H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.
(A Unit of H.P. Government Undertaking)

# e-Tender

# for

# Rate Contract for Firewall

E-Tender No: HPSEDC/RC-FW/2K24-19128

H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.,
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.
Tel. Nos.: 0177-2623259, 2623043, 2623513 (Telefax): 0177-2626320.
Email: procurement@hpsedc.in

Website: www.hpsedc.in, tender document can also be downloaded from https://hptenders.gov.in

02-01-2024

INDEX

SECTION-l

INVITATION FOR E-BIDS

E-TENDER NO: HPSEDC/RC-FW/2K24-19128

**Note:** The Press e-Tender Notice published on 02/01/2024 in following daily Newspapers for inviting e-Tenders for Rate Contract for Firewall during warranty period and post warranty period. In case there is any decrease/ increase in prices, HPSEDC may asked the bidders to submit revised quotes in sealed envelopes. The rates finalised in this tender will also be considered for General Rate Contract for Firewall and will be valid for two years. The tender notice will be published in the following new papers.

1. Amar Ujala (Chandigarh/ Delhi Edition)
2. Indian Express (Chandigarh/ Delhi Edition)

The detailed e-Tender document contained in following sections has been prepared to elaborate all techno-commercial conditions of this tender. In case of any discrepancy between the Press Advertisement and detailed provisions of this Tender Document, the latter will prevail. For any further changes (if any, based on feedback/ queries from any quarter and pre-bid meeting) in this tender document, please see its updated version/corrigendum on www.hpsedc.in and https://hptenders.gov.in.

A) e-Tenders are invited by the undersigned from eligible bidders, i.e., Original Equipment Manufacturers (O.E.M.)/ Principal National Distributors/ Country Channel Partners in India (in case of imported equipment)/ Large Scale Systems Integrator duly authorised by the manufacturer for these Hardware Equipment as per technical specifications in Annexure-I and providing after sale support during warranty period.

GIST OF IMPORTANT GENERAL CONDITIONS

1) The tender has been floated for Rate Contract for Firewall as per specifications mentioned in Annexure- "I'. The rate will be finalised for all the components involved in the specified hardware, where the bidder has quoted lowest (L1) rate, for each individual item, L1 bidder shall be determined based on the lowest item wise amount. **Only L1 rates** will be conveyed and accordingly purchase orders would be placed for only L1 bidder's rates for each item. However, since the equipment is to be procured and supplied so reasonability of the rates would be ascertained by the tender committee w.r.t. other tenders/ rate contracts in the market. Bidders have to ensure that the **rates quoted for this tender/ rate contract are better** (or at least equal) than the rates in other rate contracts/ government supplies or open market anywhere else in the country.
2) The rates, as discovered through this RFP, shall also be considered for Rate Contract, valid for two years. The terms and conditions of the Rate Contract shall be same as per this tender document.
3) After finalizing the L1 rates, the work order will be placed to L1 bidder for the quantity mentioned in this RFP and only L2 bidder may be given opportunity to match the prices of L1 bidder if variation of rate will be 20% of L1 bidder, if tender committee deems fit to ensure healthy competition and timely supply of hardware. Therefore, bidders are advised to quote their best rates.
4) Unless otherwise specified for a part of the order, the supplies should be completed within **6-8 weeks** from the date of placing the supply order except for snowbound/ tribal areas, where delivery can be made within 8-10 weeks. Delivery is to be made FOR destination and Installation has to be completed within **1 week** after supply of material. In Remote and snowbound areas delivery may be done at nearest district head quarter, in case the area is cut-off for the time being. The Managing Director, HPSEDC reserves the right to extend the delivery period based on the request of the supplier, wherever required.
5) The committee reserves the right to negotiate the rates with L1 bidder to bring them to a reasonable level based on the best prices offered by other bidders and current market rates.
6) If the bidder quotes/ reduces, its price to render similar goods, works or services at a price lower than any tender/ rate contract price to anyone in the Country at any time during the currency of this tender, the price shall be automatically reduced with effect from the date of reducing or quoting lower price, for all delivery of the subject matter of procurement under this tender shall be amended, accordingly. The tender holder shall furnish the certificate to the HPSEDC that the provisions of this clause have been complied with in respect of

supplies made or billed for upto the date of this certificate. On the conclusion of the tender the successful bidder shall furnish a certificate that the provision of this clause has been complied with during the period of tender/ rate contract.

7) Any prospective bidder can procure the Tender Document from the "H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD., FIRST FLOOR, I.T. BHAWAN, MEHLI, SHIMLA-171013, (H.P)". Tender can also be downloaded from website http://www.hpsedc.in and https://hptender.gov.in.

The tender document will be available on all working days upto last date of bids submission on payment of Rs.5000/- (Rupees Five Thousand only) non-refundable, by demand draft/ RTGS in favour of "HP State Electronics Development Corporation Ltd., Shimla" payable at Shimla. If the tender document is downloaded from the website, the tender fee will have to be deposited along with the bid as a separate bank draft. E-tenders will be uploaded on HP Government e-Procurement portal https://hptenders.gov.in as well on HPSEDC website www.hpsedc.in. Interested bidder can participate by procuring tender.

3.) SCHEDULE OF THE TENDER PROCESS:

| S. No. | Information | Details |
|---|---|---|
| 1. | RFP No. and Date | No: HPSEDC/RC-FW/2K24-19128<br>Date: 02/01/2024 |
| 2. | Price of Tender Document | Rs 5000/- |
| 3. | Earnest Money Deposit | Rs 1,00,000/- |
| 4. | Bid validity period | 180 days from the last date (deadline) for submission of e-Tenders |
| 5. | Pre-Bid Meeting | Pre-Bid meeting will also be held on 10/01/2024 at 11:30AM through video conference.<br><br>Video Conferencing link is as under:<br>https://meet.google.com/zns-pxaw-rvs |
| 6. | Bid submission start date | 17/01/2024 (11:00 AM) |
| 7. | Bid submission End date | 30/01/2024 (02:30 PM) |
| 8. | Opening of e-Tenders Bids | 31/01/2024 (02:30 PM) |
| 9. | Tender Download Site | www.hpsedc.in & https://hptenders.gov.in |
| 10. | Venue | H.P. State Electronics Development Corporation Ltd., 1st Floor, I.T. Bhawan, Mehli, Shimla-171013, H.P. |

*(i)* Eligibility-cum-Technical Bids shall be opened initially, and eligibility documents will be evaluated.

