مجليس باندرايا كوانتن
MAJLIS BANDARAYA
KUANTAN
CITY COUNCIL

KENYATAAN TAWARAN

Terbuka kepada mana-mana pihak yang berminat untuk mengemukakan tawaran bagi membekal **WEB APPLICATION FIREWALL** kepada Majls Bandaraya Kuantan. Kertas cadangan yang dikemukakan hendaklah merangkumi perkara-perkara berikut seperti di **lampiran 1**

Mana-mana pihak yang berminat adalah dipelawa untuk mengemukakan Surat Niat dan Kertas Cadangan bagi membekal **Web Application Firewall** kepada Majlis Bandaraya Kuantan untuk pertimbangan majlis.

Pihak yang berminat perlu menyenaraikan semua kos yang terlibat dan lain-lain tawaran secara jelas.

Semua cadangan hendaklah dihantar sebelum atau pada **14 Januari 2022 (Jumaat)** melalui emel **khaizal@mbk.gov.my.** Pihak MBK tidak terikat untuk menerima tawaran serta tidak bertanggungjawab di atas apa jua perbelanjaan yang ditanggung oleh pemohon untuk mengemukakan tawaran ini.

Sebarang pertanyaan sila hubungi En Khaizal Asyraf Bin Suhaimi, Bahagian Teknologi Maklumat di talian 09-5121555 Samb: 7506 atau emel kepada **khaizal@mbk.gov.my**.

LAMPIRAN 1

Spesifikasi Web Application Firewall

No.	Item	Min. Requirement	Mandatory	Mandatory Answer (Yes/No)	Proposal (Please State Details)
1	Country of origin	Please state			
2	Solution Proposed (Make and Model)	Please state			
A)	**Capacity, Performance and Deployment Requirements**				
1	Proposed solution MUST be appliance-based solution		M		
2	Proposed solution MUST comply with standalone WAF function		M		
3	Proposed hardware must come with the following specifications: - CPU: Two-Core Processor running 3.1Ghz or higher - Memory: 16GB RAM - Storage: 500GB SSD or 1TB SATA HDD (customer can select during ordering) - 1U height and rack mountable - Come with 2 x 10Gbe Fiber Port (SFP+), or 4 Pair of 10Gbe Fiber (SFP) port or 6 pair x 1GbE Copper (customer can select during ordering) - Comes standard with dual power supplies (hot-swappable)		M		
4	Propose WAF solution must be able to support up to 600Mbps Internet throughput		M		
5	Propose WAF solution must be able to support up to 4,000,000 concurrent sessions		M		
6	Propose WAF solution must be able to support up to 50,000 CPS (L7)		M		
7	Propose WAF solution must be able to support up to 80,000 TPS (L7)		M		

8	Propose WAF solution must be capable of supporting hardware-based SSL accelerator		M		
9	Proposed must support the following deployment mode: - Rapid in-line (Bridge) - Reverse Proxy or One-Armed Reverse Proxy - Transparent Reverse Proxy - Mirroring - Hybrid: Combine with mirroring and in-line mode				
B)	**Key Features & Functionalities Requirements**				
1	Proposed solution must support the following WAF features - Request inspection - Response inspection - Learning - Cloaking		M		
2	Proposed solution must support application access control, Form field inspection, Cookie inspection, WEB DoS protection, HTTP DoS protection, SQL injection, XSS, Inspection avoidance block, and WISE Filter		M		
3	Proposed solution must support predefined and customize WAF signature		M		
4	Proposed solution must support Web rewriting protection, credit card, account, and social security number protection, Response format inspection, Code leakage block, WISE Filter		M		
5	Proposed solution must support SQL, Script, Shell code, Access Control, Form Field, and Cookie learning		M		
6	Proposed solution must support URL/Server Cloaking, Improper Error handling		M		
7	Proposed solution must support Dynamic Application Proxy to simplify a complex network stack to remove bottleneck points between user and kernel		M		

