HIGH COURT OF MADHYA PRADESH : JABALPUR

NOTICE INVITING TENDER

e-Tenders are invited by the High Court of Madhya Pradesh for the "Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh". The last date of online tender submission is **14th October, 2024 before 06:00 P.M. (mandatory).** The sealed tender complete in all respect addressed to **"Registrar General, High Court of Madhya Pradesh, Jabalpur"** must be submitted before **05:00 P.M. on 15th October, 2024 (mandatory).** The technical bids of the tender shall be opened online on **16th October, 2024 at 11:00 A.M.** The detailed tender document is available in the official website of the High Court of Madhya Pradesh **www.mphc.gov.in** and Government e-procurement portal **www.mptenders.gov.in.**

Sd/-

REGISTRAR GENERAL

HIGH COURT OF MADHYA PRADESH : JABALPUR

//TENDER//

No. Reg(IT)(SA)/2024/1263 **Dated:22.08.2024**

Bid Document for

Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh

Note: - This document contains total **59 pages** including cover. No change and modification in the document by the bidder is permissible.

Table of Contents

Section – I
NOTICE INVITING TENDER

No. Reg(IT)(SA)/2024/1263 **Dated:22.08.2024**

The Registrar General, on behalf of High Court of Madhya Pradesh invites ***e-tenders / online tenders*** from experienced and reputed firms/organizations/ Original equipments manufacturer (OEM) for the "***Supply, Installation, Commissioning, Maintenance Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh"***

S. No.	Estimated project cost (In Lakh Rs.)	EMD (In Lakh Rs.)	Cost of online Tender Document (In Rs.)	Date and Time of Pre-Bid Meeting	Last Date / Time of online tender Submission	Last Date/ Time of tender submission in hardcopy	Date and Time of Opening of Technical Bid (online/ hardcopy)	Time for Completion of the work / project
1.	1.50 Crore	03 Lakh	5,000/-	12th September, 2024 at 11:30 A.M in the Committee Hall No. 03 of High Court of Madhya Pradesh, Jabalpur.	14th October, 2024 before 06:00 PM	15th October, 2024 before 05:00 PM	16th October, 2024 at 11:00 AM	60 days

1. *Tender documents may be viewed or purchased online by interested and eligible bidders from the website* ***https://mptenders.gov.in*** *after paying Tender fee of* ***Rs.5,000/-*** *and Processing Fee, as applicable. The tender document is also available in website* ***http://www.mphc.gov.in****.*
2. *Bidders can submit its tender online at* ***https://mptenders.gov.in/*** *on or before the key dates given above. The Physical copy of the Technical Bid along with copy of online EMD should also be submitted at the address below latest by* ***15th October, 2024 at 05:00 P.M.***
3. *All further notifications/amendments, if any shall be posted on* ***https://mptenders.gov.in*** ***and*** ***www.mphc.gov.in*** *only. No separate communication shall be made with individual Bidders.*

4. **<u>The financial bids are to be submitted online and no hard sheet/ copy is to be submitted along with the bid.</u>**

All other terms and conditions for submission of tender are contained in this document. If the date of submission/opening of the Bid is declared as holiday then the bids shall be submitted / opened on next working day.

The Registrar General, High Court of Madhya Pradesh, Jabalpur (M.P.) reserves the right to accept or reject any or all bids without assigning any reason thereof.

<u>Address for communication:-</u>

Registrar General,
High Court of Madhya Pradesh
Jabalpur (M.P.)
Email ID: regithcjbp@mp.gov.in & copy to on: - mphc@nic.in
Landline: 0761-2623358

Section – II

2. INSTRUCTIONS TO BIDDERS:-

2.1 DEFINITIONS:-

a) "**The Employer**" or **"The Purchaser"** means the "Registrar General, High Court of Madhya Pradesh, Jabalpur" and the "District Judge" of the District Courts.

b) **"The Bidder"** means a firm which participates in the tender and submits its proposal.

c) **"Successful Bidder"** means the Bidder, who, after the complete evaluation process, gets the Letter of Award. The Successful Bidder shall be deemed as "Contractor" appearing anywhere in the document.

d) "**The Letter of Award**" means the issue of a signed letter by the Purchaser of its intention to award the work mentioning the total Contract Value. The timeline for delivery of products and services will start from the date of issue of Letter of Award.

e) **"The Contract"** means the agreement entered into between the Employer and the Contractor, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

f) **"The Contractor"** means the individual or firm or OEM supplying the Goods / items and Services under this Contract.

g) **"The Contract Price**" means the price payable to the Successful Bidder under the Letter of Award for the full and proper performance of its contractual obligations. The Contract Price shall be deemed as **"Contract Value"** appearing anywhere in the document.

h) **"Site Acceptance Test (SAT)"** is a process of testing the contracted services provided by the Bidder at the locations specified by the Registrar General, High Court of Madhya Pradesh. SAT comprises of Product Acceptance Tests with respect to Technical Specifications and Bill of Materials as specified in this tender, checking the installation,

commissioning and integration of sub-components and integration with High Court software and acceptance of the Training at the site.

i) **"Services"** means System Integration, Training and coordinating with the original equipment manufacturer (OEM) for installation, commissioning, system integration and maintenance for proper working of supplied equipments/items etc.

j) **"NIT"** is the Notice Inviting Tender. It is essentially the Press Notification of the Tender.

k) **"OEM"** - means Original Equipment Manufacturer and/or Original Software Developer.

l) This tender is subject to availability of funds / Budget from the State Government/ Department of Justice, Govt. of India.

2.2 BID DOCUMENT:-

2.2.1 The process and procedures of bidding, the materials to be supplied and the various terms and conditions of this tender are provided in the Bid Document. The Bid Documents include**:-**

i.	Section I	Notice Inviting Tender
ii.	Section II	Instructions to Bidders
iii.	**Section III**	***Terms and Conditions for E-Tendering*.**
iv.	Section IV	General Conditions of Contract
v.	Section V	Special Conditions of Contract
vi.	Section VI	Scope of work
vii.	Section VII	Technical Specifications
viii.	Section VIII	Format to be used for submission of proposal
ix.	Section IX	Certificates

2.2.2 The Bidder should carefully read all the instructions, terms and conditions, specifications and various forms that are provided in the Bid Document. The tender may be rejected if any or all of the information asked for in this document are not furnished along with the tender or if the tender is not responsive with the Bid Document.

2.3 AMENDMENT OF BID DOCUMENTS:-

At any time, prior to the date of submission of Bids, the Purchaser may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify bid documents by amendments by issuing corrigendum / addendum in the website of the High Court.

2.4 COST OF BIDDING:-

The Bidder has to bear all the costs associated with the preparation and submission of the bid. Purchaser will, in no case, be responsible or liable for any of the costs, regardless of the conduct or outcome of the bidding process.

2.5 EARNEST MONEY DEPOSIT (EMD):-

2.5.1 The proposal should be submitted along with **only online** application fee of **Rs.5,000/- (Rs. Five Thousand only)** and Earnest Money Deposit (EMD) of **Rs.03 Lakh (Rupees Three Lakh only)** in the form of **online mode** through e-procurement tender portal www.mptenders.gov.in valid for the period of 06 months in favour of "***Registrar General, High Court of Madhya Pradesh, Jabalpur***". The Bid submitted without EMD and/or the application fee shall be summarily rejected.

2.5.2 The EMD of the successful Bidder will be returned when the Bidder has signed the Contract Agreement with the purchaser and has furnished the required Performance Guarantee.

2.5.3 The EMD will be forfeited:

(i) If a Bidder withdraws its bid during the period of bid validity.

or

(ii) If the Bidder fails to accept the Purchaser's corrections of arithmetic errors in the Bidder's bid (if any),

or

(iii) If the Successful Bidder fails to sign the contract agreement with the purchaser,

or

(iv) If the Successful Bidder fails to furnish the Performance Guarantee with in the stipulated time.

2.6 BID PRICES:-

2.6.1 The Bidder shall give the pricing as individual and as a total composite price inclusive of all levies & taxes, packing, forwarding, freight and insurance etc.

2.7 DISCOUNTS:-

The Bidders are informed that discount, if any, should be included in the total price.

2.8 BID VALIDITY:-

The bids shall remain valid for the period of **180 days from the date of last submission.**

2.9 ONLY ONE BID PER PARTY:-

Each bidder is permitted to submit ONLY ONE BID. In case it is found that any party has submitted more than one bid for the subject work(s) in any of the above capacities, all bids so submitted shall be summarily rejected and the EMPLOYER shall not entertain any further request/ correspondence in this matter.

2.10 SUBMISSION OF PROPOSALS:-

2.10.1 All physical proposals have to be submitted ONLY in HARD **BOUND (Hard bound implies such binding between two covers through stitching or otherwise whereby it may not be possible to replace any paper without disturbing the document)** form with all pages sequentially numbered either at the top or at the bottom right corner of each page. It should also have an index giving page wise information of above documents. Incomplete proposal or those received without hard bound will summarily be rejected. ***All the Pages and Papers to be signed and sealed by the authorized signatory of the bidder.***

2.10.2 The Bidders are required to fill up and submit the **Section VIII (only online)** documents with their proposals.

2.10.3 The proposals shall be submitted in two parts, viz**.:-**

(a) **Envelope-1:** Containing Copy of Earnest Money Deposit (EMD) valid for the period of six months. The envelope should be superscribed as **"Envelope-1: EMD"** at the top left corner of the envelope.

