RFP for procurement of Web Application Firewall (WAF) - NPCI/RFP/2018-19/IT/17 dated 25.02.2019

Consolidated list of Replies to Pre-bid Queries

S.No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	NPCI Response
1	RFP for supply and installation of Web Application Firewall	35	9	The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion	2 no. of 10G ports may be less considering investment for 5 years , network requirements and future traffic growth of NPCI	No Change in RFP, its minimum requirement
2	RFP for supply and installation of Web Application Firewall	6	57	The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)	Support for TLS 1.3 must be available once with draft 28 implemented (draft 26 can be used for testing , production traffic not recommended)	No Change in RFP, as we are projecting for 5 yrs and shoud be accessible for use when avaiable.
3	RFP for supply and installation of Web Application Firewall	12	41	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.	9K RSA and 5K ECC (2K Key Size) is too low considering the 2 Gbps of WAF throughput seeked and no. of transactions expected by NPCI considering future growth and ROI	Please refer to the Corrigendum - 1
4	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."	JavaScript and CAPTCHA are two different technologies and both must be added to deliver best in class secuirty features available with OEM. Also all features of BOT protection should be available to NPCI	Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
5	RFP for supply and installation of Web Application Firewall	64	63	The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause	This type of tracking is requird the activities of VPN user.	No Change in RFP
6	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.	This option and feature will help to identify non client browsers or request or bot attack as well.	No Change in RFP
7	RFP for supply and installation of Web Application Firewall	20	7.4	After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1
8	RFP for supply and installation of Web Application Firewall	21	1	Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
9	RFP for supply and installation of Web Application Firewall	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
10	RFP for supply and installation of Web Application Firewall	74	23	The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
11	RFP for supply and installation of Web Application Firewall	21	8.6	Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation?		Please refer to the Corrigendum - 1
12	RFP for supply and installation of Web Application Firewall			Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.	Segmentation controls application flow to respective gateway per server and should help multiple segment controls	No Change in RFP
13	RFP for supply and installation of Web Application Firewall			Request clarification if this is a One OEM- One Bidder Bid or OEM can submit multiple bid through multiple bidders			One OEM can participate through multiple bidders/SI
14	Technical Specifications	35	1.1	Solution should failover to standby site without compromising security policy defined or without impacting any changes at End users level	As this is a DC & DR requirement, failover to standby site (DC to DR) is acheived via Link load balancer. Suggest if a Load balancer is already there or need to be provisioned. If participants has to supply, Load balancer technical specification has to be circulated for commercial proposal.		If Proposed solution has managment infrastructure invloved, then gateways to report to alterante managment servers, also considering no lose in any alerts and logs
15	Technical Specifications	35	1	Proposed WAF Solution should be in the Leaders quadrant in the Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years	As per Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years only two vendors are eligible to participate. Requesting to allow other Challengers quadrant players from last 2 years to participate. Kindly relax the clause as mentioned below. Proposed WAF Solution should be in the Leaders/Challengers quadrant in the Gartner Magic Quadrant for Web Application Firewalls in last 2 years.		No Change in RFP
16	Technical Specifications	35	2	The solution must be hardware appliance-based	As this is Web application Firewall requirement, suggest to have a dedicated WAF appliance instead of having Server load balancer loaded with WAF module over it. Kindly change clause as mentioned below. The solution must be dedicated hardware of WAF		To clarifiy proposed soluion shoud be appliance base

17	Technical Specifications	35	8	The solution appliances must have 4x1G Ethernet Interfaces	As per clause clause 3, if NPCI deployes WAF in Layer-2 transparent mode, then during both device failover in DC, appliance interface must support Bypass mode. Kindly change clause as mentioned below. Solution appliancem ust have 4x1G (bypass mode supported) ethernet interfaces,		No change in RFP
18	Technical Specifications	35	1	The proposed solution should SSL handling.	Since, we are doing SSL traffic inspection for more then 99% of traffic, would recommend to have hardware based SSL/TLS processing module on box for low latency processing. Kindly change clause as mentioned below. The proposed solution must have hardware based SSL/TLS processing module on box for low latency processing.		No change in RFP
19	Technical Specifications	36	12	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Mentioned performance number for SSL TPS should be higher supporting hardware based SSL module. Recommend to have below mentioned TPS. The solution must have a SSL hardware module to support minimum 18K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key		Please refer to the Corrigendum - 1
20	Technical Specifications	36	4	The system must support protection of Common Web Application attacks including OWASP Top 10 vulnerabilities, etc	There are multiple version of OWASP vulnerabilities report. Suggest to have latest 2017 reference on same. Kindly change clause as mentioned below. The system must support protection of Common Web Application attacks including 2017 - OWASP Top 10 vulnerabilities, etc and brief reference report mapping all threat types to be submitted.		No Change in RFP, as refernce would be always latest OWASP top 10 Vulnerabilites
