RFP for procurement of Web Application Firewall Solution- NPCI/RFP/2021-22/IT/12 dated 17.11.2021

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	7.3 Technical Scoring Matrix:	21	7.3	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	Kindly confirm if the Customer BFSI reference asked is specific to the Bidder for the proposed OEM only? i.e Pls clarify If it is the Bidder who should provde atleast 5 India BFSI References of the Proposed OEM only?		Bidder Should provide atleast 5 BFSI references in INDIA for proposed OEM. No Change in RFP Terms
2	8.8 Key Deliverables	24	9	OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution.	Can OEM propose the yearly review through Authorised Services Partner or OEM employee only?		OEM (Checker) is required to review as SI (maker) will be performing deployment. No Change in RFP Terms.
3	Section 9 - Technical Specifications	36	1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Pls clarify if OS, VM and Hardware will be provided by NPCI or Bidder needs to factor the same ?		Underlying Virtualization platform, OS & Hardware will be provided by NPCI. No Change in RFP Terms
4	Section 9 - Technical Specifications	44	8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Pls clarify if OEM can leverage the existing F5 BIG IQ Centralised Manager and logger setup(Hardware and Licenses) since the setup is already available in NPCI and will be free once the exisgting NPCINet devices will be removed?		OEM will have to do a sizing consideration if existing solution can handle additional load. No Change in RFP Terms
5	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, AND Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Magic Quadrant and Forrester benchmark vendors on many capabilities like - Product reach/coverage, execution capabilities, easy of deployment, market adaption etc…If we mention OR, this will open up for many none standard enterprise grade WAF solutions. Leading vendors cannot compete on commercial grounds. If you mention AND, atleast NPCI will receive bids from leading vendors	No Change in RFP Terms
6	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in the latest Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution	We request NPCI to consider only the Gartners REport considering the acceptance of Gartner in India BFSI customers and RFPS's in most of PSU customers. Almost none of the RFP's ever ask for Forrester report. Even NPCI has referred to Gartner in the past. Mentionining Forrrester Report will dilute the vendor selection criteria who lacks in features , support , stability, references in India Market.	No Change in RFP Terms

7	Section 9 - Technical Specifications	36	1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	L2 Trasnparent mode is supported feature by most vendors, but this usecase is directly not applicable to NPCI UPI segment. Kindly make this Good to have feature		No Change in RFP Terms
8	Section 9 - Technical Specifications	37	2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Requested change: Per WAF Instance must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to per instance ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Kindly confirm if the following understanding is correct- Per WAF instance should support ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) and per instance should be scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future.	Please refer to the Corrigendum - 1
9	Section 9 - Technical Specifications	37	2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	NPCI has a very good vision for SSL visibility in near future. We request NPCI to ask for SSL visibility references in banking sector, deployment should be up and running in PROD.		No Change in RFP Terms
10	Section 9 - Technical Specifications	38	3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Only Objuscation might not help much as there are many tools on internet to reverse engineer on obfuscation.Kindly change the point to The Proposed WAF solution must provide capabilities to obfuscate / encrypt / subsitute sensitive field names to defeat Man-in-The-Browser Attacks .		No Change in RFP Terms
11	Section 9 - Technical Specifications	40	3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	What is the use case of Converting back slash to forward slash character. ? Within UPI segment, traffic being XML, these usecases are not directly applicable. Kindly change to good to have.		No Change in RFP Terms, Its as per requirement
12	Section 9 - Technical Specifications	40	3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1

13	Section 9 - Technical Specifications	40	3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
14	Section 9 - Technical Specifications	41	3.67	The proposed Solution should be session aware and should be able to enforce and report session	What type of enforcement is expected here on session?		Policy enforcement. No Change in RFP Terms
15	Section 9 - Technical Specifications	42	3.73	The proposed Solution should remove application error messages from pages sent to users	What is the usecase here? If error message is removed, user will not have visibility of what is going wrong. Is it that we should send a custom response page ?		Application error messages may expose sensitive information. No Change in RFP Terms
16	Section 9 - Technical Specifications	42	3.74	The proposed Solution should prevent leakage of server code	What is meant by Server code ? DLP functionality can be achieved by integrating with network DLP via ICAP. Is that the usecase ?		Server Error Codes may expose sensitive information. No Change in RFP Terms
17	Section 9 - Technical Specifications	42	4.6	The Solution must be based on Intent oriented and User behavior Oriented	Are we referring to behaviour based detection / mitigation ?		Yes. No Change in RFP Terms.
18	Section 9 - Technical Specifications	43	4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	c. Semi Supervised machine learning to identify emerging Bot Patterns. - Need more clarity on this point. Why use semi level of AI/ML. The solution should have a full fledge AI/ML capabilities.		No Change in RFP Terms
19	Section 9 - Technical Specifications	43	4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
20	Section 9 - Technical Specifications	43	4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition

21	Section 9 - Technical Specifications	43	5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Apart from TOP 10 API security, NPCI should consider below list of security features for API security: Protect REST/JSON, XML, and GWT APIs. JSON Schema validation for API calls Protects against OWASP API Security Top 10 L7 Volumetric Behavioral DoS Protection Support and BOT mitigation GraphQL content profile and policy template Attack signatures on GraphQL traffic Query depth enforcement Support GraphQL batching Policy tuning with GraphQL violations DataGuard support (sensitive data protection) Declarative policy support Supports OpenAPI/Swagger format		No Change in RFP Terms, as reference would be always latest OWASP top 10 Vulnerabilites
22	Section 9 - Technical Specifications	43	5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	GraphQL is an open source data query language is a new way of developing API calls. NPCI should consider to have GraphQL security needs incorporated into RFP. GraphQL Landscape: https://landscape.graphql.org/zoom=150		No Change in RFP Terms
23	Section 9 - Technical Specifications	43	5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.			Mentioned as Good to have feature in RFP. No Change in RFP Terms.
24	Section 9 - Technical Specifications			Does NPCI Require inbuilt Additional capabilities of SSL VPN on the solution in future?	Since the ask is for Sotfware Based Solution, NPCI should have the flexibility for Addon Functionalities on the software for best Optimisation of Cost and Infrastucture		No Change in RFP Terms
25				Does NPCI Require Anti-bot Mobile SDK Support with Addon license in future?	Support for Mobile apps anti-bot sdk ensures that application access via handheld can be secured. WAF Should supports anti-bot SDK module for IoS and Android Apps which provides features such as Mobile Bot mitigation, Device Identification, Behavioral analysis, Jailbroken/root device detection, Emulator detection		No Change in RFP Terms
26	Section 8 - Terms and Conditions	28	8.19 Payme	AMC: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.	Request to change as Yearly advance instead of End of the Quarter.		No change in RFP