(b) **Envelope-2:** Pre-qualification Proposal and Technical Proposal super scribed as **"Envelope 2 – Pre-qualification and Technical Proposal"** (Containing duly signed PRE-QUALIFICATION PROPOSAL SUBMISSION FORM as prescribed in tender, Other required Prequalification documents, clause-by-clause compliance to the technical specifications of the equipments as prescribed in Section-VII, all technical literature, brochures etc.). In the technical proposal, there should not be any indication about the prices (printed or otherwise) of any of the products offered.

2.10.4 All the sealed envelopes should again be placed in a **single sealed cover** superscribed as *"Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh" bid from: M/s ----------"* "**NOT TO BE OPENED BEFORE 11:00 A.M.** on **16th October, 2024**", which will be received as time mentioned in the Schedule of Events. The Bid is to be submitted to the "***Inward / Receipt Section of the High Court of M.P., Jabalpur***"**.**

2.10.5 The Bids and all correspondence and documents relating to the bids, shall be written in English language.

2.10.6 **The financial bids are to be submitted online and no hard copy to be submitted along with the bid.**

2.11 LATE BIDS:-

Any bid received by the Purchaser after the time and date for receipt of bids prescribed by the Purchaser in the tender may be rejected and returned unopened to the Bidder.

2.12 MODIFICATION AND WITHDRAWAL OF BIDS:-

2.12.1 The Bidder is allowed to withdraw its submitted bid any time prior to the last date prescribed for receipt of bids, by giving a written notice to the Purchaser.

2.12.2 Subsequent to the last date for receipt of bids, no modification/ withdrawal of bids shall be allowed.

2.12.3 The Bidders cannot withdraw the bid in the interval between the last date for receipt of bids and the expiry of the bid validity period specified in the Bid. Such withdrawal may result in the forfeiture of its EMD from the Bidder.

2.13 LOCAL CONDITIONS:-

2.13.1 Each Bidder is expected to fully get acquainted with the local conditions and factors, which would have any effect on the performance of the contract and /or the cost.

2.13.2 The Bidder is expected to know all conditions and factors, which may have any effect on the execution of the contract after issue of Letter of Award as described in the bidding documents. The Purchaser shall not entertain any request for clarification from the Bidder regarding such local conditions.

2.14 CONTACTING THE PURCHASER:-

Any effort by a Bidder influencing the Purchaser's bid evaluation, bid comparison or contract award decisions may result in the rejection of the bid.

2.15 ELIGIBILITY/ PRE-QUALIFICATION CRITERIA:-

Bidders that meet **ALL** of the following pre-qualification criteria need only apply.

2.15.1 (i) Average Annual Financial turnover of the bidder during last 03 financial years, ending **31st March of previous financial year i.e. 2023-24 should be at least Rs. 05 Crore.**

2.15.2 (ii) Experience in Supply, Installation, commissioning, Maintenance of firewall, WAF, NMS tool and similar IT equipments during last 05 years ending last day of month previous to the month of publication of this tender, should be either of the following:-

(a) Three similar completed work costing not less than the amount equal to **40% of the estimated cost**.

OR

(b) Two similar completed work costing not less than the amount equal to **50% of the estimated cost**.

OR

(c) One similar completed work costing not less than the amount equal to **80% of the estimated cost**.

Similar works means: Supply, installation and System Integration of firewall, WAF, NMS tool and similar IT equipments.

2.16 SCHEDULE OF EVENTS:-

The tentative dates for the schedule of key events of this tender are given as under:-

Sl. No.	Events	Date
01	**Date of Pre-Bid meeting**	**12th September, 2024 at 11:30 A.M in the Committee Hall No. 03 at the High Court of M.P. Note: -** The vendor are requested to send their suggestions / queries on following e-mail id:- regithcjbp@mp.gov. as per format of pre-bid query.
02	**Last date and time of online submission of proposal (mandatory).**	**14th October, 2024 before 06:00 PM**
03	**Last date and time of submission of hardcopy of proposal (mandatory).**	**15th October, 2024 before 05:00 PM**
04	**Date and time of opening of the technical Bids**	**16th October, 2024 at 11:00 AM**
05	**Date and time of opening of the financial Bid at High Court of Madhya Pradesh, Jabalpur**	**Date and time of opening of financial bids will be intimated to qualified bidders via e-mail / letter / telephone.**

2.17 OPENING OF PROPOSAL:-

The Evaluation Committee or its authorized representative will open the tenders.

2.18 EVALUATION:-

2.18.1 The Purchaser reserves the right to modify the Evaluation Process at any time during the Tender Process, without assigning any reason,

whatsoever, and without any requirement of intimating the Bidders of any such change.

2.18.2 Any time during the process of evaluation, the Purchaser may seek for clarifications from any or all Bidders.

2.18.3 The tender has been invited under two bid system i.e. Technical Bid and Financial Bid. The interested agencies are advised to submit sealed envelopes super as mentioned above under clause ***2.10.3***

Phase-1: Online Application Fee & EMD: First, the envelope containing Online Application fee and Copy of Earnest Money Deposit will be opened and if both are found furnished by the Bidders in the prescribed manner, then the second envelope containing Pre-Qualification & Technical Proposal documents shall be opened. At any stage during the evaluation, if the EMD is found invalid, the respective Bidder's bid will be summarily rejected.

Phase-2: Pre-Qualification and Technical Proposal Evaluation: The Bidder shall have to fulfill all the Pre-qualification Criteria. These documents will be scrutinized along with the Technical Proposal in this phase of evaluation. Those bidders who do not fulfill the terms and conditions of Pre-qualification Criteria as specified in this tender or whose Technical Proposal is non-responsive will not be eligible for further communication. Technical Proposals of the Bidders would be evaluated for the clause-by-clause compliance of the technical specifications as mentioned in the Bid document. Evaluation of Prequalification and Technical Proposal by Registrar General, High Court of Madhya Pradesh shall not be questioned by any of the Bidders. The Purchaser reserves the right to ask for a technical elaboration/clarification in the form of a technical presentation from the Bidder on the already submitted Technical Proposal at any point of time during evaluation process. The proposals shall be opened in presence of their representatives who wish to attend.

Phase-3: Online Financial proposal of only qualified bidders will be opened for further evaluation.

The Commercial Proposal Evaluation will be based on the "individual cost", which would be the total payouts including all taxes, duties and levies for the supply, installation, commissioning, system integration of equipments and Maintenance cost.

2.19 DECIDING AWARD OF CONTRACT:-

2.19.1 The Purchaser reserves the right to ask for a **technical elaboration/clarification** in the form of a technical presentation from the Bidder on the already submitted Technical Proposal at any point of time before opening after opening of the proposals. The Bidder has to present the required information to the Registrar General, High Court of Madhya Pradesh and its appointed representative on the date asked for, at no cost to the Purchaser.

2.19.2 Arithmetical errors will be rectified on the following basis: If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If the Bidder does not accept the correction of the errors, his bid will be rejected. If there is a discrepancy between words and figures, the amount mentioned in words will prevail.

2.19.3 The Purchaser will notify the Successful Bidder on its intention to award the work through **"Letter of Award/ acceptance"** mentioning the total Contract Value. The timeline for delivery of products and services will start from the date of issue of Letter of Award.

2.19.4 The Purchaser will subsequently send the Successful Bidder the Form of Contract Agreement provided in the Bidding Documents, incorporating all agreements between the parties.

2.19.5 As soon as practically possible, following receipt of the Form of Contract Agreement, the successful Bidder shall sign and date the Form of Contract Agreement and return it to the Purchaser. This is

deemed as the “Contract” or “Contract Agreement” defined elsewhere in this tender document.

2.19.6 *The Registrar General, High Court of Madhya Pradesh, Jabalpur may award the entire contract to a single firm or to multiple firms depending upon rates available with the bid.*

2.20 GENERAL INSTRUCTIONS TO THE BIDDERS:-

2.20.1 The cost of preparing the proposal, cost involved for the technical presentation and of visit to the High Court of Madhya Pradesh is not reimbursable.

2.20.2 All cutting, overwriting in the proposal should be authenticated by the initials of the authorized signatory. In case of any calculation error the unit rates would prevail. The amount will also have to be written in words.

2.20.3 ***Successful bidder must ensure his establishment in India and in the State of Madhya Pradesh for post-installation services and support of the supplied equipments.***

2.20.4 Canvassing in any form will lead to disqualification of the bid.

2.21 CONFIDENTIALITY:-

2.21.1 The Bidder shall keep confidential any information related to this tender with the same degree of care as it would treat its own confidential information. The Bidders shall note that the confidential information will be used only for the purposes of this tender and shall not be disclosed to any third party for any reason whatsoever.