21	Technical Specifications	37	16	The solution must provide the ability to comply to A+ Certification at the click of a button	A+ certification is for hardware. Are we looking at hardware based A+ certification. Is our understanding correct?		There is no need for hardware to have A+ certification .WAF solution should have ability to apply an SSL handshake configuration to an application that will achieve A+ certification from SSL Labs
22	Technical Specifications	40	59	The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat	Supporting VA tools will be differnet for all vendor. Kindly relax clause as mentioned below. The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. HP Fortify WebInspect b. IBM AppScan c. Qualys d. WhiteHat		No Change in RFP, where as any additional functionalilty /tools would be considered as value add
23	Technical Specifications	43	12	The solution must provide Role-Based Access Control. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest	Role based access control will vary from vendor to vendor. Kindly relax this clause.		No Change in RFP
24	Bid Schedule and Address	8	13,14	Tender Fee:- Rs.11,800/- (Rs.10,000.00 plus applicable GST@18%) (Bid cost should be in Indian Rupees only) EMD:- Rs 5,00,000 (Rupees Five Lakhs)	we registered under Single Point Registration Scheme of NSIC are eligible to get the benefits under “Public Procurement Policy for Micro & Small Enterprises (MSEs) Order 2012” as notified by the Government of India, Ministry of Micro Small & Medium Enterprises, New Delhi vide Gazette Notification dated 23.03.2012. as per above clause we are exemted from EMD. so reuest to you kindly allow MAME,NSIC certificate.		National Payments Corporation of India (NPCI) is neither a Government Company nor it is any Department of Government of India. As such the extant provisions would not apply to NPCI.
25	Section 9: Technical Specification	35	Clause 5 : General	The solution must support both Active-Passive & Active-Active deployment modes for high availability	Require the upstream device to segregate traffic and provide to WAF appliance.		Active - Passive
26	RFP for supply and installation of Web Application Firewall	35	9	The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion	2 no. of 10G ports may be less considering investment for 5 years , network requirements and future traffic growth of NPCI	No Change in RFP, its minimum requirement
27	RFP for supply and installation of Web Application Firewall	6	57	The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)	Support for TLS 1.3 must be available once with draft 28 implemented (draft 26 can be used for testing , production traffic not recommended)	No Change in RFP, as we are projecting for 5 yrs and shoud be accessible for use when avaiable.
28	RFP for supply and installation of Web Application Firewall	12	41	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.	9K RSA and 5K ECC (2K Key Size) is too low considering the 2 Gbps of WAF throughput seeked and no. of transactions expected by NPCI considering future growth and ROI	Please refer to the Corrigendum - 1

29	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."	JavaScript and CAPTCHA are two different technologies and both must be added to deliver best in class secuirty features available with OEM. Also all features of BOT protection should be available to NPCI	Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
30	RFP for supply and installation of Web Application Firewall	64	63	The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause	This type of tracking is requird the activities of VPN user.	No Change in RFP
31	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.	This option and feature will help to identify non client browsers or request or bot attack as well.	No Change in RFP
32	RFP for supply and installation of Web Application Firewall	20	7.4	After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1
33	RFP for supply and installation of Web Application Firewall	21	1	Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
34	RFP for supply and installation of Web Application Firewall	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
35	RFP for supply and installation of Web Application Firewall	74	23	The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
36	RFP for supply and installation of Web Application Firewall	21	8.6	Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation?		Please refer to the Corrigendum - 1
37	RFP for supply and installation of Web Application Firewall			Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.	Segmentation controls application flow to respective gateway per server and should help multiple segment controls	No Change in RFP
38	RFP for supply and installation of Web Application Firewall			Request clarification if this is a One OEM- One Bidder Bid or OEM can submit multiple bid through multiple bidders			One OEM can participate through multiple bidders/SI
39	Scope of Work	10	3.1	WAF Appliance – 04 Nos. as active-active for two DC	Number of DC and DR location Needed	Want to more of DR Location	2 at each location for DC (Hyderabad)and DR(Chennai)
40	Technical Specification	35	9	The solution must support both Active-Passive & Active-Active deployment modes for high availability	HA should be Active- Active or Active –Passive	Need to Mention Exact Requirement	Active - Passive
41	Scope of Work	10	3.1	Not Mentioned	Type and Number of Application to Be Secured		Will be shared with L1 bidder
42	Scope of Work	10	3.1	Not Mentioned	Bandwidth per Location Needed		Will be shared with L1 bidder
43	RFP for supply and installation of Web Application Firewall	35	9	The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion	2 no. of 10G ports may be less considering investment for 5 years , network requirements and future traffic growth of NPCI	No Change in RFP, its minimum requirement
44	RFP for supply and installation of Web Application Firewall	6	57	The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)	Support for TLS 1.3 must be available once with draft 28 implemented (draft 26 can be used for testing , production traffic not recommended)	No Change in RFP, as we are projecting for 5 yrs and shoud be accessible for use when avaiable.
45	RFP for supply and installation of Web Application Firewall	12	41	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.	9K RSA and 5K ECC (2K Key Size) is too low considering the 2 Gbps of WAF throughput seeked and no. of transactions expected by NPCI considering future growth and ROI	Please refer to the Corrigendum - 1
46	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."	JavaScript and CAPTCHA are two different technologies and both must be added to deliver best in class secuirty features available with OEM. Also all features of BOT protection should be available to NPCI	Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
47	RFP for supply and installation of Web Application Firewall	64	63	The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause	This type of tracking is requird the activities of VPN user.	No Change in RFP
48	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.	This option and feature will help to identify non client browsers or request or bot attack as well.	No Change in RFP
49	RFP for supply and installation of Web Application Firewall	20	7.4	After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1

50	RFP for supply and installation of Web Application Firewall	21	1	Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
51	RFP for supply and installation of Web Application Firewall	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
52	RFP for supply and installation of Web Application Firewall	74	23	The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
53	RFP for supply and installation of Web Application Firewall	21	8.6	Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation?		Please refer to the Corrigendum - 1
54	RFP for supply and installation of Web Application Firewall			Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.	Segmentation controls application flow to respective gateway per server and should help multiple segment controls	No Change in RFP
55	RFP for supply and installation of Web Application Firewall			Request clarification if this is a One OEM- One Bidder Bid or OEM can submit multiple bid through multiple bidders			One OEM can participate through multiple bidders/SI
56	RFP for supply and installation of Web Application Firewall	14	5.8	Return of EMD - The EMDs of successful Bidder/s shall be returned / refunded after furnishing Performance Bank Guarantee as required in this RFP. EMDs furnished by all unsuccessful Bidders will be returned on the expiration of the bid validity / finalization of successful Bidder, whichever is earlier.	Emd 5 LAKHS SHOULD BE RETURNED IMMEDIATELY IF WE DO NOT QUALIFY.WAITING FOR SIX MONTH OR TILL FINALISATION OF ORDER TO OTHER VENDOR IS A LONG TIME		No change in RFP
57	RFP for supply and installation of Web Application Firewall	21	8.2	Terms of the order - The term of the Notification of Award/Purchase Order shall be for a period of 3 years wherein the price of the specified Web Application Firewall in the RFP would be at a fixed rate and the subsequent purchase orders with varying quantities will be issued as when requirement arises.	PRICES MAY VARY EVERY YEAR.HENCE THIS CLAUSE SHOULD BE CHANGED		No change in RFP
58	RFP for supply and installation of Web Application Firewall	21	8.4	Performance Bank Guarantee - The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 3 years, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder is not in a position to submit the PBG for any reason, the successful bidder has to submit a Demand Draft drawn in favour of NPCI for equivalent amount or electronically transfer equivalent amount for credit in NPCI's account. Details of the NPCI's bank account will be furnished on request	Claim period should be 3 to 6 months and not 1 year.		No change in RFP
59	RFP for supply and installation of Web Application Firewall	12	4.1 clause 2	4.1 Eligibility Criteria 2. The bidder should have reported minimum annual turnover of Rs. 10 Crores as per audited financial statements in each of the last three financial years (i.e.2015-2016, 2016-2017 & 2017-2018) and should have reported profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e., 2015-2016, 2016-2017 & 2017-2018). In case audited financial statements for 2017-2018 are not ready, then management certified financial statement shall be considered for 2017-2018, however, this exception is not available in case of previous financial years. In case of a JV / Consortium / Strategic partnership, the bidder should have reported profits as per above criteria	Request you to change eligibility to - any one of the below - 1) Positive net worth 2)Cash Profit 3)EBIDTA 4) Net Profit IN ANY TWO OUT OF FIVE YEARS		No change in RFP
60	RFP for supply and installation of Web Application Firewall	8	section I clause 6	Last date and time for Bid Submission 08.03.2019 05.00 pm	We request you to kindly extend the date of submission to March 20, 2019		Please refer to the Corrigendum - 1
61		22	8.7	Delivery Schedule and Location Delivery Installation Training	Kindly change the schedule as per below - Deliver 12 weeks Installation - 10 weeks Training - 3 weeks		No Change in RFP
62	RFP for supply and installation of Web Application Firewall	35	9	The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion	2 no. of 10G ports may be less considering investment for 5 years , network requirements and future traffic growth of NPCI	No Change in RFP, its minimum requirement
63	RFP for supply and installation of Web Application Firewall	6	57	The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)	Support for TLS 1.3 must be available once with draft 28 implemented (draft 26 can be used for testing , production traffic not recommended)	No Change in RFP, as we are projecting for 5 yrs and shoud be accessible for use when avaiable.
64	RFP for supply and installation of Web Application Firewall	12	41	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.	9K RSA and 5K ECC (2K Key Size) is too low considering the 2 Gbps of WAF throughput seeked and no. of transactions expected by NPCI considering future growth and ROI	Please refer to the Corrigendum - 1

65	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."	JavaScript and CAPTCHA are two different technologies and both must be added to deliver best in class secuirty features available with OEM. Also all features of BOT protection should be available to NPCI	Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
66	RFP for supply and installation of Web Application Firewall	64	63	The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause	This type of tracking is requird the activities of VPN user.	No Change in RFP
67	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.	This option and feature will help to identify non client browsers or request or bot attack as well.	No Change in RFP
68	RFP for supply and installation of Web Application Firewall	20	7.4	After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1
69	RFP for supply and installation of Web Application Firewall	21	1	Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
70	RFP for supply and installation of Web Application Firewall	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
71	RFP for supply and installation of Web Application Firewall	74	23	The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
72	RFP for supply and installation of Web Application Firewall	21	8.6	Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation?		Please refer to the Corrigendum - 1
73	RFP for supply and installation of Web Application Firewall			Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.	Segmentation controls application flow to respective gateway per server and should help multiple segment controls	No Change in RFP
74	RFP for supply and installation of Web Application Firewall			Request clarification if this is a One OEM- One Bidder Bid or OEM can submit multiple bid through multiple bidders			One OEM can participate through multiple bidders/SI
75	Scope of work:	10	3.1	The bidder should perform a detailed configuration assessment after 1 year from date of installation.	Please confirm Scope for Detailed Configuration assessment after 1 year.		Will be shared with L1 bidder
76	Scope of work:	10	3.1	The bidder should migrate to new setup with no/minimum downtime as possible.	Please confirm existing WAF Solution in use if any		Its a new implementation
77	Scope of work:	10	3.1	The bidder should migrate to new setup with no/minimum downtime as possible.	Please confirm no of policies which we need to migrate to new WAF solution. As WAF policies created based on learning, implementaion timeline is dependent on the same.		Its a new implementation
78	Detailed Scope of Work	11	3.1	Bidder to specify the need of VM or other hardware for storage or hosting of application. Also, to mention rack, cable, space, power and storage required to host in-scope solutions. The bidder shall provide the year wise requirement of storage at both DC & DRS if required.	Please confirm Alerts/Sec generated on existing solution for sizing. Do we need to provide rack, cable, space, power and storage as part of solution for specified warranty & AMC duration i.e Total - 3years.		Will be shared with L1 bidder
79	Detailed Scope of Work	11	3.1	NPCI will provide the required Ethernet switch ports. However, bidder is required to mention the number of Ethernet switch ports required for in- scope solution.	Please confirm on following point as RFP ask is for. The solution appliances must have 2x10G SR Fiber Interfaces. The solution appliances must have 4x1G Ethernet Interfaces. NPCI need to provide no of port connectivity on switch as specified in RFP.		It’s a Minimum Requirement
80	Delivery schedule and location	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Based on our past experience, we have observed Hardware Appliance is delivered in 6 week's due to delivery & custom clearance. Request you to please change delivery timeline to 6 week.		No Change in RFP
81	Delivery schedule and location	22	8.7	All the trainings to be completed within 1 week from the date of request for training of NPCI officials and vendor resource based in NPCI.	Kindly mentioned no of days & participant per batches required for training		Atleast 3 to 5 days for selected NPCI per batch
82	Service Level Agreement (SLA) Requirements:	24	8.13	The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to NPCI or its designated personnel to the tools used for SLA monitoring.	Please clarify more in details		Will be shared with L1 bidder
83	Penalty on non-adherence to SLAs:	26	8.14	If a breach occurs even after a proper policy in WAF solution is in place, a penalty of Rs. 10,000/- per event will be deducted or the loss due to the breach whichever is higher	We will configure the WAF policies as per best recommended practices and NPCI requirement. An occurrence of breach may not be limited to WAF configuration, it all depends entire security posture within NPCI. Request you to eliminate this point		No Change in RFP
84	Service Level Agreement (SLA) Requirements:	24	8.13	All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.	Please confirm the how the solution needs to deployed in DC-DR scenario or Active-Active for two DC		Active - Passive
85	Penalty on non-adherence to SLAs:	26	8.14	The following Resolution Service Level Agreement (SLA) would be applicable during Warranty and AMC and are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only.	Resolution depends on nature of issues and the environment hnece it is difficult to provide resolution tome for any severity incidents. Request to change ot Response time SLA		Will be shared with L1 bidder
86	Section 9 - Technical Specifications	35	2.2	The solution must have a dedicated centralized management module/appliance.	Please confirm does bidder need to provide Hardware/VM to host centralized management & storage for next 3 years.		Yes Bidder to provide it and has be part of solution
87	RFP for supply and installation of Web Application Firewall	35	9	The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion	2 no. of 10G ports may be less considering investment for 5 years , network requirements and future traffic growth of NPCI	No Change in RFP, its minimum requirement

88	RFP for supply and installation of Web Application Firewall	6	57	The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)	Support for TLS 1.3 must be available once with draft 28 implemented (draft 26 can be used for testing , production traffic not recommended)	No Change in RFP, as we are projecting for 5 yrs and shoud be accessible for use when avaiable.
89	RFP for supply and installation of Web Application Firewall	12	41	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.	9K RSA and 5K ECC (2K Key Size) is too low considering the 2 Gbps of WAF throughput seeked and no. of transactions expected by NPCI considering future growth and ROI	Please refer to the Corrigendum - 1
90	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."	JavaScript and CAPTCHA are two different technologies and both must be added to deliver best in class secuirty features available with OEM. Also all features of BOT protection should be available to NPCI	Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
91	RFP for supply and installation of Web Application Firewall	64	63	The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause	This type of tracking is requird the activities of VPN user.	No Change in RFP
92	RFP for supply and installation of Web Application Firewall			Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.	This option and feature will help to identify non client browsers or request or bot attack as well.	No Change in RFP
93	RFP for supply and installation of Web Application Firewall	20	7.4	After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1
94	RFP for supply and installation of Web Application Firewall	21	1	Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
95	RFP for supply and installation of Web Application Firewall	22	8.7	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
96	RFP for supply and installation of Web Application Firewall	74	23	The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
97	RFP for supply and installation of Web Application Firewall	21	8.6	Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation?		Please refer to the Corrigendum - 1
98	RFP for supply and installation of Web Application Firewall			Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.	Segmentation controls application flow to respective gateway per server and should help multiple segment controls	No Change in RFP
99	RFP for supply and installation of Web Application Firewall			Request clarification if this is a One OEM- One Bidder Bid or OEM can submit multiple bid through multiple bidders			One OEM can participate through multiple bidders/SI
100	RFP for supply and installation of Web Application Firewall	11	Detailed Scope of Work	In case the bidder has not indicated any peripherals /equipment in their proposed solution and these may be required for the successful implementation of the Information Security Awareness solution, the successful bidder has to provide the required peripherals/equipment at no additional cost to NPCI.	If NPCI is looking for WAF integration with any NPCI's Information security solution , pls share the details		Soultion should be integragted with market standards avaiable solutions
