الهيئــة المستقلــة للانتخـــــاب

منطقة تلاع العلي/ شارع اسماعيل حجازي / بجانب ديوان المحاسبة
ص.ب (375) / (11953) عمان الاردن
تليفون (9626 5501111)

لجنة العطاءات الخاصة:

اسم دعوة العطاء :

Gateway Firewalls

رقم دعوة العطاء : (02/2021)

وتتضمن:

اولاً: مقدمة

ثانياً: الشروط المرجعية والخاصة

- نموذج كفالة حُسن التنفيذ
- نموذج جدول مواد العطاء
- نموذج كفالة دخول العطاء
- نموذج تعهد شخصي.
- ملحق رقم (1) المواصفات الفنية.

اولاً: مقدمة

تسعى الهيئة المستقلة للانتخاب لشراء خدمة ال Gateway Firewalls

وفقاً للمواصفات والشروط الخاصة والعامة المرفقة.

ونظـرا لخبـرتكم فـي هـذا المجـال فـان الهيئـة تـدعوكم وفـي حـال رغبـتكم بتنفيـذ الأعمـال المطلوبـة والمحـددة بالشـروط المرجعيـة المرفقـة، التكـرم بتقـديم عرضـكم الفنـي والمـالي وذلـك في موعد أقصاه الساعة الثانية من عصر يوم الاربعاء الموافق 2021/06/09.

ثانياً: الشـــــروط الخاصـــــة

إضافة إلى الالتزام بالشروط العامة الواردة في نظام اللوازم والأشغال للهيئة المستقلة للانتخاب رقم (41) لعام 2012 النافذ وتعديلاته والتعليمات الصادرة بموجب نظام اللوازم رقم (32) لعام 1993 وتعليمات رقم (1) لعام 2008، يشترط لتقديم دعوة استدراج العروض ما يلي:

1. أن تكون الشركة مسجلة في وزارة الصناعة والتجارة، ولديها رخصة مهن سارية المفعول تخولها ممارسة العمل في المجال المطلوب.
2. ان تكون الشركة وكيلة من الشركة الام (للمنتج المقدم).

الوثائق المطلوبة

3. ان يتضمن العرض المقدم الوثائق التالية:

أ- وصف مختصر موضح ضمنها معلومات عن الشركة ومنها سنة الانشاء وعدد العاملين فيها، مجالات العمل، مجموعة الخدمات التي تقدمها، والخبرات السابقة في تنفيذ اعمال مشابهة.

ج -قائمة بالجهات التي تم العمل معها سابقا بأعمال مشابهة.

د- العرض المالي (**على ان يتم تقديم سعر المنتج والخدمة لمدة (من 1 -3 سنوات)**.

4. وللهيئة الحق باستبعاد أي عرض غير متضمن جميع الوثائق المحددة بالبند(2) أعلاه.

تقديم وتسليم العرض:

5. يقوم المناقص بتقديم العرض المالي على النحو التالي:

أ- عرض مالي شاملا (لتسعير المنتج والخدمة من 1-3 سنوات) وللهيئة الحق في اختيار عدد السنوات التي تلزمها.

ب- عرض فني يحتوي على جميع المواصفات المطلوبة في دعوة العطاء وفي الملحق رقم (1).

6. توضع الوثائق المطلوبة في مغلف مغلق يؤشر عليه بكتابة اسم دعوة العطاء ورقمه بشكل واضح.

7. يتم تقديم العروض على نسختين (أصل وصورة).

8. اخر موعد لشراء نسخة العطاء الساعة الثانية من يوم الثلاثاء الموافق (2021/06/08).

9. يوضع المغلف في صندوق العطاءات الموجود لدى قسم المشتريات والتزويد في الهيئة، وذلك في موعد أقصاه الساعة (الثانية) من بعد ظهر يوم (الأربعاء) الموافق 2021/06/09، وذلك على العنوان التالي:

الهيئة المستقلة للانتخاب

منطقة تلاع العلي/ شارع إسماعيل حجازي

بجانب ديوان المحاسبة

ص.ب (375) / (11953) عمان

الاردن

تليفون: (5501111 6 962) -الرقم الفرعي (5504935) رئيس قسم المشتريات والتزويد او على الرقم الفرعي (5504934).

