`

RFQ for two Unit of Modular Chassis based Hardware Load balancer		
SL	**Hardware features Description**	**Bidder Respond**
1.	Brand (Please Mention)	
2.	Model (Please Mention)	
3.	Country of Origin (Please Mention)	
4.	Solution shall be dedicated, purpose built, & Appliance based solution with blade architecture required for future scalability & strong virtualization capabilities.	
5.	Solution must support Global server load balancing as well as local server load balancing	
6.	Solution must support high availability functionality	
7.	The Solution must be able to scale vertically by adding cards and horizontally by clustering. The performance of the system must scale linearly with the addition of each blade to the System.	
8.	System shall have 16 x 10 Gigabit SFP+ pluggable optical ports and in addition should have QSFP+ 40 Gig ports available from day 1 or higher	
9.	Each Blade must have 64 GB RAM or higher	
10.	Appliance should have LCD screen /LED on the on the front	
11.	Device must support 80 Gbps L7/L4 layer of throughput & must support 2 Mn L7/L4 requests/second or higher	
12.	Device must support 30 Gbps throughput after applying the hardware compression techniques	
13.	Device must support SSL offloading & should support 25 Gbps (of each blade) SSL offloading traffic or higher	
14.	The solution must support atleast 40K SSL TPS (2K keys) (each blade), support and max scalable to 160k SSL TPS (2k Keys). SSL Key strength must be 2048	
15.	Device must be capable to protect against DDoS attacks & be able to process SYN cookies. Must support processing of 45 Mn cookies/second (per blade) & must be scalable to support the processing of 200 Mn cookies/second	
16.	Device must support active/active and active/passive configuration	
17.	Device must support out of band management	
18.	For all BRAC bank (in scope) applications all features are must & all the modules, licenses, support contract, accessories etc. must be from same OEM.	
19.	Solution must support following deployment topologies but not limited to: One arm mode 2 arm mode Transparent mode	

`

20.	The proposed solution should have capability to handle and Configure multiple load balancing (Layer 7) protocols (http, https, ftp, TCP, TCPS, SIP, Radius) on same appliance be able to route the applications independently of server location or network schema, hence more applications will benefit from load balancer services.	
21.	The proposed solution should have capability of rate limiting and TCP surge protection	
22.	Solution must be configurable to support DNS queries. Must support 1.2 Mn DNS responses/second (per blade) & if all blades are used the same should be scalable enough to support processing of 7 Mn DNS responses/second or higher	
23.	The proposed solution should have the capability to configure multiple services on same virtual IP with different ports & service options	
24.	The solution should support the capability of rate shaping & QoS support.	
25.	The proposed solution must support virtualization & at least 80 guests should be supported (20 guest machines on each blade) without requiring any additional licenses or higher	
26.	The appliance should have the feature of cluster failover & should failover as per industry failover benchmarks (industry benchmark is within 3 seconds failover)	
27.	Solution must support load balancing based on following load balancing protocols but not limited to these only: Round robin Least connection Weighted least connection Agent based adaptive load balancing Weighted response time Source IP hash	
	Software defined networking (SDN) adaptive	
28.	Solution must support SDN networking & other protocols that bank may use for implementing next gen networking technologies like SDN, network virtualization, network automation	
29.	Solution should support server side multiplexing	
	SSL Offloading	
30.	The solution must have feature of SSL offloading which should have following but not limited to : Dedicate SSL chipset for SSL offloading Support 25 Gbps SSL throughput (bulk crypto) per blade.	
31.	SSL should be card based for 1024 & 2048 bits certificates	
32.	Solution must support end to end SSL if required in future	
33.	Solution must support hardware & software based SSL acceleration	

`

	HTTP & TCP layer optimization & acceleration	
34.	Solution must support HTTP compression & acceleration	
35.	Solution must use intelligence to support selective compression to avoid known compression problems in commonly used browsers.	
36.	Solution should support TCP optimization	
	Caching	
37.	Solution must support caching	
38.	Solution should support per file type/content type TTL control	
39.	Solution should support dynamic content caching	
40.	Solution should be able to push static content to local client machine	
41.	Solution Should support change lifetimes of content passed by the backend servers to the client.	
42.	Should support image optimization	
43.	Solution should support per service caching filter support	
44.	Solution should support content and white space stripping	
45.	Solution should support content reordering	
	IPv6 support	
46.	The product should support IPv6 ALG and NAT64	
47.	Appliance should support IPv4 and IPv6 Support	
48.	**Global server load balancing**	
49.	The appliance should have feature of GSLB with: Per host name TTL (time to live) value control	
50.	GSLB for application failover across datacenter	
51.	GSLB should be capable of monitoring the health of the application across data center & DR site.	
52.	Solution should support DNS rate limiting and DNS DDoS protection	
	Functionalities required for application delivery	
53.	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2	
54.	Proposed solution should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover for all connections which are offloaded on the device so that existing SSL connections are not lost during a failover event	
55.	The proposed appliance should support centralized Security policies enforcement, SSL Certificates management for workloads on Private DC and public cloud	
56.	The solution should support a mechanism to auto-discover and auto-scale workloads deployed in Public Cloud.	