101	RFP for supply and installation of Web Application Firewall	22	8.7 Delivery schedule and location	Delivery--The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order. Installation--The hardware and software Installation should be completed within 6 weeks of delivery of the hardware and software.Trainings--All the trainings to be completed within 1 week from the date of request for training of NPCI officials and vendor resource based in NPCI.	Request NPCI to Provide 6 weeks for delivery of hardware and software , 10 Weeks from Delivery date for the implimentation and 2 weeks to arrange trainings		No Change in RFP
102	RFP for supply and installation of Web Application Firewall	26	8.16 Repeat Order:	NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and services at the agreed unit rate, i.e. the rate contract for individual categories of WAF solution during the period of 1 year from the date of award / 1st Purchase Order.	Request NPCI to reduce this repeat order validity period to a maximum of 90 days from price discovery date.		No change in RFP
103	RFP for supply and installation of Web Application Firewall	27	8.18 Payment Terms:	AMC:AMC charges shall be paid quarterly in arrears after availing maintenance services after expiry of warranty period.	Request NPCI to release AMC payment as Yearly advance		No change in RFP
104	RFP for supply and installation of Web Application Firewall	26	8.14 Penalty on non-adherence to SLAs:	a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total contract value.	Request NPCI to revise the clause as below a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of **INR 5,000/-** (Indian Rupees **Five** Thousand only) for each hour of delay up to 24 hours, beyond 24 hours penalty would be **INR 10,000** for each hour with a max cap of 5% of total contract value.		No Change in RFP
105	RFP for supply and installation of Web Application Firewall	26	8.14 Penalty on non-adherence to SLAs:	b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total contract value.	Request NPCI to revise the clause as below: b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR **2,000**/- (Indian Rupees Two Thousand only) for each hour of delay up to **24** hours, beyond 24 hours penalty would be INR 5,000 for each hour with a max cap of 5% of total contract value.		No Change in RFP

106	RFP for supply and installation of Web Application Firewall	26	8.14 Penalty on non-adherence to SLAs:	c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total contract value.	Request NPCI to revise the clause as below: c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of **INR 1,000/-** (Indian Rupees one Thousand only) per hour with a max cap of 2% of total contract value.		No Change in RFP
107	22	8.7		**Delivery:** The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order. **Installation:** The hardware and software Installation should be completed within 6 weeks of delivery of the hardware and software. **Trainings:** All the trainings to be completed within 1 week from the date of request for training of NPCI officials and vendor resource based in NPCI.	**Delivery:** The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order. **Installation:** The hardware and software Installation should be completed within 8 weeks of delivery of the hardware and software. **Trainings:** All the trainings to be completed within 2 week from the date of request for training of NPCI officials and vendor resource based in NPCI.		No Change in RFP
108	27	8.18		**Payment Terms:** **Hardware:** 100% hardware cost shall be paid within 30 days after delivery and submission of correct invoice. **Installation:**100% installation cost shall be paid post implementation of the solution completely and duly certified by NPCI official. **AMC:** AMC charges shall be paid quarterly in arrears after availing maintenance services after expiry of warranty period.	**Payment Terms:** **Hardware:** 100% hardware cost shall be paid against delivery. **Installation:**100% installation cost shall be paid post implementation of the solution completely and duly certified by NPCI official. **AMC:** AMC charges shall be paid quarterly advance in arrears after availing maintenance services after expiry of warranty period.		No change in RFP
109	14	5.7		**Earnest Money Deposit (EMD): Rs 5, 00,000/-** (Rs Five Lakhs only) in the form of a Demand Draft / Pay order in favor of “National Payments Corporation of India” payable at Mumbai or Bank Guarantee issued by a scheduled commercial bank valid for six months, with a claim period of 12 months	EMD exemption against MSME certificate		National Payments Corporation of India (NPCI) is neither a Government Company nor it is any Department of Government of India. As such the extant provisions would not apply to NPCI.