*(ii)* Thereafter Technical Bids of Eligible Bidders shall be evaluated.

*(iii)* Commercial Bids of Eligible and Technically qualified bidders will be opened thereafter.

** *Any corrigendum, modifications, changes related to this tender before the day of bid submission shall be notified on website www.hpsedc.in or https://hptenders.gov.in only.*

**4)** Notwithstanding anything else contained to the contrary in this Tender Document, the Managing Director, H.P. State Electronics Development Corporation Ltd., Shimla reserves the right to cancel/withdraw/ modify fully or partially the "Invitation for Bids" or to reject one or more of the bids without assigning any reason and shall bear no liability whatsoever consequent upon such a decision.

## 5) INSTRUCTIONS TO BIDDERS FOR ELECTRONIC TENDERING SYSTEM

### 5.1 Registration of bidders on e-Procurement Portal: -

All the bidders intending to participate in the tender processed online are required to get registered on the centralized e - Procurement Portal i.e., https://www.hptenders.gov.in. Please visit this website for more details. In case of any problem in registration, please contact on toll free No. 1800-3070-2232

### 5.2 Obtaining a Digital Certificate:

5.2.1 The Bids submitted online should be encrypted and signed electronically with a Digital Certificate to establish the identity of the bidder bidding online. These Digital Certificates are issued by an Approved Certifying Authority, by the Controller of Certifying Authorities, Government of India.

5.2.2 The bidders may obtain Class-II or III digital signature certificate from any Certifying Authority or Sub-certifying Authority authorized by the Controller of Certifying Authorities or may obtain information and application format and documents required for the issue of digital certificate from:

5.2.3 Bid for a particular tender must be submitted online using the digital certificate (Encryption & Signing), which is used to encrypt and sign the data during of bid preparation stage. In case, during the process of a particular tender, the user loses his digital certificate (due to virus attack, hardware problem, operating system, or any other problem) he will not be able to submit the bid online. Hence, the users are advised to keep a backup of the certificate and keep the copies at safe place under proper security (for its use in case of emergencies).

5.2.4 In case of online tendering, if the digital certificate issued to the authorized user of a firm is used for signing and submitting a bid, it will be considered equivalent to a no objection certificate/power of attorney /lawful authorization to that User. The firm must authorize a specific individual through an authorization certificate signed by all partners to use the digital certificate as per Indian Information Technology Act 2000.

Unless the certificates are revoked, it will be assumed to represent adequate authority of the user to bid on behalf of the company/firm in the department tenders as per Information Technology Act 2000. The digital signature of this authorized user will be binding on the firm.

5.2.5 In case of any change in the authorization, it shall be the responsibility of management/ partners of the company/firm to inform the certifying authority about the change and to obtain the digital signatures of the new person / user on behalf of the firm / company. The procedure for application of a digital certificate however will remain the same for the new user.

5.2.6 The same procedure holds true for the authorized users in a private/public limited company. In this case, the authorization certificate will have to be signed by the directors of the company.

5.2.7 Pre-requisites for online bidding:

In order to bid online on the portal https://www.hptenders.gov.in, the user machine must be updated with the latest Java & DC setup. The link for downloading latest java applet & DC setup is available on the Home page of the e-tendering Portal.

### 5.3 Online Viewing of Detailed Notice Inviting Tenders (N.I.T.):

The bidders can view the detailed N.I.T and the time schedule (Key Dates) for all the tenders floated through the single portal e-Procurement system on the Home Page at https://www.hptenders.gov.in

### 5.4 Download of Tender Documents:

The tender documents can be downloaded free of cost from the e-Procurement portal https://www.hptenders.gov.in and www.hpsedc.gov.in.

### 5.5 Key Dates:

The bidders are strictly advised to follow dates and times as indicated in the online Notice Inviting Tenders. The date and time shall be binding on all bidders. All online activities are time tracked and the system enforces time locks that ensure that no activity or transaction can take place outside the start and end dates and the time of the stage as defined in the online Notice Inviting Tenders.

### 5.6 Bid Preparation (Qualification & Financial)

5.6.1 Payment of Tender Document Fee & EMD of online Bids: The payment for Tender document fee and EMD can be made as mentioned in Section 3, at Sr. No. 1 and 2 of the Table.

5.6.2 The bidders shall upload their eligibility and technical offer containing documents, qualifying criteria, technical specifications, schedule of deliveries, and all other terms and conditions except the rates (price bid).

5.6.3 The bidders shall quote the prices in price bid format only.

5.6.4 If bidder fails to complete the Online Bid Preparation at Submission stage on the stipulated date and time, his/hers bid will be considered as bid not submitted and hence not appear during tender opening stage.

5.6.5 Bidders participating in online tenders shall check the validity of his/her Digital Signature Certificate before participating in the online Tenders at the portal https://www.hptenders.gov.in.

5.6.6 For help manual please refer to the 'Home Page' of the e-Procurement website athttps://www.hptenders.gov.in., and click on the available link 'How to ...?' to download the file.

5.6.7 Post registration, bidder shall proceed for bidding by using both his digital certificates (one each for encryption and signing). Bidder shall proceed to select the tender he is interested in.

NB: Any changes/corrigendum/revised tender related to this Tender Document will be published on our website www.hpsedc.in and https://hptenders.gov.in. Therefore, prospective bidders are requested to see the updates on these websites regularly.

