دائرة اللوازم والمشتريات

عطاء رقم T23-2024.25

Web Application Firewall System (WAF)

2024-2025

عطاء Web Application Firewall System (WAF)

وثائق العطاء:

أ- الجزء الأول:

(1) دعوة العطاء

(2) الشروط والتعليمات التنظيمية للعطاء

(3) طريقة الدفع

ب- الجزء الثاني:

(1) جدول الكميات والمواصفات الفنية

الجزء الأول (1)

إعلان طرح عطاء رقم T23-2024.25

Web Application Firewall System (WAF)

تدعو الجامعة العربية الأمريكية الشركات المختصة الى المشاركة في العطاء المذكور أعلاه.
يمكن الاستفسار أو الحصول على وثائق العطاء من دائرة اللوازم والمشتريات في الجامعة/ مبنى الدوائر الإدارية الطابق الثاني، هاتف- 2418888 04- تحويلة 1488 فاكس 2510972 04 بريد الكتروني pnp@aaup.edu
مقابل مبلغ غير مسترد مقداره (50 دولار) تدفع في إحدى البنوك المعتمدة وذلك اعتباراً من
يوم (الخميس) الموافق 2025/5/1

ملاحظات :

1. تقديم عرضين: فني ومالي، وسيتم دراسة العروض فنياً ومالياً لاختيار العرض المناسب.
2. آخر موعد لتسليم العطاءات هو في تمام الساعة الثانية من يوم (الخميس) 2025/5/15 ولنفس المكان.
3. يجب تقديم كفالة دخول عطاء 5% من قيمة العطاء على شكل كفالة بنكية أو شيك بنكي مصدق لصالح الجامعة العربية الأمريكية .
4. الأسعار (بالدولار) وتشمل جميع الضرائب بما فيها ضريبة القيمة المضافة وعلى المورد تقديم الفواتير الضريبية وشهادة خصم المصدر.
5. الجامعة غير ملزمة بأقل الأسعار وبدون إبداء الأسباب.
6. رسوم الاعلان على من يرسو عليه العطاء.
7. بإمكانكم الاطلاع على النظام الداخلي لدائرة اللوازم والمشتريات من خلال زيارة صفحة الجامعة العربية الامريكية على الانترنت. www.aaup.edu

(2) الشروط والتعليمات التنظيمية للعطاء

1. على جميع المشاركين في العطاء الالتزام التام بهذه الشروط والتعليمات، وهي تعتبر جزءاً لا يتجزأ من أي أمر شراء أو عقد يبرم مع المشارك الفائز ما لم ينص صراحة على خلاف ذلك في أمر الشراء أو العقد.
2. في هذه الشروط والتعليمات يرمز إلى "الجامعة العربية الامريكية بالاختصار (AAUP).
3. يجب أن تكون الشركة المتقدمة للعطاء مسجلة رسمياً ومشتغلاً مرخصاً.
4. **تقدم الأسعار (بالدولار) شاملاً لجميع الضرائب** بما في ذلك ضريبة القيمة المضافة (VAT).
5. يلتزم المشارك الفائز بتقديم شهادات خصم المصدر والفواتير الضريبية اللازمة وأية مستندات قانونية أخرى تغطي عملية الشراء.
6. يجب أن تشتمل الأسعار على جميع المصاريف المطلوبة من النقل والتركيب والتشغيل والفحص **والصيانة والتدريب** في المواقع المحددة في جدول المواصفات والكميات المرفق.
7. يجب أن تكون الأسعار المقدمة سارية المفعول لمدة لا تقل عن (90) يوماً من تاريخ تقديم العرض.
8. على المشارك الفائز تقديم كفالة حسن تنفيذ خلال أسبوع من تاريخ الاتفاقية بحيث تعادل (10%) من قيمة الاتفاقية على شكل كفالة بنكية صادرة عن إحدى البنوك العاملة في فلسطين أو شيك مصدق صادر لصالح "الجامعة العربية الامريكية".
9. إذا تخلف المناقص الفائز عن تقديم كفالة حسن التنفيذ عن الموعد المحدد في البند السابق فإنه يحق لـ (AAUP) إلغاء الإحالة.
10. إذا تخلف المناقص الفائز عن التوقيع على عقد التنفيذ و تسليم الكفالات والتأمينات المطلوبه منه خلال أسبوع من تاريخ قرار الاحالة، يعتبر مستنكفا عن تنفيذ العطاء ويصادر مبلغ الكفالة أو التأمين دخول العطاء بالاضافة الى ذلك يتحمل فرق السعر و/أو اي أضرار أخرى قد تلحق بالجامعة نتيجة استنكافه ويحرم من لمشاركة في عطاءات الجامعة لمدة عام.
11. اذا تخلف المناقص الفائز عن تنفيذ العطاء الذي احيل عليه او خالف شرطا من شروط العقد يحق للجامعة مصادرة كفالة دخول العطاء أو حسن التنفيذ أو جزء منها وتنفيذ العطاء مباشرة من الجامعة أو اية جهة تراها مناسبة بالاسعار والشروط والطريقة المناسبة ويتحمل المناقص أي فروقات بالاسعار مضاف اليها 15% من اجمالي قيمة العطاء.
12. يتحمل المناقص المتخلف دفع تعويض بدل اي عطل او ضرر قد يلحق بالجامعة نتيجة لذلك.