فاكس: (5504660 6 962)

www.iec.jo

10. سيتم فتح العروض الساعة (2:15) من بعد ظهر يوم الاربعاء الموافق 2021/06/09.

الالغاء او الاستبعاد:

11. للهيئة الحق في إلغاء أو تأجيل أو إعادة طرح الاعمال كاملة أو أي جزء منها دون إبداء الأسباب أو توضيح أو تفسير للقرار ويتنازل المتقدم لدعوة العطاء عن الحق بالمطالبة بتعويض عن أية خسارة أو ضرر مادي أو معنوي يلحق بهم جراء ذلك.

12. للهيئة الحق باستبعاد اي عرض دون ان يحق للمناقصين بالرجوع اليها بأية خسائر مادية او معنوية او اي ضرر ناشئ عن تقديم او استثناء العرض وذلك للحالات التالية:

- عدم تضمين العرض كافة الوثائق المطلوبة ضمن البند (2) من الشروط الخاصة.
- عدم التزام المناقص بطريقة تقديم وتسليم العرض المحددة بالبنود(4،5) من الشروط الخاصة.

الاسعار وطريقة الدفع:

13. تقدم الأسعار بالدينار الاردني شاملة كافة الضرائب والرسوم والعوائد الحكومية والضريبة العامة على المبيعات وأية رسوم إضافية أخرى.

14. تكون الدفعات على النحو التالي:

100% بعد التسليم النهائي.

تقييم العروض:

15. سيتم تقييم العروض المقدمة لتنفيذ الاعمال استنادا لمعادلة فنية وحسب الأوزان الترجيحية المبينة في البند (16) (فني ومالي)، وذلك لكون طبيعة الأعمال المطلوبة تعتمد بشكل أساسي على مدى الكفاءة والفاعلية في مجال اللوازم المطلوبة.

16. الأوزان الترجيحية المعتمدة للمعايير الأساسية للتقييم هي:

- تقييم العروض الفنية (فني) (70%)
- تقييم العروض المالية (مالي) (30%)

17. ستقوم لجنة العطاءات بفتح العروض للمتقدمين بعد انتهاء المدة المحددة لتسليم العروض والتوقيع عليها.

18. يتم تقييم العروض الفنية باستخدام معايير المفاضلة والأوزان الترجيحية التالية:

(1) حجم وإمكانات الشركة (15%):

عدد سنوات انشاء الشركة، عدد الموظفين، انتشار الشركة او المؤسسة، مجالات عمل الشركة وتنوع مجموعة الخدمات المادية والفنية التي تقدمها.

(2) خبرة سابقة في تنفيذ اعمال مشابهة 15%:

مدى تناسب الخبرات السابقة في تنفيذ اعمال مشابهة، سيعطى افضلية من تتوفر لديه خبرات سابقة في هذا المجال.

(3) المدة الزمنية للتوريد: (10%)

سيتم إعطاء العلامة الأعلى لمدة التوريد الأقل على ان لا تتجاوز مدة التوريد في جميع الحالات عن (7) أيام.

(4) جودة المواد المطلوبة والخدمات المقدمة: (30%)

سيتم التقييم على أساس جودة ونوعية المواد المقدمة ومدى مطابقتها للمواصفات المطلوبة ولقدرة تلبيتها لاحتياجات الهيئة (ويرجع الحكم فيها الى لجنة فنية متخصصة مشكلة من قبل الهيئة)

19. يلتزم الفريق الثاني بتسديد كافة الضرائب والرسوم والعوائد الحكومية المترتبة على كل فاتورة قبل تقديمها بما في ذلك الضريبة العامة على المبيعات.
20. يرفق بالعروض تأمين للدخول في العطاء على شكل كفالة بنكية أو شيك مصدق باسم عطوفة أمين عام الهيئة المستقلة للانتخاب صادرة / صادر عن بنك محلي وبنسبة لا تقل عن (3%) من قيمة العرض الإجمالية وحسب النموذج المرفق، وسوف لن ينظر في أي عرض غير معزز بالتأمين المطلوب.
21. يلتزم المتعهد بتقديم كفالة حسن تنفيذ بنسبة (10%) من قيمة الاعمال الاجمالية المحالة عليه وتكون سارية المفعول طيلة فترة العقد.
22. يجب ان ألا تكون الشركة قد سبق وأن تم مصادرة كفالات حسن التنفيذ الخاصة بالعقود السابقة التي كلفت بتنفيذها من أي جهة حكومية أو وقفها عن العمل وأن لا تكون الشركة من الشركات المدرجة ضمن القائمة السوداء