SECTION 2

INSTRUCTIONS TO BIDDERS

## A- INTRODUCTION

### 2.1. Eligible Bidders

| Sr. No. | Pre- Qualification Criteria | Required details to be accompanying the Bid document |
|---|---|---|
| 1. | The bidder should be registered under the Indian Companies Act, 1956/ 2013 or Proprietor's firm/ Partnership Firms (LLP) registered under LLP Act 2008 or subsequent amendments.<br>There to having valid Government licence and GSTN and PAN. | Memorandum of Association (MoA), Articles of Association (AoA) of bidder and detailed profile of the Company/ Firm/ Government License and COI, GSTN, PAN for proprietors/ bidder |
| 2. | (i) Tender Document Fee in favour of Managing Director, H.P. State Electronics Development Corporation, I.T. Bhawan, Mehli, Shimla-13.<br><br>(ii) Earnest Money Deposit (EMD) in the shape of Demand Draft/ RTGS valid for 180 days in favour of Managing Director, H.P. State Electronics Development Corporation, I.T. Bhawan, Mehli, Shimla-13. | (i) Demand Draft (DD) of Rs. 5,000/- (Rupees Five Thousand only)<br>(ii) Earnest Money (Rs. 1,00,000) Deposit (EMD)<br><br>DD / EMD may be submitted through RTGS in HPSEDC A/c: (State bank of India Khalini, Shimla-2 Account no. 55069383586 IFSC Code-SBIN 0051132)<br><br>Receipt/Copy of the demand draft/RTGS should be uploaded. |
| 3. | The Bidder should have a valid GST Number, PAN Number | Relevant Registration Certificates (copies to be enclosed) |
| 4. | A Bidder should be Original Equipment Manufacturer (OEM) or Authorised Principal National Distributor/ Regional Distributor/ Authorized Reseller/ Importer/ large Scale system integrator duly authorised by the OEM (Original Equipment Manufacturer) of the required Firewall respectively. It will, however be, preferred that the Original Equipment Manufacturers (O.E.M.) quotes directly. | Authorization letter from OEM in format given at Performa-A in case OEM not bidding directly. |
| 5. | The annual turnover (in terms of sales of hardware of similar nature as that of items listed in the RFP in India) of the OEM whose equipment are sought to be supplied, should be at least Rs. 200 Crores per annum for the last | Audited Balance sheets from company Statutory Auditor/ CA from OEM & financial data of the last three years |

| | | |
|---|---|---|
| | 3 years, i.e., for year 2020-21, 2021-22 and 2022-23. | |
| 6. | The Bidder should have an average annual turnover of at least Rs. 5 Crores during last three financial years from similar activities, i.e., should have supplied hardware equipment and related services, from India Operations i.e., for year 2020-21, 2021-22 and 2022-23. | Audited Balance sheets from company Statutory Auditor/ CA from Bidders & financial data of the last three years to be submitted. |
| 7. | The Bidder or its OEM {themselves or through re-seller(s)} should have at least 3 years of experience in supply and maintenance of such hardware in Government/Semi Govt./ PSUs/ Autonomous bodies of Central/ State Govt./Private Institution /Enterprises | Certificates from client regarding satisfactory supply and maintenance along with purchase orders. In case of non-disclosure agreement, confirmation regarding size and value of the project may be submitted from the client. |
| 8. | A Bidder quoting for these items, each item must have supplied /installed Minimum 200 Nos similar equipment by the OEM/ Bidder during the last three years in Government/Semi Govt. / PSUs/ Autonomous bodies of Central/ State Govt. /corporate sector. | Certificates from client regarding satisfactory supply and maintenance along with purchase orders. In case of non-disclosure agreement, confirmation regarding size and value of the project may be submitted from the client. |
| 9. | The bidder should either have positive Net worth in last three years or should be a profit-making Company/ firm in any two years during the immediately preceding last 3 financial years as per audited balance sheets. | Supporting financial documents/Balance sheet/ certificate from company's Statutory Auditor/ CA. |
| 10. | OEM should have presence in INDIA for more than 10 years | Supporting documents such as Company registration certificate etc. |
| 11. | OEM Toll Free Technical Assistance Centre should be available 24X7, without any holidays. The bidder and OEM should have its own website having product related information (for OEM) and support related information (for both bidder and OEM). | Contact information and availability hour's details. |
| 12. | The Bidder should not have been declared ineligible at the time of bid submission and at the time of placing of supply order due to corrupt and fraudulent practices with any of the departments of the Central, State Governments Deptt. and PSUs of Central/ State Govt. | Certificate from the authorized signatory prescribed in Form-E. |
| 13. | The bidder should have submitted the declaration of acceptance of terms and conditions of this RFP as per FORM B | Declaration from Authorized Signatory as per FORM B |
| 14. | The Bidder should already have reasonable support base in this region. The Purchaser's discretion regarding reasonableness of support base shall be final. It is | Supporting documents/ certificate from company's authorised signatory shall be |

| | | |
|---|---|---|
| | clarified that this clause pertains to only the existing level of support. The actual support required to implement this arrangement has been described in the relevant section. | submitted by the bidder. |

**Note: -**

Purchase Preference for Local Micro and Small-Scale units/ Startup Enterprises of the state: -

The following purchase preference ratio shall be applicable to the Local Micro and Small-Scale Units of State and Local Micro and Small-Scale categories under H.P. State Startup Scheme: -

1. Local Micro and Small-Scale Units of State of H.P. =15%
2. Local Micro and Small-Scale categories under H.P. State, Startup Scheme=15%

**Total Purchase Preference =30%)**

Provided that if Startup Enterprises will not be available, then 30% purchase preference shall automatically be given to Local Micro & Small-Scale Unit and vice versa as the case may be.

*Exemption, if any in evaluation criteria or any other terms & conditions of this document, will be as per Notification No. 4-Ind/SP/Misc/F/6-10/4/80-Vol-V dated 16.05.2020 issued by Controller of Stores Himachal Pradesh or any other orders issued by Govt. of Himachal Pradesh in case the committee deems it fit.*

It is reiterated that Purchaser's decision regarding Bidder's eligibility will be final and binding on all the Bidders.

The Bidder can choose to have a separate Authorised Service Provider (ASP). There is no turnover criterion for the ASP, but it should provide the first level of OEM's support which is fully backed up by the O.E.M. by means of a written understanding regarding maintenance. However, the Purchaser shall have the final discretion in this regard and can even ask for a trilateral agreement with the Bidder and the OEM in such cases to ensure timely delivery and maintenance.

If the bidder happens to be a System Integrator (SI), should have a National presence besides meeting the turnover criteria and having a sustained relationship with the O.E.M. in the past. The Bidder (or his OEM) must be able to establish his capability to execute the order(s) by showing satisfactory/ timely delivery, where similar numbers of equipment(s) and its allied accessories are involved.