13. تعاد كفالة حسن التنفيذ بعد استكمال التوريد وجميع شروط العقد أو أوامر الشراء وبموجب الوثائق الأصولية اللازمة للاستلام.
14. على المشاركين في العطاء ارفاق كتالوجات عن المنتج.
15. يلتزم من يرسو عليه العطاء بدفع غرامة تأخير بواقع (0.1%) عن كل يوم تأخير من قيمة الأعمال المنجزة عن الوقت المحدد في الاتفاقية، ويتم احتساب هذه الغرامات من الدفعات المستحقة له أو من كفالة حسن التنفيذ.
16. يحق لـ (AAUP) إلغاء العطاء دون إبداء الأسباب كما أن (AAUP) غير ملزمة بإحالة العطاء على أقل العروض سعراً دون إبداء الأسباب. ولها أن ترفض كل أو بعض العروض المقدمة لها دون أن يكون لأي من المشاركين الحق في الرجوع إليها بأي خسارة أو ضرر ناجم عن تقديم عرضه ولا يترتب على (AAUP) أي التزامات مادية أو غير مادية مقابل ذلك، كما يحق ل (AAUP) تجزئة العطاء بما تراه مناسبا ودون ابداء أسباب.
17. يلتزم من يرسو عليه العطاء بتقديم كفالة بنكية (صيانة) بقيمة (5%) من قيمة الأعمال المنجزة صالحة لمدة عام من تاريخ تسليم الأعمال.
18. على المشارك في العطاء تقديم عرضه على أساس المواصفات الفنية االمبينة في وثائق العطاء وبموجب الكميات المحددة في جدول الكميات المرفق.
19. لا يجوز للمشارك في العطاء أن يتنازل لأي طرف آخر عن كل أو جزء من أمر الشراء دون الحصول على إذن خطي من (AAUP) مع الاحتفاظ بكامل حقوق (AAUP) وفقاً لشروط أمر الشراء.
20. عند دراسة العروض يؤخذ بعين الاعتبار كفاءة المناقص من الناحيتين المالية والفنية وقدرته على الوفاء بالتزامات العطاء وخبرته في تقديم اللوازم المطلوبة والسمعة التجارية والتسهيلات التي يقدمها ويجوز استبعاد عرضه لنقص كل أو بعض هذه المتطلبات.
21. لا تقبل العروض أو التعديلات التي ترد بعد التاريخ والموعد المحدد كآخر موعد لتقديم العروض.
22. يجب تعبئة جداول المواصفات المرفقة و لن ينظر بأي عرض لا يلتزم بتعبئة الجداول.