2.21.2 As used herein, the term “Confidential Information” means any written information, including without intimation, information created by or for the other party, which relates to internal controls, computer or data processing programs, algorithms, electronic data processing applications, routines, subroutines, techniques or systems, or information concerning the financial affairs and methods of operation or proposed methods of operation, accounts, transactions, proposed transactions or security procedures of either party or any of its affiliates, or any client of either party, except such information which is

in the public domain at the time of its disclosure or thereafter enters the public domain other than as a result of a breach of duty on the part of the party receiving such information. It is the express intent of the parties that all the business process and methods used by the Bidder in rendering the services hereunder are the Confidential Information of the Bidder.

2.21.3 At all times during the performance of the Services, the Bidder shall abide by all applicable High Court of Madhya Pradesh security rules, policies, standards, guidelines and procedures. The Bidder should note that before any of its employees or assignees is given access to the Confidential Information, each such employee and assignees shall agree to be bound by the term of this tender and such rules, policies, standards, guidelines and procedures by its employees or agents.

2.21.4 The Bidder should not disclose to any other party and keep confidential the terms and conditions of this tender, any amendment hereof, and any Attachment or Annexure hereof.

2.21.5 The obligations of confidentiality under this section shall survive rejection/termination/expiry of the contract for a **period of five years**.

2.22 The Government of India had amended the General Financial Rules 2017 to enable the imposition of restrictions under Rule 144(xi) on bidders from countries which share a land border with India on grounds of defense of India, or matters directly or indirectly related thereto including national security. The bidder has to submit proper documents in this regards as per the policy.

As per the Public Procurement (Preference to Make in India), Order 2017, the Class-I local suppliers shall get preference in procurement of goods, services or works. In furtherance of the Revised PPP-MII Order dated 04.06.2020, the Ministry of Electronics & Information Technology (MEIT) has notified the mechanism for calculation of local content for the 13 electronic products vide Notification no. 43/4/2019-IPHW-MeitY dated 07.09.2020.

Section – III

3. Terms and Conditions for e-Tendering:-

3.1 For participation in e-tendering module, it is mandatory for prospective bidders to get registration on website **https://mptenders.gov.in/**. Therefore, it is advised to all prospective bidders to get registration by making on line registration fees payment at the earliest.

3.2 Tender documents can be purchased *only online* on payment of tender fees and downloaded from website **https://mptenders.gov.in/** by making online payment for the tender document fee.

3.3 Service and gateway charges shall be borne by the bidders.

3.4 Since the bidders are required to sign their bids online using class – III Digital Signature Certificate, they are advised to obtain the same at the earliest.

3.5 For further information regarding issue of Digital Signature Certificate, the bidders are requested to visit website **https://mptenders.gov.in/.** Please note that it may take upto 07 to 10 working days for issue of Digital Signature Certificate. Department will not be responsible for delay in issue of Digital Signature Certificate.

3.6 If bidder is going first time for e-tendering, then it is obligatory on the part of bidder to fulfill all formalities such as registration, obtaining Digital Signature Certificate etc. well in advance.

3.7 Bidders are requested to visit our e-tendering website regularly for any clarification and / or due date extension.

3.8 Bidder must positively complete online e-tendering procedure at **https://mptenders.gov.in/**

3.9 Department shall not be responsible in any way for delay /difficulties /inaccessibility of the downloading facility from the website for any reason whatever.

3.10 For any type of clarification bidders can / visit **https://mptenders.gov.in**. In case of any assistance please call Help desk numbers 0120-4200462, 0120-4001002. Support timings: Monday to Saturday from 10:00 AM to 7:00 PM.

3.11 Interested bidders may attend the free training programme in Bhopal at their own cost. For further query please contact help desk.

3.12 The bidder who so ever is submitting the tender by his Digital Signature Certificate shall invariably upload the scanned copy of the authority letter as well as submit the copy of same in physical form with the offer of particular tender.

3.13 The firms registered under NSIC and MSME (The vendor to be registered with both NSIC and MSME for claiming exemption of tender fees) are exempted for submission of tender fees only. But they have to submit valid EMD as per the tender requirement.

Section – IV

4 GENERAL CONDITIONS OF THE CONTRACT (GCC):-

4.1 GENERAL:-

The Products/equipments supplied under this contract shall conform to the Technical Specifications given in this tender under **Section VII**.

4.2 PERFORMANCE GUARANTEE:-

4.2.1 The Successful Bidder will be required to furnish performance guarantee in the form of unconditional Bank Guarantee issued by a Nationalized / Scheduled Bank in India equivalent to 05% of the Contract Value initially valid for a period of 36 months within 30 days from the date of issue of Letter of Award / acceptance. For remaining 24 months Bidder will submit fresh BG before expiry of the initial BG.

4.2.2 **BANK GUARANTEE:-**

The Bank Guarantee issued by following banks would be accepted. SBI or its subsidiaries, any Indian Nationalized Bank/Scheduled Bank, Export Import Bank of India**,** a foreign bank (issued by a branch outside India) with counter guarantee from SBI or its subsidiaries or any Indian Nationalized Bank, and any scheduled commercial bank approved by RBI having a net worth of not less than Rs.500 Crores as per the latest annual report of the bank.

4.2.3 The Performance Guarantee shall be as per the format approved by the Registrar General, High Court of M.P., Jabalpur.

4.2.4 The Performance Guarantee shall be payable to the Purchaser as a compensation for any loss resulting from the Bidder's failure to complete its obligations under the contract. The Purchaser will discharge the Performance Guarantee after completion of the Bidder's performance obligations, including any warranty obligations, under the contract.

4.3 DELIVERY OF MATERIALS AND RELATED DOCUMENTATION:-

4.3.1 Delivery, Installation and Commissioning of the materials along with the related documents as per the tender document and technical specification section **(Section VII)** are the responsibility of the Bidder.

4.3.2 The Successful Bidder shall ensure that all Products/equipment is supplied within the Implementation schedule mentioned in the tender document under Section V.

4.3.3 The Successful Bidder shall submit all the Software Kits (CDs), License Papers, Warranty Papers and any other relevant documentation related to the supplied products to the Purchaser along with the supplied products/equipments.

4.4 WARRANTY:-

4.4.1 The Bidder is required to provide on-site comprehensive warranty **valid for 60 months for all supplied hardware items from the date of installation**.

4.4.2 The Bidder shall warrant that all the equipment supplied under the contract is newly manufactured and shall have no defect arising out of design, materials or workmanship or from any act or omission of the Bidder that may develop under normal use of the supplied equipments in the conditions prevailing across the country.

4.4.3 The Bidder shall warrant that the services provided under the contract shall be as per the Warranty Service Level Requirements given under **Section-VI**. During the warranty, the Bidder shall perform all the functions as enunciated in Section-VI at no extra cost to the Purchaser. All the penalty clauses shall be applicable during the period of warranty in case of failure on part of Bidder. The terms and conditions for Warranty are given in **Section-VI**.

4.4.4 The bidder shall quote for **comprehensive On-Site warranty and support for FIVE years**, which shall become effective after the Final Acceptance Sign-off. The cost, including visits of the engineers etc. shall be quoted as part of the individual equipment prices. No separate charges shall be paid for visit of engineers or attending to faults and repairs or supply of spare parts.

4.4.5 The Registrar General, High Court of Madhya Pradesh shall promptly notify the Bidder about any claims arising under this warranty. Upon receipt of such notice, the Bidder shall repair / replace / reconfigure / re-

provisions the defective equipments or service. Replacement under warranty clause shall be made by the Successful Bidder free of all charges at site including freight, insurance and other incidental charges.

4.4.6 **The Bidder shall, at the time of submitting the bid submit the Technical Proposal specifying how the Bidder proposes to carry out repair under Warranty. The Bidder shall also indicate what spares will be kept for immediate replacement. The infrastructure planned to be created by the Bidder to fulfill his obligations under Warranty and his action plan to deal with the various situations arising out of hardware and software faults shall be clearly indicated.**

4.4.7 If the Bidder, having been notified, fails to remedy the defect(s) within the period specified in the Service Level Agreement, the Registrar General, High Court of Madhya Pradesh may proceed to take such remedial action as may be necessary at the Bidder's risk and expense and without prejudice to any other rights, which Registrar General, High Court of Madhya Pradesh may have against the Bidder under the contract.

4.5 PAYMENT TERMS:-

4.5.1 For the supply, installation, commissioning, testing and warranty maintenance of all hardware items for the period of 60 months:-

Payments will be made in **Indian Rupees only**

4.5.1.1 ***80%** of total price against delivery* of the equipments at the site after submitting the duly verified delivery challan of the site / locations certified by the Office of District and Session Judge of District Courts.

4.5.1.2 ***20%** of total price against* successful installation and getting Sign-off from all the District Courts.

4.6 PRICES:-

4.6.1 The rate contract of all the quoted items shall be valid for the period of 01 year from the date of agreement/contract.

4.6.2 The rates and prices quoted by the bidder shall be fixed for the duration of the contract and shall not be subjected to adjustment.