## 2.2 Cost of Bidding:

2.2.1 The Bidder shall bear all costs associated with the preparation and submission of its bid and H.P. State Electronics Development Corporation Ltd., Shimla (hereinafter referred to as the 'Purchaser' or "HPSEDC" in short) will in no case be responsible or liable for these costs, whether or not the Bid is finally accepted.

## B- TENDER DOCUMENT

2.3 Contents of Tender Document:

2.3.1 This Tender Document comprises of the following Parts/ Sections.

Section-1: Invitation for e-Bids

Section-2: Instructions to Bidders

Section-3: General Conditions of the Tender & Contract

Section-4: Technical Specifications and Maintenance Conditions

Section-5: Technical Specifications & Annexures.

2.4 The Bidder is expected to examine the Tender Document carefully. Failure to furnish all information required as per the Tender Document may result in the rejection of the Bid.

2.5 Clarification regarding Tender Document:

2.5.1 The clarifications/ changes in tender document/ corrigendum can be uploaded upto 3 days before the bid-submission date.

2.6 Amendment of Bids:

2.6.1 Bids once submitted cannot be amended. However, in some circumstances (such as major anomaly in the technical specifications having a major impact on pricing), the Purchaser may decide to take fresh bids from all the Bidders before actually opening of the Commercial Bids.

2.6.2 In order to afford prospective Bidders reasonable time to make amendment in their bids, the Purchaser may, at his discretion, extend the deadline for the submission of bids. However, no such request in this regard shall be binding on the Purchaser.

## C - PREPARATION OF BIDS

2.7 Language of Bid & Correspondence:

2.7.1 The Bid will be prepared by the Bidder in English language only. All the documents relating to the Bid (including brochures) supplied by the Bidder should also be in English and the correspondence between the Bidder & Purchaser will be in English Language only. The correspondence by Fax / E-mail must be subsequently confirmed by a duly signed copy (unless already signed digitally).

2.8 Documents comprising of Bid:

The Bidder will prepare the bid in two parts.

## I. FEE-ELIGIBILITY CLAIM-CUM-TECHNICAL BID:

In support of his eligibility cum technical bid, a Bidder must submit/upload the relevant documents strictly in accordance with Proforma B marked with page numbers on e-portal https://hptenders.gov.in.

Packet-I (Fee/other Eligibility Documents/Technical) (to be uploaded in Packet-1 on e-procurement portal)

## II. COMMERCIAL BID:

Commercial Bids of only eligible and technically qualified bidders will be opened as per the date notified by the purchaser on its website (www.hpsedc.in and https://hptender.gov.in). Those technically qualified bidders which have also deposited the tender cost and Bid Security shall be termed as Substantially Responsive (i.e., eligible and technically qualified and have also deposited Bid Security & tender cost). The Tender Committee's determination of a Bid's responsiveness is to be based on the contents of the Bid itself and not on any extrinsic evidence. However, while determining the responsiveness of various Bidders, the Tender Committee may waive off any minor infirmity, which does not constitute a material deviation. The decision of the Tender Committee in this regard shall be final.

The bidder has to submit their Commercial Bids online as per BOQ in Packet-2 on the e-procurement portal.

*(i)* Sample BOQ / Price Bid will be as per Schedule I.

2.9 Bid Currencies:

2.9.1 Prices shall be quoted in Indian Rupees.

2.9.2 The contract price shall be paid in Indian Rupees.

2.10 Bid Security:

2.10.1 The Bidder shall furnish Bid security, as part of its bid as mentioned hereunder. Any bid submitted without bid security or with the lesser bid amount, as indicated below may be rejected being non-responsive.

| **Sr. No.** | **Description** | **Bid security amount in Rupees.** |
|---|---|---|
| 1. | Tender for Rate Contract for Firewall | Rs 1,00,000/- (Rupees one lakh only). |

2.10.2 The Bid Security is required to protect the Purchaser against the risk of Bidder's conduct which may require forfeiture of security pursuant to Para 2.10.8.

2.10.3. The Bid Security shall be in the shape of Demand Draft/ through RTGS in favour of "M.D., H.P State Electronics Development Corporation Ltd., Shimla" Payable at Shimla.

2.10.4 Any bid not secured in accordance with Para 2.10.1 and 2.10.3 will be rejected by the Purchaser.

2.10.5 Unsuccessful Bidders' Bid Security will be refunded as promptly as possible.

2.10.6 The successful Bidder's bid-security will be discharged upon the Bidders executing the contract and furnishing the performance security in accordance with Para 3.5.1.

2.10.7 No interest will be payable by the Purchaser on the above-mentioned Bid Security.

2.10.8 The Bid Security may be forfeited:

1. If a Bidder withdraws its bid during the period of bid validity specified by the bidder and required by the Purchaser.
2. During the tendering process, if a Bidder indulges in any such activity as would jeopardise or unnecessarily delay the tender process. The decision of the Purchaser regarding forfeiture of the Bid Security/EMD shall be final & shall not be called upon question under any circumstances.
3. In the case of a successful Bidder, if the Bidder fails,

(i) to sign the contract by raising issues contrary to the provisions of the RFP or the Bid or undertakings given during evaluation of bids, or

(ii) to furnish Performance Security, or

(iii) Violates any of such important conditions of this tender document or indulges in any such activity as would jeopardise the interest of the Purchaser. The decision of the Purchaser regarding forfeiture of the Bid Security shall be final & shall not be called upon question under any circumstances.

2.11 Period of validity of Bids:

2.11.1 For the purpose of placing the order, the Bids shall remain valid for at least 180 days after the date of bid opening. A bid valid for a shorter period may be rejected by the Purchaser as being non-responsive. During the period of validity of Bids, the rates quoted shall not change. However, in case of general fall in prices of a product in the IT/ Electronics Industry before despatch of goods, such a reduction shall be passed on to the Purchaser after mutual negotiations.

2.11.2 In exceptional circumstances, the Purchaser may ask for extension of the period of validity and such a request shall be binding on the Bidder. The Purchaser's request and the response to such a request by various Bidders shall be in writing. A Bidder agreeing to such an extension will not be permitted to increase its rates.

## D-SUBMISSION OF BIDS

2.12 Submission of Bids:

2.12.1 Bidder(s) shall submit their bids only on online e-procurement portal www.hptenders.gov.in. All the instructions regarding e-bids submission are also available on www.hptenders.gov.in.