ملاحظات

- **يسمح بتقديم عرضين اثنين فقط كحد اقصى لكل بند.**
- **يجب تقديم عرضي الاسعار الفني والمالي بنسختين: الأولى ورقية، والأخرى الكترونية (محوسبة).**
- **تقديم العرضين المالي والفني الورقيين بالظرف المختوم، مع ضرورة وضع ختم الشركة والتوقيع على كل الصفحات (للعرض المالي بالذات).**
- **قد تكون المواصفات مأخوذة من منتجات وعلامات تجارية معروفة ولكنها ليست إلزامية.**

(3)

طريقـــة الدفـــــع

خلال (90) يوماً من التوريد والقبول والاستلام النهائي، مقابل تقديم الكفالات المطلوبة.

الجـزء الثانـــي

1. جـــــدول الكميـــــات والمواصفات الفنية

No.	Product	Qty	Unit Price USD	Total Price USD
	Web Application Firewall System (WAF)	1		
Total				

في حالة وجود استفسار يرجى تزويدنا بها من خلال البريد الالكتروني للرد عليها pnp@aaup.edu

1 WAF (Web Application Firewall) TENDER

Contents

Request for Proposal (TENDER) - General Requirements and Technical Specifications

1-1 General Requirements

1. The proposed solution must meet all specifications outlined in the 'Mandatory Requirements' section.
2. The solution should support both hardware-based and virtualized deployment options.
3. The vendor must not be currently blacklisted by any government agency or public sector organization.
4. The solution should be recognized by industry-standard benchmarks such as Gartner Magic Quadrant, Forrester Wave, OWASP, MITRE ATT&CK Evaluations, CyberRatings, or equivalent certifications.
5. The solution provider should have been listed in the Gartner Magic Quadrant for "Web Application Firewalls" for the past three years.
6. The vendor should have implemented similar solutions in the past two years in comparable environments.
7. The vendor must have a local support presence or an established partner network.
8. The solution should provide protection against common web threats, including those identified in the latest OWASP Top 10.
9. The solution must incorporate artificial intelligence (AI) and machine learning (ML) techniques for enhanced security.
10. Vendors must be prepared to provide a product demonstration and proof-of-concept (PoC) upon request.
11. Official in-person overseas training for two designated team members responsible for security.

1-2 Technical Mandatory Requirements

1-2-1 1. General Architecture

- The solution should support multiple deployment modes, including Inline Transparent, Transparent Proxy, Reverse Proxy, Full Proxy, and Non-Inline Sniffing.
- Must support both Active-Active and Active-Standby configurations.
- Should be a dedicated platform-based solution.
- Should align with a Zero Trust security model.
- Should provide predefined security policies for common applications such as content management systems, learning platforms, and cloud-based services.

1-2-2 2. Platform Requirements

- Must support 10/100/1000 Ethernet ports and SFP+ slots for 10G interfaces.
- Should include a dedicated management port.
- Should provide a redundant (hot-swappable) dual power supply.
- Should offer at least 1TB of internal storage.
- Must support a minimum throughput of 1Gbps.

1-2-3 3. Performance Requirements

- Should effectively handle HTTP and HTTPS transactions for public applications and e-services.
- Must be scalable to accommodate future expansion.
- Minimum throughput: HTTP 750Mbps / HTTPS 1Gbps.
- Concurrent connections: HTTP 700,000 CPS / HTTPS 100,000 CPS.
- Should include SSL re-encryption and acceleration with a minimum 2048-bit encryption standard.

1-2-4 4. Web Application Firewall (WAF) Features

- Protection against web protocol threats and network-based attacks while ensuring legitimate traffic is not disrupted.
- Support for Positive, Negative, and Hybrid Security Models.
- Auto-learning capabilities with an option for manual configuration.
- Signature-based protection against:
  - Cross-site scripting (XSS)
  - DoS/DDoS attacks (Layer 4 & Layer 7)
  - SQL Injection, LDAP, and XPath Injection
  - Brute force attacks
  - Known exploits and malware
  - Unauthorized data access and leakage
- Protection against sensitive data leaks, including prevention of:
  - PHP information disclosures
  - Directory listings and source code exposure
  - SQL error leaks and HTTP header vulnerabilities
- Ability to enforce geo-location-based access control.
- Implementation of anti-defacement features, including real-time monitoring and restoration capabilities.
- Compliance with HTTP RFC standards and enforcement of business logic rules.

1-2-5 5. Application Delivery Features

- Load balancing capabilities with support for:
  - Round Robin
  - Weighted Round Robin
  - Least Connection
- Session persistency options, including:
  - Persistent IP, Cookie-based persistency
  - Support for ASP, PHP, and JSP session IDs
- Connection draining mode for seamless server maintenance.
- Health checks for backend servers with administrator alerts.

1-2-6 6. Policy Migration from FortiWeb 1000E

- The proposed solution must facilitate the seamless migration of existing FortiWeb 1000E policies, Rules, and ML if possible.
- The current deployment includes around 40 server policies, which must be successfully transferred and optimized for the new platform.

- The migration process should include:
  - Policy mapping and transformation assistance
  - Automated or semi-automated migration tools to streamline the process
  - Validation and testing of migrated policies to ensure security effectiveness and functionality
  - Dedicated technical support throughout the transition period

1-2-7 7. Updating Policies

- Support for manual and online signature updates.
- Updates should not cause system downtime.
- Predefined security policies categorized by risk level (e.g., Alert Only, Medium Security, High Security).
- Signature groups should be logically structured and easily searchable.

1-2-8 8. Administration, Monitoring, and Reporting

- The solution should offer:
  - Local and remote logging capabilities.
  - Integration with external logging systems (e.g., Syslog, SNMP).
  - Granular attack logs, including raw packet data, source/destination details, and parameter analysis.
  - Aggregated logging per day and per attack type.
  - Graphical user interface (GUI) with attack visualizations, top threats, and geolocation data.
  - Customizable reports with export options (Excel, PDF, etc.).
  - Compliance reporting for standards such as PCI DSS.
  - Incident correlation for threat prioritization.

1-2-9 9. Support and Training

Support:

A. Vendors should provide details on their professional service offerings and support structure.
B. Clear SLA should be provided.
C. Support should be available 24/7/365.
D. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response.

Training:

E. **Knowledge Transfer:** The bidder must conduct mandatory knowledge transfer sessions for the IT team covering storage administration, expansion, and troubleshooting. This should be considered part of the implementation service and not as formal training.
F. **Training Option:** The bidder should provide an official vendor-certified training program with a per-seat pricing model. The training must be:

o In-person and conducted outside the country (offshore).
o Exclusive of accommodation, travel, or per diem expenses.

Other capabilities

G. Knowledge transfer for any new products and updates in regular bases
H. Please set out any additional capabilities or other services you provide beyond the scope of those contained in this request which may be of interest to AAUP.

1-2-10 10. Total Cost

- All pricing must be inclusive of VAT and clearly itemized.
- The Financial proposals should differentiate between the costs (One-Time payments / Subscriptions) of hardware, software, services, training, and optional add-ons.

1-2-11 11. Evaluation Criteria

- Compliance with technical specifications
- Plan for Successfully Migrating the Current FortiWeb 1000E.
- Total cost (including warranty and support)
- Ability to protect AAUP web services including Moodle, Drupal, HR, and Custom Developed Applications and APIs
- Expandability and vendor-neutral architecture
- Lead time and implementation plan
- Support service levels (SLA)
- Payment flexibility
- Proposed training