 x 1/10G SFP+ • RJ-45 console port • USB port.
<p>Required licenses</p>	<p>NGFW must be equipped with the required licenses for Five Years to enable the following advanced security capabilities, With NBD replacement.</p> <ul style="list-style-type: none"> • Advanced Threat Prevention (NGIPS, Anti-Malware {cloud-based sandboxing} and Anti-Virus). • Advanced URL Filtering • Warranty and support services. <p>Optional Three Years</p>
<p>Transceivers</p>	<ul style="list-style-type: none"> • 6 x 10G SR SFP+ Transceivers with 6 x <u>MM Patch cords</u>
<p>The NGFW must support</p>	<ul style="list-style-type: none"> • The NGFW must support context-based policies to adopt a Zero Trust Model. The NGFW must support explicit proxy and transparent proxy method. • The NGFW must be able to acquire User Identities from LDAP, Captive Portal, VPN, NACs (XML or API), Syslog. • The NGFW must offer full and unfettered open API Support. • The NGFW must support the ability to regroup user/s based on security events relating to that user. • The NGFW must provide scalable clustering and multi-DC clustering. • The NGFW must be able to enable any new security offering without impacting the performance of the traffic flowing through it. • The NGFW must support App-ID or Application visibility control capability to get visibility into the applications on the Mutah network and learn how they work their behavioral characteristics and their relative risk.

<p>Architecture, Physical & Performance Specifications</p>	<ul style="list-style-type: none"> • Active/Standby & Active/Active High availability support • Minimum of 10 Gbps of Layer 7 “Application Mix” firewall throughput • Minimum of 9 Gbps of Threat Prevention “Application Mix” throughput with services of IPS, Antivirus & Advanced Anti-Malware. • Minimum of 5 Gbps of IPsec VPN throughput • Minimum of 1.4 million concurrent sessions • Minimum of 120,000 New sessions per second • 480 GB SSD Storage • Hot-swappable Redundant AC power supplies. • Redundant fans.
<p>Centralized management</p>	<p>Centralized configuration, logging, monitoring, and reporting are performed on-box or through external management center.</p>
<p>Firewall Decryption & Tunnel Inspection features:</p>	<ul style="list-style-type: none"> • SSL decryption policies covering SSL encapsulated protocols such as HTTP(S)
<p>Firewall Threat Prevention (IPS)</p>	<p><u>Vulnerability Protection (IPS) against:</u></p> <ul style="list-style-type: none"> • Block viruses, spyware, malware and network worms and vulnerability exploits within content of application content. • File blocking. • Data Leakage Prevention (scan for keywords and credit card numbers) • Port Independent Protocol Inspection
<p>Firewall other Features</p>	<ul style="list-style-type: none"> • IP version 4 and version 6 support • Network address translation (NAT) using static IP, dynamic IP, dynamic IP and port (PAT) • DNS Proxy support • LACP and Aggregate interfaces (802.3ad) support • High-Availability link & path monitoring support • Remote user VPN agent for Windows, MAC, Linux, Chrome, IOS, and Android • Command Line Interface (CLI) • Built-in web interface (GUI) • Interactive graphical summaries around the applications, users, URLs, threats, and content traversing the network

Professional Training (QTY: 2 Seat): - (Optional)

- Must be conducted for a minimum of two persons, prior to the deployment of a specialized training center.
- Training for the Security solution provided (Specialist/Advanced Training).
- The instructor must be professional for the product he will train (not necessarily certified instructor).
- All training material (Hard and Soft Colored Copy) for the courses provided must be original and provided on the first day of training.

Lot #2: - (DDI)

DHCP & DNS Solutions

Solution Brief:

Mutah University is looking to implement a secure DDI solution to secure its core network services from evolving cybersecurity and zero-day threats, The solution should protect Mutah University users and services from emerging threats at the cyberattack preparation stage at the DNS level. Additionally, it will represent a foundational visibility and cybersecurity layer in the Mutah University network. The DNS firewalling and analytics will protect against DNS tunneling, and data exfiltration/infiltration threats and stop C2 callbacks and malicious communication channels at the DNS level. The solution will be used to offer internal authoritative DNS/DHCP for users connected to the network.