2.12.2 The original DD or RTGS documents related to tender cost and bid security should be deposited in HPSEDC on or before the last date and time for bids opening.

2.12.3 Every envelop and forwarding letter of various parts of the Bid shall be addressed as follows:

The Managing Director,
H.P. State Electronics Development Corporation Ltd., First Floor,
IT Bhawan, Mehli, Shimla-171013.

2.13 Deadline for Submission of Bids:

2.13.1 Bids will be online submitted/uploaded on e-procurement portal https://hptenders.gov.in on or before the deadline mentioned on the e-portal.

2.13.2 The Purchaser may, at its discretion, extend this deadline as per Para 2.6.2. The Purchaser may also extend this deadline for any other administrative reason.

2.14. Bids not submitted online:

2.14.1 Any bid not submitted/uploaded through e-portal will not be received by the Purchaser after the deadline for submission of bids prescribed by the Purchaser, as per clause 2.13.1 or 2.13.2, will be rejected.

2.15 Modification and withdrawal of Bids:

2.15.1 E-bids can be modified upto last date & time has not been closed by e-procurement system.

2.15.2 E-Bids cannot be withdrawn in the interval after its submission of bids and before the expiry of Bid's validity specified by the Purchaser. Withdrawal of Bid during this interval may result in the forfeiture of Bidder's Bid security pursuant to clause 2.10.8.

## E-BID OPENING AND EVALUATION

### 2.16. Opening of bids by Purchaser:

2.16.1 The e-Bids shall be opened on the date and time already described in the tender/e-portal or on any other later day and time fixed as per Para 2.6.2 or other enabling provisions in this behalf, in H.P State Electronics Development Corporation Ltd, First Floor, IT Bhawan, Mehli, Shimla-13 (H.P.) in the presence of representatives of the Bidders who may choose to attend the proceedings. The representatives of Bidders will sign a register in evidence of their presence.

2.16.2 In order to assist in the examination, evaluation and comparison of Bids, the Purchaser may at its discretion ask the Bidder for a clarification regarding its Bid. The clarification shall be given in writing, but no change in the price or substance of the Bid shall be sought, offered or permitted.

2.16.3 In the first instance, Eligibility bid documents uploaded on the e-portal will be opened and evaluated for eligibility of each Bidder will be ascertained. Technical Bids of only those Bidders shall be evaluated who are found to be eligible as per the criteria laid down in para 2.2.1/ 2.8 (I) and submitted bid security and tender cost as per Para 2.10. In doubtful cases (where further documents or clarification are required to establish eligibility), the Purchaser in its discretion, may decide to open/evaluate Technical Bid. However, such Bids can be rejected subsequently, if it is found that the bidder has claimed eligibility on false grounds.

2.16.4 The Technical e-Bids of only the Eligible Bidders will be opened and the contents (particularly Compliance Sheets) will be announced/ displayed in the presence of all Bidders or their representatives.

2.16.5. **Scrutiny of Technical Bid:**

The product proposed in the bid document of only eligible bidders will be evaluated as per the requirements specified in the RFP/ Tender Document. The "Compliance Sheets" submitted by the Bidders shall be compared against the Product Catalogue and authenticated circulars regarding latest changes in the specifications. It will thus be ascertained whether the product offered by the Bidder matches with the minimum requirement of the Purchaser as given in the Technical Specifications in this Tender Document. In case of a doubt the Purchaser may require the bidder to produce the quoted equipment for physical

inspection and demonstration, so that components could be seen to ascertain the veracity of the Bidder's claim about specifications.

The Tender Committee may undertake oral and or written clarifications with the bidders. The primary function of clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the bid documents. The financial bids of only eligible and technically qualified bidders will be opened for further processing. It is, however, clarified that subject to other provisions of this document, every bidder will have to fulfil the minimum technical specifications laid down in this document for being qualified technically. In order to assist in the examination, evaluation and comparison of Bids, the Tender Committee may at its discretion ask the Bidder for a clarification regarding its Bid. The clarification shall be given in writing immediately, but no change in the price shall be sought, offered or permitted. The Technical e-Bids of only the Eligible Bidders will be opened and the contents (particularly Compliance Sheets) will be announced in the presence of all Bidders or their representatives. An open discussion regarding technical parameters quoted by various Bidders may also take place, if required. The Compliance/ Deviation statement submitted by the Bidders shall be compared against the Product Catalogues and authenticated circulars regarding latest changes in the specifications. It will thus be ascertained whether the product offered by the Bidder matches with the minimum requirement as given in the Technical Specifications in this Tender Document. The Financial Bids of only those eligible and technically qualified bidders will be opened who also fulfil minimum technical requirements mentioned in this document. However, the Tender Committee reserves the right of giving minor relaxation, if a particular Bidder is not able to exactly match the specifications given in the Tender Document, provided that such a minor deficiency does not substantially reduce the performance level and is suitably compensated by some extra feature in the product. Therefore, all Bidders must indicate in the Compliance/Deviation, if any, in Schedule III, extra features offered by them. Similarly, the Tender Committee can give any other such minor relaxation, which does not change substance of the bid or does not prejudice the bid process from the point of view of equity and fair play. The decision of the Tender Committee about

giving minor relaxation shall be final and shall not be called upon question under any circumstances.

*The commercial Bids of only those bidders will be opened who fulfils the minimum technical requirements of the purchaser and are found substantially responsive as per Para* 2.8 *(II) read in conjunction with other relevant clauses/Forms.* However, the Purchaser reserves the right of giving minor relaxation, if a particular Bidder is not able to exactly match the specifications given in the document, provided that such a minor deficiency does not substantially reduce the performance level and is suitably compensated by some extra feature in the product. Therefore, all Bidders must indicate in the Compliance Sheets, deviations, if any, extra features offered by them. The decision of the Purchaser about giving minor relaxation shall be final and shall not be called upon question under any circumstances. The evaluation committee, if so, desire may ask for the demonstration of the quoted solution/products, for which sufficient time will be given for arranging demonstration.

2.16.6. Opening of Bid Security:

The document containing bid security will be opened and checked at the time of determining eligibility of the bidders at the time of eligibility bid opening.

