

Ref: Federal/CO/IT/2023-24/RFP001

RFP for Purchase of Web Application Firewall



The Federal Bank Limited
IT Department, Corporate Office,
Federal Towers, Bank Junction,
Aluva – 683101, Kerala

Table of Contents

Contents

Control Document.....	4
Disclaimer.....	5
INVITATION OF BID	6
Introduction	6
Tender related Terminology	7
Terms and Conditions of bid	8
Eligibility Criteria	8
Eligibility Criteria OEM	10
Mandatory Requirements.....	11
General solution.....	11
WAF Features for both On premise WAF and SaaS based Cloud WAF.....	13
Application Delivery Features	16
Device Administration, Monitoring and Reporting.....	17
Support and Training	18
Evaluation process	19
Bidding Procedure.....	19
Evaluation and Comparison of bids	19
Price-Bid Evaluation	19
Price Bid	20
Indemnity	20
Scope of Work.....	20
Delivery Period.....	22
Quarterly Preventive Maintenance for On Premise WAF device and SaaS based WAF solution:.....	22
INSTRUCTIONS TO BIDDERS (ITB)	23
Cost of Bidding	23
Content of Bidding Document	23
Clarification of Bidding Documents	23
Amendment of Bidding Documents	24
Procedure for Submission of Bids	24

RFP for WAF

Documents Comprising the Bids 25

TERMS & CONDITIONS OF CONTRACT 31

ANNEXURE – A1 40

ANNEXURE – A2 41

ANNEXURE – A3 50

ANNEXURE – A4 51

ANNEXURE – A5 53

Check List – Vendor / Bidder Submission 54

RFP for WAF

Control Document

Name of the Company		The Federal Bank Limited	
RFP Reference No		Federal/CO/IT/2023-24/RFP001	
Date of issue		08/11/2023	
Submission of Pre-Bid Queries	Date:	15/11/2023	
Time		5.00 pm	
Schedule of Pre-Bid Meeting	Date:	16/11/2023	
Time		11.00 am	
Schedule for Receipt of Bids	Date:	22/11/2023	
Time		5.00 pm	
Schedule for Opening of Technical Bids	Date:	23/11/2023	
Time		11.00 am	
Place of Pre–bid meeting/ Opening of Bids / address for Communication		The Federal Bank Limited IT Department, Corporate Office, Federal Towers, Bank Junction, Aluva – 683101, Kerala	
Contact person details:		Mr. Gipson Augustine. Vice President The Federal Bank Ltd Information Technology Dept	
Person To Contact: Queries Related to RFP- Technical			
Name : Mr. Gipson Augustine			
Mobile : +91 – 85475 23457			
Land Line : +91 – 48426 34023			
Email : gipson@federalbank.co.in			

Note:

1. This tender document is the property of the Bank & is not transferable.
2. This bid document has 54 pages.
3. If a holiday is declared on the dates mentioned above, the bids shall be received / opened on the immediate next working day at the same time specified above and at the same venue unless communicated otherwise.
4. No queries will be entertained after the date and time mentioned in this schedule, therefor.
5. Notice regarding corrigenda, addenda, amendments, time-extensions, clarifications, Bank's response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other mass media. Prospective bidders shall have to regularly visit Bank's website for any changes / development in relation to this RFP.

Disclaimer

- The information contained in this Request for Proposal (“RFP / Bid Document”) or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of FEDERAL Bank Limited (“FEDERAL Bank / Bank”), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.
- This RFP document is not an agreement and is neither an offer. The purpose of this RFP is to provide applicants who are qualified to submit the bids (“Bidders”) with information to assist them in formulation of their proposals (“Bids”). This RFP does not claim to contain all the information each Bidder may require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Bank makes no representation or warranty, express or implied, and shall incur no liability whatsoever under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.
- The information contained in the RFP document is selective and is subject to update, expansion, revision, and amendment. FEDERAL Bank does not undertake to provide any Bidder with access to any additional information or to update the information in this RFP or to correct any inaccuracies therein, which may become apparent. FEDERAL Bank reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be intimated or made accessible to all Bidders. Any information contained in this document will be superseded by any later written information on the same subject made available/accessible to all recipients by FEDERAL Bank.
- FEDERAL Bank reserves the right to reject any or all the responses to RFPs / Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision of FEDERAL Bank shall be final, conclusive and binding on all the parties directly or indirectly connected with the bidding process.
- **It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders’ queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. Prospective bidders shall regularly visit Bank’s website for any changes / development in relation to this RFP.**

INVITATION OF BID

Introduction

The Federal Bank Limited ("Federal Bank") is a banking company incorporated in India under Companies Act 1956 and having its registered office at "Federal Towers", Bank Junction, Aluva 683101, Kerala, India and having branches / offices all over India. Federal Bank is also a scheduled commercial Bank as notified by the Reserve Bank of India under the Reserve Bank of India Act, 1934 which categorizes Federal Bank under the group of "private sector banks". Federal Bank has engaged in wholesale banking, retail banking, treasury operations and other banking operations.

The Federal Bank Limited is a major private sector commercial bank headquartered at Aluva, Kochi, Kerala, along with having Data Centre at Aluva, Kochi. As on 30 September 2023, Federal Bank has 1389 branches spread across 24 states, 1937 ATMs across the country and 199 Cash recyclers

The company has plans to purchase Web Application Firewall to protect its Web applications, mobile applications and API's hosted in cloud and on premise and invites tenders for the same.

- (i) The schedule is subject to change and notice in writing of any change will be provided where feasible.
- (ii) **Bidders are requested to give bids in accordance with the terms and conditions contained herein. Bidders can quote for On Premise WAF solution or/and SaaS based Cloud WAF solution. Bank decides on the type of solution to be adopted based on evaluation criteria and evaluation of the responses to the bids will be entirely at Company's discretion. The Company's decision will be final and no correspondence about the decision will be entered into.**
- (iii) Bidders are advised to study the Bid Document carefully. Submission of Bid shall be deemed to have been done after careful study and examination of the Bid Document with full understanding of its implications. Sealed Bids prepared in accordance with the procedures enumerated in the RFP Document should be submitted to the Company not later than the date laid down, at the address given in Schedule mentioned above.

Tender related Terminology

Definitions

Throughout this RFP document, unless inconsistent with the subject matter or context:

- I. Bidder/Proponent/Prime Proponent/Vendor/System Integrator/recipient – A firm submitting bid in response to this RFP.
- II. Company/Purchaser/FEDERAL - Reference to “the Company” and “Company” and Purchaser shall be determined in context and may mean without limitation “FEDERAL Bank Limited”.
- III. Proposal/Bid – the Bidder’s written reply or submissions in response to this RFP.
- IV. SaaS – Software as a Service
- V. Solution/Services/Work/System – “Solution” or “Services” or “Work” or “System” or “IT System” means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP document and include services ancillary to the supply of the Systems, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance and other obligation of the Supplier covered under the Tender.
- VI. ITB – Instructions to Bidders as Contained below.
- VII. Supplier/Contractor: Selected Bidder/System Integrator under this RFP.
- VIII. “Contract” means the Agreement entered between the supplier along with the OEM and the Company including all attachments and annexure thereto, the Tender document, proposal and all annexure thereto and the agreed terms as set out in the bid, all documents incorporated by reference therein and amendments and modifications to the above from time to time.
- IX. “Commissioning of System”: The system shall be deemed to have been commissioned when all the activities defined under the Scope of work, for commissioning of system, have been successfully executed and completed and a certificate from the Company is obtained by the System Integrator. The date of commissioning of system will be the one stated in the Certificate from the Company.
- X. “Acceptance of System”: The system shall be deemed to have been accepted by the Company, subsequent to its commissioning, when all the activities as defined in the scope of work related to the acceptance of system have been successfully executed and completed and a certificate from the Company is obtained by the System Integrator. The date of acceptance of system will be the one stated in the Certificate from the

Company. The entire System deployed should function continuously without any problem for 30 days as a pre-requisite for the Acceptance Certificate as required.

- XI. "Delivery of System" shall be deemed to have completed when the delivery of all the goods/items under the proposed bill of materials has reached the respective designated site in good condition for installation.

Terms and Conditions of bid

Cost of preparation and submission of Bid

The Vendor/bidder shall bear all costs associated with the preparation and submission of its response to RFP and company, will in no way be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process. The Purchaser is not liable for any cost incurred by vendor/bidder in replying to queries /clarifications required.

Project Completion Time

The Delivery, installation & commissioning will be completed within 10 weeks from placement of the purchase Order.

RFP Methodology

- The methodology proposed to be adopted will be as follows:
- The bidder will have to submit technical bids in one envelop and must be sent at the address mentioned in Schedule A2. The Bid will be opened on the date prescribed in Schedule of Various RFP related events.
- Company reserves the right to accept or reject in part or full any or all the bids without assigning any reason whatsoever.
- Company reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity, or discrepancy in regard thereof.
- Before bidding, the Bidders are requested to carefully examine the RFP documents and the terms and conditions of the contract thereof, and if there appears to be any ambiguity and / or discrepancy between any of the RFP documents they should forthwith refer the matter to Company for necessary clarifications.

Eligibility Criteria

- a. The bidder must possess the requisite experience, strength, and capabilities in providing the services necessary to meet the requirements, as described in the tender document.
- b. The bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully install, implement, and configure the Firewall as sought by the FEDERAL BANK LIMITED The bids must be complete in all respect and should cover the entire scope of work as stipulated in the tender document.
- c. The invitation to bid is open to all bidders who qualify the eligibility criteria as given below.
- d. Eligibility criteria for Vendor / system Integrator are mandatory and any deviation in the same will attract bid disqualification. Eligibility criteria and Mandatory requirement supporting documents are the part of technical proposal.