`

57.	The solution must support automatic updation of certificate bundles of CA installed on it to reduce administrative workload and simply SSL certificate management .	
58.	The solution must support Constrained Certificate delegation which will allow the device to generate SSL certificates on behalf of the application servers which then can be used to authenticate clients for which SSL certificate based authentication has been enabled.	
59.	Device should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	
60.	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration.	
	Web application functionalities	
61.	The proposed solution Should have Web application firewall functionality	
62.	The Appliance should be able to handle Top 10 OWASP 2017 Attacks as well as Zero Day Attacks , Should Support IP Reputation, Should have Vulnerability Scanner or Support	
63.	Solution should support Integration with 3rd Party Vulnerability Scanner example Mcafee, Nessus, Qualys Whitehat etc.	
64.	Solution Should Support Application compliance reporting, should support HTTP, XML, JASON & AJAX protocol	
65.	Solution Should support positive and negative signature Module, should support inbuilt reporting.	
66.	Solution should support Layer 3 to Layer 7 support with advance protection for http request and response	
67.	Solution should support Geolocation IP address database to identify the source of the attack origin and IP Reputation Mechanism to identify the Blacklisted TOR Networks or Proxy IP address to Block the request immediately.	
68.	Solution should dynamically read new modules of applications, and WAF should also provide the option of deploying the rules learnt dynamically for these new modules without manual intervention.	
69.	WAF correlation should also identify complex attack chains, and not just aggregate events based on attacks or sources along with advanced BOT detection mechanism based on smart combination of signature-based and heuristic analysis	
70.	Solution Must be able to take threat intelligence feed to reveal inbound communication with malicious IP addresses, and enable granular threat reporting and automated blocking.	
71.	Solution should Support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	
72.	Solution should able to encrypt the user credentials in real time so as to protect the credentials especially password/National Identity number or any other sensitive parameter as defined by department to protect from key loggers and credential stealing malware residing in the end users system	

`

73.	Solution must be able to detect the presence of Remote Access Trojans (RATs) residing in the user's web browser.	
74.	Solution should perform comprehensive countermeasure to protect against zero day attack, Challenge – Response Mechanism, which should be able to detect and protect attacks in real time through inbuilt Captcha Mechanism	
75.	Solution should be able to defend against browser based key loggers that attempt to capture user's key strokes and steal user credential	
76.	Solution must provide advanced L7 DOS protection features including but not limited to : L7 Behavioral DOS Stress Based DOS	
77.	Solution should support API protection	
78.	Solution must support Websocket and Secure Websocket	
79.	Solution must have advanced Anti-Bot detection and protection measures including ability to detect Bots which can execute JavaScript. It should also protect against Web Scraping.	
	DDoS functionalities	
80.	Solution should support auto signaling to OEM's own Cloud scrubbing center	
81.	Solution should detect any DDoS traffic and mitigate any DDoS attack without interrupting any legitimate traffic and customer services.	
82.	The offered solution should provide DNS Caching , high-speed authoritative DNS and Resolving capabilities	
83.	The offered solution should provide DNS Firewall functionality by detection and mitigation of DNS refelction or amplification DDoS attacks, DNS Flood, protocol violations, bad request types attacks and other DNS threats	
84.	Solution must support BGP Route based black holing so that the appliance can redirect the traffic to the ISP's scrubbing center using BGP route injection to prevent the ISP pipe from getting choked.	
	Reporting , Management & others	
85.	Solution should Support integration with SIEM solution (current & future as well). Solution should support syslogging with regex option available for external log collection	
86.	Solution should support customized logging attributes to reduce logging size	
87.	Solution must support real time reporting & monitoring and Administration tools eg – real server response and outstanding requests, real server/virtual server request status & other system (RAM/CPU usage etc.) statistics.	
88.	Bidder should provide the central Management Appliance or software that have the capability of Administration, monitoring and reporting etc (chassis, blades, vCMP and legacy devices)	

`

	Please mentioned the details:	
89.	Solution must be centrally manageable with options of multiple management options which are secure & easy to configure (SSH or HTTPs)	
90.	Solution must be able to capture the client logs for HTTP requests with various required details	
91.	Solution should provide DNS trending report and can help application request and DNS planning and also help prevent DNS DoS attacks	
92.	Solution should have feature of inbuilt packet logging and support packet capture as required	
93.	OEM should have support centers /service center preferably in Bangladesh.	
94.	Appliance should have next business day turn around for hardware replacement within 4 hours and 24*7 offsite support center availability	
95.	OEM should have Global Technical Assistance Center across many parts of the World, Customers 24x7. OEM should have local technical resources available in Bangladesh	
96.	OEM should provide required full administration technical training to certified Training center of OEM for 4 person with certification and Technical training should include updated documentation readily available for reference (whenever required by BRAC bank).	
97.	On technology roadmap front, OEM should provide demos & solution walkthrough to BRAC bank team at least on quarterly basis. The demos & solution walkthrough must be directly aligned with BRAC bank environment & requirements.	
98.	Bidder must provide details of escalation matrix to be used for resolving technical & functional issues in the solution that is implemented in BRAC bank environment.	
99.	Bidder must provide the SLA for response & resolution of technical cases / incidents opened by BRAC bank with technical support team of bidder.	
100	The Products or any part thereof which are offered in the response of this RFP shall not reach end of life /end of support (which includes all kind of support viz. Hardware, software etc.) till next three years from contract start date	
101	The OEM should be in the Gartner's Leaders Magic Quadrant for "Application Delivery Controllers" and "Web Application Firewall" as per the last 2 published reports .	
102	Please share the complete technical BOQ	
103	All quoted features license should be include within the offered product	
104	**Warranty-** Product should have 5 years full 24/7 and 365 days online/onsite support	