The rates shall be valid for the period of one year from the date of agreement. *However on introduction of new taxes / duties , the*

rates of the quoted items shall be change in same proportionate. Further, order on approved rates shall be placed by High Court of Madhya Pradesh, Jabalpur on need basis.

4.7 PURCHASER'S RIGHTS:-

4.7.1 The Purchaser reserves the right to make changes within the scope of the work and Contract and configuration of items at any point of time.

4.7.2 The Purchaser reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids, at any time prior to award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds of purchaser's action.

4.8 TIME SCHEDULE TO COMPLETE THE CONTRACT:-

4.8.1 The successful bidder shall complete the assignment within **60 days from the date of issue of Letter of Acceptance / Letter of Intent**.

4.8.2 In case the purchase order is received directly from the District Court then the period of supply and installation will be 60 days.

4.8.3 The Successful Bidder shall ensure that the delivery of Products/ equipment and/or the delivery of the services are in accordance with the time schedules specified in tender documents. In case of any deviation from the schedule, the Purchaser reserves the right to either cancel the Contract and/or recover Liquidated Damage charges.

4.8.4 The Successful Bidder, if faced with problems in timely delivery of services, which have dependencies on the Service Provider and/or the Purchaser, which are beyond their control at any time before the Final Acceptance Signoff, shall immediately inform the Purchaser in writing, about the causes of the delay and tentative duration of such delay etc. The Purchaser, on receipt of such notice, shall analyze the facts at the earliest and may at its sole discretion, extend the contract period as deemed reasonable.

4.8.5 Any delay by the Successful Bidder in the delivery of Products/ equipment and/or the services will make the Successful Bidder liable to any or all of the following:

i. Forfeiture of Performance Bank Guarantee
ii. Imposition of Liquidated Damage charges
iii. Termination of the contract for default.
iv. Blacklisting of the vendor.

4.9 LIQUIDATED DAMAGES (LD):-

If the Bidder fails to deliver any or all of the equipment or to perform the services within the time period(s) as mentioned in tender document. Registrar General, High Court of Madhya Pradesh shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to the 0.5% of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the contract price. Once the maximum is reached, Registrar General, High Court of Madhya Pradesh may consider termination of the contract.

4.10 FORCE MAJEURE:-

4.10.1 Neither party shall be responsible to the other for any delay or failure in performance of its obligations due to any occurrence commonly known as Force Majeure which is beyond the control of any of the parties, including, but without limited to, fire, flood, explosion, Acts of God or any governmental body, public disorder, riots, embargoes, or strikes, acts of military authority, epidemics, strikes, lockouts or other labour disputes, insurrections, civil commotion, war, enemy actions.

4.10.2 If a Force Majeure arises, the Bidder shall promptly notify the Registrar General, High Court of Madhya Pradesh in writing of such condition and the cause thereof. Unless otherwise directed by the Registrar General, High Court of Madhya Pradesh the Bidder shall continue to perform his 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. The Bidder shall be excused from performance

of his obligations in whole or part as long as such causes, circumstances or events shall continue to prevent or delay such performance.

4.11 TERMINATION:-

4.11.1 Termination on expiry of the CONTRACT: The Agreement shall be deemed to have been automatically terminated on the expiry of the Contract period unless the Registrar General, High Court of Madhya Pradesh has exercised its option to extend the Contract in accordance with the provisions, if any, of the Contract.

4.11.2 Termination on account of Force Majeure: Either party shall have the right to terminate the Contract on account of Force Majeure.

4.11.3 Termination on account of insolvency: In the event the Successful Bidder at any time during the term of the Contract becomes insolvent or makes a voluntary assignment of its assets for the benefit of creditors or is adjudged bankrupt, then the Registrar General, High Court of Madhya Pradesh shall, by a notice in writing have the right to terminate the Contract and all the Successful Bidder's rights and privileges hereunder, shall stand terminated forthwith.

4.11.4 Termination for breach of contract: A breach by the Successful Bidder of its obligations hereunder and such breach not being rectified by the Successful Bidder within 30 days of receipt of the Purchaser's notice intimating such breach. Upon termination, the Successful Bidder shall surrender all the data and materials belonging to the Purchaser.

4.11.5 Termination for delay: Successful Bidder shall be required to perform all activities/services as per tender document If the Successful Bidder fails to do so, the Contract may be terminated by the Registrar General, High Court of Madhya Pradesh by giving 30 days written notice unless the Registrar General, High Court of Madhya Pradesh has extended the period with levy of Liquidated Damages, as per conditions of the tender.

4.11.6 The Registrar General, High Court of Madhya Pradesh may at any time terminate the Contract by giving 30 days notice without assigning any reason.

4.11.7 Consequences of termination: In all cases of termination herein set forth, the obligation of the Registrar General, High Court of Madhya Pradesh to pay shall be limited to the period upto the date of effective termination. Notwithstanding the termination of the Agreement, the parties shall continue to be bound by the provisions of the Agreement that reasonably require some action or forbearance after such termination.

4.11.8 In case of termination of Contract herein conditions of the tender document the Contractor shall be put on holiday *[i.e. neither any enquiry will be issued to the party by the Registrar General, High Court of Madhya Pradesh against any type of tender nor their offer will be considered by the Registrar General, High Court of Madhya Pradesh against any ongoing tender(s) where contract between the Registrar General, High Court of Madhya Pradesh and that particular Contractor (as a bidder) has not been finalized]* for two years from the date of termination by the Registrar General, High Court of Madhya Pradesh to such Contractor.

4.12 ARBITRATION:-

In the event of any dispute or difference arising out or touching upon any of the terms and conditions of this contract and / or in relation to the implementation or interpretation hereof, the same shall be resolved initially by mutual discussion and conciliation but in the event of failure thereof, the same shall be referred to the Registrar General, High Court of Madhya Pradesh or his nominee. The sole arbitrator will be appointed by Hon'ble the Chief Justice, High Court of M.P. and the decision of the Arbitrator shall be final and binding on the parties. The arbitration shall be in Jabalpur and the Arbitrator shall give his award in accordance with "***The Arbitration and Conciliation Act, 1996***".

4.13 GOVERNING LAWS AND JURISDICTION:-

The Agreement shall be governed by the laws in force in India. Any dispute arising in relation to the Agreement shall be subject to the Jurisdiction of the Court at Jabalpur.

Section – V

5. SPECIAL CONDITIONS OF THE CONTRACT (SCC):-

5.1 GENERAL:-

The conditions given in this Section V, supplement the “Instructions to the Bidders” given in Section II & “GCC" given in Section IV and in case of any conflict, the conditions given herein shall prevail over those in Sections II and IV.

5.2 EQUIPMENTS AND SUPPORTING SOFTWARE:-

5.2.1 All the equipments / system and related software to be supplied shall conform to the relevant technical specifications as mentioned in Section-VII of this document.

5.3 SITE ACCEPTANCE TESTS (SAT):-

5.3.1 The Purchaser shall carry out the entire test detailed in the Acceptance test schedule to be furnished by the Contractor to confirm that the performance of the different modules, sub-systems and the entire installation satisfies the specification requirements. The Purchaser reserves the right to include any other tests which in his opinion is necessary to ensure that the equipment meets the specifications.

5.3.2 The Purchaser reserves the right to ask for modifications/additions to the Site Acceptance Test Procedure at any point of time till the Site Acceptance signoff at each location.

5.3.3 The Site Acceptance Tests shall cover the intended functioning of the equipments with proper integration with other sub components and software’s.

5.3.4 The contractor shall carry out the Site Acceptance Tests in the presence and supervision of the Purchaser or its designated Officer / agency at the site. The contractor, at its own cost, shall provide the testing equipment/instruments/software programs necessary for performing and demonstrating the Site Acceptance Tests.

5.3.5 The Purchaser or its appointed testing authority shall supervise the tests at each site, as described in the Site Acceptance Test Procedure and performed by the contractor to confirm that the complete solution at each

site satisfies the requirement of specifications including the service performance.

5.3.6 The contractor shall rectify all deficiencies immediately, if found, in the performance of the system as per the requirement during the Site Acceptance Tests, at no cost to High Court of Madhya Pradesh, Jabalpur.

5.3.7 Any components or parts failing during the acceptance tests shall be replaced free of cost by the Contractor. These replacements shall not be made out of spares supplied by the Contractor as part of supplies under this Contract. This shall also not entitle the contractor to any extension of completion time.

5.3.8 The cost of all test and / or analysis shall be fully borne by the contractor. Material put up for inspection shall be those to be supplied and in quantities laid down in the Schedule of Quantities. Any variation shall require the prior approval of the Purchaser before the material is manufactured/ offered for inspection.

5.3.9 All material brought to site shall be permitted to be installed only after inspection and acceptance by the Purchaser.

5.3.10 The completed installation at all stages shall be subjected to checks and tests as decided by Purchaser. The contractor shall be liable to remedy all of such defects as discovered during these checks and test and make good all deficiencies brought out. The complete installation shall be taken over finally on successful commissioning in entirety.