للتعامل مع الجهات الحكومية وأن يقوم المتقدم بالإفصاح عن أي مشاكل سابقة من هذا القبيل وتحت طائلة المسؤولية.

23. يلتزم المناقص أن يقدم ضمن عرضه شهادات الخبرة المطلوبة مصدقة حسب الأصول من الجهات التي عمل لديها وبراءة ذمة من الضمان الاجتماعي ومن ضريبة الدخل وشهادة تسجيل في الضريبة العامة على المبيعات.

24. يجب على المناقص تقديم شهادات حسن تنفيذ من الدوائر التي عمل لديها تبين كيفية الاداء مرفقة مع شهادات الخبرة والعقود التي يحصل عليها.

25. على الشركة أن تبين وبشكل واضح عنوانها الدائم (الموقع / صندوق البريد والهاتف والفاكس والبريد الالكتروني أن وجد) وتسمية الشخص المفوض بالإدارة.

26. على الشركة أن ترفق في العرض جميع الوثائق والشهادات الثبوتية الأصولية المذكورة في البنود أعلاه ويعتبر ذلك جزءاً لا يتجزأ من العرض.

27. مدة التسليم: لا تتجاوز ال (7) أيام عمل.

28. يكون الدعم الفني طوال فترة تقديم الخدمة على شكل على النحو التالي:

أ- **يكون الدعم الفني بشكل عام (7/24) من ال (vendor and Partner).**

ب- **تكون الاستجابة خلال (ساعة) في حالات الطوارئ.**

ت- **تكون الاستجابة خلال (4) ساعات، في الحالات الاعتيادية.**

المواصفات الفنية الخاصة بالعطاء رقم (2021/02)

1. *Gateway FortiGate Firewalls for Main Site (Qty 2):*

Item	Feature / Specification	Compliance (Comply/ Not Comply/ Partially Comply)
Performance Specifications		
1	The proposed solution must be recognized as a Leader in the latest Gartner Magic Quadrant for Enterprise Firewalls.	
2	The proposed solution must be from a family of products that achieves "Recommended" rating from NSS Labs for NGFW testing	
3	Firewall throughput of the device for all packet size (1500 bytes, 512 bytes, 64 bytes) should be above 35/ 35 / 25 Gbps	
4	The Maximum Concurrent sessions should be: 8 Million	
5	The New sessions per second should be 450,000	
6	The latency of the Firewall should be below 1.6 µs for all packet sizes.	
7	It should support IPsec VPN throughput of 20 Gbps	
8	It should have inbuilt SSL VPN capability to support up to 10,000 concurrent users. If this is a licensed component, the equivalent of 5,000 user licenses should be quoted.	
9	The device should support Firewall Throughput with Application control enabled: 15 Gbps	
10	The device should support an IPS throughput of 10 Gbps	
11	The device should also support a NGFW Throughput (FW + IPS + Application control) of 9 Gbps as minimum.	
12	The device should also support Threat Protection Throughput (FW + IPS + Application Control + Antimalware) of 7 Gbps as minimum.	
Hardware Specifications		
13	The device should have RJ45 Console Port, 2x GE RJ45 Management Ports, 8 x 1 Gig copper ports, 8 x 1 Gig SFP slots, and 2 x 10 Gig SFP+ slots for fiber connectivity.	
14	The device is to be quoted in High Availability active/active AND active/passive with required licenses and identical features on both units	
15	Each device should be equipped with 2x10 Gig SFP+ Transceivers Multi Mode	
17	Each device should have 2x240 GB SSD local storage minimum	
Technical Specifications		
18	Should be provided with licenses for IPS, Antispam Service, Advanced Malware Protection (AMP) (Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and Sandbox Cloud Service) and Web and Video Filtering Service, Application Control.	
19	Should be supplied with 10 Virtual System, Security context licenses	
20	It should have inbuilt feature of Two-Factor Authentication (2FA) for SSL-VPN and for Admin login, without needing a separate software/hardware to deploy the solution.	
21	The NGFW proposed should be NSS recommended for Next Generation Firewall 2019	
22	The NGFW appliance should be able to scan HTTP traffic and intercept HTTPS/SSL web traffic without requiring additional appliance	
23	The NGFW appliance should be able to send logs to the Centralized Logging and Reporting Appliance supplied along with this solution.	
OS		