RFP for WAF

Sl. No.	Eligibility Criteria	Documents to be Submitted
1.	The bidder must be an Indian firm/ organization registered under Indian Companies Act.	Copy of Certificate of Incorporation issued by Registrar of Companies
2.	The bidder should have a minimum turnover of Rs. 10 Crores in each year for last 3 audited Financial Years) in relevant services	Copy of the audit Annual Reports and /or certificate of the Chartered Accountant
3.	The bidder should not be currently blacklisted by any Central/State Govt. dept. /Public Sector Unit.	Certificate from the Chief Executive / Authorized Officer of Company
4.	The bidder should be Original Equipment Manufacturer [OEM] or authorized partner of OEM.	In case of authorized partner of OEM the bidder should submit Manufacturer Authorization Form (MAF) as per format given in Annexure A5
5.	The Bidder must have experience of implementing web application firewall involving same WAF tool in India in at least -5-institutions out of which at least -1- institution should be from the banking industry.	Copy of order and/or certificate of completion of the work
6.	The bidder shall commit that the key personnel to be employed for the project have been sufficiently involved in similar implementations and that once assigned to the project will not be moved out of it, except for reasons beyond the control of the bidder or with the prior consent of the concerned The Federal Bank Limited official. In such case an equally competent employee shall be provided as a replacement. The resources may work on other assignments but should be available for The Federal Bank Limited requirements as and when required.	Self-Declaration required
7.	The vendor/bidder must have its must have its own support offices in Cochin / Bangalore	Details of Registered Office, corporate Office and support Offices.

Eligibility Criteria OEM

- a) Eligibility criteria for OEM are mandatory and any deviation in the same will attract bid disqualification.
- b) Eligibility criteria and Mandatory requirement supporting documents are the part of technical proposal.

Sl. No.	Eligibility Criteria	Documents to be Submitted
1.	The OEM Solution must possess all the required specifications mentioned in Part 'B'	
2.	The OEM can have hardware-based appliance / SaaS based WAF solution appliance to support the requirement	
3.	The OEM should not be currently blacklisted by any Central/State Govt. dept. /Public Sector Unit.	
5.	The Bidder must have experience of implementing web application firewall involving same WAF tool in India in at least -5-institutions out of which at least -1- institution should be from the banking industry.	Copy of order and/or certificate of completion of the work
6.	The OEM must have its own support offices in India	Details support Offices and support system is required
7.	Compliance Solution should protect against common threats such as those identified in the OWASP top 10 2021 for web applications and OWASP top 10 2023 for API's.	Certificates giving details about the same

Mandatory Requirements

The following is the list of the mandatory requirements that will form a part of the Web Application Firewall which can be hosted On premise or a SaaS based WAF solution as per Banks decision.

General solution

Requirements for Vendors bidding SaaS based Cloud WAF:

- The solution should be able to protect API's, Mobile applications as well as Web applications hosted in Cloud or on premise.
- All the existing 100 (web/mobile) applications currently hosted in Bank's on premise WAF device should be migrated to the proposed SaaS based WAF solution.
- WAF and DDoS protection services should be provided on Security-as-a-Service model.
- Banks Cloud WAF configuration should be hosted and maintained only in India including the logs captured.
- The service should be comprehensive and should include Configuration, Operations and Management of the solution.
- No hardware & software is to be installed at Bank premises for the provision of the services.
- WAF shall ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and other operational activities as required.
- The solution should ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.
- Solution should support different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy, Full Proxy and Non-Inline Sniffing. Describe each deployment mode.
- Should be compliant for OWASP top 10 2021 and SANS top 25 vulnerabilities for web applications hosted on premise and cloud and OWASP TOP 10 2023 for API's hosted on prem and cloud.
- Solution should be able to prevent all application security threats including Cross Site Scripting (XSS), SQL injection, remote file inclusion, Brute Force Attack, Buffer overflow, Cookie poisoning & Cookie Protection and Parameter tampering.
- The solution should support both Positive and Negative security models.
- The solution should ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.
- The solution should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic.
- Solution should be able to mitigate DOS and DDoS attacks. The DDoS solution should provide protection against Layer 3, 4 volumetric attacks and Layer 7 DDoS attacks
- The solution should include options to develop unlimited Custom Rules, Proof of Concepts and Virtual Patching for detected vulnerabilities.

- WAF should support different policies for different web applications and allow modification of these policies upon request.
- On request integration of new applications, increase in data transfer and throughput should be provided at quoted rates.
- The WAF should allow for exception handling like Whitelisting and Blacklisting of IPs, and allow blocking of IPs based on geographic location.
- WAF should provide a real-time single management console to manage multiple WAF instances protecting multiple websites. The dashboard should contain data such as top attacks view, traffic monitoring view, etc.
- WAF and DDoS should be from same OEM so that there is a tight integration between both in terms of integration and security.
- The WAF solution should have inter alia capability of protection from BOT and Man-in-The-Browser Attack. Administrators must be alerted through mail/SMS in case of such attack.
- Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement
- The service should be comprehensive and include Configuration, Operations and Management of the solution.
- Solution should be able to identify Bad bots and take action.
- Should Support IPv4 and Ipv6.
- Bandwidth capabilities. - Cloud provider billing can be either based on the Throughput or based on number of applications hosted through the SaaS based WAF solution. Bank is currently looking for a throughput of 400 Mbps and hosting of 100 applications. The WAF should support millisecond latency so as not to impact Web application performance.

Requirements for Vendors bidding On premise Hardware WAF:

- The solution should be able to protect API's, Mobile applications as well as Web applications hosted in Cloud or on premise.
- All the existing 100 (web/mobile) applications currently hosted in Bank's on premise WAF device should be migrated to the proposed On Premise Hardware WAF solution.
- Solution should support Active-Active and Active-Standby mode.
- Solution should be hosted in both DC & DR environment of Bank Separately.
- Should be Dedicated Platform based solution.
- Should be compliant for OWASP top 10 2021 and SANS top 25 vulnerabilities for web applications hosted on premise and cloud and OWASP TOP 10 2023 for API's hosted on prem and cloud.

- The solution should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic.
- Solution should support different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy, Full Proxy and Non-Inline Sniffing. Describe each deployment mode.
- Solution should be able to mitigate DOS and DDoS attacks. The DDoS solution should provide protection against Layer 3, 4 volumetric attacks and Layer 7 DDoS attacks
- Solution should be able to identify Bad bots and take action.
- The solution should include options to develop unlimited Custom Rules, Proof of Concepts and Virtual Patching for detected vulnerabilities.
- Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement.

Hardware requirements for On premise WAF solution:

- Memory : 32 GB or higher.
- Ports : 10G / 25G ports.
- Should have Management Port.
- Should Support Ipv4 and Ipv6.
- Bandwidth capabilities.

Throughput	3 Gbps
WAF TPS For Sizing	30,000 TPS
RSA/Sec (2048bit)	4000 TPS (Hardware should support increment of the same up to 10000 TPS as per usage)

WAF Features for both On premise WAF and SaaS based Cloud WAF

- Solution should be able to protect against UDP, TCP, SIP, DNS, HTTP, SSL and other network attack targets while delivering uninterrupted service for legitimate connections.
- SSL Re-encryption required /Encryption: 2048 bits SSL
- Should support Positive Security Model (Describe in detail)
- Should have auto learning protection and easy manual deployment controls. Auto Learning and Auto Protection should co-exist
- Should have signature based Negative Security Model, which should protect against:

Broken Access Control
Layer 4 & Layer 7 DoS and DDoS

Cryptographic Failures
SQL Injection
Cross-Site Scripting (XSS)
Command Injection
LDAP Injection
XML Injection
Server-Side Template Injection
Insecure Design
Software and Data Integrity Failures
Identification and Authentication Failures
Security Misconfiguration
Server-Side Request Forgery
Generic Attacks
Brute Force
Trojans
Known Exploits
Information Disclosure
Form Field Parameter Tampering and HPP tampering
Session high-jacking
Cookie manipulation and poisoning Buffer Overflows
Bad Bot
Credit Card Detection
Protection against known database and Web server vulnerabilities
Forceful browsing
Broken access control
Request smuggling

In addition to the above the solution should also comply OWASP top 10 2023 for API's

- Broken Object Level Authorization
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Server Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management
- Unsafe Consumption of APIs

- Should protect against Sensitive Data Leakage protection using response scrub. It should have minimum features like
 - PHP information leakages
 - IIS default location

ASP / JSP source code leakages
SQL error leakages
Directory Listing
HTTP Header Leakage
Access to admin folder
Slowloris and other low & slow availability attacks
Prevention of Error messages leakage.

- Should support Policy evasion Detection.
- Should be able to do manipulation of invalidated input.
 - Should protect against Remote File inclusion attacks.
 - Should protect against request for restricted objects and file types.
 - Should protect against Directory/ Path Traversal xii. Should protect against known worms and vulnerabilities xiii. Should be able to implement geo-location policies to restrict access
 - Should prevent OS and web server fingerprinting.
- WAF should support,
 - Schema validation
 - Parser Protection (XMS Bombs)
 - XPATH injection
 - RSS/ Atom feed injection
 - ICAP protocol
- Should provide XML filtering and validation.
- Should protect from low reputation source from known bot, malicious source, anonymous proxy, known scanners, Windows exploits.
- Anti-DDoS solution
 - The solution should offer Layer 4 and Layer 7 DDOS capabilities.
 - The application layer detection should support:
 - HTTP Request limit per source
 - TCP Connections using same cookie.
 - HTTP requests using the same cookie.
 - A challenge response mechanism which will be fully transparent for the end user
- Anti-Web Defacement
 - Solution should have the ability to prevent, detect and restore web defacement.
 - Solution should copy the content of the webserver to its own hard drive and compare on a definable time schedule if files have been changed on the webserver
 - Optionally it should be possible to restore the changed files
 - Multiple protocols should be supported (FTP/SSH/Windows File Share) in order to maximize compatibility with the target server platform. xx. HTTP RFC Compliance validation
 - Solution should have the option to verify the HTTP RFC standards
 - The following objects need to be checked and enforced:

- Illegal Host Name
- Illegal HTTP Version
- Illegal HTTP Request Method
- Content Length
- Body Length
- Header Length
- Header Line Length
- Number of Header Lines in Request
- Total URL and Body Parameters Length
- Number of URL Parameters
- Number of Cookies in Request
- Number of ranges in Range Header
- Malformed Request
- Application Business Logic Enforcement
 - The solution should be capable of enforcing start pages.
 - The solution should be capable of enforcing application logic by defining a set of page access rules.
 - Appropriate page access methods should be learned and enforceable by the solution.
 - Required parameters on a given URL page should be learned and enforceable by the solution.
 - Solution should be able to track the use of cookies on a URL page-by-page granularity.