✦ Solution Requirements for Secure DDI:

- The proposed solution should support internal secure DNS, DHCP, IPAM, NTP, TFTP services, and VLAN, VRF repositories.
- The solution should include a dedicated internal secure DNS layer consisting of two appliances.
- The solution should include a dedicated centralized management, IPAM, DHCP, and network discovery layer consisting of two appliances.
- The solution should support IPAM and network discovery for L2/L3 Network devices with centralized management.
- The DHCP should be protected against Storm/Starvation attacks.
- The proposed solution should include reporting and analytics functions providing default reports (Most requested domains, Top clients, Top queries returning NXDOMAIN, Top queries returning SERVFAIL,....).
- The proposed solution should be available as hardware appliances independent from other solutions (Preferred).
- The proposed solution should support being deployed as virtual appliances on VMware and Hyper.
 - All proposed components of the active services including DNS, DHCP, and centralized management should support high availability.

- The proposed solution should include a DNS firewall from the same technology vendor.
- The DNS solution should be protected against Zero-day Vulnerability on the BIND engine.
- The proposed DDI solution should offer flexible licenses that can be moved to/from HW platforms to/from virtual-based platforms and vice versa if needed.
- The proposed solution should support protection against the following DNS threats:
 - DNSBomb attack.
 - DNS DoS and DNS amplification attacks.
 - NXDOMAIN and SERVFAIL attacks.
 - DGA and Random subdomain attacks.
 - Sloth domain attack.
 - Phantom domain attack.
 - Water Torture attacks.
 - Pulsar attacks.
 - Zero-day Vulnerability and DNS-Based Exploits.
 - DNS tunneling and Data Exfiltration.
 - Protocol Anomalies.
 - DNS-Based Malware.
 - DNS Cache Poisoning.
 - DNS phishing.
 - Man in the middle and Kaminsky DNS Vulnerability.
- Support of the DNS records below:-
 - A
 - AAAA
 - NS
 - MX
 - TXT
 - SOA
 - CNAME
 - SRV
 - DNSKEY
 - NSEC3PARAM

- The proposed DNS solution should offer support for DNSSEC validation.
- The proposed solution should be offered by a technology vendor/manufacturer that can support Threat Intelligence from the same vendor for DNS-based Firewalling.
- The proposed solution should support protecting remote users.
- The proposed Security Solution should activate the right countermeasure on the source IP address of the attack.
- The proposed solution provides DNS behavioral analysis and DNS firewall on the same DNS appliance.
- The proposed solution should be capable of integrating with 3rd party security ecosystems from NGFWs and SIEM solutions.
- The proposed Security Solutions should control IoT (or Cameras for example) access to infrastructure or the Internet via an Allow or deny list. Only the destinations allowed will be answered and the other queries will be dropped.
- The solution should provide a Threat Research Portal that helps analysts with on-demand access to threat severity.
- The proposed solution should support integration with other solutions through APIs.
- The proposed solution should allow the management of DNS/DHCP servers from the architectural level instead of managing server by server.
- The delegation should be granular and role-based with an unlimited number of groups (RBAC):
such feature will identify the following:
 - 1- The users or group of users who have access to the Platform.
 - 2- The resources which they must control.
 - 3- The class of resources that the users are authorized to use.
 - 4- The type of control that they have.
- The solution should support integrating with AD/LDAP, RADIUS, and OpenID, for external authentication.
- The IPAM should be able to interface with DNS and DHCP, making the IPAM the cornerstone tool in the provisioning.
- The solution should embed workflow for streamlining Request Management processes.
- The proposed solution should offer a Holistic global search (including filters on metadata)
- The proposed Solution should support integration with any SIEM solution that complies with the Standard Syslog format (e.g., Graylog, Splunk, ArcSight,..).

Subscription and Support Requirements

- Proposed solution must be introduced for two options (Five years & Three Years) about subscription license & support for DDI and DNS Security
- Annual Renewal price to be provided after the free warranty period.

Professional Training for LOT#2 (QTY: 2 Seat): - (Optional)

- Must be conducted for a minimum of one person prior to the deployment (in training center or online).
- The instructor must be professional for the product he will train (not necessarily certified instructor).