2.16.7. Opening of Commercial Bids of substantially Responsive Bidders:

The Commercial Bids of only those Bidders will be opened who are found substantially responsive. A Substantially Responsive Bidder is one which conforms to all the stipulations of para 2.8 (II and III) read with para 2.16.6 above. The Purchaser's determination of a Bid's responsiveness is to be based on the contents of the Bid itself and not on any extrinsic evidence. However, while determining the responsiveness of various Bidders the Purchaser may waive off any minor infirmity, which does not constitute a material deviation. The decision of the Purchaser in this regard shall be final.

2.16.8 A Bid determined as not substantially responsive will be rejected by the Purchaser. Such a Bid will not be normally allowed to be made responsive subsequently by way of correction/ modification.

2.17. Evaluation and Comparison of Commercial Bids:

2.17.1 The comparison of Commercial Bids shall be done as follows:

2.17.2 Bid Comparison:

The Bidders are required to complete their Commercial Bid/ BOQ in Schedule - I. Initial evaluation/ comparison of items within a Category given in the Tender Document will be done as per clause 2.17.3.

2.17.3. Item Rate:

Item Rate for each item for all will be calculated as under.
Item Rate = FOR Destination Unit Price of the Item under a category including installation charges (if any) with three years warranty inclusive GST of the Item in a Category.

***Note 1:***

*The Bidder shall not quote prices subject to certain conditions. Bids containing any conditional prices may be rejected or the Purchaser may take a final decision in its discretion about such conditionality.*

2.17.4 In the procurements of goods, the following procedure shall be followed:

(i) Among all qualified bids, the lowest bid will be termed as L1. If L-1 is from a local supplier, the contract for full quantity will be awarded to L1.

(ii) If L-1 bid is not from a local supplier, 50% of the order quantity shall be awarded to L-1.

2.17.5 Thereafter, the lowest bidder among the local suppliers, will be invited to match the L-1 price for the remaining 50% quantity subject to the local supplier's quoted price falling within the margin of @5% and contract for that quantity shall be awarded to such local supplier subject to matching the L-1 price. In case such lowest eligible local supplier fails to match the L-1 price or accepts less than the offered quantity, the next higher local supplier within the be invited to match the L-1 price for remaining quantity and so on, and contract shall be awarded accordingly.

2.17.6 In case some quantity is still left uncovered on local suppliers, then such balance quantity may also be ordered on the L1 bidder.

2.18. RANKING OF BIDDERS:

2.18.1. Bidders will be ranked in the inverse order of Item Rate. The criterion for selection of lowest Bidder (L1) for individual item.

2.18.2 Reduction in Statutory Duties and Levies:

If any reduction in taxes takes place after opening the commercial bids, but before despatch of goods; the Successful Bidder shall pass on the proportional benefit to the Purchaser. However, if any such reduction takes place after the opening of bids but before the finalisation of tender, revised sealed commercial bids shall be taken.

2.19. NEGOTIATIONS:

2.19.1 The Purchaser may finalise the Tender & award the Contract without any negotiations if it is satisfied with reasonableness & workability of the lowest offers. Therefore, the bidders are advised to quote lowest possible rates in the first instance only.

2.19.2 During the negotiations a revised offer will be taken from the representative of the Bidder by way of sealed bids. This revised offer will replace/supersede the earlier Technical & Commercial Bid, provided that the original offer (i.e., Technical/ Commercial) will not be allowed to be changed to the detriment of the Purchaser, as far as rates of every individual item & terms/ conditions are concerned. Therefore, Bidders are advised to send sufficiently senior representatives (who can take spot decisions) for negotiations.

2.19.4 During the negotiations on prices & other related terms/conditions, prevalent worldwide street-prices of such product, prices finalised in bids of similar size on GEM portal/Other State Government tender/rate contract etc. will be kept in mind. The scope of negotiations may also include precise *modus-operandi* of after-sales service, mode of delivery, system integration and price of add-ons & consumables etc.

2.19.5 During the negotiations, the Purchaser may even go in for marginally higher or lower configurations as per its absolute discretion.

2.19.6 After this final ranking is done based on negotiated prices, award of tender/rate contract will be made to the lowest Bidder, subject to post qualification in Para 2.20 below.

## F - AWARD OF CONTRACT

2.20 Post Qualification:

2.20.1 HPSEDC will devise a performance criterion in consultation with successful bidders which will include online after sales feedback from the Government departments. The lowest Bidder can be denied the right of continuing with the contract, if the equipment being supplied by him, fails the standard performance criteria. In such an event, the next lowest bidder (L-2) shall be considered.

2.21 Purchaser's right to vary Quantities:

2.21.1 The Purchaser reserves the right to place the supply received from various Government departments/ Govt. Institutions/ Autonomous bodies on the approved vendors during the currency of the tender/rate contract.

2.22 Purchaser's Right to accept any Bid and to reject any or all Bids:

2.22.1 Notwithstanding anything else contained to contrary in this Tender Document, The Purchaser reserves the right to accept or reject any Bid or to annul the bidding process fully or partially or modifying the same and to reject all Bids at any time prior to the award of Contract, without incurring any liabilities in this regard.

2.23 Notification of Award:

2.23.1 Prior to the expiry of the period of Bid validity, the Purchaser will notify the successful Bidder in writing by speed post or Fax or email that his Bid has been accepted.

2.23.2 The liability of the supplier(s) to deliver the Goods and perform the services will commence from the "date of Notification of Award". The Delivery Period shall be counted from the date of 'Placing the Supply Order'. The "date of delivery" shall be the date on which the equipment / material is received at the destinations.

2.23.3 Upon the successful Bidders' furnishing of performance security, the purchaser will promptly notify each unsuccessful Bidder and will refund his Bid Security.

**2.24** Signing of Contract:

2.24.1 After the Purchaser notifies the successful Bidder(s) that his 'Bid' has been accepted, the Purchaser will sign an agreement (described as Contract herein after) within 10 days with the successful Bidder on mutually agreed terms for efficacious implementation of the order.

2.24.2 The Purchaser's liability of taking the goods from the selected supplier(s) shall commence only from date of signing the date of the Contract.

## SECTION-3

## GENERAL CONDITIONS OF THE TENDER &CONTRACT

### 3.1 Definitions:

3.1.1 In this part, the following interpretation of terms shall be taken:

(a) "The Contract" means an agreement regarding supply of the goods & provision of services entered into between the HPSEDC and the Supplier, as recorded in the Contract Form signed by the parties, including all appendices thereto and all documents incorporated by reference therein.