24	Upgradeable via Web UI or TFTP	
25	The configurations on the device shall:	
26	Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk	
27	Provide CLI command configuration file that is readable by Windows Notepad	
28	Have option for encrypted backup file	
29	Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision.	
30	The proposed system shall minimally provide management access through:	
31	GUI using HTTP or HTTPs access which administration service port can be configured, example via tcp port 8080	
32	CLI console using console port, SSHv2, telnet or on GUI's dashboard	
33	The proposed system shall offer option to automatically redirect HTTP management access to HTTPS	
34	The proposed system shall have option to implement local administrator password policy enforcement	
35	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACACS+	
36	The proposed system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access	
37	From certain trusted network or host with corresponding administrator account	
38	The proposed system should be able to facilitate administration audits by logging detailed activities to event log - management access and also configuration changes.	
Integration		
39	Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system	
40	External threat feeds: URL list, IP list, domain name list and malware file hash	
Network		
41	Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed system transmits to improve network performance	
42	Administrators shall be able to configure physical interfaces on the proposed system for one-armed sniffer	
43	Administrators shall be able to combine two or more physical interfaces to provide link redundancy. This feature allows administrators to connect to two or more switches to ensure connectivity if one physical interface, or the equipment on that interface, fails. In a redundant interface, traffic travels only over one interface at a time.	
44	The proposed system shall support multiple virtual wire pairs that logically bind two physical interfaces so that all traffic from one of the interfaces can exit only through the other interface if allowed by firewall policy.	
45	The proposed system shall support wildcard VLANs for a virtual wire pair. Doing this allows all VLAN-tagged traffic to pass through a virtual wire pair if a virtual wire pair firewall policy allows the traffic.	
46	The proposed system shall support various enterprise DNS settings, including:	
47	Support for both IPv4 and IPv6 routes	
48	Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes.	

49	Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database.	
50	The proposed system shall support blackhole routing. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator won't discover any information from the target network.	
51	The proposed system shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing.	
52	The proposed system shall support IPv4 policy routing	
53	The proposed system shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols	
54	The proposed system shall support BGP4 and BGP4+ routing protocols	
HA	Thex proposed system shall support high availability with industry-standard VRRP with the following characteristics:	
55	Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP	
56	Be able integrated into a VRRP group with any third-party VRRP devices	
57	Supports IPv4 and IPv6 VRRP	
58	The proposed system shall support high availability by setting up a cluster with the following characteristics:	
59	Supports up to 4 cluster members	
60	Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)	
61	Cluster units communicate with each other through their heartbeat interfaces	
SDWAN	SD-WAN	
62	The proposed system shall support aggregation of up to 255 interfaces to create a virtual WAN link.	
63	The proposed system shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include:	
64	Predefined performance SLA profiles such as Office 365, AWS and Gmail	
65	Health check probes using IPv4/IPv6 Ping and HTTP	
66	Selection of multiple destinations(or servers) to probe	
67	Interfaces relating to the performance SLA profile	
68	The proposed system shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic take. These constraints should include:	
69	Latency threshold	
70	Jitter threshold	
71	Packet loss threshold	
72	The proposed system shall provide settings to the charactistics of probes, including check interval, link failure and restoration considerations.	
73	The proposed system shall provide option to disable the implicated static route when an interface is inactive.	
74	The proposed system shall allow organizations to define SD-WAN rules that are used to control how sessions are distributed to SD-WAN interfaces. The definition of these rules shall include:	