27	Section 7 - Bid Evaluation	21	7.3 Technical Scoring Matrix: Part – B Vendor Evaluation Matrix	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	We request you to allow other Organisation reference as apart from BFSI Sector like Defence, MHA, Governement organisations. Otherwise this clause will not allow MSME Companies to participate in the tender.		Bidder Should provide atleast 5 BFSI references in INDIA for proposed OEM. No Change in RFP Terms
28	Section 7 - Bid Evaluation	21	7.3 Technical Scoring Matrix: Part – B	Work experience in past (similar project)	We request you to allow other Organisation reference as apart from BFSI Sector like Defence, MHA, Governement organisations. Otherwise this clause will not allow MSME Companies to participate in the tender.		No Change in RFP Terms
29	Section 8 - Terms and Conditions	23	8.2 Term 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 deliverables as specified in the RFP would be at a fixed rate.	Please confirm warranty is for one years or three years.		1 year Warranty + 2 year AMC. No Change in RFP Terms.
30	Section 8 - Terms and Conditions	23	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 1 year, 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 does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.	Please confirm warranty is for one years or three years. Or we have to submit PBG for 12 Months with claim period of 12 Months.		Warranty is to be provided for 1 year and 2 year AMC. PBG needs to be provided with the validity 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). Same will be notified in corrigendum shortly.
31	Section 9 - Technical Specifications	36	1.4	The bidder should have support offices in Mumbai, Hyderabad and Chennai.	Requested to allow relaxation on this. As many bidders will not have offices in all the three cities. Requested you to allow atleast bidder should have one office in these cities and should have support staff at remaining places before the project is implemented.		Support offices required in Mumbai, Hyderabad and Chennai as a part of Datacenter support in case of technical issues which cannot be resolved remotely. No Change in RFP Terms
32	Section 9 - Technical Specifications	36	1.5	The bidder should have minimum 2 skilled OEM certified staff (Web Application Firewall - Subject Matter Experts) for the product proposed.	Requested you to allow bidder should have certified Engineer of WAF Technology, otherwise it will give advantage to limited bidders only.		No Change in RFP Terms

33	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	65	3.8	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	Different OEM have different ways to mitigate and build policy, Virtual Patching with third party integration is very slow and inefficient process since to scan a website it takes more than 3-4 days depending on size of application and recommendations based on scanning still requires learning. There are OEM who also have building Virtual Patching like feature to scan for vulnerability and build policy automatically and continuously.	**Hence request to modify the clause as per below:** The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Either Internally within WAF or via external tools like Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value add
34	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	DAM Solution is altogether different technology and there is no correlation between DAM and WAF to protect the application and both can work independently to protect the application. **This is single OEM Specific, no other OEM's support this.**	**Hence request to delete this clause.**	Mentioned as Good to have in RFP. No Change in RFP Terms.
35	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	4	Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation	BOT Solution with advance BOT detection needs sizing with respect to number of monthly flows volume and not based on Concurrent session. **Hence needs sizing based on how many requests volume the application has to handle in multiples of 50Million request per month.**	**Request to share the Sizing details for BOT**	It has to match mentioned workloads in this RFP
36	Section 8 - Terms and Conditions	24	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 1 year, 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 does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.	Request NPCI to reduce the value of performance Bank Guarantee to 3% based on the circular No.F.9/4/2020-PPD dated 12th November,2020 issued by the Government of India, Ministry of Finance, Department of Expenditure Procurement Policy Division.		These rules prima facie are directed at CPSEs. NPCI is a not for profit company established under section 25 of Companies Act. Therefore the contents of circular No.F.9/4/2020-PPD dated 12th November,2020 do not seem to apply to a private entity like NPCI. We have, however, not done an in depth analysis of this circular hence vendor to come back with specifics in case they believe the circular applies to private entities.

37	Section 8 - Terms and Conditions	26	8.9 Delivery schedule	Delivery, installation & commissioning of the proxy solution should be completed within 16 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks. • Installation & commissioning should be completed in next 10 weeks. • Installation Certificate for each installation should be signed by NPCI and the bidder	As there global chip shortage all OEM in this space have major delivery issues. Can NPCI move delivery of hardware to 16 weeks without any LD and modify the project schedule accordingly. Also request npci to change this to "Delivery, installation & commissioning of the proxy solution should be completed within 24 weeks from the date of receipt of purchase order."		These rules prima facie are directed at CPSEs. NPCI is a not for profit company established under section 25 of Companies Act. Therefore the contents of circular No.F.9/4/2020-PPD dated 12th November,2020 do not wseem to apply to a private entity like NPCI. We have, however, not done an in depth analysis of this circular hence vendor to come back with specifics in case they believe the circular applies to private entities.
38	Section 8 - Terms and Conditions	25	8.11 End of Sale	The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.	Reqeust NPCI to consider the End of Sale (EOSL) period as maximum 1 year only as there will be revision and updage on products every year. Request NPCI to consider the clause as :- "The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL)~~ or would become EOSL during the contract period~~. Further, if any of the components is declared **End of Support** ~~EOSL~~ during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI."		Refer to Maharashtra Stamp Act and stamp duty payable for Power of Attorney of this specific type

39	Section 8 - Terms and Conditions	28	8.15 Penalty on non-adherence to SLAs:	The following Resolution Service Level Agreement (SLA) would be applicable during Warranty are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only. 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 value. 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 value. 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 value. d) The penalty amount would be calculated and deducted from the performance bank	Reqeust NPCI to specify the CAP for SLA penalty as 10% of product value.		No change in RFP
40	Section 8 - Terms and Conditions	30	8.17 Repeat Order:	NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and/or services included in the Solution at the agreed unit rate for individual categories of purchase order during the period of 3 years from the date of award / 1st Purchase Order.	Request NPCI to consider the repeat order validity as maximum 6 months from the price discovery date.		No change in RFP
41	Section 9 - Technical Specification	36	1.1 - Techni	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		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.
42	Section 9 - Technical Specification	37	3.2 - Techni	Proposed solution should be ICSA Lab Certified	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		Mentioned as Good to have feature in RFP. No Change in RFP Terms.