5.4 CONSIGNEE AND SECURITY OF MATERIAL:-

Security of all material at the site where the work is in progress shall be the contractor's responsibility and he shall arrange to guard the same from theft/pilferage/vandalism. In the event of any loss the contractor shall be responsible for the same. Any stores lost, prior to formally taking over by the Purchaser, shall be made good by the contractor at no cost to the Purchaser.

Section – VI

6. SCOPE OF WORK:-

6.1 The Registrar General, High Court of Madhya Pradesh Jabalpur is interested to assign the task for Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh.

6.2 SUPPLY:-

Supply of all equipments, materials, components, accessories, mounting hardware, software, wires and cable for connection, etc. as per requirement of High Court of Madhya Pradesh.

6.3 INSTALLATION & WIRING:-

6.3.1 Installation & wiring of all equipments, components and accessories. Installation of all necessary software's and drivers.

6.4 INSTALLATION PRACTICE AND METHOD OF WORK:-

6.4.1 The work shall be executed to the highest standards using best quality material. The system design shall use state-of-the art techniques/tools. The contractor shall ensure that the entire specification is complied with the technical specifications. It shall be the responsibility of the contractor to demonstrate compliance of technical as well as functional specifications. Meeting individual requirements shall not be deemed as meeting the overall efficient functioning of the total system.

6.4.2 The completed installation shall be subject to checks at all stages and tests as prescribed in the bid or as deemed necessary by the Registrar General. The same shall be done by the Purchaser and the contractor shall be liable to rectify such defects as brought out by the Purchaser during these checks and tests and make good all deficiencies at his own cost.

6.5 COMPREHENSIVE WARRANTY:-

The contractor will be required to maintain the installed systems for the period of **FIVE years after the taking-over certificate / installation certificate.**

6.6 WARRANTY TERMS AND CONDITIONS:-

6.6.1 The Contractor shall be solely responsible for the maintenance, repair of the whole equipments / items supplied and integrated and the Registrar General; High Court of Madhya Pradesh shall not be liable to interact with any of the partners/ collaborators of the Contractor.

6.6.2 The Contractor shall have adequate Technical Support Center to meet the criteria for fault restoration/faulty unit repair times as mentioned in the Section-VI. The Contractor shall furnish the names, locations, complete postal address, telephone numbers and FAX numbers of all Technical support Centers at the time of signing the Contract.

6.6.3 The Contractor shall also provide the name of alternate contact person or Technical Support Center with address & telephone / fax numbers / E-mail which may be contacted by the Registrar General, High Court of Madhya Pradesh or its authorized Officer / staff for support in case of no response/poor response from the designated Technical support center. This however shall not preclude from imposing the penalties, if any, as applicable as per the terms & conditions of this tender.

6.6.4 Any change in Address, Phone number, FAX Number, e-mail etc., shall have to be intimated in writing by the Contractor to the Registrar General, High Court of Madhya Pradesh, Jabalpur

6.6.5 The Contractor shall ensure that all the Technical support centers are manned by fully competent and responsible Engineers and are capable of attending faults / supporting their engineers at the High Court of Madhya Pradesh and District Courts

6.7 WARRANTY SERVICE LEVEL REQUIREMENTS – SLA:-

6.7.1 Service Hours:-

The Service window for all the equipments would be all working days from 09:00 A.M. to 06:00 P.M.

6.7.2 Scheduled Downtime:-

(a) Scheduled downtime is defined as the period of time when software application will remain unavailable for conducting necessary preventive maintenance, urgent repairs etc. This is the maximum

duration, which the Contractor can take for scheduled downtime purposes.

(b) It will be expressed in hours.

(c) The maximum scheduled downtime for any equipment would be 02 days in every calendar month.

(d) The preventive maintenance would be carried out with a minimum advance notice of 24 hours in writing and subsequent acceptance of the same by Registrar General, High Court of Madhya Pradesh or officer who will execute the contract.

6.7.3 Mean Time to Resolve / solve the problem (MTTR): -

(a) MTTR is defined as the arithmetic average of the time taken to attend to resolve the issues logged over a defined period of time.

(b) The Severity Levels for measuring MTTR are provided in the following table:-

S. No.	Severity Level
1	High
2	Low

6.7.4 The various Service Level Requirements and related penalties for default are given below**:-**

Parameter	***Details***	***Measurement Criteria***	***Penalties per day of delay / per fault / per occasion***
Mean time to resolve (MTTR)	*(i) Within 48 working Hours from the call logging time – for all High Severity events* *(ii) Within 72 working hours from the time of attending the problem for all Low severity events*	*Calculation of fault duration per instance based on Fault Docket*	*(i) For High Severity events,* ***Rs.1000/-.*** *(ii) For Low Severity events,* ***Rs.500/-*** *Delay will be counted in steps of one hour.*

6.7.4.1 The Successful Bidder needs to maintain the Service Levels as follows:

(a) 99% of the times for the MTTR of High Severity Events

(b) 95% of the times for the MTTR of Low Severity Events

6.7.4.2 The penalty will be applicable on per fault basis even if there is a commonality of fault at any point causing full or part failure of services.

6.7.4.3 After the expiry of warranty, it shall be optional for Registrar General, High Court of Madhya Pradesh not to enter the contract further with the contractor. If Registrar General, High Court of Madhya Pradesh is not satisfied with the performance of the Contractor during Warranty it reserves the right to terminate the same during its currency, after **giving a notice** to the Contractor.

6.7.4.4 The Contractor has to maintain adequate spares for maintaining the SLA (Service Level Agreement) parameters as mentioned below. Any cost involved to meet the service level requirements specified above is to be borne by the Bidder.

6.7.4.5 In case the Service Level Requirements are violated continuously for a period of three months, the Purchaser reserves the right to terminate the Contract by giving a notice to the Successful Bidder.

6.7.4.6 <u>The preventive maintenance of all the installed equipments / products to be carried on yearly basis during the warranty period and the report is to be submitted to the Registrar General, High Court of Madhya Pradesh or his authorized officer</u>.

Section – VII

7. TECHNICAL SPECIFICATIONS:-

All the products/equipment/items supplied should be quoted with:-

(i) *Five years comprehensive Onsite Warranty and support on all hardware equipments*.

(ii) All the necessary required cables and other accessories.

(iii) Enclose all product catalogues and technical brochures of the products / items along with **MANUFACTURER AUTHORIZATION FORM (MAF) addressed to the "Registrar General, High Court of Madhya Pradesh", Jabalpur (M.P.)**

(iv) The bidder has to quote only 01 product of single make / brand at a time and not multiple brands for same item.

(v) The Original equipment manufacturer can authorize more than one partner for participation in the bid.

(vi) Back-to-Back support letter is to be submitted by OEM regarding support of their quoted products.

The details of the Hardware articles along with technical specifications is enumerated as given below:-

S. No.	Items	Minimum Specifications* / Make
01	Firewall Technical Specifications	**Minimum Specification – A**
02	Web Application Firewall with Server Load Balancer	**Minimum Specification – B**
03	Network Monitoring System	**Minimum Specification – C**

Note: - Please submit the product catalogue / brochure in above serial *ORDER* only.

"Specification – A"
Firewall Technical Specifications

S. No.	Feature	Technical Specification	Compliance Yes / No
1	Type	Next Generation Enterprise Firewall	
2	3rd party Test Certification	The proposed firewall vendor must have over 97% of Exploit Block rate in latest NGFW NSS Lab Test report.	
		The proposed vendor must be in the Leader's or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report.	
3	Interface and Connectivity Requirement	6 X 10G Copper/RJ45 Day 1	
		8 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords.	
		4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one	
		Minimum 2 x 10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port	
		Should have support 2x40/100G for future use.	
4	Hardware Architecture	The appliance based security platform should provide Next-Gen Firewall functionality like IPS, Application Control, URL and content filtering and Anti-malware functionality in a single appliance from day one.	
		The appliance hardware should be a multicore CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one.	
		The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution	
5	Performance & Scalability	The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps.	
		The firewall should provide 12 Gbps of IPSEC VPN throughput	
		NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions	
		NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second – Min 90,000	
		High Availability: Active/Active and Active/Passive and should support session state synchronization among firewalls from day 1.	