(b) "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.

c) "The Goods" means all the equipment and/or other material, which the Supplier is required to supply to the Purchaser under the Contract.

d) "Services" mean services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, training, maintenance and other such obligations of the Supplier covered under the Contract.

e) "The Purchaser" means the H.P. State Electronics Dev. Corporation Ltd" or "HPSEDC" in short.

f) "The Supplier", means short listed Bidder supplying the goods and services under this Contract.

g) "End User" means various Government Departments, Boards, and Corporation etc. in the State of Himachal Pradesh.

*Note: The aforesaid definitions will be valid with respect to one or more Suppliers short-listed to execute the Project. Services to be executed by each Supplier have been explained in detail in this Tender Document.*

3.2. Application:

3.2.1 These General Conditions shall apply to the extent that these are not superseded specific by provisions in other parts of this tender document. A detailed Contract agreement shall be signed after the order is placed. Detailed provisions of such a contract-agreement shall have an over-riding effect vis-a-vis this Tender Document.

3.3 Standards:

3.3.1 The goods supplied under this Contract shall conform to the standards mentioned in the Technical Specifications and the latest improvements incorporated after the finalisation of contract, but before the dispatch.

3.4 Patent Rights of the Goods:

3.4.1 The Supplier shall indemnify the Purchaser against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the goods or any part thereof in India.

3.5 Performance Security:

3.5.1 Performance Security for delivery/ installation and maintenance during warranty period.

3.5.2 Within 10 days of 'Notification of Award', the successful bidder/ Supplier shall initially furnish a 3% Performance Bank Guarantee of total order value valid for 39 months to safeguard the purchaser against timely delivery/installation and maintenance of ordered Firewall during the currency of the contract.

(1) In case supply orders increases the above-mentioned quantity then 3% amount of each supply order will be deducted as PBG from due payment from bidder & same will be released after expiry of the warranty period or bidder has an option to submit additional PBG against the supply order.

(3) EMD of successful bidder(s) will only be released after signing of agreement and submission of PBG.

3.5.3 The proceeds of the Performance Bank Guarantee/ additional Performance Bank Guarantee shall be payable to the Purchaser as compensation for any loss resulting from the Supplier's failure to complete his obligations under the Contract. The Purchaser may claim such compensation in addition to initiating any other legal proceedings.

3.5.4 The Performance Bank Guarantee shall be given in one of the following forms:

An irrevocable and unconditional Bank Guarantee in favour of the Purchaser issued by a Nationalised/schedule bank in a format given by the Purchaser. This Bank Guarantee should be of a sufficient duration to cover the risk of the Purchaser.

3.5.5 The Performance Bank Guarantee, regarding delivery & installation will be discharged by the Purchaser and returned to the Supplier not later than 30 days following the date of completion of the Supplier's performance related obligations, under the Contract (excluding after sales maintenance for which separate performance guarantee has been taken).

3.6 Inspections and Tests:

3.6.1 The Purchaser or its representative shall have the right (if so desire) to test the goods to ascertain their conformity to the specifications. The Purchaser shall notify to the Supplier in writing of the identity of the representative deputed for this purpose & nature of tests that may be conducted (if found necessary) for benchmarking.

3.6.2 The inspections and tests may be conducted in the factory premises of the Supplier. All reasonable facilities and assistance including access to drawings and production data shall be furnished to the inspecting officers at no charge to the Purchaser. The Contractor shall inform the Purchaser in advance the time of starting of manufacture and the progress of manufacture of the Firewall offered by him so that arrangements can be made for inspection at the premises, if so desired by the purchaser.

3.6.3 Should any inspected or tested Goods fail to conform to the Specifications, the Purchaser may reject them, and the Supplier shall either replace the rejected goods or make all alterations necessary to meet specification requirements to the Purchaser.

3.6.4 If the Purchaser decides to conduct the inspection at supplier's premises as per clause 3.6.1 to 3.6.3, no material being furnished against this specification shall be dispatched until inspected and approved by the Purchaser/ or his representative. Such inspection and approval will not relieve the Contractor of full responsibility for furnishing equipment conforming to the specifications nor will it prejudice any claim, right or privilege which the Purchaser may have on account of any loss sustained by it due to defective or unsatisfactory equipment supplied by the contractor. Should the inspection be waived off by the Purchaser, such waiver shall not relieve the contractor in any way from his contractual obligations.

3.6.5 The sample of the proposed Equipment, if desired by the purchaser, to be supplied for approval/testing.

3.6.6 Bidder has to provide the required drivers etc. if essentially required for the quoted

equipment/peripherals being supplied.

3.6.8 Bidder has to provide necessary support by providing required drivers for connecting the hardware devices being used at the user site. All these drivers should be freely available on the OEM website for which necessary links may be provided.

3.6.9 Bidder has to install the patches/upgrades during warranty period at no extra cost.

3.6.10 GUI tools for configuring devices with Multilingual support for Hindi.

3.6.12 Bidder should provide service maintenance of System Software / driver software up-gradations, installing patches etc., at no extra cost during the warranty period.

3.6.13 All drivers' patches required at site are to be arranged by the supplier and should be available on the website of the respective OEM.

3.16.14 The Supplier of items shall depute its technical person if end user is facing problem in installation/working of software. On-line support will be made available without any charges to end user.

3.7 Packing Delivery & Documentation:

3.7.1 The supplier shall provide such packing as is required to prevent damage or deterioration of the goods during transit to their final destination as indicated in the Contract. The packing shall be sufficient to withstand, without limitations, rough handling during transit and exposure to extreme temperatures and precipitation during transit and open storage. The Supplier shall be responsible for any defect in packing.

3.7.2 The packing, marking and documentation within and outside the packages shall comply strictly with such special requirements as will be specifically provided for in the contract.

3.7.3 Delivery of the goods and associated documentation will be done in such manner as may be prescribed by the Purchaser in the Contract.

3.8 Insurance:

3.8.1 The Goods supplied under the Contract shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery.

3.8.2 The supplier will indemnify the Purchaser from all responsibility of compensation etc. caused by third party injury including death while he is discharging his duties

under the contract.