Application Delivery Features

Load balancing

- a. The solution should be capable of load balancing the protected traffic to multiple servers.
- b. The following algorithms should be supported.
 - i. Round Robin
 - ii. Weighted Round Robin
 - iii. Least Connection
- c. The solution should have configurable persistency features to maintain sessions to the load balanced backend servers.
- d. The solution should be capable of supporting the following persistency features:
 - i. Persistent IP
 - ii. Persistent Cookie
 - iii. Insert Cookie
 - iv. ASP Session ID
 - v. PHP Session ID
 - vi. JSP Session ID

- e. The solution should support a connection draining mode in order to allow maintenance of a protected server without disrupting the client experience with the application.
- f. The solution should be capable of implementing health-checks for your protected servers for the purpose of load balancing pool removal and administrator notification. This feature should work on both load-balanced and non-load-balanced servers if desired.

Policy Updating

- a. Should support manual as well as online updation of signatures.
- b. Signature Updation should not cause any downtime
- c. Default policies should be available in various classifications, Alert Only, Medium Security, High Security
- d. Signatures should be grouped in logical, searchable dictionaries.

Device Administration, Monitoring and Reporting

Logging and Reporting

- a. The solution should be able to locally store event (audit) information.
- b. The solution should be able to locally store alert information.
- c. The solution should be able to locally store traffic information.
- d. The solution should be able to send all log types above to an external syslog server.
- e. The alert information should contain at least the following information:
- f. Source to Destination connection information
- g. Extensive packet header information
- h. Raw and Hex body presentation for POST parameters
- i. Full Parameter view
- j. Highlighting the attack in the attack log
- k. With cookie alerts show the alerted cookie and changed values
- l. The solution should aggregate logging per day and per attack type
- m. The log should show both original encoding and decoded values for analysis
- n. Log should be able to provide top attacks, top source and countries of attacks in GUI
- o. Should be able to create customized reports
- p. Should be able to provide PCI DSS compliance and reporting
- q. Should be able to group incidents with violation correlation
- r. Solution must be capable for sending the logs to existing In-house SOC of bank RSA security analytics.

Data Analytics

- a. The solution should have a dashboard for data analytics in which you can see:
- b. Attacks per Country
- c. Hits per Country
- d. Data per Country

- e. Exportable to PDF
- f. Clickable view of the various attacks per website
- g. Zoom-able world map with colour coding of attacks

Blocked IP's

- a. The solution should have a view of all blocked IP addresses and the blocked time period.
- b. From the above view it should be possible to release the blocked IP addresses.

Administration

- a. Should provide HTTPS and SSH interface for management
- b. Should have multiple configuration version option on the appliance
- c. DC & DR must be in HA Mode
- d. For Cloud deployment, Bank officials should be able to create custom policies in addition to the OEM provided ones and dedicated support for Cloud WAF is required.

Support and Training

- a. The responding company will describe the professional services structure for the proposing vendor.
- b. Support should be available 24/7/365 according to follow the sun principle.
- c. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response.
- d. OEM Training for Bank Officials.

Detailed Technical Evaluation sheet for OEM Product Evaluation

- Provided in selection process for the Bidder
- Issue of tender notification
- Submission of Bids
- Opening of Technical Bids
- Technical bids evaluation
- Discussion by Purchase Committee.
- Finalization and Signing of SLA.

Evaluation process

The following are the key considerations that form part of the bid evaluation process:

- Alternate bids are not allowed.
- The evaluation team will thoroughly review the proposals submitted by various bidders.
- Based on multiple parameters, the evaluation team will calculate the technical evaluation score for each bidder at the end of this phase. The Company, in observance of best practices, shall:
 - (i) Maintain the bid evaluation process strictly confidential
 - (ii) Reject any attempts or pressures to distort the outcome of the Evaluation, including fraud and corruption.

Bidding Procedure

Initially, only the technical proposals will be opened at the date and time as advised by FEDERAL BANK LIMITED. The price proposals shall remain sealed and are held in custody by the purchaser/Evaluation Committee. The technical proposals will be evaluated by the Evaluation Committee. No amendments or changes to the technical proposals will be permitted. The objective of the exercise is to allow the purchaser to evaluate the technical proposals without reference to price. Bids of bidders which do not conform to the mandatory requirements may be termed as nonresponsive and will not be evaluated further. Following the approval of the technical evaluation, and at an address, date and time advised by the purchaser, the price proposals will be opened in presence of qualified bidders from technical evaluation phase.

Evaluation and Comparison of bids

Initially the bidder's responses will be reviewed for compliance with the terms and conditions mentioned across different sections of this RFP document. The bidders who fail to comply with any of the terms and conditions mentioned may be termed as non-responsive and will not be evaluated further. For those bidders who have qualified the terms and conditions, technical evaluation will be conducted followed by the price-bid evaluation. The bidders who qualify the minimum technical requirement will be considered for the price-bid evaluation. The price proposals will remain sealed until the technical evaluation is complete.

Price-Bid Evaluation

The Price-Bid evaluation is done only for those bids which are responsive and which have Compliance Meeting.

Price Bid

- a) The Bidder shall indicate in the Price Schedules the all-inclusive Unit Rates for supply and erection of each goods and services which includes supply, erection and commissioning.
- b) The Bidder shall quote rates exclusive of all statutory levies, taxes, charges, surcharges, VAT GST & other taxes etc. The Prices for supply portion and execution portion shall be FIRM throughout the period of contract. No component of cost / tax shall be paid by the Company unless the same is included specifically in the quotations.
- c) Any alteration in the rates etc. will not be allowed on any ground, such as mistake, misunderstanding etc., after the Bid has been submitted.
- d) The Bidder shall quote rate only in Indian Rupees.

Indemnity

The Bidder hereby covenants and agrees to indemnify and shall at all times keep indemnified the FEDERAL BANK LIMITED against any loss or damage that the FEDERAL BANK LIMITED may sustain as result of the failure or neglect of the Bidders to faithfully carry out its obligations under this tender / agreement. The bidder shall pay for all losses, damages, costs, charges and expenses which the FEDERAL BANK LIMITED may incur or suffer as a result of the failure or neglect of the Bidders to faithfully carry out its obligations under this tender / agreement and the bidder shall indemnify and keep indemnified the FEDERAL BANK LIMITED in all respects

Scope of Work

The proposal from the desired vendors shall include an end-to-end solution for supply, install & implement the solution either on premise or on cloud as per the decision of Bank, which shall include:

For On premise WAF solution:

- i. All the existing 100 (web/mobile) applications currently hosted in Bank's on premise WAF device should be migrated to the proposed On Premise WAF solution.
- on premise WAF solution should be done Directly by OEM.
- ii. Supply and Preventive Maintenance can be done by Vendor / Bidder
- iii. Supply of Hardware complying with the technical specifications, along with accessories and necessary documentation at Federal's locations as indicated in the RFP.
- iv. Power ON Test of appliances.
- v. Installation and commissioning of 2 WAF devices in high availability (HA) mode both in DC & DR locations of Bank.
- vi. Physical installation of WAF Appliances so that WAF devices work in protection mode.

- vii. Installation & Configuration of WAF Appliances.
- viii. Demonstrate the automatic updates of signatures.
- ix. Demonstrate the WAF appliance graphical reporting capability to show, detailed and summary reports, with trending analysis available within the appliance.
- x. WAF Appliance must detect, block & report attack.
- xi. Configuration and Integration of web application firewalls in HA mode with existing LAN/WAN.
- xii. The successful bidder has to suggest and implement new policies in line of standard best practices in BFSI environment.
- xiii. Vendor to provide the following documentation
 - a. Deployment documentation & Network diagram.
 - b. Description of the complete WAF implementation.
 - c. Detail about how to handle day to day administrative activities & good practices to be followed.

Vendor should provide a detailed time schedule for the total implementation of the WAF. The timelines should not exceed 10 weeks from placement of the purchase or work order.

For SaaS based WAF solution:

- i. All the existing 100 (web/mobile) applications currently hosted in Bank's on premise WAF device should be migrated to the proposed SaaS based WAF solution.
- ii. WAF and DDoS protection services should be provided on Security-as-a-Service model.
- iii. The service should be comprehensive and include Configuration, Operations and Management of the solution.
- iv. No hardware & software is to be installed at Company's premises for the provision of the services.
- v. WAF shall ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.
- vi. WAF shall ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.
- vii. The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities, SANS Top 25 Vulnerabilities.
- viii. The WAF should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data and re-encrypt the SSL/TLS traffic.
- ix. The solution should support different policies for different web applications and allow modification of these policies upon request.
- x. The solution should support both Positive and Negative security models.
- xi. Should demonstrate the automatic updates of signatures.
- xii. Should demonstrate the WAF appliance graphical reporting capability to show, detailed and summary reports, with trending analysis available within the appliance.
- xiii. WAF Appliance must detect, block & report attack.
- xiv. The successful bidder has to suggest and implement new policies in line of standard best practices in BFSI environment.

xv. Vendor to provide the following documentation

- a. Deployment documentation & Network diagram.
- b. Description of the complete WAF implementation.
- c. Detail about how to handle day to day administrative activities & good practices to be followed.

Delivery Period

The Delivery, installation & commissioning will be completed within 10 weeks from placement of the purchase or work order. Any delay by the Tender in the delivery of goods and services shall render the Tenderer liable to any or all of the sanctions viz. invocation of Bank Guarantee / forfeiture of security deposit, imposition of liquidated damage, blacklisting etc.

If the tenderer fails to deliver any or all of the goods and services or complete the installation / commissioning within the period specified in the purchase/work order, the FEDERAL BANK LIMITED shall without prejudice to its other remedies deduct as liquidated damage as per the liquidated damages clause mentioned in this tender.

Any delay in installation & commissioning will attract a penalty of 1% of the purchase order value per week. Maximum cap is of 10% of the Purchase Order.

Quarterly Preventive Maintenance for On Premise WAF device and SaaS based WAF solution:

In the case of On premise WAF device, vendor will have to conduct quarterly preventive maintenance to ensure that the device functioning without defect. Non- compliance will attract penalty of 0.25% of AMC Value per week delay of the asset being serviced. No calls will be logged for this activity and has to be done by the vendor. The Preventive Maintenance should be completed in the first month of each quarter quarters being mentioned as Jan- March, April- June, July-September and October- December. Maximum cap is of 10% of the PO.

The Preventive Maintenance Activity will include

- Review of system logs
- Configuration items support coverage .
- Configuration of good practices and vulnerability review.
- Upgrade updates and patches shall be applied as required.

In the case of SaaS base WAF solution, vendor will have to conduct quarterly review mechanism to ensure that all the applications are being enabled without any false positives. Non- compliance will

attract penalty of 0.25% of AMC Value per week delay of the asset being serviced. No calls will be logged for this activity and has to be done by the vendor. The Preventive Maintenance should be completed in the first month of each quarter quarters being mentioned as Jan- March, April- June, July-September and October-December. Maximum cap is of 10% of the PO.

Recommendations / suggestions should be prioritised and typically included in a detailed report which should be submitted quarterly.

INSTRUCTIONS TO BIDDERS (ITB)

Cost of Bidding

- The Bidder shall bear all costs associated with the preparation and submission of its bid and Company will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.
- The Company is not liable for any cost incurred by bidder in replying to this RFP, presentations etc, regardless of the conduct or outcome of the bidding process.

Content of Bidding Document

- The bidding document provides overview of the requirements, bidding procedures and contract terms.
- The Bidder is expected to examine all instructions, statements, Forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not responsive to the bidding documents in every respect will be at the Bidder's risk and may result in rejection of his bid.
- While the Company has made considerable effort to ensure that accurate information is contained in this document, the information contained in this RFP is supplied solely as a guideline for Bidders.
- Confidentiality: The contents of this document and the supporting documentation are confidential to Company and are provided solely for the purpose of response to the Tender.
- Address for Correspondence: The bidder shall designate the official mailing address, email address, place and fax number to which all correspondence shall be sent by the Company.

Clarification of Bidding Documents

- Bidder requiring any clarification of the bidding documents may notify the Company in writing or by mail. The Company will respond to any request for clarification of the bidding documents which it receives no later than 7 days prior to the deadline for submission of bids prescribed by the Company. Written copies of the Company's response (including an explanation of the query but without identifying the source of the inquiry) will be sent to all bidders, which have received the bidding documents.
- Pre Bid meeting with the vendors will be held on DATE, The Company will respond to any queries raised during the pre-bid meeting as per time lines mentioned above

- Any questions concerning this Tender must be submitted in writing or by e-mail at gipson@federalbank.co.in on or before DATE to:

Mr. Gipson Augustine
Vice President
IT Department, Corporate Office,
Federal Towers, Bank Junction,
Aluva – 683101, Kerala

- No requests for clarification will be accepted by telephone.
- If a Bidder discovers any significant ambiguity, error, conflict, discrepancy, omission, or other Deficiency in this document, the Bidder should immediately notify the above official of such error and request modification or clarification of the RFP document.

Amendment of Bidding Documents

- At any time prior to the deadline for submission of bids, the Company may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective participant bidder, modify the bidding document by amendment.
- All the bidders in this bidding process will be notified of the amendment in writing or by email and will be binding on them.
- In order to allow the participant bidders reasonable time in which to take the amendment into account in preparing their bids, the Company, at its discretion, may extend the deadline for the submission of bids.
- Company may at any time during the bidding process request the bidder to submit revised Commercial Bids and /or Supplementary commercial bids or some additional documents/submissions without thereby incurring any liability to the affected bidder or bidders.
- Please note that prices should not be indicated in the Technical Bid and should only be indicated in the Commercial Bid. However, a blank Commercial Bid, i.e., the commercial bid without prices should necessarily be included with the Technical Bid. This would provide idea about the components for which the commercials are quoted.

Procedure for Submission of Bids

- A well bounded hard (paper) copy of response with all annexures and one soft copy of response on a non-re-writeable CD and should be covered in sealed covers super scribing "Commercial Bid" along with CD's duly labelled containing technical details.
- The cover containing the Technical Bid should be marked appropriately with the tender subject, reference number, due date.
- The cover should clearly indicate the name, address and telephone number of the Bidder.
- Each copy of the bid should be a complete document and should be bound as a volume. The document should be page numbered and appropriately flagged and must contain the list of contents (Index) with page numbers.

Documents Comprising the Bids

The bid prepared by the Bidder shall comprise the following components:

Technical Bid

The Technical Bid shall comprise of the following:

- a) Letter of Submission (Annexure - A1)
- b) Documents as per the Eligibility Criteria as mentioned.
- c) Documents as per the Mandatory Requirements as mentioned.
 - d) Detailed Technical Evaluation sheet (Annexure - A2) filled in with necessary supporting documents.
 - e) Letter from Chief Executive Certifying Companies should not have been declared ineligible/blacklisted by any State or Central Government or PSU. Certificate from the Company Secretary certifying the same to be submitted.
- f) Non-Disclosure Agreement executed as per the requirement (Annexure - A3)
- g) Details of Litigations – (Annexure – A4)
- h) An undertaking from the bidder that the bidder is complying with all the conditions of the terms & conditions and technical specifications of the bidding document as no deviation will be acceptable to the company. Undertaking from the Bidder, confirming his unconditional acceptance of full responsibility for executing the 'Scope of work' and meeting all obligations of this Bid.
- i) Manufacturer Authorization Format (Annexure A5)

Financial Bid

Bidders are also requested to submit cost break-up and assumptions in arriving at the quoted price. The details about the BID to be submitted as per (Annexure –A5).

Bid Prices

- Prices quoted by the Bidder shall be negotiated and fixed during the award of the Contract and not subject to variation on any account subject to ITB Clause
- A bid submitted with an adjustable price quotation will be treated as non-responsive and rejected.
- The commercial bid should clearly indicate the price to be charged without any qualification whatsoever and should include all taxes(sales, service, GST etc) , duties (excise, customs etc), octroi, fees, levies, works contract tax and any other charges as may be applicable in relation to the activities proposed to be carried out. It is mandatory that such charges wherever applicable/payable should be indicated separately.
- However, should there be a change in the applicable taxes, Company reserves the right to negotiate with the Bidder.
- Discount: The Bidders are advised not to indicate any separate discount. Discount, if any, should be merged with the quoted prices. Discount of any type, indicated separately, will not be considered for evaluation purpose. However, in the event of such an offer, without

considering discount, is found to be the lowest, the Company shall avail such discount at the time of award of contract.

Period of Validity of Bids

- Bids shall remain valid for 90 days after the date of opening of the bid prescribed by the Company. A bid valid for a shorter period shall be rejected by the Company as non-responsive.
- In exceptional circumstances, the Company may solicit the Bidder's consent to an extension of the period of validity. The request and the response thereto shall be made in writing (or by fax). A Bidder granting the request will not be required nor permitted to modify its bid.

Format and Signing of Bid

- Bidder should submit a well bounded paper copy of response with all annexures and soft copy of response (Technical Details) on a non-re-writeable CD.
- The bid shall be typed and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The later authorization shall be indicated by written power-of-attorney accompanying the bid. All pages of the bid shall be initialled by the person or persons signing the bid.
- COVER LETTER/BIDDER CERTIFICATIONS: Include here any cover letter included with the bid and those certifications required for submittal of a proposal. Proposals submitted in response to this RFP must be signed by the person in the bidder's organization who is responsible for the decision as to the prices being offered in the bid or by a person who has been authorized in writing to act as agent for the person responsible for the decision on prices. Each bid shall stipulate that it is predicated upon the terms and conditions of this Tender and any supplements or revisions thereof. By submitting a signed proposal, the bidder's signatories certify that in connection with this procurement:
 - The bidder's organization or an agent of the bidder's organization has arrived at the prices in its bid without consultation, communication or agreement with any other respondent or with any competitor for the purpose of restricting competition.
 - The prices quoted in the bid have not been knowingly disclosed by the bidder's organization or by any agent of the bidder's organization and will not be knowingly disclosed by same, directly or indirectly, to any other respondent or to any competitor.
 - No attempt has been made or will be made by the bidder's organization or by any agent of the bidder's organization to induce any other person or firm to submit or not to submit a bid for the purpose of restricting competition

Sealing and Marking of Bids

- The envelopes shall be addressed to the Company at the following address

Gipson Augustine
Vice President
IT Department, Corporate Office,
Federal Towers, Bank Junction,
Aluva – 683101, Kerala

- The envelope to be marked as: **RFP for Purchase of Web Application Firewall**, title and reference number and the name and address of the Bidder.
- If the envelope is not sealed and marked as required, the Company will assume no responsibility for the bid's misplacement or premature opening.
- Telex, Email or fax bids will be rejected.

Deadline for Submission of Bids

Financial Bids must be received by the Company at the address specified under ITB Clause by date and time. In the event of the specified date for the submission of Bids being declared a holiday for the Company, the Bids will be received up to the appointed time on the next working day.

The Company may, at its discretion, extend this deadline for submission of bids by amending the bid documents in accordance with ITB Clause, in which case all rights and obligations of the Company and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

Late Bids

- Any bid received by the Company after the deadline for submission of bids prescribed by the Company will be rejected.

Modification and Withdrawal of Bids

- The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification or withdrawal is received by the Company prior to the deadline prescribed for submission of bids.
 - The Bidder's modification or withdrawal notice shall be prepared, sealed, marked and dispatched in accordance with the provisions of ITB Clause withdrawal notice may also be sent by fax by a signed confirmation copy, post marked not later than the deadline for submission of bids.
 - No bid may be modified subsequent to the deadline for submission of bids.
 - No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of period of bid validity specified by the Bidder on the bid form.

- If any change becomes necessary due to any clarification, revised commercial bid in a separate sealed cover shall be submitted with prior written permission of the Company.

Contacting the Company

- No Bidder shall contact the Company on any matter relating to its bid, from the time of the bid opening to the time the Contract is awarded. If the bidder wishes to bring additional information to the notice of the Company, it should do so in writing.
- Any effort by a Bidder to influence the Company in its decisions on bid evaluation, bid comparison or contract award may result in rejection of the Bidder's bid.

Evaluation Criteria

The successful bidder will be the one who is evaluated with Compliance as mentioned.

Award Criteria

- Subject to Instruction to Bidders (ITB) clause, the financial evaluation committee will select vendor with the highest rating as the successful bidder, for the system and services as requested vide this RFP and who satisfy all the conditions of the contract and meet the qualification requirement of the bidding document. The financial evaluation committee of the Company reserves the right to negotiate the price with the successful vendor. The Company will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid (qualified and with highest rating) as per the evaluation criteria defined in the RFP process
- Company is not bound to accept the best evaluated bid or any bid and reserves the right to accept any bid, wholly or in part or to reject any or all bids.

Time Line / Critical Dates

- Upon request of the Company, the vendor shall provide a detailed work plan, with details of the resources proposed to be deployed, for approval by the Company. The work plan must be satisfactory to the Company and will be approved by the company before going ahead with the activity.
- Vendor shall recommend relevant and viable strategies to achieve all the work objectives and requirements contained in this RFP.

Company's right to accept any Bid and to reject any or All Bids

- The Company reserves the right to accept or reject any or all Bids. Bids may be accepted or rejected in total or in any part or items thereof. Any Bid not containing sufficient information, in view of the Company, to permit a thorough analysis may be rejected.
- The Company reserves the right to accept a combination of parts of more than one bid and to negotiate with any or all Bidders.

- The Company reserves the right to verify the validity of bid information, and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate in the Company's estimation.
- The Company shall have the right to determine in its own best judgment, the Bidders whose bids will qualify for the short list, if any, and thereafter, the final selected firm to undertake the work.
- Bids not conforming to the requirements of the RFP Document may not be considered by the Company. However, the Company reserves the right, at any time, to waive any of the requirements of the RFP, if, in the sole discretion of the Company, the best interests of the Company would be served.
- If, in the opinion of the Company, any Bidder has clearly misinterpreted the Work and /or underestimated the hours and / or value of the Work to be performed as reflected in the bid content and submitted price(s)/rate(s), then the Company may reject the bid as unbalanced (i.e. not representative of the Work Scope) .
- Furthermore, the Company shall have the right to cancel the RFP process at any time prior to contract award, without thereby incurring any liability to the affected Bidder or bidders. Reasons for cancellation, as determined by the Company in its sole discretion, include, but are not limited to , the following:
 - a) Services contemplated are no longer required
 - b) Requirements and terms of reference (scope of work) of the RFP document were not adequately or clearly defined due to unforeseen circumstances and /or factors and /or new developments;
 - c) The RFP did not allow for consideration of all significant elements of the Company for the work (e.g. new/additional matters have arisen);
 - d) Proposed price is unacceptable for the Work; and
 - e) The Project ceases to be in the best interest of the Company

Notification of Award

- a) Prior to the expiration of the period of bid validity, the Company will notify the successful bidder in writing by letter or by fax, to be confirmed in writing by a letter, that its bid has been accepted.
- b) The notification of award will constitute the formation of the Contract.

Signing of Contract

- a) At the same time as the Company notify the successful bidder that its bid has been accepted, the Company will send the bidder the Contract Form incorporating all agreements between the parties.
- b) The successful bidder shall sign and date the SLA and return it to the Company.

Company's right to vary scope of Contract at the time of award and during the term of the contract.

- a) Company may at any time, by a written communication given to the winning bidder, make changes within the scope of the contract as specified.

- b) If any such change causes an increase or decrease in the cost of, or the time required for the vendor's performance of any part of the work under the contract, whether changed or not changed by order, an equitable adjustment shall be made in the Contract Price or time schedule, or both and the Contract shall accordingly be amended. Any claims by the vendor for adjustment under this Clause must be asserted within thirty (30) days from the date of the vendor's receipt of the Company's changed order.

Rejection Criteria

- a) Besides other conditions and terms highlighted in the RFP document, bids may be rejected under following circumstances:
- b) Bids received by the Company after the last date of receipt of bids prescribed.
- c) Bidder not qualifying the Eligibility criteria mentioned in A.2
- d) Any effort on the part of the bidder to influence the Company's bid evaluation, bid comparison or contract award decisions.
- e) Bids without power of attorney and any other document consisting of adequate proof of the ability of the signatory to bind the bidder.
- f) Revelation of prices in any form or by any reason before opening of commercial bids
- g) Failure to furnish all information required by the RFP document or submission of a bid not substantially responsive to the RFP Document in every respect or submission of incorrect / misleading information.
- h) Incomplete price bid or Financial bid.
- i) Total lump sum price quoted by the bidder does not include all statutory taxes and levies applicable, Includes GST as extra
- j) Bidder not quoting for the applicable complete scope of work as indicated in the RFP document
- k) Bids with deviations or conditions unacceptable to the Company.

Local Conditions

- a) It will be imperative on each bidder to fully acquaint himself with the local conditions, any limitations, existing systems, network and factors at the respective location of the Company site which would have any effect on the performance of the contract and / or the cost.
- b) The bidder is expected to obtain for himself on his own responsibility all information that may be necessary for preparing the bid and entering into contract. Obtaining such information shall be at bidder's own cost.
- c) It is the responsibility of the bidder that such factors have been properly investigated and considered while submitting the bid proposal and that no claim whatsoever including those for financial adjustment to the contract awarded under the RFP document will be entertained by the Company and that neither any change in the time schedule of the contract nor any financial adjustment arising thereof shall be permitted by the Company on account of failure of the bidder to appraise themselves of such conditions/limitations.

TERMS & CONDITIONS OF CONTRACT

Responsibility

- The Federal Bank intends the contractor/vendor appointed under the RFP shall have the single point responsibility for fulfilling all obligations and providing all deliverables and services required for successful implementation of the project.
- The Vendor is requested to quote in Indian Rupees ('INR'). Bids in currencies other than INR would not be considered.
- The prices quoted by the Vendor shall include all costs such as, taxes, levies, cess, excise and custom duties that need to be incurred except GST Tax, which will be extra and mentioned separately as applicable.

Payment

Company shall make payments only to the vendor at the times set out in the Payment Schedule subject always to the fulfilment by the vendor of the obligations herein. The vendor must accept the payment terms proposed by Federal Bank. The financial bid submitted by the vendor must be in conformity with the payment terms proposed by Federal Bank. Any deviation from the proposed payment terms would not be accepted.

100% payment on delivery, installation & receipt of licenses for hardware/software, implementation, support and on production of acceptance certificate and performance guarantee. In case of a delay during installation due to technical reasons from Bank's end,

- 1) 90% payment on delivery
- 2) 10% on installation & receipt of licenses for hardware, implementation, and support and on production of acceptance certificate and performance guarantee.

Prices

- Prices payable to the vendor as stated in the Contract shall be fixed at the time of finalization of the contract.
- Escalation of Costs: The vendor shall in no circumstance be entitled to any escalation of costs or price of any material / items supplied or services mentioned under the contract.

Contract Amendments

- Subject to Scope of work, no variation in or modification of the terms of the contract shall be made except by written amendment signed by both the parties.

Assignment

- The vendor shall not assign, in whole or in parts its obligations to perform under the Contract, except with the Company's prior written consent.

Delays in the vendor's Performance

- If at any time during performance of the Contract the vendor should encounter conditions impeding timely delivery and performance of Services, the vendor shall promptly notify the Company in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the vendor's notice the Company shall evaluate the situation and may, at its discretion, extend the vendor time for performance with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

- Except as provided under conditions of contract clause, a delay by the vendor in the performance of its delivery obligations shall render the vendor liable to the imposition of liquidated damages pursuant to conditions of Contract unless an extension of time is agreed upon pursuant to conditions of Contract without the application of liquidated damages.

Liquidated Damages and Penalties

- If the Tenderer fails to deliver any or all of the goods and services or complete the installation/commissioning within the period specified in the purchase/work order, FEDERAL BANK LIMITED., shall without prejudice to its other remedies, deduct as liquidated damage 1.0(one) percent of the price of the delayed goods and services for every week of delay or part thereof up to a maximum deduction of 10%. Once the maximum is reached, the Company may consider termination of the Contract pursuant to conditions of Contract Clause.
- Penalty based on downtime of the equipment will be calculated and penalty will be charged as per the table below:

S. No.	Uptime of Equipment computed on Monthly basis	Penalty as a percentage of Total Order Cost Computed on Quarterly basis
1	98% to 99%	1.00%
2	97% to 98%	2.00%
3	95% to 97 %	3.00%
4	90% to 95 %	5.00%
5	< 90 %	10.00%

If the Uptime committed falls below 90% the company may impose any one or more of the following viz. invocation of Bank Guarantee / forfeiture of security deposit, imposition of liquidated damage, blacklisting etc.

Termination of Contract

- Either party may terminate the contract without assigning any cause by giving 120 days written notice. Further, any pending or unresolved operational issues, performance, unpaid fees and any other remedies shall continue by both the parties during the period of termination notice and the same must be satisfied before this agreement is terminated.
- The Contract in whole or part can be terminated at the option of the FEDERAL BANK LIMITED., if the FEDERAL BANK LIMITED. for any reason whatsoever does not require the whole or part of the job thereof as specified in the tender to be carried out and in the said event the FEDERAL BANK LIMITED. shall give notice of one month in writing of the fact with reason to the Tenderer / Bidder, who shall have no claim to any payment or compensation whatsoever on account of any profit or advantage, which would have derived from the execution of the work in full, but which he did not derive in consequences the full amount of the work not having been carried out, neither shall he have any claim on compensation / damage for the loss suffered by him by reason of termination of contract by the FEDERAL BANK LIMITED. and of any alterations having been made by the FEDERAL BANK LIMITED. in the original

specification or the designs and instruction which shall involve any curtailment of the work contemplated.

- The Company without prejudice to any other remedy, reserves the right to terminate the Tender / Contract in whole or in part and also to blacklist a Tenderer / Bidder for a suitable period in case he fails to honour his bid / contract without sufficient grounds or found guilty for breach of condition /s of the tender / contract, negligence, carelessness, inefficiency, fraud, mischief and misappropriation or any other type of misconduct by such Tenderer / Bidder or by its staff or in case there are more than 3 penalties on Service Provider in any month

Termination for Default

- The Company may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Supplier, terminate the Contract in whole or part: If the vendor fails to deliver any or all of the deliverables mentioned in scope Part B or perform services and obligations within the period(s) specified in the Contract, or within any extension thereof granted by the Company pursuant to conditions of contract clause
- In the event the Company terminates the Contract in whole or in part, pursuant to the conditions of contract clause Company may procure, upon such terms and in such manner as it deems appropriate. Systems or Services similar to those undelivered, and the vendor shall be liable to the Company for any excess costs for such similar systems or Services. However, the vendor shall continue the performance of the Contract to the extent not terminated

Force Majeure

- Notwithstanding the provisions of conditions of contract clause the vendor shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.
- For purpose of this Clause, "Force Majeure" means an event beyond the control of the vendor and not involving the vendor's fault or negligence and not foreseeable. Such events may include, but are not limited to, acts of the Company either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
- If a Force Majeure situation arises the vendor shall promptly notify the Company in writing of such conditions and the cause thereof. Unless otherwise directed by the Company in writing, the vendor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

Termination for Insolvency

- The Company may at any time terminate the Contract by giving written notice to the vendor, if the vendor becomes bankrupt or otherwise insolvent. In this event termination will be without compensation to the vendor, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Company.

Termination for Convenience

- The Company, by written notice sent to the vendor may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Company's convenience, the extent to which performance of the vendor under the Contract is terminated, and the date upon which such termination becomes effective.

Settlement of Disputes/Arbitration

- All disputes or differences of any kind, whatsoever, arising out of or in connection with this contract or in discharge of any obligation arising out of this Contract (whether during the progress of work or after completion of such work and whether before or after the termination of this contract, abandonment or breach of this contract), the Parties to this contract shall endeavour to settle such disputes and/or difference amicably. If both the parties fail to reach such amicable settlement, either party(the Company or the vendor) may within 30 days of such failure, give a written notice to the other party clearly setting out there in the specific dispute/s and/or difference/s, which require to be arbitrated upon. Such dispute/s and/or difference/s shall be referred to a sole arbitrator mutually agreed upon. In the absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrator, one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings .In case, a party fails to appoint an arbitrator within 30 days from the receipt of the Request to do so by the other party or the two Arbitrators so appointed fail to agree on the appointment of third Arbitrator within 30 days from the date of their appointment upon request of a party, the Chief Justice of the High Court or any person or institution designated by him within whose jurisdiction the subject purchase order/contract has been placed/made, shall appoint the arbitrator/Presiding Arbitrator upon request of one of the parties.
- Arbitration proceedings shall be held at Aluva, Kerala, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.
- The arbitration shall be covered by the provision of the Arbitration & Conciliation Act, 1996 or any statutory modification or re-enactment thereof and rules framed there under from time to time.
- In the event of the arbitrator or any of the arbitrators, as the case may be, dying or resigning or being unable to act by reason of physical disability or as the case may be, it shall be lawful

for the appointing party of such arbitrator(s) to appoint another arbitrator in the place of the said arbitrator in the manner provided herein above.

- The arbitrator or the arbitrators, appointed under this contract, shall have the power to extend the time to make the award with the consent of the Parties hereto.
- Pending reference to arbitration and award thereon, the parties hereto shall make all endeavour to complete all the items of work, obligations etc. under this Contract in all respects and disputes/differences, if any, shall be finally settled in arbitration
- Upon every or any such reference to arbitration, as provided herein, the cost of the incidental to the reference and award respectively shall be at the discretion of the arbitrator or the arbitrators and the presiding arbitrator, as the case may be. However the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.
- In case, during the arbitration proceeding , the parties hereto mutually settle, compromise or compound their dispute/s or difference/s, the reference to the arbitrator and the appointment of the arbitrator or the arbitrators or the presiding arbitrator, as the case may be, shall stand withdrawn or terminated with effect from the date on which the parties hereto file a joint memorandum of settlement thereof with the arbitrator or the arbitrators and the presiding arbitrator, as the case may be.
- The arbitrator/s or the presiding arbitrator, as the case may be, shall give detailed reasons in respect of each claim or counter claim, irrespective of the amount, while passing the award.
- The decision of the arbitrator/s or the presiding arbitrator as the case may be shall be final and binding upon both parties.

Governing Language

- The Contract shall be written in English or Hindi language Subject to condition of contract clause, English language version of the Contract shall govern its interpretation. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall be written in the same language.

Applicable Law

- The Contract shall be interpreted in accordance with the Laws of India.
- Governing laws / Jurisdiction all matters relating to this activity shall be governed by the laws of India. Courts at Cochin, Kerala shall have the jurisdiction to decide or adjudicate on any matter, which may arise.

Notices

Any notice given by one party to the other pursuant to this Contract shall be sent to other party in writing or by Fax and confirmed in writing to the other Party's address. For the purpose of all notices, the following shall be the address of the Company and vendor.

Mr. Gipson Augustine
Vice President , IT Department,
Corporate Office, Federal Towers,
Bank Junction, Aluva – 683101,
Kerala

Vendor: (To be filled in at time of Contract signature)

.....

.....

A notice shall be effective when delivered or on the notice's effective date whichever is later

Taxes and Duties

- Vendors shall be entirely responsible for all taxes, duties, license fees etc. incurred.
- If there is any reduction in taxes/ duties due to any reason whatsoever, after Notification of Award, the same shall be passed on to the Company.

Vendor Integrity and Vendor's Obligations

- The vendor is responsible for and obliged to conduct all contracted activities in accordance with the contracts using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the contract.
- The vendor is obliged to work closely with the Company's staff, act within its own authority and abide by directives issued by the Company.
- The vendor is responsible for managing the activities of its personnel and will hold itself responsible for any misdemeanours.
- The vendor will treat as confidential all data and information about the Company, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Company.
- The vendor shall perform the activities/services and carry out its obligations under the contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional engineering and consulting standards recognized by international professional bodies and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe and effective equipment, machinery, material and methods. The vendor shall always act, in respect of any matter relating to this Contract, as faithful advisor to the Company and shall , at all times, support and safeguard the Company's legitimate interests in any dealings with third parties.
- The vendor is to abide by the job safety measures prevalent in India and will free the Company from all demands or responsibilities arising from accidents or loss of life the cause of which is the vendor's negligence. The vendor will pay all indemnities arising from such incidents and will not hold the Company responsible or obligated.

Components of the Contract

- The Contract will be based, on response to this RFP document, the Bidder(s) response to the questions in the RFP document; clarifying questions raised in writing by Company and the response in writing to those questions; clarifying questions raised in writing by the bidder(s) and the responses in writing to those questions.
- If any of the terms and conditions under this Contract is held invalid, illegal or unenforceable, this will not affect the validity, legality or enforceability of the other terms and conditions under this Contract.

Scope of work/Contract

- Scope of the Contract shall be as defined of this RFP document and any addenda, corrigendum, and Annexes thereto of this RFP document.

Reporting Progress

- Vendor shall monitor progress of all the activities related to the execution of this contract and shall submit to the Company, at no extra cost, progress reports with reference to all related work, milestone and their progress during the implementation phase on a weekly basis.
- The Company reserves the right to inspect and monitor the progress/performance of the work/services at any time during the course of the Contract. At any time during the course of the Contract, the Company shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance of the vendor of its obligations/functions in accordance with the standards committed to or required by the Company.

Indemnification

- The vendor shall indemnify the company (Federal Bank) AGAINST loss of data / damage to data / any loss arising as a result of any negligence/ of vendor or arising out of misuse of any data or any loss during the work as decided/quantified by the Company maximum indemnification up to Purchase Order Value.

Terms of Payment

- a. The contract price shall be paid in the manner specified in the bid document. No invoice for extra work/change order on account of change order will be submitted by the bidder unless the said extra work/change order has been authorized/ approved by the FEDERAL BANK LIMITED. in writing.
- b. Final Payment on the supplied goods and services shall be made after supply, physical acceptance, successful installation and commissioning of the goods and services (i.e. acceptance test" imply running of goods and services for 15 days) on the bills submitted duly authenticated by an authorized officer of the Company. Purchase/work Order will be issued by the FEDERAL BANK LIMITED. indicating therein the details of the goods & services and the delivery schedule.
- c. The bidder's request for payment shall be made to the FEDERAL BANK LIMITED. in writing, accompanied by invoices describing, as appropriate, the goods and Related Services performed and delivered, accompanied by the supporting documents.

Payments shall be made promptly by the FEDERAL BANK LIMITED., no later than forty-five (45) days after submission of an invoice or request for payment by the bidder, and the FEDERAL BANK LIMITED. has accepted it.

- d. If any excess payment has been made by the FEDERAL BANK LIMITED. due to difference in quoted price in proposal and bidder's invoice, the FEDERAL BANK LIMITED. may without prejudice to its rights recover such amounts by other means after notifying the bidder or deduct such excess payment from any payment subsequently falling due to the FEDERAL BANK LIMITED.
- e. Bidder has to ascertain that the Performance Bank Guarantee has been submitted before issue of any invoice. No payment will be processed if the PBG is not submitted.
- f. The currency in which payment shall be made to the supplier under this contract is Indian Rupees (INR).
 - i. No payment separately towards taxes & duties etc. other than the quoted in the price schedule for each item of work shall be payable by the FEDERAL BANK LIMITED.
 - ii. It may be noted that all taxes, duties, levies, Inspectorate charges and other charges are to be included in the unit / total contract price and FEDERAL BANK LIMITED. is not liable to pay any taxes, duties, levies over and above the unit contract value. Also the bidder has to include all types of freight and insurance charges in the unit/total contract value and FEDERAL BANK LIMITED. is not liable to pay any charges towards insurance or freight.
 - iii. "Service Level Agreement" (SLA) shall mean the Service Level Agreement entered into between the FEDERAL BANK LIMITED. and the successful bidder.
 - iv. "Intellectual Property Rights" means any patent, copyright, trademark, trade name, service marks, brands, propriety information, whether arising before or after the execution of the Contract and the right to ownership and registration of these rights.

The work as detailed in this tender shall be executed and completed within the period stipulated in the Work Order that will be issued in accordance with the Tender documents. Technical Specifications, Bill of Quantities and Drawings are required to the satisfaction of FEDERAL BANK LIMITED. The work shall however be carried out and completed in phases for which start date and completion date shall be mutually discussed and agreed upon before the award of work order. The work shall not be considered as completed until FEDERAL BANK LIMITED. certifies in writing that the same has been completed.

SLA Signing

The successful bidder has to sign a SLA with the Company within 10 days of issuing the LOA for the provision and execution of services as per the tender terms.

Performance Bank Guarantee

The bidder needs to supply the Performance Bank Guarantee for an amount of 10% of the Purchase Order, within 7 days of release of Purchase Order. The PBG will be applicable for the period of 3 years. The Performance Bank Guarantee shall be invoked if the bidder fails to complete the implementation within stipulated period and if the bidder fails to provide the uptime provided under SLA.

Other Terms

- The Bidder will not have any direct interaction with any third party agency on behalf of the Company.
- All communications to the employees or third party agencies would be through designated channels as directed to by the Company.
- The bidder shall not use or disclose any Confidential Information of the Company except as specifically contemplated herein. For purposes of this tender / contract "Confidential Information" means information that:
 - is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
 - is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.
- Except in cases of criminal negligence or will full misconduct and in case of infringement of intellectual property rights, both parties shall not be liable, whether in contract, tort or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of supplier/vendor to pay liquidated damages to the Corporation and the aggregate liability of both the parties whether under the Contract, in tort or otherwise, shall not exceed the total Contract price with Federal Bank under this Contract provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.
- This clause must be read along with the clause of Indemnity.

ANNEXURE – A1

LETTER OF SUBMISSION

Ref: Federal/CO/IT/2023-24/RFP001

Place:

Date:

To,
Senior Vice President - IT
IT Department, Corporate Office
Federal Towers, Bank Junction
Aluva – 683101, Kerala

Sir,

Being duly authorized to represent and act on behalf of(bidder) and having reviewed and fully understood all the qualifications and requirement and information provided, the undersigned hereby expresses its interest and submit the commercial bid in accordance with your RFP No. Ref Federal/CO/IT/2023-24/RFP001 dated :XX XX XX We are hereby submitting our Response with all the desired information and documents.

We hereby declare that all the information and statements made in this Response are true and accept that any misrepresentation contained therein may lead to our disqualification.

We confirm our unconditional acceptance and full responsibility for executing the 'Scope of work' and meeting all obligations of this Bid without any deviation.

We understand you are not bound to accept this or any other response that you may receive.

Yours sincerely,

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

ANNEXURE – A2

Technical Evaluation Criteria – SaaS based WAF solution

Area Consideration	Compliance (Yes/NO)
General solution	
Banks Cloud WAF configuration should be hosted and maintained only in India including the logs captured.	
All the existing 100 applications (mobile and web) currently hosted in Bank's on premise WAF device should be migrated to the proposed SaaS based WAF solution.	
WAF and DDoS protection services should be provided on Security-as-a-Service model.	
The service should be comprehensive and should include Configuration, Operations and Management of the solution.	
No hardware & software is to be installed at Bank premises for the provision of the services.	
WAF shall ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.	
Should be compliant for OWASP top 10 2021 and SANS top 25 vulnerabilities for web applications hosted on premise and cloud and OWASP TOP 10 2023 for API's hosted on prem and cloud. Solution should support Active-Active and Active-Standby mode	
Solution should be able to prevent all application security threats including Cross Site Scripting (XSS), SQL injection, remote file inclusion, Brute Force Attack, Buffer overflow, Cookie poisoning & Cookie Protection and Parameter tampering.	
The solution should support both Positive and Negative security models.	
The solution should ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required.	
Solution should support different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy, Full Proxy and Non-Inline Sniffing. Describe each deployment mode.	
The WAF should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic. Should be compliant for OWASP top 10 2021 and SANS top 25 vulnerabilities for web applications hosted on premise and cloud and OWASP TOP 10 2023 for API's hosted on prem and cloud.	
Solution should be able to mitigate DOS and DDOS attacks. The DDoS solution should provide protection against Layer 3, 4 volumetric attacks and Layer 7 DDoS attacks. Solution should be able to mitigate DOS and DDOS attacks.	

RFP for WAF

The solution should include options to develop unlimited Custom Rules, Proof of Concepts and Virtual Patching for detected vulnerabilities.	
Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement	
The service should be comprehensive and include Configuration, Operations and Management of the solution.	
Solution should be able to identify Bad bots and take action	
WAF should support different policies for different web applications and allow modification of these policies upon request.	
On request integration of new applications, increase in data transfer and throughput should be provided at quoted rates.	
The WAF should allow for exception handling like Whitelisting and Blacklisting of IPs, and allow blocking of IPs based on geographic location.	
WAF should provide a real-time single management console to manage multiple WAF instances protecting multiple websites. The dashboard should contain data such as top attacks view, traffic monitoring view, etc.	
WAF and DDoS should be from same OEM so that there is a tight integration between both in terms of integration and security.	
The WAF solution should have inter alia capability of protection from BOT and Man-in-The-Browser Attack. Administrators must be alerted through mail/SMS in case of such attack. Should have Management Port	
Should Support IPv4 and IPv6	
Performance Should Support IPv4 and IPv6	
Cloud provider should provide Throughput of 400 Mbps and hosting of 100 applications. The WAF should support millisecond latency so as not to impact Web application performance.	

RFP for WAF

Technical Evaluation Criteria – On Premise WAF

Area Consideration	Compliance (Yes/NO)
General solution	
Product Architecture: The solution should support different deployment modes: Inline Transparent, True Transparent Proxy, Reverse Proxy, Full Proxy and Non-Inline Sniffing. Describe each deployment mode	
Solution should support Active-Active and Active-Standby mode	
Should be Dedicated Platform based solution	
Should be compliant for OWASP top 10 2021 and SANS top 25 vulnerabilities for web applications hosted on premise and cloud and OWASP TOP 10 2023 for API's hosted on prem and cloud	
Solution should be able to mitigate DOS and DDOS attacks.	
Solution should be able to identify Bad bots and take action.	
The solution should include options to develop unlimited Custom Rules, Proof of Concepts and Virtual Patching for detected vulnerabilities.	
Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement.	
Platform	
Memory : Minimum 32 GB	
Ports: Should support minimum 10G	
Should have Management Port	
Should Support IPv4 and IPv6	
Performance	
Throughput	3 Gbps
WAF TPS For Sizing	30,000 TPS
RSA/Sec (2048bit)	4000 TPS (Hardware should support increment of the same up to 10000 TPS as per usage)
Latency	< 5ms

RFP for WAF

SSL Re-encryption required	
2048 bits SSL	
WAF Features (for both cloud and on premise)	
Solution should be able to protect against UDP, TCP, SIP, DNS, HTTP, SSL and other network attack targets while delivering uninterrupted service for legitimate connections	
Should support Positive Security Model (Describe in detail)	
Should have auto learning protection and easy manual deployment controls. Auto Learning and Auto Protection should co-exist	
Should have signature based Negative Security Model, which should protect against:	
<ul style="list-style-type: none"> ○ Cross site scripting (XSS) 	
<ul style="list-style-type: none"> ○ Layer 4 & Layer 7 DoS and DDoS 	
<ul style="list-style-type: none"> ○ SQL Injection 	
<ul style="list-style-type: none"> ○ SQL LDAP and XPath Injections 	
<ul style="list-style-type: none"> ○ Generic Attacks 	
<ul style="list-style-type: none"> ○ Brute Force 	
<ul style="list-style-type: none"> ○ Trojans 	
<ul style="list-style-type: none"> ○ Known Exploits 	
<ul style="list-style-type: none"> ○ Information Disclosure 	
<ul style="list-style-type: none"> ○ Form Field Parameter Tampering and HPP tampering 	
<ul style="list-style-type: none"> ○ Session high-jacking 	
<ul style="list-style-type: none"> ○ Cookie manipulation and poisoning 	
<ul style="list-style-type: none"> ○ Buffer Overflows 	
<ul style="list-style-type: none"> ○ Bad Bot 	
<ul style="list-style-type: none"> ○ Credit Card Detection 	
<ul style="list-style-type: none"> ○ Protection against known database and Web server vulnerabilities 	
<ul style="list-style-type: none"> ○ Forceful browsing 	
<ul style="list-style-type: none"> ○ Broken access control 	
<ul style="list-style-type: none"> ○ Request smuggling 	
Should protect against Sensitive Data Leakage protection using response scrub. It should have minimum features like	

RFP for WAF

a) PHP information leakages	
b) IIS default location	
c) ASP / JSP source code leakages	
d) SQL error leakages	
e) Directory Listing	
f) HTTP Header Leakage	
g) Access to admin folder	
h) Slowloris and other low & slow availability attacks	
i) Prevention of Error messages leakage	
Should support Policy evasion Detection	
Should be able to do manipulation of invalidated input	
Should protect against Remote File inclusion attacks	
Should protect against request for restricted objects and file types	
Should protect against Directory/ Path Traversal	
Should protect against known worms and vulnerabilities	
Should be able to implement geo-location policies to restrict access	
Should prevent OS and web server fingerprinting	
WAF should support	
a. Schema validation	
b. Parser Protection (XMS Bombs)	
c. XPATH injection	
d. RSS/ Atom feed injection	
e. ICAP protocol	
Should provide XML filtering and validation	
Should protect from low reputation source from known bot, malicious source, anonymous proxy, known scanners, Windows exploits	

Anti-DoS solution	
a. The solution should offer Layer 7 DDOS capabilities	
b. The application layer detection should support:	
c. HTTP Request limit per source	
d. TCP Connections using same cookie	
e. HTTP requests using the same cookie	

RFP for WAF

f. A challenge response mechanism which will be fully transparent for the end-user	
Anti-Web Defacement	
a. Solution should have the ability to prevent, detect and restore web defacement.	
b. Solution should copy the content of the webserver to its own hard drive and compare on a definable time schedule if files have been changed on the webserver	
c. Optionally it should be possible to restore the changed files	
d. Multiple protocols should be supported (FTP/SSH/Windows File Share) in order to maximize compatibility with the target server platform.	
HTTP RFC Compliance validation	
a. Solution should have the option to verify the HTTP RFC standards	
b. The following objects need to be checked and enforced:	
c. Illegal Host Name	
d. Illegal HTTP Version	
e. Illegal HTTP Request Method	
f. Content Length	
g. Body Length	
h. Header Length	
i. Header Line Length	
j. Number of Header Lines in Request	
k. Total URL and Body Parameters Length	
l. Number of URL Parameters	
m. Number of Cookies in Request	
n. Number of ranges in Range Header	
o. Malformed Request	
Application Business Logic Enforcement	
a. The solution should be capable of enforcing start pages	
b. The solution should be capable of enforcing application logic by defining a set of page access rules	
c. Appropriate page access methods should be learned and enforceable by the solution	
d. Required parameters on a given URL page should be learned and enforceable by the solution	

e. Solution should be able to track the use of cookies on a URL page-by-page granularity	
--	--

Application Delivery Features	
Load balancing	
a. The solution should be capable of load balancing the protected traffic to multiple servers	
b. The following algorithms should be supported	
c. Round Robin	
d. Weighted Round Robin	
e. Least Connection	
f. The solution should have configurable persistency features to maintain sessions to the load balanced backend servers.	
g. The solution should be capable of supporting the following persistency features:	
Persistent IP	
Persistent Cookie	
Insert Cookie	
ASP Session ID	
PHP Session ID	
JSP Session ID	
h. The solution should support a connection draining mode in order to allow maintenance of a protected server without disrupting the client experience with the application.	
i. The solution should be capable of implementing healthchecks for your protected servers for the purpose of load balancing pool removal and administrator notification. This feature should work on both load-balanced and non-loadbalanced servers if desired.	
Policy Updating	
a. Should support manual as well as online updation of signatures	
b. Signature updation should not cause any downtime	
c. Default policies should be available in various classifications, Alert Only, Medium Security, High Security	
d. Signatures should be grouped in logical, searchable dictionaries.	
Device Administration, Monitoring and Reporting, Logging and Reporting.	

RFP for WAF

a. The solution should be able to locally store event (audit) information.	
b. The solution should be able to locally store alert information.	
c. The solution should be able to locally store traffic information.	
d. The solution should be able to send all log types above to an external syslog server.	
e. The alert information should contain at least the following information:	
f. Source to Destination connection information	
g. Extensive packet header information	
h. Raw and Hex body presentation for POST parameters	
i. Full Parameter view	
j. Highlighting the attack in the attack log	
k. With cookie alerts show the alerted cookie and changed values	
l. The solution should aggregate logging per day and per attack type	
m. The log should show both original encoding and decoded values for analysis	
n. Log should be able to provide top attacks, top source and countries of attacks in GUI	
o. Should be able to create customized reports	
p. Should be able to provide PCI DSS compliance and reporting	
q. Should be able to group incidents with violation correlation	
Data Analytics	
a. The solution should have a dashboard for data analytics in which you can see:	
b. Attacks per Country	
c. Hits per Country	
d. Data per Country	
e. Exportable to PDF	
f. Clickable view of the various attacks per website	
g. Zoom-able world map with colour coding of attacks	
Blocked IP's	

RFP for WAF

○ Submission of Bids	
○ Opening of Technical Bids	
○ Technical bids evaluation	
○ Discussion by Purchase Committee.	
○ Finalization and Signing of SLA.	
a. The solution should have a view of all blocked IP addresses and the blocked time period.	
b. From the above view it should be possible to release the blocked IP addresses.	
Administration	
Should provide HTTPS and SSH interface for management	
Should have multiple configuration version option on the appliance	
Support and Training	
a. The responding company will describe the professional services structure for the proposing vendor	
b. Support should be available 24/7/365 according to follow the sun principle	
c. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response	
Detailed Technical Evaluation sheet for OEM Product Evaluation	
○ Issue of tender notification	

Date:

**Name and Signature of Bidder
With Corporate Seal**

ANNEXURE – A3

Details of Litigations

Details of litigation(s) the Bidder is currently involved in, or has been involved in for the last three years.

1. Party in dispute with	
2. Year of initiation of dispute	
3. Detailed description of dispute	
4. Resolution / Arrangement arrived at (if concluded)	

Blacklisted by any Govt. /PSU/Reputed Listed company for corrupt or fraudulent practices or non-delivery, non-performance in the last three years.

Witness:

Bidder:

Signature:

Authorized Signatory:

Name and Address:

Name and Address:

Date:

Date:

ANNEXURE – A4

Please note that Bidders can bid for SaaS based WAF solution or/and On Premise WAF device. Bank can decide on what mode of deployment to be adopted.

Details of Commercial BID - For SaaS based WAF solution

The proposal for SaaS based WAF can be either based on throughput provided or based on number of applications being hosted on the SaaS based solution.

SI No	Requirement	Cost Details Per Annum				
		Year 1	Year 2	Year 3	Year 4	Year 5
A	Cost of the solution for throughput of 400 Mbps and hosting of 100 applications					
B	Support cost (if any)					
C	One time implementation cost (if any)					
D	GST					
E	Total cost (A+B+C+D)					
F	Incremental cost for additional 50 Mbps					
G	Incremental cost for additional 5 applications being hosted on SaaS based WAF solution					

I/We hereby declare that the taxes mentioned/charged in the annexure are as per the tax laws applicable in India.

Authorized Signature:

Name and Title of Signatory:

Name and Address of Firm/Company: (With Company Seal)

Details of Commercial BID - For On Premise WAF solution

Sl. No.	Item	Unit Cost	QTY	Total Price	GST	Total Price
DC						
1	Mention Product Make & Model WAF Make and Model (HA Mode) with Centralized Management and three-year warrantee and support.					
2	OEM Licenses (if any)					
3	Installation & Commissioning Charges					
4	4th Year AMC & Support Charges					
5	5th Year AMC & Support Charges					
DR						
1	Mention Product Make & Model WAF Make and Model (HA Mode) with Centralized Management and three-year warrantee and support.					
2	OEM Licenses (if any)					
3	Installation & Commissioning Charges					
4	4th Year AMC & Support Charges					
5	5th Year AMC & Support Charges					
Total Cost of Ownership - TCO						

I/We hereby declare that the taxes mentioned/charged in the annexure are as per the tax laws applicable in India.

Authorized Signature:

Name and Title of Signatory:

Name and Address of Firm/Company: (With Company Seal)

ANNEXURE – A5

Manufacturer Authorization Format (On OEM's letter head)

Ref:

Date:

To

Senior Vice President
The Federal Bank Ltd
Corporate Office, Federal Towers,
Alwaye – 683101
Kerala, India

Dear Sir,

Sub: Manufacturer Authorization for RFP No **Federal/CO/IT/2023-24/RFP001**

We <OEM Name>having our registered office at <OEM Address>are an established and reputed manufacturer of <hardware/ software details>do hereby authorize M/s_____ (Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/sfor all the products quoted for and supplied to the Bank during the three year product warranty period.

<OEM Name>

<Authorized Signatory> Name:

Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

Check List – Vendor / Bidder Submission

Sl. No.	Documents to be submitted	Submitted Yes / No
1	Annexure – A1 Letter of Submission Undertaking from the Bidder, confirming his unconditional acceptance of full responsibility for executing the ‘Scope of work’ and meeting all obligations of this Bid without any deviation	
2	Eligibility criteria for Vendor / System Integrator with documents supporting documents	
3	Eligibility criteria for OEM Integrator with document supporting documents	
4	Letter from Chief Executive Certifying Companies should not have been declared ineligible / Blacklisted by any State or Central Government or PSU	
5	Annexure - A2 Technical Evaluation Criteria (Supporting documents to be submitted)	
6	Details of Litigations – (Annexure – A3)	
7	Undertaking from the Bidder, confirming his unconditional acceptance of full responsibility for executing the ‘Scope of work’ and meeting all obligations of this Bid without any deviation	
8	Annexure- A4: Commercial Bid (Tentative Prices)	
9	Annexure- A5 : Manufacturer Authorization Format	