C)	**Security Requirements**				
1	Protection against SQL injection		M		
2	Protection against Command Injection		M		
3	Protection against XSS		M		
4	Protection against Cross-Site Request Forgery (CSRF)		M		
5	Protection against cookie modify		M		
6	Protection against cookie take over		M		
7	Protection against directory listing		M		
8	Protection against DoS (Rudy, Slowloris)		M		
9	Protection against File upload limit based on file extension		M		
10	Protection against Upload file content diagnosis		M		
11	Protection against File size limit		M		
12	Protection against File download diagnosis		M		
13	Protection against Include injection		M		
14	Protection against Error message clocking		M		
15	Protection against Modify hidden field		M		
16	Protection against Parameter modify (tampering)		M		
17	Protection against Web access through tool		M		
18	Protection against Leakage of privacy information		M		
19	Protection against Privacy information Download		M		
20	Protection against Request method limit		M		
21	Protection against Access limit based on extension		M		
22	Protection against Limit forbidden word		M		
23	Protection against Block webpage forgery		M		
24	Protection against Block source code exposure		M		
25	Protection against Block server information exposure that included response header		M		
26	Protection against Block Dos attack based on IP (WEB QoS)		M		

27	Protection against Block Dos attack based on session (WEB QoS)		M		
28	Protection against Duplicate parameter detection		M		
29	Protection against Access control of illegal URL encoding		M		
30	Protection against buffer overflow		M		
30	Protection against buffer overflow		M		
31	Must support SSL decryption		M		
32	Must support SSL performance with 2048 bit RSA key		M		
D)	**System Administration and Management Requirements**				
1	Must be able to support Web-based GUI management via the following browser:		M		
	· Google Chrome				
	· Internet Explorer				
	· Firefox				
	· Opera				
	Must be able to support automatic updates of version and patches		M		
2	Must support multiple configuration save slot		M		
3	Must support server error monitoring		M		
4	Must able to provide reporting		M		
5	Must be able to backup and restore configuration file for fast recovery purpose		M		
6	Must support SNMP		M		
7	Must support syslog		M		
8	Must support Server Load Balancing		M		
9	Must support IPv6 Management		M		
10	Must support IPv6 SSL Offloading		M		

E)	**Reporting Requirements**				
1	Tenderer must supply additional reporting software to install in customer virtual environment for centralized management and logging - Analyzer V2 Reporting software		M		
1	Must be able to support security monitoring and analysis solution via centralized management solution		M		
2	Must be able to support real-time monitoring and event management		M		
3	Must be able to supports a variety of report formats with visualized graph and charts to realize a type of attacks and patterns		M		
4	Must be able to provide log provides you detail information of web packet source, a type of attack, and attack clues		M		
5	Must be able to supports an email alert whenever breaching user-defined security policy or detecting a certain attack		M		
6	The centralized management reporting tools shall be able to provide the following reports as well:		M		
	- Network Traffic Monitoring				
	- System Resources Usage Monitoring				
	- System Availability Monitoring				
	- Database Monitoring				
	- Bandwidth Monitoring				
7	Integration to the following supported protocols for data extraction and report generation:		M		
	- WMI				
	- Packet Sniffing				
	- SSH				
	- NetFlow, IPFIX, jFlow, and sFlow				

	- Ping				
	- HTTP requests and push data				
F)	**High-Availability Requirements**				
1	Must be able to support active-standby failover		M		
2	Must support active-active mode		M		
G)	**Warranty & Maintenance**				
1	12 months of 8x5xNBD Advance Hardware Replacement + Onsite Certified Engineer Support				
			M		
2	On-Site / Remote Preventive Maintenance (Twice a year)		M		
3	Remedial Maintenance		M		
4	12 months Parts under Warranty		M		
5	Manufacturer's Standard Warranty, please attach warranty letter from the manufacturer's/distributor's		M		
H)	**Professional Services**				
1	Installation, Configuration, commissioning and implemention must be done by Distributor's Certified Engineer		M		
2	Standard Administration Training for 5 pax (1-day)		M		
I)	**Others**				
1	Letter of authorization from distributor/principal		M		
2	Brochure				
3	Training Documentation				