43	Section 5	15	5.6 - EMD	EMD - 500000	As per latest circular from Government of Finacne EMD shall be relax the bidder.		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. Hence EMD and tender cost are to be paid by Bidder.
44	7.3 Technical Scoring Matrix:	21	7.3	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	Kindly confirm if the Customer BFSI reference asked is specific to the Bidder for the proposed OEM only? i.e Pls clarify If it is the Bidder who should provde atleast 5 India BFSI References of the Proposed OEM only?		Bidder Should provide atleast 5 BFSI references in INDIA for proposed OEM. No Change in RFP Terms
45	8.8 Key Deliverables	24	9	OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution.	Can OEM propose the yearly review through Authorised Services Partner or OEM employee only?		OEM (Checker) is required to review as SI (maker) will be performing deployment. No Change in RFP Terms.
46	8.9 Delivery Schedule	25	8.9	Delivery, installation & commissioning of the proxy solution should be completed within 16 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks.	Kindly confirm if the OS, VM and Hardware would be provided by NPCI or Bidder needs to factor in their proposal?	In view of the material shortages across the semiconductor industry impacting global supply chains, the lead time for hardware delivery would be 24-27 weeks. Reqeust to amend the delivery timelines in the RFP accordingly.	Underlying Virtualization platform, OS & Hardware will be provided by NPCI.No Change in RFP Terms
47	Section 9 - Technical Specifications	36	1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Pls clarify if OS, VM and Hardware will be provided by NPCI or Bidder needs to factor the same ?		Underlying Virtualization platform, OS & Hardware will be provided by NPCI. No Change in RFP Terms
48	Section 9 - Technical Specifications	44	8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Pls clarify if OEM can leverage the existing F5 BIG IQ Centralised Manager and logger setup(Hardware and Licenses) since the setup is already available in NPCI and will be free once the exisgting NPCINet devices will be removed?		OEM will have to do a sizing consideration if existing solution can handle additional load. No Change in RFP Terms
49	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, AND Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Magic Quadrant and Forrester benchmark vendors on many capabilities like - Product reach/coverage, execution capabilities, easy of deployment, market adaption etc…If we mention OR, this will open up for many non standard enterprise grade WAF solutions. Leading vendors cannot compete on commercial grounds. If you mention AND, atleast NPCI will receive bids from leading vendors	No Change in RFP Terms

50	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in the latest Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution	We request NPCI to consider only the Gartners Report considering the acceptance of Gartner in India BFSI customers and RFPS's in most of PSU customers. Almost none of the RFP's ever ask for Forrester report. Even NPCI has referred to Gartner in the past. Mentionining Forrester Report will dilute the vendor selection criteria who lacks in features , support , stability, references in India Market.	No Change in RFP Terms
51	Section 9 - Technical Specifications	36	1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	L2 Trasnparent mode is supported feature by most vendors, but this usecase is directly not applicable to NPCI UPI segment. Kindly make this Good to have feature		No Change in RFP Terms
52	Section 9 - Technical Specifications	37	2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Requested change: Per WAF Instance must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to per instance ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Kindly confirm if the following understanding is correct- Per WAF instance should support ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) and per instance should be scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future.	Please refer to the Corrigendum - 1
53	Section 9 - Technical Specifications	37	2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	NPCI has a very good vision for SSL visibility in near future. We request NPCI to ask for SSL visibility references in banking sector, deployment should be up and running in PROD.		No Change in RFP Terms
54	Section 9 - Technical Specifications	38	3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Only Obfuscation might not help much as there are many tools on internet to reverse engineer on obfuscation.Kindly change the point to "The Proposed WAF solution must provide capabilities to obfuscate / encrypt / subsitute sensitive field names to defeat Man-in-The-Browser Attacks."		No Change in RFP Terms
55	Section 9 - Technical Specifications	40	3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	What is the use case of Converting back slash to forward slash character. ? Within UPI segment, traffic being XML, these usecases are not directly applicable. Kindly change to good to have.		No Change in RFP Terms, Its as per requirement

56	Section 9 - Technical Specifications	40	3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
57	Section 9 - Technical Specifications	40	3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
58	Section 9 - Technical Specifications	41	3.67	The proposed Solution should be session aware and should be able to enforce and report session	What type of enforcement is expected here on session?		Policy enforcement. No Change in RFP Terms
59	Section 9 - Technical Specifications	42	3.73	The proposed Solution should remove application error messages from pages sent to users	What is the use case here? If error message is removed, user will not have visibility of what is going wrong. Is it that we should send a custom response page ?		Application error messages may expose sensitive information. No Change in RFP Terms
60	Section 9 - Technical Specifications	42	3.74	The proposed Solution should prevent leakage of server code	What is meant by Server code ? DLP functionality can be achieved by integrating with network DLP via ICAP. Is that the usecase ?		Server Error Codes may expose sensitive information. No Change in RFP Terms
61	Section 9 - Technical Specifications	42	4.6	The Solution must be based on Intent oriented and User behavior Oriented	Are we referring to behaviour based detection / mitigation ?		Yes. No Change in RFP Terms.
62	Section 9 - Technical Specifications	43	4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	c. Semi Supervised machine learning to identify emerging Bot Patterns. - Need more clarity on this point. Why use semi level of AI/ML. The solution should have a full fledge AI/ML capabilities.		No Change in RFP Terms

63	Section 9 - Technical Specifications	43	4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
64	Section 9 - Technical Specifications	43	4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
65	Section 9 - Technical Specifications	43	5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Apart from TOP 10 API security, NPCI should consider below list of security features for API security: Protect REST/JSON, XML, and GWT APIs. JSON Schema validation for API calls Protects against OWASP API Security Top 10 L7 Volumetric Behavioral DoS Protection Support and BOT mitigation GraphQL content profile and policy template Attack signatures on GraphQL traffic Query depth enforcement Support GraphQL batching Policy tuning with GraphQL violations DataGuard support (sensitive data protection) Declarative policy support Supports OpenAPI/Swagger format		No Change in RFP Terms, as reference would be always latest OWASP top 10 Vulnerabilites
66	Section 9 - Technical Specifications	43	5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	GraphQL is an open source data query language is a new way of developing API calls. NPCI should consider to have GraphQL security needs incorporated into RFP. GraphQL Landscape: https://landscape.graphql.org/zoom=150		No Change in RFP Terms
67	Section 9 - Technical Specifications	43	5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.			Mentioned as Good to have feature in RFP. No Change in RFP Terms.
68	Section 9 - Technical Specifications	NA	NA	Does NPCI Require inbuilt Additional capabilities of SSL VPN on the solution in future?	Since the ask is for Sotfware Based Solution, NPCI should have the flexibility for Addon Functionalities on the software for best Optimisation of Cost and Infrastucture		No Change in RFP Terms

69	Section 9 - Technical Specifications	NA	NA	Does NPCI Require Anti-bot Mobile SDK Support with Addon license in future?	Support for Mobile apps anti-bot sdk ensures that application access via handheld can be secured. WAF Should supports anti-bot SDK module for IoS and Android Apps which provides features such as Mobile Bot mitigation, Device Identification, Behavioral analysis, Jailbroken/root device detection, Emulator detection		No Change in RFP Terms
70	Section 1	36	1.8	The Proposed Solution should have capability to deploy/integrate in Virtualized Environment/Opensource environments - Openstack, LinuxKVM etc.	Need more clarification		Solution to be deployed in Opensource Virtualization Software. No Change in RFP Terms
71	Section 1	36	1.9	The proposed solution should provide integrated functionalities of server load balancer, SSL Offloading, SSL Bridging.	WAF is dedicate solution for Web Application security so request to remove Load balancer requirement from this section		No Change in RFP Terms
72	Section 1	36	1.10	The proposed solution must support TCP multiplexing, TCP optimization and dynamic Service chaining for SSL Offload with TCP session mirroring and persistence mirroring, compression, caching etc. in active-passive mode.	This is Load balancing features so request to remove this clause		No Change in RFP Terms
73	Section 1	36	1.11	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event	Need more clarity or explanation		Mentioned as Good to have feature in RFP. No Change in RFP Terms.
74	Section 1	36	1.19	Should support IPv4 & IPv6 addressing, IPv6 client and IPv4 servers with NAT44/NAT66/NAT64/NAT46 with full support for IPv6	WAF does support IPv4 & IPv6 Traffic Inspection as well onbaording application on WAF using IPv4 & IPv6 but NAT features are either used by Load Balancer or Network Firewall so request to revise this clause as **"Should Support IPv4 & IPv6 Adressing"**		No Change in RFP Terms
75				Should support routing protocols RIP, OSPF and BGP to participate in Dynamic routing	Request to to remove this clause as WAF should be dedicately used for Application security purpose instead routing		No Change in RFP Terms
76	Section 3	37	3.2	Proposed solution should be ICSA Lab Certified WAF	Request to revise this clause as **"Proposed Solution should be ICSA. Or ISO270001 certified WAF"**		Mentioned as Good to have feature in RFP. No Change in RFP Terms.
77	Section 3	37	3.7	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over.	Staging requirement is single OEM specific so request to revise this clause as **"Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage."**		Please refer to the Corrigendum - 1

78	Section 4 Eligiblity Criteria	42	4.7	The Solution must able to detect below type of attacks created by Bad Bots. a. Account take over b. Web Scrapping c. Application DDoS e. Form Spam f. API Abuse	Most of the points are relevant to Advanced Bot Protection which does require separate license in order to support this requirement. So need clarification is there Advanced Bot Protection Licnese should be consider here or not.		Additional licenses to be considered as per technical requirements. No Change in RFP Terms
79	Section 4 Eligiblity Criteria	43	4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	Most of the points are relevant to Advanced Bot Protection which does require separate license in order to support this requirement. So need clarification is there Advanced Bot Protection Licnese should be consider here or not.		Additional licenses to be considered as per technical requirements. No Change in RFP Terms
80	Section 4 Eligiblity Criteria	43	4.14	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, Image and Sound 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.	Most of the points are relevant to Advanced Bot Protection which does require separate license in order to support this requirement. So need clarification is there Advanced Bot Protection Licnese should be consider here or not.		Additional license to be considered as per technical requirement mentioned in RFP. Please refer to the Corrigendum - 1
81	Section 4 Eligiblity Criteria	43	4.15	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup	Most of the points are relevant to Advanced Bot Protection which does require separate license in order to support this requirement. So need clarification is there Advanced Bot Protection Licnese should be consider here or not.		Additional licenses to be considered as per technical requirements. No Change in RFP Terms
82	Section 5	43	5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	This is Advanced API security feature requirement which is currently not available for on-prem WAF solution so request to remove this caluse.		Mentioned as Good to have feature in RFP. No Change in RFP Terms.

83	Section 6	44	6.2	Should support seamless failover between devices in active-active/ active-standby, the failover should be transparent to other networking devices with SSL session mirroring capabilities	WAF does have dependency on upstream device to for failover so session mirroring is not available in WAF or other WAF vendor who provides WAF along with LB can only provide SSL session mirroring capabilities so request to revise rhis clause as **"Should support seamless failover between devices in active-active/ active-standby, the failover should be transparent to other networking devices"**		No Change in RFP Terms
84	Section 6	44	6.5	Proposed solution should provide SSL offloading with the TCP connection and persistence session mirroring during the HA failover for all connections so that TCP connections are not lost during a failover event.	WAF vendor who provides WAF along with LB can only provide SSL session mirroring capabilities so request to rremove this clause		No Change in RFP Terms
85	Section 7 - Bid Evaluation	44	7.1	Should provide individual health check for each Link and In case of link failure device should detect it in not more than 30 seconds	This are Load Balancing feature to check healt check of servers or application and WAF is dedicate solution for application security only so request to remove this clause		No Change in RFP Terms
86	Section 7 - Bid Evaluation	44	7.2	Should be able to do health check on protocols like HTTP, HTTPS, SMTP, POP, TCP Ports etc.	This are Load Balancing feature to check healt check of servers or application and WAF is dedicate solution for application security only so request to remove this clause		No Change in RFP Terms
87	Section 7 - Bid Evaluation	44	7.3	Should provide AND , OR mechanisms between multiple health checks	This are Load Balancing feature to check healt check of servers or application and WAF is dedicate solution for application security only so request to remove this clause		No Change in RFP Terms
88	Section 7 - Bid Evaluation	21	7.3	Please provide at least 5 India References	Kindly confirm whether we need to provide 5 refences only WAF. Or any 5 security solution references are acceptable		Reference for WAF only will be considered. No Change in RFP Terms.
89	Section 8 - Terms and Conditions	23	8.4	Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order	Kindly consider PBG equal to 3% of total value of the PO (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months		These rules prima facie are directed at CPSEs. NPCI is a not for profit company established under section 25 of Companies Act. Therefore the contents of circular No.F.9/4/2020-PPD dated 12th November,2020 do not wseem to apply to a private entity like NPCI. We have, however, not done an in depth analysis of this circular hence vendor to come back with specifics in case they believe the circular applies to private entities.
90	Section 8 - Terms and Conditions	25	8.9	Delivery period -16 weeks	Kindly consider the delivery period to 18 weeks as migration and fine tunning can take some time.		No Change in RFP Terms

91	RFP	3	Checklist	Remittance proof in favor of “National Payments Corporation of India” payable at Mumbai” amounting to Rs. 11,800/- (Rs. 10,000/- plus GST @18 %) towards bid purchase cost and Rs. 5,00,000/- towards Bid Security.	As per the Finance ministry circular dt: 12th Nov. 2020, it is reiterated in the Procurement Manuals, no provisions regarding Bid Security should be kept in the Bid Documents in future and only provision for Bid Security Declaration should be kept in the Bid Documents. Request to Waive off the EMD against which we shall provide Bid Security Declaration that we may be liable to be suspended from participation in any future tenders of the Bank if 1. The bid submitted by us is withdrawn/modified during the period of bid validity. 2. If any statement or any form enclosed by us as part of this Bid turns out to be false / incorrect at any time during the period of prior to signing of Contract. 3. In case of we becoming successful bidder and if: a) we fail to execute Contract within the stipulated time. b) we fail to furnish Performance Bank Guarantee within the timelines stipulated in this RFP document.	Request to wavie off EMD with Bid Security Declaration	These rules prima facie are directed at CPSEs. NPCI is a not for profit company established under section 25 of Companies Act. Therefore the contents of circular No.F.9/4/2020-PPD dated 12th November,2020 do not seem to apply to a private entity like NPCI. We have, however, not done an in depth analysis of this circular hence vendor to come back with specifics in case they believe the circular applies to private entities.
92	RFP	25	8.9 Delivery schedule	• Delivery of hardware, software, and license should be within 6 weeks.	Kindly extend the delivery schedule to 8-10 weeks as delivery of related hardware would be a challenge in present difficult times.		No Change in RFP Terms
93	RFP	25	8.10 Penalty for default in delivery	Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5%.	Request not to impose penalty before 16 weeks as delivery will be difficult within 6 weeks .		
94	RFP	28	8.19 Payment Terms:	AMC: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.	AMC for Software solution is charged by the OEMs yearly in advance. Inorder to unneccessary load interest charges on the overall project cost. Kindly consider payment terms on AMC as yearly in advance.		No change in RFP

95	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	65	3.8	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	Different OEM have different ways to mitigate and build policy, Virtual Patching with third party integration is very slow and inefficient process since to scan a website it takes more than 3-4 days depending on size of application and recommendations based on scanning still requires learning. There are OEM who also have building Virtual Patching like feature to scan for vulnerability and build policy automatically and continuously.	**Hence request to modify the clause as per below:** The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Either Internally within WAF or via external tools like Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value add
96	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	DAM Solution is altogether different technology and there is no correlation between DAM and WAF to protect the application and both can work independently to protect the application. **This is single OEM Specific, no other OEM's support this.**	**Hence request to delete this clause.**	Mentioned as Good to have in RFP. No Change in RFP Terms.
97	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	4	Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation	BOT Solution with advance BOT detection needs sizing with respect to number of monthly flows volume and not based on Concurrent session. **Hence needs sizing based on how many requests volume the application has to handle in multiples of 50Million request per month.**	**Request to share the Sizing details for BOT**	It has to match mentioned workloads in this RFP
98	NPCI/RFP/2021-22/IT/12	Page no. 36	Section 9 / Technical Specification / Point no. 1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		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.
99	NPCI/RFP/2021-22/IT/12	Page no. 37	Section 9 / Technical Specification / Point no. 3.2	Proposed solution should be ICSA Lab Certified WAF	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		Mentioned as Good to have feature in RFP. No Change in RFP Terms.

100	NPCI/RFP/2021-22/IT/12	Page n	Section 1 /Bid Schedule and Address/Point no.12	Bid Cost Rs. 11,800/- (Rs. 10,000/- plus GST @18 %)	Can we get Exemption Allow through MSME Certificate for Bid Cost		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. Hence EMD and tender cost are to be paid by Bidder irrespective of being a MSME
101	NPCI/RFP/2021-22/IT/12	Page n	Section 1 /Bid Schedule and Address/Point no.13	Rs. 5,00,000/- (Rupees Five lakhs only)	Can we get Exemption Allow through MSME Certificate for EMD/Bid security		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. Hence EMD and tender cost are to be paid by Bidder irrespective of being a MSME
102	NPCI/RFP/2021-22/IT/12	Page no.17	Section 5/ Instruction to Bidders/Point no.5.15 Bid Submission	The Bidder should bear all the costs associated with the preparation and submission of their bid and NPCI will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process. Bids sealed in accordance with the instructions to Bidders should be delivered at the address as mentioned in the Section 1.	Bid's hard copy submission required?		Due to Covid Pandamic electronic bid response submission is acceptable. For further details on electronic bid submission kindly refer Section 1 - Bid Scheduled and Address
103	NPCI/RFP/2021-22/IT/12	Page no.16 & 17	Section 5/ Instruction to Bidders/point no.5.13	5.13 Envelope/Folder bidding process The Bid shall be prepared in 3 different folders i.e Folder A, Folder B and Folder C. Each of the 3 folders shall then be sealed and put into an outer Envelope/Folder marked as “Request for Proposal for procurement of Web Application Firewall Solution”.In light of the lock imposed due to the COVID-19 pandemic, bids should be submitted through email. Folder A (Eligibility) & Folder B (Technical) and Folder C (Commercial) to the following email ids:	when to submit a Comercial bid? /Folder C.		Eligiblity, Technical and Commercial Bid Submission date is same i.e. 10th December 2021. Commercial Bid to be submitted in the Password protected PDF document. The password to be shared only after request from NPCI’s designated authority. For further details kindly refer Section 1 - Bid Scheduled and Address.
104	NPCI/RFP/2021-22/IT/12	Page no. 17	Section 5/ Instruction to Bidders/ point no. 5.14/folder	Folder C - Commercial Bid (should be password encrypted) 1 Commercial Bid Form – Annexure M 2 Commercial Bid – Annexure N 3 Detailed Bill of Material – Annexure L	File type Xecel or PDF?		The file format of bids submitted should be in PDF.
105	NPCI/RFP/2021-22/IT/12	Page no.56	Annexure G / Format Power of Attorney	On Stamp paper of relevant value	Please specify the amount (INR) to be mentoned on stamp paper as power of attorney		Refer to Maharashtra Stamp Act and stamp duty payable for Power of Attorney of this specific type

106	NPCI/RFP/2021-22/IT/12	Page no.63	Section 11 / Documents to be put in Envelope/ Annexure-J/Point no. 1.4	The bidder should have support offices in Mumbai, Hyderabad and Chennai.	Is this compulsory?		Support offices required in Mumbai, Hyderabad and Chennai as a part of Datacenter support in case of technical issues which cannot be resolved remotely. No Change in RFP Terms
107	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	65	3.8	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	Different OEM have different ways to mitigate and build policy, Virtual Patching with third party integration is very slow and inefficient process since to scan a website it takes more than 3-4 days depending on size of application and recommendations based on scanning still requires learning. There are OEM who also have building Virtual Patching like feature to scan for vulnerability and build policy automatically and continuously.	**Hence request to modify the clause as per below:** The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Either Internally within WAF or via external tools like Whitehat, Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value add
108	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	DAM Solution is altogether different technology and there is no correlation between DAM and WAF to protect the application and both can work independently to protect the application. **This is single OEM Specific, no other OEM's support this.**	**Hence request to delete this clause.**	Mentioned as Good to have in RFP. No Change in RFP Terms.
109	RFP-for-procurement-of-WAF-Solution; Annexure J - Technical Compliance	70	4	Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation	BOT Solution with advance BOT detection needs sizing with respect to number of monthly flows volume and not based on Concurrent session. **Hence needs sizing based on how many requests volume the application has to handle in multiples of 50Million request per month.**	**Request to share the Sizing details for BOT**	It has to match mentioned workloads in this RFP
110	4.1 Eligibility Criteria	12	2.1	The bidder should have reported minimum annual turnover of Rs. 15 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered.	We request to amend the caluse as " Should we have **Positive NETWORTH** instead of profit after tax in last 3 financial years (FY 2018-19, 2019-20, 2020-21). Or should be Profit **After Tax in any two FY.**	We request you to amend the caluse as Due to Pandemic our Profit after Tax is not there in FY-20-21 however we have postive networth. In lockdown the profit after tax affected due to many reason. All other PSU BFSI considering this caluse and giving relaxation for FY20-21. PLease help to amend so that we can submit our BID.	No change in RFP

111	8.19 Payment Terms:	28	8.19	AMC: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.	Please help to amend this as AMC payment Yearly advance agsint PBG		No change in RFP
112	NPCI/RFP/2021-22/IT/12	Page no. 36	Section 9 / Technical Specification / Point no. 1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		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.
113	NPCI/RFP/2021-22/IT/13	Page no. 37	Section 9 / Technical Specification / Point no. 3.2	Proposed solution should be ICSA Lab Certified WAF	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		Mentioned as Good to have feature in RFP. No Change in RFP Terms.
114	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Request to consider last two years as 2019-20. Last Forrester wave report released was in 2020. Latest Gartner Magic Quadrant has more focus on Cloud Vendors & SaaS Offerings for evaluation. Gartner believes the future of the Web Application and API (WAAP) market will be dominated by solutions delivered via cloud rather than as an on-premise, appliance or VM solution. However customers today need a full range of deployment options, including on premise, hybrid, and cloud, and that we serve our customers best by delivering a full range of deployment Hence request you to change this clause as **"The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution (Two of last 3 years), or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years)."**		No Change in RFP Terms

115	Section 9 - Technical Specifications	36	1.11	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event	This is vendor specific, we offer same function through the GUI and for us scripting is not required. Hence request you to modify this clause as "**The proposed solution must offer out of band programming for control plane along with data plane scripting or through GUI for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event or capable to configure through GUI.**"		Mentioned as Good to have feature in RFP. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value add
116	Section 9 - Technical Specifications	36	1.12	The proposed solution must support policy nesting at layer4 and layer? to address the complex application integration	This Clause is related to ADC vendors and not a WAF specific. Hence request you to remove this clause.		No Change in RFP Terms
117	Section 9 - Technical Specifications	36	1.14	The proposed solution should have a feature to generate device snapshot reports which then should be uploaded to an OEM provided online tool and get feedback on the health of the unit & missing Hotfixes and best practices	This Clause is vendor specific and hence request you to modify this clause as "**The proposed solution should have a feature to generate device snapshot reports which then should be uploaded to an OEM provided online tool and get feedback on the health of the unit & missing Hotfixes and best practices or share the configuration to OEM TAC Support to get the recommendations**"		No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value add
118	Section 9 - Technical Specifications	37	1.20	Should support routing protocols RIP, OSPF and BGP to participate in Dynamic routing	What is use case from WAF perspective? WAF is more "near-to-server" kind of deployment. Hence request you to remove this clause from the RFP.		No Change in RFP Terms
119	Section 9 - Technical Specifications	37	3.4	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions to address the compliances and configure policies for it.	Kindly modify this clause as "**The solution should provide OWASP Compliance Dashboard / Report which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions to address the compliances and configure policies for it.**"		No Change in RFP Terms
120	Section 9 - Technical Specifications	38	3.18	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Kindly also include the use case like BOT and crawlers apart from only Brute Force. Hence request you to modify this clause as "**Proposed solution should have capability to redirect Brute force attack or BOT or Crawlers traffic to Honey Pot page.**"		No Change in RFP Terms

121	Section 9 - Technical Specifications	39	3.29	Should be able to uniquely detect and block if required the end user on the basis of internal IP address, Plugins Installed in the browser, OS, Screen Resolution, Fonts etc. instead of going with traditional IP based blocking only	This was a older method called as Device Fingerprinting. And request you to add advance way of identifying clients on basis of unique Session ID. Hence request you to modify this clause as "**Should be able to uniquely detect and block if required the end user on the basis of internal IP address, Plugins Installed in the browser, OS, Screen Resolution, Fonts etc. and identifying clients on basis of unique Session ID instead of going with traditional IP based blocking only**"		No Change in RFP Terms
122	Section 9 - Technical Specifications	41	3.71	The proposed Solution should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.	This was a older method called as Device Fingerprinting. And request you to add advance way of identifying clients on basis of unique Session ID. Hence request you to modify this clause as "**The proposed Solution should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc and identifying clients on basis of unique Session ID**"		No Change in RFP Terms
123	Section 9 - Technical Specifications	42	3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	This is vendor specific and hence request you to remove this clause from the RFP.		Mentioned as Good to have in RFP. No Change in RFP Terms.
124	Section 9 - Technical Specifications	42	4.4	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot h. Custom business logic	Custom Business logic is a vendor specific and hence request you to remove point "Custom business logic" from the RFP.		Please refer to the Corrigendum - 1
125	Section 9 - Technical Specifications	42	4.6	The Solution must be based on Intent oriented and User behavior Oriented	kindly clarify the use case of this clause. What is Intent oriented ?		No Change in RFP Terms
126	Section 9 - Technical Specifications	43	4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	If a Anti-DDOS solution already in place then the DDOS attack should not hit the Web Application Firewall which is in a Application Segment. Again this is vendor specific and hence request you to remove this clause from the RFP.		No Change in RFP Terms

127	Section 9 - Technical Specifications	43	4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	If a Anti-DDOS solution already in place then the DDOS attack should not hit the Web Application Firewall which is in a Application Segment. Again this is vendor specific and hence request you to remove this clause from the RFP.		No Change in RFP Terms
128	Section 9 - Technical Specifications	43	4.14	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, Image and Sound 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.	Kindly make the or statement for Image or Sound CAPTCHA challenges. Because other OEM don’t support Sound captcha function.		Please refer to the Corrigendum - 1
129	Section 9 - Technical Specifications	44	7.1	Should provide individual health check for each Link and In case of link failure device should detect it in not more than 30 seconds	This is a Link load balancer function and not the WAF. Again ADC vendor support this function but not the WAF vendor and hence request you to remove this cluase from the RFP. Kindly let us know what is the use case of doing link health check from WAF.		No Change in RFP Terms
130	Section 9 - Technical Specifications	44	7.2	Should be able to do health check on protocols like HTTP, HTTPS, SMTP, POP, TCP Ports etc.	What is the use case of SMTP and POP helth checks in WAF. The WAF is for HTTP/HTTPS and not for SMTP and POP. Hence request you to modify this clause as "**Should be able to do health check on protocols like HTTP, HTTPS, , TCP Ports etc.**"		No Change in RFP Terms
131	7.3 Technical Scoring Matrix:	21	7.3	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	Kindly confirm if the Customer BFSI reference asked is specific to the Bidder for the proposed OEM only? i.e Pls clarify If it is the Bidder who should provde atleast 5 India BFSI References of the Proposed OEM only?		Bidder Should provide atleast 5 BFSI references in INDIA for proposed OEM. No Change in RFP Terms

132	8.8 Key Deliverables	24	9	OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution.	Can OEM propose the yearly review through Authorised Services Partner or OEM employee only?		OEM (Checker) is required to review as SI (maker) will be performing deployment. No Change in RFP Terms.
133	Section 9 - Technical Specifications	36	1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Pls clarify if OS, VM and Hardware will be provided by NPCI or Bidder needs to factor the same ?		Underlying Virtualization platform, OS & Hardware will be provided by NPCI. No Change in RFP Terms
134	Section 9 - Technical Specifications	44	8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Pls clarify if OEM can leverage the existing F5 BIG IQ Centralised Manager and logger setup(Hardware and Licenses) since the setup is already available in NPCI and will be free once the exisgting NPCINet devices will be removed?		OEM will have to do a sizing consideration if existing solution can handle additional load. No Change in RFP Terms
135	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, AND Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Magic Quadrant and Forrester benchmark vendors on many capabilities like - Product reach/coverage, execution capabilities, easy of deployment, market adaption etc…If we mention OR, this will open up for many none standard enterprise grade WAF solutions. Leading vendors cannot compete on commercial grounds. If you mention AND, atleast NPCI will receive bids from leading vendors	No Change in RFP Terms
136	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in the latest Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution	We request NPCI to consider only the Gartners REport considering the acceptance of Gartner in India BFSI customers and RFPS's in most of PSU customers. Almost none of the RFP's ever ask for Forrester report. Even NPCI has referred to Gartner in the past. Mentionining Forrrester Report will dilute the vendor selection criteria who lacks in features , support , stability, references in India Market.	No Change in RFP Terms
137	Section 9 - Technical Specifications	36	1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	L2 Trasnparent mode is supported feature by most vendors, but this usecase is directly not applicable to NPCI UPI segment. Kindly make this Good to have feature		No Change in RFP Terms
138	Section 9 - Technical Specifications	37	2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Kindly confirm if the following understanding is correct- Per WAF instance should support ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) and overall solution should be scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future.		Please refer to the Corrigendum - 1

139	Section 9 - Technical Specifications	37	2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	NPCI has a very good vision for SSL visibility in near future. We request NPCI to ask for SSL visibility references in banking sector, deployment should be up and running in PROD.		No Change in RFP Terms
140	Section 9 - Technical Specifications	38	3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Only Objuscation might not help much as there are many tools on internet to reverse engineer on obfuscation.Kindly change the point to The Proposed WAF solution must provide capabilities to obfuscate / encrypt / subsitute sensitive field names to defeat Man-in-The-Browser Attacks .		No Change in RFP Terms
141	Section 9 - Technical Specifications	40	3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	What is the use case of Converting back slash to forward slash character. ? Within UPI segment, traffic being XML, these usecases are not directly applicable. Kindly change to good to have.		No Change in RFP Terms, Its as per requirement
142	Section 9 - Technical Specifications	40	3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
143	Section 9 - Technical Specifications	40	3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
144	Section 9 - Technical Specifications	41	3.67	The proposed Solution should be session aware and should be able to enforce and report session	What type of enforcement is expected here on session?		Policy enforcement. No Change in RFP Terms
145	Section 9 - Technical Specifications	42	3.73	The proposed Solution should remove application error messages from pages sent to users	What is the usecase here? If error message is removed, user will not have visibility of what is going wrong. Is it that we should send a custom response page ?		Application error messages may expose sensitive information. No Change in RFP Terms

146	Section 9 - Technical Specifications	42	3.74	The proposed Solution should prevent leakage of server code	What is meant by Server code ? DLP functionality can be achieved by integrating with network DLP via ICAP. Is that the usecase ?		Server Error Codes may expose sensitive information. No Change in RFP Terms
147	Section 9 - Technical Specifications	42	4.6	The Solution must be based on Intent oriented and User behavior Oriented	Are we referring to behaviour based detection / mitigation ?		Yes. No Change in RFP Terms.
148	Section 9 - Technical Specifications	43	4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	c. Semi Supervised machine learning to identify emerging Bot Patterns. - Need more clarity on this point. Why use semi level of AI/ML. The solution should have a full fledge AI/ML capabilities.		No Change in RFP Terms
149	Section 9 - Technical Specifications	43	4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
150	Section 9 - Technical Specifications	43	4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
151	Section 9 - Technical Specifications	43	5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Apart from TOP 10 API security, NPCI should consider below list of security features for API security: Protect REST/JSON, XML, and GWT APIs. JSON Schema validation for API calls Protects against OWASP API Security Top 10 L7 Volumetric Behavioral DoS Protection Support and BOT mitigation GraphQL content profile and policy template Attack signatures on GraphQL traffic Query depth enforcement Support GraphQL batching Policy tuning with GraphQL violations DataGuard support (sensitive data protection) Declarative policy support Supports OpenAPI/Swagger format		No Change in RFP Terms, as reference would be always latest OWASP top 10 Vulnerabilites

152	Section 9 - Technical Specifications	43	5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	GraphQL is an open source data query language is a new way of developing API calls. NPCI should consider to have GraphQL security needs incorporated into RFP. GraphQL Landscape: https://landscape.graphql.org/zoom=150		No Change in RFP Terms
153	Section 9 - Technical Specifications	43	5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.			Mentioned as Good to have feature in RFP. No Change in RFP Terms.
154	Section 9 - Technical Specifications			Does NPCI Require inbuilt Additional capabilities of SSL VPN on the solution in future?	Since the ask is for Sotfware Based Solution, NPCI should have the flexibility for Addon Functionalities on the software for best Optimisation of Cost and Infrastucture		No Change in RFP Terms
155	NPCI/RFP/2021-22/IT/12	Page no. 36	Section 9 / Technical Specification / Point no. 1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		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.
156	NPCI/RFP/2021-22/IT/13	Page no. 37	Section 9 / Technical Specification / Point no. 3.2	Proposed solution should be ICSA Lab Certified WAF	As a Class-I Make-in-India local supplier, we request exemptions / relaxations on this technical specification requirement as per latest notification by DPIIT order no. P-45021/2/2017=PP (BE-II) dated 16.09.2020 (attached) and file No.1 (10)/2017-CLES Dated: 4th March 2021 from MEITY, GOI (attached) on same subject.		Mentioned as Good to have feature in RFP. No Change in RFP Terms.
157	7.3 Technical Scoring Matrix:	21	7.3	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	Kindly confirm if the Customer BFSI reference asked is specific to the Bidder for the proposed OEM only? i.e Pls clarify If it is the Bidder who should provde atleast 5 India BFSI References of the Proposed OEM only?		Bidder Should provide atleast 5 BFSI references in INDIA for proposed OEM. No Change in RFP Terms
158	8.8 Key Deliverables	24	9	OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution.	Can OEM propose the yearly review through Authorised Services Partner or OEM employee only?		OEM (Checker) is required to review as SI (maker) will be performing deployment. No Change in RFP Terms.

159	Section 9 - Technical Specifications	36	1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Pls clarify if OS, VM and Hardware will be provided by NPCI or Bidder needs to factor the same ?		Underlying Virtualization platform, OS & Hardware will be provided by NPCI. No Change in RFP Terms
160	Section 9 - Technical Specifications	44	8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Pls clarify if OEM can leverage the existing F5 BIG IQ Centralised Manager and logger setup(Hardware and Licenses) since the setup is already available in NPCI and will be free once the exisgting NPCINet devices will be removed?		OEM will have to do a sizing consideration if existing solution can handle additional load. No Change in RFP Terms
161	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, AND Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Magic Quadrant and Forrester benchmark vendors on many capabilities like - Product reach/coverage, execution capabilities, easy of deployment, market adaption etc…If we mention OR, this will open up for many none standard enterprise grade WAF solutions. Leading vendors cannot compete on commercial grounds. If you mention AND, atleast NPCI will receive bids from leading vendors	No Change in RFP Terms
162	Section 9 - Technical Specifications	36	1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Suggested Change: The WAF Solution quoted by the bidder should be in the latest Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution	We request NPCI to consider only the Gartners REport considering the acceptance of Gartner in India BFSI customers and RFPS's in most of PSU customers. Almost none of the RFP's ever ask for Forrester report. Even NPCI has referred to Gartner in the past. Mentionining Forrrester Report will dilute the vendor selection criteria who lacks in features , support , stability, references in India Market.	No Change in RFP Terms
163	Section 9 - Technical Specifications	36	1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	L2 Trasnparent mode is supported feature by most vendors, but this usecase is directly not applicable to NPCI UPI segment. Kindly make this Good to have feature		No Change in RFP Terms
164	Section 9 - Technical Specifications	37	2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Requested change: Per WAF Instance must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to per instance ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Kindly confirm if the following understanding is correct- Per WAF instance should support ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) and per instance should be scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future.	Please refer to the Corrigendum - 1
165	Section 9 - Technical Specifications	37	2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	NPCI has a very good vision for SSL visibility in near future. We request NPCI to ask for SSL visibility references in banking sector, deployment should be up and running in PROD.		No Change in RFP Terms

166	Section 9 - Technical Specifications	38	3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Only Objuscation might not help much as there are many tools on internet to reverse engineer on obfuscation.Kindly change the point to The Proposed WAF solution must provide capabilities to obfuscate / encrypt / subsitute sensitive field names to defeat Man-in-The-Browser Attacks .		No Change in RFP Terms
167	Section 9 - Technical Specifications	40	3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	What is the use case of Converting back slash to forward slash character. ? Within UPI segment, traffic being XML, these usecases are not directly applicable. Kindly change to good to have.		No Change in RFP Terms, Its as per requirement
168	Section 9 - Technical Specifications	40	3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
169	Section 9 - Technical Specifications	40	3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	When we talk of SSL offloading or SSL termination , the solution will be placed in reverse-proxy (L3) mode. Kindly refer to the provided article for more justification - https://support.f5.com/csp/article/K65271370 If any specific vendor is stating that they can do SSL offload/termination they are internally acting as a proxy. Please make this feature to be Good to have, as this point is very specific to one vendor.		Please refer to the Corrigendum - 1
170	Section 9 - Technical Specifications	41	3.67	The proposed Solution should be session aware and should be able to enforce and report session	What type of enforcement is expected here on session?		Policy enforcement. No Change in RFP Terms
171	Section 9 - Technical Specifications	42	3.73	The proposed Solution should remove application error messages from pages sent to users	What is the usecase here? If error message is removed, user will not have visibility of what is going wrong. Is it that we should send a custom response page ?		Application error messages may expose sensitive information. No Change in RFP Terms
172	Section 9 - Technical Specifications	42	3.74	The proposed Solution should prevent leakage of server code	What is meant by Server code ? DLP functionality can be achieved by integrating with network DLP via ICAP. Is that the usecase ?		Server Error Codes may expose sensitive information. No Change in RFP Terms

173	Section 9 - Technical Specifications	42	4.6	The Solution must be based on Intent oriented and User behavior Oriented	Are we referring to behaviour based detection / mitigation ?		Yes. No Change in RFP Terms.
174	Section 9 - Technical Specifications	43	4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	c. Semi Supervised machine learning to identify emerging Bot Patterns. - Need more clarity on this point. Why use semi level of AI/ML. The solution should have a full fledge AI/ML capabilities.		No Change in RFP Terms
175	Section 9 - Technical Specifications	43	4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
176	Section 9 - Technical Specifications	43	4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Are we referring to Cloud DDOS or on-prem DDOS ?		On-Prem DDOS. No Change in RFP Terms, where as any additional functionalilty /tools would be considered as value addition
177	Section 9 - Technical Specifications	43	5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Apart from TOP 10 API security, NPCI should consider below list of security features for API security: Protect REST/JSON, XML, and GWT APIs. JSON Schema validation for API calls Protects against OWASP API Security Top 10 L7 Volumetric Behavioral DoS Protection Support and BOT mitigation GraphQL content profile and policy template Attack signatures on GraphQL traffic Query depth enforcement Support GraphQL batching Policy tuning with GraphQL violations DataGuard support (sensitive data protection) Declarative policy support Supports OpenAPI/Swagger format		No Change in RFP Terms, as reference would be always latest OWASP top 10 Vulnerabilites
178	Section 9 - Technical Specifications	43	5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	GraphQL is an open source data query language is a new way of developing API calls. NPCI should consider to have GraphQL security needs incorporated into RFP. GraphQL Landscape: https://landscape.graphql.org/zoom=150		No Change in RFP Terms

179	Section 9 - Technical Specifications	43	5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.			Mentioned as Good to have feature in RFP. No Change in RFP Terms.
180	Section 9 - Technical Specifications			Does NPCI Require inbuilt Additional capabilities of SSL VPN on the solution in future?	Since the ask is for Sotfware Based Solution, NPCI should have the flexibility for Addon Functionalities on the software for best Optimisation of Cost and Infrastucture		No Change in RFP Terms