		Firewall should support creating security policies with source/destination zones, network subnets/ranges, relocation objects, ports/protocols, applications, user/group attributes, URL/URL categories and action on traffic. The actions on the traffic should be to allow, alert, block, block and continue, reset. The firewall should provide time based polices with options for reccurrecing schedule or one time schedule.	
		The firewall should supports NAT's like source NAT , destination NAT , U-Turn NAT. Firewall should support Nat66, Nat 64 or Nat46 functionality	
		Solution should provides capabilities like dynamic real-time metrics based , policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.	
		The solution should provide the following routing capabilities: OSPF, EIGRP, BGP, RIP, Multicast, Static,	
		Route Tracking(SLA) PBR, ISIS, BFD, ECMP, VRF, Application based Routing	
		Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance	
6	Next Gen Firewall Features	The solution should be able to provide contextual information about the hosts and the network subnets present such that the admins are able to capture all the required information and build the security profiles based on the details shown on the solution. The details captured should consist of the following: IOC's , MAC addresses, IP address, Applications, Ports & protocols, vulnerabilities etc.	
		Should support capability to integrate with other security solutions to receive contextual information like security group tags/names.	
		Should support more than 4000+ (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency	
		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
		Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's.	
		The firewall solution should have the following capabilities to make sure the current solution is future ready for technologies like WAN routing, SASE etc. The firewall should have application aware	

		routing with HTTP and ICMP ping, ZTNA based clientless access to applications from day1.	
		The firewall solution should have capabilities like Application Aware Routing, Health Monitoring, DIA, Dual ISP, Data interface Management for simplified branch capabilities	
		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
		The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box. The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.	
		The solution should have ML/AI capability to detect client apps and process. Moreover it should be able identify malicious encrypted traffic even when it is destined for a trustworthy service. This is required to help administrators control specific applications and improve network security	
		The solution should provide traffic hit count, Rule Conflict Detection (Redundant &	
		Shadowed) and policy warning for streamlining firewall policies.	
		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	
		Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control.	
		The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor. Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist. The solution should have the capability to detect MD5, SHA256 and SHA512 traffic hashes to detect any malicious traffic pattern	
		The solution should provide Configuration Deployment History, Pending Changes and Policy Compare capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall.	
		The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	

		Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
		The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
		Should be IPv6 Logo or USGv6 certified	
7	URL Filtering Features	Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
		Should must support URL threat intelligence feeds to protect against threats	
		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories from day1.	
8	Anti-APT / Malware Features	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis.	
		Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
9	Management	Proposed solution shall have required subscription like Threat Intelligence for proper functioning	
		The management platform must be accessible via a web-based interface and ideally with no need for additional client software and must provide centralized logging and reporting functionality	
		The management platform must be a dedicated OEM appliance or VM (bidder to consider Required computing / hardware resource) running on server.	
		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
		Should support troubleshooting techniques like Packet tracer and capture	
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. The management platform support running on-demand and scheduled reports	

		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
		The centralized management platform must not have any limit in terms of handling logs per day	
		The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
		The management platform must risk reports like advanced malware, attacks and network	
10	Support	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
		OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The NGFW should be proposed with 5 years onsite support and subscription licenses for NGFW, NGIPS, Anti Virus, Anti Spyware, URL Filtering, DNS, VPN and Anti Botnet.	
11	DNS Security	The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1.	
		Solution should maintain a database containing a list of known botnet command and control (C&C) addresses which should be updated dynamically.	
		DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control.	
		DNS security should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains.	
		It should prevent against new malicious domains and enforce consistent protections for millions of emerging domains.	
		The solution should integrate and correlate to provide effective prevention against. New C2 domains, file download source domains, and domains in malicious email links. Ingegrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence.	
		Should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.	

		Solution should prevent against DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection	
		The solution should have capabilities to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers.	
		The solution should have dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink holing malicious domains to cut off Command and control and quickly identify infected users.	
12	SD-WAN	Proposed firewall should support for internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,	
		Support for WAN Link-Load balancing and Fail-over with 4 Links or more.	
		Integrated Traffic Shaping functionality for both inbound and outbound traffic.	
		The proposed firewall should support SD-Wan functionality for application aware traffic control	
13	VPN	The proposed system shall comply/support industry standards, supports without additional external solution, hardware or modules: IPSEC VPN , PPTP VPN, L2TP VPN,SSL VPN	
		The system shall support 2 forms of site-to-site VPN configurations: Route based IPSec tunnel ,Policy based IPSec tunnel	
		The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.	
		The proposed system shall support TWO modes of SSL VPN operation:	
		Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS, SMB/CIFS, SSH, RDP.	
		Tunnel mode, for remote computers that run a variety of client and server applications	
		The proposed solution shall support to a minimum of 2000 concurrent IPSEC-VPN and 1000 concurrent SSL-VPN users from day 1	
14	Automation & Incident Response	The Proposed system shall support automation response based on following events:	
		Compromised Hosts detected	
		Configuration Change	
		Event Log	
		High CPU	
		License Expiry	
		Email Alert	
		IP Ban	

15	Device Storage	Minimum 800GB SSD	
16	Logs & Reporting	Bidder has to propose on premise dedicated logging, analytics & reporting solution from same OEM (Virtual /Physical Appliance) from day1, the logging solution to be deployed at Data Center only. In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. **Required Features:** Should Deliver single-pane visibility, also have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event corelation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be available on public website to validate the capabilities.	
17	Installation and Migration	The bidder must migrate the existing configuration and policies from the SonicWall NSA6600 firewall to the new one and provide six days of training on the configuration and management of all key security aspects to the technical team of the High Court of Madhya Pradesh, Jabalpur	

"Specification – B"
Web Application Firewall with Server Load Balancer

S. No.	Specifications	Compliance (Yes/No)
	Web Application Firewall with Server Load Balancer	
1	The proposed appliance should be a dedicated ADC/WAF/SLB appliance having DDoS protection, SSL inspection, and real-time threat intelligence. it should not be part of any Firewall or UTM.	
2	**Traffic Ports support:** 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. **Device L4 Throughput**: 20 Gbps and scalable upto 40 Gbps **Layer 7 requests per second:** 1300,000 **Layer 4 connection per second:** 500,000 **Concurrent Connection:** 38 Million **RSA CPS (2K Key):** 20,000 **ECC CPS (EC-P256):** 12,000 with TLS1.3 Support **Processor:** Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port.	
3	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2	
4	The solution must be able to decrypt SSL web traffic between clients and web servers.	
5	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1	
6	**The proposed appliance should support the below metrics:** — Minimum Misses, — Hash, — Persistent Hash, — Tunable Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc	
7	**Following Load Balancing Topologies should be supported:** • Virtual Matrix Architecture • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding	

8	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, d) Operating System	
9	The proposed Hardware must have Bandwidth Management feature from Day 1	
10	The solution should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode using standard/ RFC compliant redundancy protocol like VRRP or equivalent, for HA interconnection over network from day 1.	
11	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend	
12	The solution should have support for multiple VLANs with tagging capability	
13	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure	
14	Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications	
15	Should have ability to upgrade/downgrade device software Images.	
16	The device should support following health check types: • Link Health Checks • TCP Health Checks • UDP Health Checks • ICMP Health Checks • HTTP/S Health Checks • TCP and UDP-based DNS Health Checks • TFTP Health Check • SNMP Health Check • FTP Server Health Checks • POP3 Server Health Checks • SMTP Server Health Checks • IMAP Server Health Checks • NNTP Server Health Checks • RADIUS Server Health Checks • SSL HELLO Health Checks • WAP Gateway Health Checks • LDAP/LDAPS Health Checks • Windows Terminal Server Health Checks • ARP Health Checks • DHCP Health Checks • RTSP Health Checks • SIP Health Checks • Virtual Wire Health Checks • DSSP Health Checks • Script-Based Health Checks • Cluster-based Health Checks	

17	Device should be accessed through the below: • Using the CLI • Using SNMP • REST API • Using the Web Based Management	
18	The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.	
19	WAF should have the flexibility to be deployed in the following modes: Reverse proxy Out of Path (OOP)	
20	Solution should dynamically understand the Changes on the Web/Application Server	
21	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures). The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	
22	The WAF should support the following escalation modes: a) Active, b) Bypass, c) Passive	
23	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	
24	**Hiding Sensitive Content Parameters:** It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)	
25	**Auto Policy Optimization**	
a	• Known Types of Attack Protection - Rapid Mode	
b	• Zero Day Attack Blocking - Extended Mode	
c	• Working in Learn Mode	
d	• Auto Discovery	
26	**Following Threats should be protected by the proposed WAF solution:**	
a	Parameters Tampering	
b	Cookie Poisoning	
c	SQL Injection	
d	Session Hijacking	
e	Web Services Manipulation	
f	Stealth Commands	
g	Debug Options	
h	Backdoor	
f	Manipulation of IT Infrastructure Vulnerabilities	
g	3rd Party Misconfiguration	
h	Buffer Overflow Attacks	
f	Data Encoding	
g	Protocol Piggyback	
h	Cross-Site Scripting (XSS)	

f	Brute Force Attacks	
g	OS Command Injection	
h	Cross Site Request Forgery (CSRF)	
g	Information Leakage	
h	Path (directory) Traversal	
f	Predefined resource location	
g	Malicious file upload	
h	Directory Listing	
27	**The proposed WAF should support the Activity Tracking, which should include the following:**	
a	Dynamic IP	
b	Anonymity	
c	Scraping	
28	**Device Fingerprint-based tracking**	
a	The Proposed WAF should support Device Fingerprint technology or equivalent by involving various tools and methodologies to gather IP agnostic information about the source.	
29	The proposed solution should have Signature Update, Attacker Feed and Geo Location database from day1.	
30	Bidder should propose Centralized Management & Reporting Solution from Day 1.	
31	The proposed appliance/software should be EAL2 certified.	
32	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy.	
33	Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT/ full DNS server with DNSSec/DNS DDOS/ application load balancing from day one with relevant Licenses.	
34	Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6	
35	Should have a Web Vulnerability Scanner feature to detect existing vulnerabilities like SQL Injection, Cross Site Scripting, Source code disclosure, OS Commanding in the web applications.	
36	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.	
37	Appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.	
38	The solution should have configurable persistency features to maintain sessions to the load balanced backend servers	
39	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	
40	Solution must have the API protection and support Json , XML and Open API	
41	Protection for REST APIs filters malicious inputs in requests with JSON payloads.	
42	**Data Analytics , Logs and Reporting**	
a	Solution must have analytics functionality which includes logical view / tree	

	view of virtual servers and connectivity.	
b	Solution must have the various charts static and dynamics for analytics	
c	Solution must have real time monitoring views or dashboards	
d	Solution should support realty time logging and reporting functionality	
e	Solution must have support to configure SNMP	
43	**Integration**	
a	Solution must support integrations like SAP , Cloud platform and SIEM tools	
b	Solution must support REST API	
c	Solution should support virtual servers or profiles, one for internal traffic and one for external traffic. Configure load balancing rules specific to each domain. Internal traffic can be routed to internal servers, and external traffic to public-facing servers. Should have option to set up separate monitoring and logging profiles for internal and external traffic to track performance and security incidents.	
d	The solution should be scalable enough to support future growth in traffic and applications.	
44	**Support**	
a	Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P.	

"Specification – C"
Network Monitoring System

S. No.	**The proposed solution should be able to monitor the availability, health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, end point devices like desktop, Kiosks, display boards, URL monitoring, other snmp enabled devices like UPS and AC from single dash board.**	**Compliance Yes / No**
	Discovery	
1	The solution should be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application, middleware, storage, databases) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services. This should be aided by 5000+ asset type discovery signatures to detect the DC comprehensively. System should have option for multiple options for discovery including IP address based discovery, IP address range discovery, CSV based discovery for bulk discovery.	

2	The solution should automatically group servers that work closely together based on analysis of communication between them	
3	Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details.	
4	The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them.	
5	The discovery data should be fully auditable as to where it came from and what the method to retrieve that data was.	
6	The solution should show exactly how the discovery data is obtained (i.e., Audit trail and mechanism to validate the quality of data discovered)	
7	The Discovery solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc.	
8	The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS , it should detect End of support and End of life as well. On Security , It should be able to find the patches installed on servers along with reports on vulnerable ports. . Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.	
9	The discovery solution should have the ability to capture and report on infrastructure drift in datacenter.	
10	The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of modern day DevOps platforms such as containers such as Docker, Runc, AIX WPARs and management solutions such as Kubernetes, Docker Swarm, Cloud Foundry and Open Shift.	
11	Discovers in-depth configuration data for storage systems, pools, volumes, disks drives, LUNS, File Systems	
12	It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application.	
13	The report of inventory of discovered devices should be available to export in .csv format.	
14	Automatically learn IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc. and to establish the connections and to correlate	
15	Provides provision to draw & map user specific network diagram	

16	**Integration and Development**	
17	Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML	
18	**Application monitoring**	
19	The solution should automatically provide real-time view of processes running in systems and in-depth application performance statistics after discovery/configuration of applications	
20	The solution should automatically provide real-time view of windows event logs including the level of the event logs, event ID, and source.	
21	The solution should be able to put together important parameters of an application, into one single monitoring template that can be uniformly applied to applications on different servers, including - Microsoft servers (e.g. Active Directory, Exchange, SharePoint, and Office Communications Server) - Databases (e.g. Microsoft SQL Server, PGSQL, MySQL etc.) - Major application (e.g. ERP, CRM, etc.)	
22	The solution should support monitoring various attributes(at least 50+) in Tomcat, Web Sphere MQ, Apache HTTP, IIS, and WAS	
23	The solution should support receiving events from Web Methods, IBM HTTP server, Apache Active MQ	
24	The solution should have capability to monitor HTTP service, HTTPS service, FTP server statistics, POP/SMTP services, ICMP services or any customer specific port based systems	
25	**Network Monitoring**	
26	The solution should have network monitoring data available in the same console where every other information is available.	
27	The solution should be able to capture network log errors	
28	The solution should be able to do flow analysis	
29	The solution should be able to track connectivity between network endpoints and display the delay between nodes	
30	The solution should allow query of network events and performance data	
31	The solution should provide network path monitoring	
32	The solution should provide live network topology view	
33	The solution should also provide configuration management on network devices	
34	**Servers/System Monitoring**	
35	The solution should allow monitoring of Server Status and Availability, CPU Utilization, Memory Utilization, Process Monitoring, File System Monitoring, Disk Utilization of RHEL/Centos, SUSE, Ubuntu servers/Windows 2008, 2012,2016,2019,2022.	
36	The solution should support extensive monitoring capabilities from an OS (Linux, Windows)/ platform standpoint and should provide	

	capabilities for customer to develop, deploy customized monitoring requirements	
37	The solution should do performance monitoring of Redhat Open Shift VM/containers and VMware environments, including VMware ESX/ESXi, vSphere, vCenter Server.	
38	The solution should be able to monitor database from different aspects of the system including SQL Statements (memory, I/O , CPU intensive), wait types, server resources, storage I/O`s, virtualization layer, default users status , table spaces status and threshold utilization , raise warning or critical alerts where applicable.	
39	The solution should be able to report on hardware details (like CPU, memory, fan state, power etc.) of servers from multi vendors like IBM, HP, Cisco, Dell and also VMware Hosts.	
40	The solution should be able to gather capacity data from vCenter, HMC, Physical servers, etc. Generate report and provide recommendation.	
41	The solution should be able to monitor disk elements like RAID controllers, hard disks, RAIDs, failure prediction, availability of the volumes.	
42	The solution should be able to monitor environment metrics like temperature, internal voltages, power supplies, fans.	
43	The solution should be able to monitor critical hardware components like processors, memory modules, ECC errors, failure prediction.	
44	**Storage Monitoring**	
45	The solution should be able to monitor performance and capacity of physical and virtual storage infrastructure	
46	The solution should be able to provide real-time, in-depth performance statistics after discovery/configuration of devices, including but not limited to: - Array performance - Controller Performance - LUN performance - Disk performance	
47	The solution should provide hardware health information for the storage array.	
48	The solution should show statistics like Total IO/sec, service time, IO response time, queue length etc.	
49	The solution should show storage growth rates and project when the storage capacity will be reached	
50	The solution should be able to analyze the data coming from Dell EMC and Hitachi disk arrays, including: - Storage units, Extent pools, Ranks, Storage volume. - File Systems: Available and consumed capacity, list of CIFS shared, list of NFS exports, number of operations, data traffic, and so on. - Physical Disks: Disk time utilization, number of operations, presence, traffic, response time, status, and so on. - Storage Pools: Subscribed and consumed capacity, over subscription operation, number of operations, data traffic, and so on. - Storage Systems: Available and subscribed capacity, number of operations, number of ports, number of operations, data traffic, status, and so on.	

	- Volumes: Consumed capacity, disk time utilization, list of hosts, host visible capacity, number of operations, paths, number of operations, data traffic, response times, status, time since last activity, and so on. - Hardware components: fans, power supplies.	
51	The solution should automatically map VMs and logical connections to physical storage environment to enable root-cause analysis	
52	The solution should be able to monitor and manage multi-vendor storage systems with the same tool to detect performance issues and take proactive actions,	
53	**Logging/Reporting/Alert/threshold**	
54	The proposed solution should support to store all log of minimum 6 months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P.	
55	Ensure logs are retained for at least six months with options for longer retention	
56	The system should allow for customizable reports on performance, security events, and compliance.	
57	Capability to schedule automated report generation and distribution via email or other channels.	
58	Provide real-time analysis and reporting dashboards for immediate insights.	
59	Enable real-time alerts for critical events, with customizable thresholds and conditions.	
60	Support for alerts via email, SMS, or other communication channels.	
61	Include options for escalating alerts based on severity and response time.	
62	System should support global threshold and it should have option to define individual resource/interface statistics level threshold	
63	Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT Infrastructure	
64	Provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let user focus on the critical event that affects the business and business processes	
65	Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement	
66	System should support separate Rule Engine based alarms apart from the generic threshold. a. Should have capability to configure Device Group based, Node Based, Resources/Interface based, and Aggregation link based. b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms d. Rules should have option configure the breach based on min, max and average values.	

	e. Should have option to configure rules n repeat counters f. Should have options to select custom alarm and clear alarm messages for individual configured rules g. Should have option to send severity levels like error, warning and information h. Notifications support based on configured rules	
67	Provides alarm suppression with hold time and aid in prevention of flooding	
68	Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk	
69	**Other Features**	
70	Cover geographically distributed networks through multi-level scalable distributed deployment architecture.	
71	The tool should have option to be deployed in HA mode (High Availability) for redundancy purpose.	
72	Capacity Reservations: tool should allow management of resource allocations and reservations (for services, applications or other needs), identify resource shortages and provide information for further analysis or procurement	
73	Event Record & Classification: possible to generate event for all the monitoring devices, tool be used to define thresholds to generate events, collect from 3rd party using REST API , on regular interval Polling API and collect events from 3rd party system, classify them , assign different levels of severity to events	
74	Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event	
75	Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc. as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.	
76	System should have capability to configure business, non-business hours or custom time polling. This configuration should be available for every device as well as every component in the device.	
77	Provision to disable and enable the polling of specific type of devices	
78	System should have capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped.	
79	Provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions	