75	Source: address and/or user group	
76	Destination: address, applications and/or dynamic IP database	
77	Path control strategies	
78	The proposed system shall provide the following path control strategies:	
79	The proposed system shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces:	
80	Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path	
81	Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces.	
82	Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces.	
83	Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path.	
84	Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface.	
85	The proposed system shall support per-packet load-balancing among IPSec tunnels.	
86	The proposed system shall support forward error correction (FEC) on VPN overlay networks.	
87	The proposed system shall support SD-WAN rules with Border Gateway Protocol (BGP) learned routes as dynamic destinations.	
88	The proposed system shall provide Dual VPN tunnel ability that is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.	
89	The proposed system shall support integration with a cloud-based solution to simplify IPsec VPN setup.	
Security		
90	1. ANTI-MALWARE	
	• Botnet server IP blocking with global IP reputation database	
	• Virus Outbreak Prevention Database query: uses real-time checksums DB of newly detected threats before	
	• AV signatures are available	
	• Content Disarm and Reconstruction option:	
	• Flow-based or proxy-based AV option:	
	○ Support for popular web, mail, and FTP protocols	
	○ Scan encrypted traffic with SSL inspection	
	• File quarantine (local storage required)	
91	2. IPS AND DoS	
	• IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom	
	• signatures, manual, automatic pull or push signature update, threat encyclopedia integration	
	• IPS Actions: Default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming	
	• interface) with expiry time	

	• Filter-Based Selection: Severity, target, OS, application, and/or protocol	
	• Packet logging option	
	• IP(s) exemption from specified IPS signatures	
	• IPv4 and IPv6 rate-based DOS protection (available on most models) with threshold settings against TCP Syn	
	• flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)	
	• IDS sniffer mode	
	• Active bypass with bypass Interfaces (selected models) and FortiBridge	
92	3. APPLICATION CONTROL	
	• Detects thousands of applications in 18 categories: Business, Cloud IT, Collaboration, Email, Game, General	
	• Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/Audio, VoIP, Web Chat and Industrial.	
	• Custom application signature support	
	• Supports detection for traffic using HTTP/2 protocol and able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 1.2	
	• Filter-based overrides by: behavior, category, popularity, technology, risk, vendor, and/or protocol	
	• Actions: Allow, block, reset session (CLI only), monitor only	
	• SSH Inspection	
	• Deep application control over popular public cloud services, such as SalesForce, Google Docs, and Dropbox	
93	5. FIREWALL	
	• Operating modes: NAT/route and transparent (bridge)	
	• Schedules: one-time, recurring	
	• Session helpers and ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)	
	• VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing	
	• Protocol type support: SCTP, TCP, UDP, ICMP, IP	
	• User and device-based policies	
	• Policy Management: Sections or global policy management view	
	• NGFW policy mode: setup policies with applications and URLs as objects	
94	6. VPN	
	• SSL VPN web mode: For thin remote clients equipped with a web browser only and support web application, such as HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix	
	• SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems	
	• IPsec VPN:	
	○ Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS	
	○ Authentication method: Certificate, pre-shared key	
	○ IPsec Phase 1 mode: Aggressive and main (ID protection) mode	
	○ Peer acceptance options: Any ID, specific ID, ID in dialup user group	
	○ Supports IKEv1, IKEv2 (RFC 4306)	
	○ IKE mode configuration support (as server or client), DHCP over IPsec	

	○ Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256	
	○ Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512	
	○ Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14	
	○ XAuth support as client or server mode	
	○ XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option	
	○ Configurable IKE encryption key expiry, NAT traversal keepalive frequency	
	○ Dead peer detection	
	○ Replay detection	
	○ Autokey keep-alive for Phase 2 SA	
	• IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,	
	• IPsec VPN Configuration options: Route-based or policy-based	
	• Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPsec, PPTP, GRE over IPEC	
95	**7. DLP**	
	• Web filtering inspection mode support: proxy-based, flow-based and DNS	
	• DLP message filter:	
	○ Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP	
	○ Predefined filter: Credit card number, Social Security ID	
	• DLP file filter:	
	○ Protocols Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP	