دائرة اللوازم والمشتريات

عطاء رقم (T35 /2020.21)

WAF (Web Application Firewall)

2020-2021

عطاء WAF (Web Application Firewall)

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 (35/2020.21

WAF (Web Application Firewall)

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 أمريكي تدفع في إحدى البنوك المعتمدة وذلك اعتباراً من يوم (الاحد) الموافق 8/8/2021

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(الاحد) 22/8/2021 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 (دولار) 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

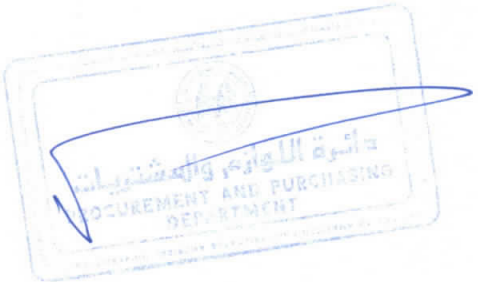
دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

(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 (دولار) 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 قرارالاحالة، 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.

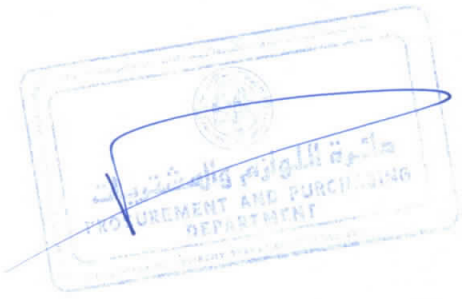
- **ويسمح بتقديم عرضين اثنين فقط كحد اقصى لكل بند.**
- **يجب تقديم عرضي الاسعار الفني والمالي بنسختين: الأولى ورقية، والأخرى الكترونية (محوسبة).**
- **تقديم العرضين المالي والفني الورقيين بالظرف المختوم، مع ضرورة وضع ختم الشركة والتوقيع على كل الصفحات (للعرض المالي بالذات)**



(3)

طريقـــة الدفـــــع

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



الجـزء الثانـــي

1. جـــــدول الكميـــــات والمواصفات الفنية
WAF (Web Application Firewall)

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

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

WAF (Web Application Firewall) RFP

RFP General Requirements

1. The OEM Solution must possess all the required specifications mentioned in Part 'Mandatory Requirements'.
2. The OEM must have hardware and VM based solutions to support the requirement.
3. The OEM should not be currently blacklisted by any Govt. dept. /Public Sector Unit.
4. The OEM must be Gartner's quadrant, NSS Labs, or any equivalent Test report & certifications.
5. The OEM should be in the 5. Gartner Magic Quadrant for "Web Application Firewalls" for last 3 years.
6. The OEM should have deployed similar type of solution within the last 2 years in Palestine.
7. The OEM must have support office in Palestine.
8. Solution should protect against common threats such as those identified in the OWASP top 10 latest release.
9. The proposed solution must use AI (Artificial intelligence) and machine learning techniques.
10. OEM must be able to provide a Presentation and POC on request.

Technical Mandatory Requirements

The following is the list of the mandatory requirements that will form a part of the Web Application Firewall.

1. General Introduction:

A. Product Architecture: - The solution should support different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy, Full Proxy and Non-Inline Sniffing. Describe each deployment mode.
B. Solution should support Active-Active and Active-Standby mode.
C. Should be Dedicated Platform based solution.
D. Should support Zero Trust approach.
E. Should support predefined Policies for the common web applications, like: Drupal, Moodle, office 365, ...etc.

2. Platform: (Minimum Requirements)

A. Ports: Should support 10/100/1000 Ethernet Ports, SFP + Slots for 10G Interface
B. Should have Management Port

C. Should have Dual Power Supply (Hot Swappable)
D. At least 1 TB internal Storage
E. Minimum Throughput 1 Gbps

3. Performance: (Minimum Requirements)

a. HTTP and HTTPS
    i. Can Cover Transactions for HTTP and HTTPS sessions for All public applications and eservices, that will include 40 public applications and eservices that serve 15,000 Student and staff,
    ii. Solution should be scalable for any future growth.
    iii. Throughput HTTP/ 750Mbps HTTPS/ 1Gbps
    iv. Concurrent Connections HTTP/ 700,000 CPS HTTPS/ 100,000 CPS
b. SSL Re-encryption and SSL acceleration required
c. Encryption: 2048 bits SSL

4. WAF Features:

A. Solution should be able to protect against Web Protocols and other network attack targets while delivering uninterrupted service for legitimate connections.
B. Should support Positive, Negative and Hybrid Security Model.
C. Should have auto learning protection and easy manual deployment controls. Auto Learning and Auto Protection should co-exist.
D. Should have signature based Negative Security Model, which should protect against:
    1. Cross site scripting (XSS)
    2. Layer 4 & Layer 7 DoS and DDoS
    3. SQL Injection
    4. SQL LDAP and XPath Injections
    5. Generic Attacks
    6. Brute Force
    7. Trojans
    8. Known Exploits
    9. Information Disclosure
    10. Form Field Parameter Tampering and HPP tampering
    11. Session high jacking
    12. Cookie manipulation and poisoning
    13. Buffer Overflows
    14. Bad Robot
    15. Credit Card Detection
    16. Protection against known database and Web server vulnerabilities
    17. Forceful browsing
    18. Broken access control
    19. Request smuggling

E. Should protect against Sensitive Data Leakage protection using response scrub. It should have minimum features like
    1. PHP information leakages
    2. IIS default location
    3. ASP / JSP source code leakages
    4. SQL error leakages
    5. Directory Listing
    6. HTTP Header Leakage
    7. Access to admin folder
    8. Slowloris and other low & slow availability attacks
    9. Prevention of Error messages leakage
F. Should support Policy evasion Detection
G. Should be able to do manipulation of invalidated input
H. Should protect against Remote File inclusion attacks
I. Should protect against request for restricted objects and file types
J. Should protect against Directory/ Path Traversal
K. Should protect against known worms and vulnerabilities
L. Should be able to implement geo-location policies to restrict access
M. Should prevent OS and web server fingerprinting
N. WAF should support
    1. Schema validation
    2. Parser Protection (XMS Bombs)
    3. XPATH injection
    4. RSS/ Atom feed injection
    5. ICAP protocol
O. Should provide XML filtering and validation
P. Should protect from low reputation source from known bot, malicious source, anonymous proxy, known scanners, Windows exploits
Q. Anti-DoS solution
    1. The solution should offer Layer 7 DDOS capabilities
    2. The application layer detection should support:
    3. HTTP Request limit per source
    4. TCP Connections using same cookie
    5. HTTP requests using the same cookie
    6. A challenge response mechanism which will be fully transparent for the end-user
R. Anti-Web Defacement
    1. Solution should have the ability to prevent, detect and restore web defacement.
    2. Solution should copy the content of the webserver to its own hard drive and compare on a definable time schedule if files have been changed on the webserver
    3. Optionally it should be possible to restore the changed files
    4. Multiple protocols should be supported (FTP/SSH/Windows File Share) in order to maximize compatibility with the target server platform.
S. HTTP RFC Compliance validation
T. Solution should have the option to verify the HTTP RFC standards, The following objects need to be checked and enforced:

1. Illegal Host Name
2. Illegal HTTP Version
3. Illegal HTTP Request Method
4. Content Length
5. Body Length
6. Header Length
7. Header Line Length
8. Number of Header Lines in Request
9. Total URL and Body Parameters Length
10. Number of URL Parameters
11. Number of Cookies in Request
12. Number of ranges in Range Header
13. Malformed Request
14. Application Business Logic Enforcement
    - The solution should be capable of enforcing start pages
    - The solution should be capable of enforcing application logic by defining a set of page access rules
    - Appropriate page access methods should be learned and enforceable by the solution
    - Required parameters on a given URL page should be learned and enforceable by the solution
    - Solution should be able to track the use of cookies on a URL page-by-page granularity

U. Should provide SMTP and FTP security, viral attacks, directory harvesting

V. Application Business Logic Enforcement
   1. The solution should be capable of enforcing start pages
   2. The solution should be capable of enforcing application logic by defining a set of page access rules
   3. Appropriate page access methods should be learned and enforceable by the solution
   4. Required parameters on a given URL page should be learned and enforceable by the solution
   5. Solution should be able to track the use of cookies on a URL page-by-page granularity

5. Application Delivery Features

Load balancing

1. The solution should be capable of load balancing the protected traffic to multiple servers
2. The following algorithms should be supported
   2.1. Round Robin
   2.2. Weighted Round Robin
   2.3. Least Connection
3. The solution should have configurable persistency features to maintain sessions to the load balanced backend servers.

4. The solution should be capable of supporting the following persistency features:
   4.1. Persistent IP
   4.2. Persistent Cookie
   4.3. Insert Cookie
   4.4. ASP Session ID
   4.5. PHP Session ID
   4.6. JSP Session ID
5. The solution should support a connection draining mode in order to allow maintenance of a protected server without disrupting the client experience with the application.
6. The solution should be capable of implementing health-checks for your protected servers for the purpose of load balancing pool removal and administrator notification. This feature should work on both load-balanced and non-load-balanced servers if desired.

6. Updating Policy

F. Should support manual as well as online updating of signatures
G. Signature updating should not cause any downtime
H. Default policies should be available in various classifications, Alert Only, Medium Security, High Security
I. Signatures should be grouped in logical, searchable dictionaries.

7. Device Administration, Monitoring and Reporting

a. Logging and Reporting
   A. The solution should be able to locally store event (audit) information.
   B. The solution should be able to locally store alert information.
   C. The solution should be able to locally store traffic information.
   D. The solution should be able to send all log types above to an external syslog server or SNMP
   E. The alert information should contain at least the following information:
      a. Source to Destination connection information
      b. Extensive packet header information
      c. Raw and Hex body presentation for POST parameters
      d. Full Parameter view
      e. Highlighting the attack in the attack log
      f. With cookie alerts show the alerted cookie and changed values
      g. The solution should aggregate logging per day and per attack type
      h. The log should show both original encoding and decoded values for analysis
   F. Log should be able to provide top attacks, top source and countries of attacks in GUI
   G. Should be able to create customized reports
   H. Should be able to provide PCI DSS compliance and reporting
   I. Should be able to group incidents with violation correlation
b. Data Analytics
   1. The solution should have a dashboard for data analytics in which you can see:

1.1.1. Can create custom reports filters for hits, attacks, Data, etc. based on country, application, IP, etc.
1.1.2. Exportable reports to Excel, PDF, etc.
1.1.3. Clickable view of the various attacks per website
1.1.4. Zoom-able world map with color coding of attacks

c. Blocked IP's
   1. The solution should have a view of all blocked IP addresses and the blocked time period.
   2. From the above view it should be possible to release the blocked IP addresses.
   3. Should provide HTTPS and SSH interface for management
   4. Should have multiple config version option on the appliance

8. Support and Training

F. The responding company will describe the professional services structure for the proposing vendor
G. Support should be available 24/7/365 according to follow the sun principle
H. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response
I. Official training for AAUP responsible team and security member.