80	System should provide many different types of topology representation. To perform the following: 1. Display physical connections of the different devices being monitored in the system. 2. Display flat maps of the entire network or networks in a single view 3. Display customer maps based on user configurations 4. Display maps based on geo locations	
81	**Licensing**	
82	**Specify a base license for monitoring a minimum of 500 devices /application (Any kind of). Ensure the license is scalable up to 3,000 devices or applications without requiring a complete reinstallation or new licenses**	
83	**Define costs for incremental license additions (per 100 devices/application(any kind))**	
84	The bidder must provide all necessary hardware or compute resources required to manage and operate the monitoring system effectively, including servers, storage, and networking components, as per the specified scale of monitoring up to 3,000 devices or applications.	
85	Ensure the software includes a robust license management tool to track and manage licenses as the environment grows.	
86	Consider options for transferring licenses between devices or reallocating licenses as needs change.	
87	The bidder must provide all necessary hardware or compute resources required to manage and operate the proposed monitoring system effectively, including servers, storage, and networking components, as per the specified scale of monitoring up to 3,000 devices /application (any kind) with required warranty /support.	
88	**The licenses should be perpetual with 05 years support /updates /upgrade.**	

Note:-

1. The specifications mentioned in tender document are minimum and the vendor can quote higher specifications items.
2. All the network points' connectivity shall be provided by respective High Court / offices; however the vendor has to cooperate for completion of the said task / project.
3. All the pages of the bids and Annexure's are to be sealed and signed by the authorized officers of the company / vendor.
4. The bidder has to quote only 01 product of single make / brand at a time and not multiple brands for same item.
5. The Original equipment manufacturer may authorize more than one partner for participation in the bid.
6. **Back-to-Back support letter is to be submitted by OEM regarding support of the quoted products for the period of five years on their letter head duly sealed and signed by authorized representative**.

Section – VIII

Detail Break up of Cost*
Name of the Bidder:
Rate contract of Hardware items

S. No.	Item Description	Make and Model	Unit Price (Rs.)	GST Applicable (Rs.)	Sales / Service Tax (Rs.) as applicable any other duties / taxes	Total Unit Price (All inclusive) with 05 onsite warranty for items (Rs.)	Number of items	Total Cost (Rs.)
01	02	03	04	05	06	07	08	09 = 08x07
01	Firewall Technical Specifications **Specification – A**						02	
02	Web Application Firewall with Server Load Balancer **Specification – B**						02	
03	Network Monitoring System **Specification – C**						Lump sum	
	Total Rs. in Words _____							

Note:- The financial bids are to be submitted online and no hard sheet/ copy is to be submitted along with the bid. The items may be considered on line item basis.

Form: PQ-1

Techno-commercial Bid

S. No.	Description	Indicate also page number where clearly the document attached
1.	Name, address & telephone number of the agency/firm	
2.	Name, designation, address & telephone number of authorized person	
3.	Please specify as to whether Tenderer is sole Proprietor/Partnership Firm/Private or Limited Company.	
4.	Name, address & telephone number of Directors/Partners, Fax No., e-mail address.	
5.	Copy of PAN Card, Copy of previous 03 Financial Year's Income tax return **(ITR) Year 2021-2022, 2022-2023 & 2023-2024.**	
6.	Valid ISO 9001 Certificate of products (Please attach copy)	
7.	GST Registration No. (Please attach copy).	
8.	Latest GST Return (Please attach copy of latest month GST return certificate).	
9.	Experience Certificates / details of last 05 years in providing services / supply of firewall, WAF, NMS tool and similar IT equipments in Central Government/State Government /Public Sector Undertakings /Autonomous Bodies /Reputed Private organizations. (Please attach copy)	
10.	Online Bid Security/Earnest Money Deposit: a) Amount: Rs…… b) Reference No. : c) Date of issue:	
11.	Online Tender Fees details a) Amount: …… b) Reference No. : c) Date of issue:	

Form: PQ-2

BIDDER'S ANNUAL TURNOVER

_____ (Location)
_____ (Date)

From (Name & Address of the Auditor)
_____
_____
_____
_____

To
The Registrar General,
High Court of Madhya Pradesh,
Jabalpur

Ref.: _____

Dear Sir/Madam,

We hereby certify that the average annual turnover of M/s. _____ (name of the bidder) is not less than Rs. **05 Crore** during the last three financial years.

S. No.	Firm	Year 2021-2022	Year 2022-2023	Year 2023-2024
		Amount	Amount	Amount
1.				

Yours Sincerely,

(Signature of Authorized Auditor)
Name of the Authorized Auditor:
Seal:

Form: PQ-3
SIMILAR WORK EXPERIENCE

_____ (Location)
_____ (Date)

From (Name & Address of the Bidder)

_____

_____

_____

_____

To,

The Registrar General,

High Court of Madhya Pradesh,

Jabalpur.

Subject: Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh.

Ref.: _____

1. We hereby declare and confirm that we, _____ (Name of the Bidder), having registered office at _____ (address) have successfully executed following projects. We are providing the details below: (Note: add rows as required).

S. No.	Name of the client organization	Purchase Order (P.O) No. & Date of issue of P.O.	Project Value	Brief Scope of Work	Whether the copies of the purchase orders / contracts from the client as required, is attached?	
					Yes/No	Pg. No. on the Proposal

Yours Sincerely,

(Signature of Authorized Signatory)

Name and Designation of the Authorized Signatory:

Name and address of the Bidder Company:

Seal:

Note:-Please clearly indicate the page numbers with documents.

Annexure - 1

Clause by Clause compliance statement on the technical specification as prescribed in the section VII of this document.

Sl. No.	Clause no.	Complied / Not complied

Annexure - 2
DEVIATION STATEMENT FORMAT

The Bidder is required to provide the details of the deviations of the tender clauses **(in any section of the tender)** in the following format.

Sl. No.	Section No.	Clause No	Clause Description	Non Compliance/ Partial Compliance	Remarks

Annexure - 3

FORMAT FOR BIDDERS TO SUBMIT PRE-BID QUERY

The Bidder has to submit their queries **(in any section of the tender/ technical speculations)** in the following format only.

S. No.	Section No. / Clause No / Specification/ Page No.	Content of RFP Requiring Clarification	Query of the bidder / remarks of the bidder, if any
1.			
2.			
cont..			
n….			

Note: - Submit the pre-bid query as mentioned in the above format till 12.09.2024 through e-mail: regithcjbp@mp.gov.in. The pre-bid query received after dated 12.09.2024 may not be considered.

PART – I

BID FORM (1 sheet)

Tender No. : **Date:**

To,

The Registrar General
High Court of M.P.,
Jabalpur (M.P.)

Respected Sir,

1. Having examined the conditions of contract and specifications in the tender document and annexure, the receipt of which is hereby duly acknowledged, we, undersigned, offer to Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh for the sum shown in the schedule of prices attached herewith and made part of this Bid.
2. We undertake, if our Bid is accepted, to complete delivery of all the items specified in the contract within the delivery schedule specified in the tender.
3. If our Bid is accepted, we will obtain the unconditional performance guarantees of a Nationalized/Scheduled Bank for a sum 05% of the purchase / contract value.
4. We agree to abide by this Bid for a period of **180 days** from the date fixed for Bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.
5. Until a formal Purchase Order of Contract is prepared and a contract is executed accordingly, this Bid together with your written acceptance thereof in your notification of award shall constitute a

contract binding on us, subject to terms and conditions mentioned in the tender document.

6. Bid submitted by us is properly sealed and prepared so as to prevent any subsequent alteration and replacement.
7. We understand that you are not bound to accept the lowest or any bid, you may receive and you may reject any bid without assigning reason therefore and you may vary, amend or alter any terms and conditions of the Tender Document at the time of execution of the Contract.

Dated this ..... day of 2024

Name and Signature .....

In the capacity of .....

Duly authorized to sign the bid
for and on behalf of .....

Witness .....

Address ..... Signature

C E R T I F I C A T E S

WE CERTIFY THAT:-

1. We will not LEAK / DISCLOSE any information of High Court of Madhya Pradesh to any other institutions/organizations, bodies and also in the market on the rates less than the prices quoted by us to the High Court.

2. The rate of TAXES / DUTIES mentioned in the tender is in accordance with the provisions of the rules in all respects and the same is payable to the Authorities.

3. The material / items and software offered shall be of the best quality strictly in accordance with the specifications and particulars as detailed in the tender.

4. The information furnished by us in the tender are true and correct to the best of our knowledge and belief.

5. We have read and understood the rules, regulations, terms and conditions of tender as applicable from time to time and agree to abide by them.

6. We will meet 100% Confidentiality and Integrity of High Court Database and software.

Authorized Signatory

(Seal of the Company)