WAF TENDER BIDDERS QUERIES AND BANK RESPONSE

Description as per RFP	Request for Amendment	Response
The Web application Firewall shall have at least one 100/1000 Base Tx Port for out of bound management	Request to remove this point	**Not considered**
The Web Application Firewall shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.	Request to remove this point	**Not considered**
The Web Application Firewall shall be able to prevent automated layer 7 DDoS attacks, web scraping, and brute force attacks from being directed to the site.	The Web Application Firewall shall be able to prevent automated layer 7 DoS attacks, web scraping, and brute force attacks from being directed to the site.	**Not considered**
The Web Application Firewall shall support attack expert system and shall provide an immediate, detailed description of the attack, as well as enhanced visibility into the mitigation techniques used to detect and prevent the attack.	The Web Application Firewall shall support attack expert system and shall provide an immediate, detailed description of the attack, and optional - enhanced visibility into the mitigation techniques used to detect and prevent the attack.	**Not considered**
Total Input as well as Output "Bytes per second" OR "Bits per second" per server/application/URL in order to have the usage of Internet Bandwidth.	Total Input as well as Output "Bytes per second" OR "Bits per second" per server/application/URL or the total throughput in the dashboard in order to have the usage of Internet Bandwidth.	**Not considered**
Total Input as well as Output "Bytes per second" OR "Bits per second" between the equipment and a particular Server.	Total Input as well as Output "Bytes per second" OR "Bits per second" OR "Total Events" between the equipment and a particular Server.	**Not considered**
The Web Application Firewall should protect against Sensitive Data Leakage protection using response scrub. It should have minimum feature like: PHP information leakages, IIS default location, ASP / JSP source code leakages, SQL error leakages, Directory Listing, HTTP Header Leakage, Access to admin folder,	The Web Application Firewall should protect against Sensitive Data Leakage protection.	The Web Application Firewall should protect against Sensitive Data Leakage protection. It should have minimum feature like: PHP information leakages, IIS default location, ASP / JSP source code leakages, SQL error leakages,

Slow Loris and other low & slow availability attacks, Prevention of Error messages leakage.		Directory Listing, HTTP Header Leakage, Access to admin folder, Slow Loris and other low & slow availability attacks, Prevention of Error messages leakage.
The Web Application Firewall shall have minimum 650 Mbps Web Application Firewall throughput. (The proposed solution should provide minimum of 650 Mbps WAF Throughput per instance from day one (with all WAF functions enabled per instance in blocking mode) with sub millisecond latency.	The Web Application Firewall shall have minimum 350 Mbps Web Application Firewall throughput.	The Web Application Firewall shall have minimum 350 Mbps Web Application Firewall throughput. (The proposed solution should provide minimum of 350 Mbps WAF Throughput per instance from day one (with all WAF functions enabled per instance in blocking mode) with sub millisecond latency.
The Web Application Firewall should have been in the Gartner's Magic Quadrant for "Web Application Firewall" in latest report.	The WAF solution should be in **Leaders or Challengers quadrant** of the latest Gartner Magic Quadrant report on WAAP	**Not considered**
The Web Application Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment	Remove this point	**Removed**
Details of minimum three major Implementations executed(At least one project should be on WAF implementation) As per **Annexure- H**	Request to consider Bidder / OEM experience for participating in the Tender.	If the Bidder is not having the experience of implementation a certificate has to submit by the bidder from OEM that the implementation and support is the responsibility of the OEM and bidder has to coordinate the same. (OEM and bidder both has to sign the document using ink to ensure the

		authenticity and legality of the signature).
Note:- NO Exemption allowed for tender fee/EMD for MSME. Both the fee are to be paid mandatorily.		