110	35	9		The solution appliances must have 2x10G SR Fiber Interfaces	Request Change: The solution appliances must have 4 x10G SR Fiber Interfaces and support 40G interfaces for future expansion		No Change in RFP, its minimum requirement
111	6	57		The system should support TLS v1.2 & TLS v1.3	Request change :The system should support TLS v1.2 or TLS v1.3 (required in future)		No Change in RFP, as we are projecting for 5 yrs
112	12	41		The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Request Change: The solution must have a SSL hardware module to support minimum 20K SSL TPS on RSA and minimum 10K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key. System should also support 3K and 4K key size.		Please refer to the Corrigendum - 1
113				Request addition	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript and CAPTCHA challenges This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot."		Covered in Technical specication (Application DDOS Protection point no 3:- The proposed solution should have the capability to proactively identify bots
114	64	63		The solution must support user tracking using both form-based and certificate-based user authentication.	Request to remove this clause		No Change in RFP
115				Request addition	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers.		No Change in RFP
116	20	7.4		After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder.	Trust this is L1 commercial bid submission and not a Reverse Auction. Request confirmation		Please refer to the Corrigendum - 1
117	21	1		Customer BFSI reference in India	Request NPCI to confirm the no. of References to be submitted		Maximum refernces to be provided
118	22	87		The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order	Request Change: The Hardware and software shall be delivered within 6 weeks from the date of acceptance of the Purchase Order.		No Change in RFP
119	74	23		The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.	Request Change:The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of installation		No Change in RFP
120	21	8.6		Key Deliverables:TECHNICAL SCORING MATRIX	What is the Technical Scoring cutoff for Technical Bid Evaluation		Please refer to the Corrigendum - 1
121				Request addition	Request addition: The proposed solution should support min 4096 contexts or partitions or multiple profiling separately for each application without any additional license.		No Change in RFP
122				Proposed WAF Solution should be in the Leaders quadrant in the Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years	Since Last 3 years Gartner report of WAF is not stable and there has been lot of ups and down, like few vendors were not present in Leaders and were introduced and again removed.Request you to consider other reputated reports as well like Forrester Wave WAF Hence request you to consider “Proposed WAF Solution should be in the Leaders/Challengers quadrant in the Gartner Magic Quadrant or In leaders/Strong Performer in Forrester Wave for Web Application Firewalls”		No Change in RFP
123				The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat	Current Vulnerability assessment tool mentioned here are based on DAST integration which has limitation and is not obsolete technology against SAST tool which are more advanced and with Agile approach, customers don’t waste time having to wait for the development to be completed before testing security. SAST is a continues security development approach which makes it more secure since its working on the best practice. Few WAF solution has SAST capability build-in and no need to have such integration since they fix the vulnerability on its own. Hence request to modify the specs as below “The solution must support all the following web application vulnerability assessment tools (Web application scanners) or build-in Virtual Patching functionality to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat”		No Change in RFP, where as any additional functionalilty /tools would be considered as value addition

124	NPCI/RFP/2018-19/IT/17	54 of 74	1	Proposed WAF Solution should be in the Leaders quadrant in the Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years	Since Last 3 years Gartner report of WAF is not stable and there has been lot of ups and down, like few vendors were not present in Leaders and were introduced and again removed. Request you to consider other reputated reports as well like Forrester Wave WAF	Hence request you to consider "Proposed WAF Solution should be in the Leaders/Challengers quadrant in the Gartner Magic Quadrant or In leaders/Strong Performer in Forrester Wave for Web Application Firewalls"	No Change in RFP
125	NPCI/RFP/2018-19/IT/17	62 of 74	59	The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat	Current Vulnerability assessment tool mentioned here are based on DAST integration which has limitation and is not obsolete technology against SAST tool which are more advanced and with Agile approach, customers don't waste time having to wait for the development to be completed before testing security. SAST is a continues security development approach which makes it more secure since its working on the best practice. Few WAF solution has SAST capability build-in and no need to have such integration since they fix the vulnerability on its own.	Hence request to modify the specs as below "The solution must support all the following web application vulnerability assessment tools (Web application scanners) or build-in Virtual Patching functionality to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat"	No Change in RFP, where as any additional functionalilty /tools would be considered as value add