3.9 Transportation:

3.9.1 The entire cost of carriage/transportation from the port of discharge to the destination shall be borne by the Supplier.

3.9.2 Where the Supplier is required to affect delivery to some other address within Himachal Pradesh, the supplier shall be required to meet all transport and storage expenses until delivery is completed.

3.10 Literature and Instruction:

3.10.1 Each supplied Firewall packing box must contain copy of illustrated literature and instruction books regarding the installation, handling, maintenance and use of the Goods at each station shall be supplied by the supplier as part of the Contract price before dispatch of the first assignment.

3.11 Payment:

3.11.1 **First Instalment:** First Instalment shall be paid after delivery of the Goods at the prescribed destinations. Amount of 1st instalment shall be regulated in such a manner that the total payment after delivery is 85% of the order value. A claim for first instalment shall be staked by the Supplier, when he has supplied adequate number of machines. The first installment of 85% will be paid only after receipt of duly acknowledged delivery challans & invoice, as required by the Purchaser.

3.11.2 **Second Instalment:** Remaining amount of 15% of the order value shall be paid after satisfactory installation of Firewall and execution of Performance Guarantee for proper maintenance during warranty period as mentioned at Clause 3.5. If the installation is delayed beyond 45 days on account of site not being ready (or any other reasons entirely attributable to the Purchaser) or any other reason attributable to the Purchaser, $^{2}/_{3}$ of the second instalment (i.e., 10% of the order value) shall be released to the Supplier subject to submission of site not ready (SNR) report from concerned department. In such an unlikely event of the site not being ready, the remaining amount $^{1}/_{3}$ of the second instalment (i.e., 5% of order value) will be released after submission of successful installation reports of the ordered equipment(s) duly singed by the competent authority of the department(s).

**Note:** *First & second instalments shall be released only on production of bill supported by delivery challan and installation report by the Supplier. Any bill supported by requisite documents will be processed within* 15 *days and objections, if any, will be conveyed in*

*one go within this period. If the claim is found in order, the payment will be made within 2 weeks from the date of submission of such bills.*

3.12 Prices:

3.12.1 Subject to the provision to Rule 2.11.1, the prices charged by the Supplier for Goods delivered and services performed under the Contract shall not vary from the prices quoted by the Supplier in his Bid. But in case of global or national fall in prices of a product in IT/ Electronics industry due to a change in Government Policy or otherwise, such a reduction shall be passed on to the Purchaser after mutual negotiations.

3.12.2 There shall be no effect of the exchange rate variation etc., on the rates to be quoted by the Vendor during one-year period. However, if rates will increase/ decrease, HPSEDC will call techno-commercial bids from the empanelled bidders on requests received from them.

3.13 Modification in the Order:

3.13.1 The Purchaser may at any time, by written order given to the Supplier make changes within the general scope of the Contract in anyone or more of the following:

(a) The specifications of the Goods

(b) The method of shipment or packing

(c) The service to be provided by the Supplier

(d) Quantity of goods

(e) Any other change that the purchaser may deem fit

3.13.2 If any such change causes an increase or decrease in the cost of, or the time required for the Supplier's performance of any part of the work under the Contract, an equitable adjustment shall be made in the Contract price or delivery Schedule, or both, and the Contract shall accordingly be amended. Any claims by the Supplier for adjustment under this clause must be put forth within 30 days from the date of the Supplier's receipt of the Purchaser's change order.

3.14 Subcontract:

3.14.1 The Supplier shall not assign in whole or in part, its obligations to perform under the Contract, except with the Purchaser's prior written consent.

3.14.2 The Supplier shall notify the Purchaser, in advance in writing, of all sub-Contracts awarded under the Contract if not already specified in his bid. Such notification, in his original bid of later (even if with prior approval of Purchaser) shall not relieve the Supplier of any liability or obligations under the Contract.

3.14.3 Subcontracts must comply with the provisions of the clause 2.3.

3.15 Delays in the Supplier's Performance:

3.15.1 Delivery of the goods and the performance of services shall be made by the Supplier in accordance with the time schedule specified by the Purchaser in the Contract.

3.15.2 Any unjustifiable delay by the Supplier in the performance of his delivery obligation may render the Supplier liable to any or all the following:

(i) Forfeiture of its performance security,

(ii) Imposition of liquidated damages @Rs 50/- per day per Firewall of the unfulfilled order. The maximum penalty will not exceed 10% of the order value.

(iii) Termination of the contract and risk purchase at Supplier's risk

(iv) Initiation of any other legal proceedings.

3.15.3 The Supplier will strictly adhere to the time-schedule for the performance of Contract. However, the Purchaser can relax this time limit in force majeure conditions.

3.16 Termination for Default:

3.16.1 The Purchaser may without prejudice to any other remedy for breach of contract, (including forfeiture of Performance Security) by written notice of default sent to the supplier, terminate the Contract in whole or in part after sending a notice to the Supplier in this regard.

**(a)** if the Supplier fails to deliver any or all of the goods within the time period(s) specified in the Contract, or any extension thereof granted by the Purchaser pursuant to clause 2.11.2, or

**(b)** If the Supplier fails to perform any other obligation under the Contract.

3.16.2 In the event the Purchaser terminates the Contract in whole or in part, he may procure, upon such terms in such manner, as it deems appropriate, goods similar to those undelivered, and the Supplier shall be liable to pay excess cost of such similar goods to the Purchaser. This liability will be in addition to forfeiture of

performance guarantee and any other legal proceedings, which the Purchaser may initiate as per Para 3.15.2.

3.17 Force Majeure:

3.17.1 Notwithstanding the provisions of the clauses 3.15 and 3.16, the Supplier shall not be liable for forfeiture of its performance security or termination for default, or payment of any damages, if and to the extent that his delay in performance under the Contract is the result of an event of Force Majeure.

3.17.2 For purpose of this clause, Force Majeure means an event beyond the control of the Supplier and not involving the Supplier's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Purchaser either in its sovereign or contractual capacity, war, revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

3.17.3 If a Force Majeure situation arises, the Supplier shall promptly notify the Purchaser in writing or such conditions and the cause thereof. Unless otherwise directed by the Purchaser in writing, the Supplier shall continue to perform its obligations under the Contract, as far as reasonably practical, and shall seek all reasonable alternative means for performance, not prevented by the *Force Majeure* event.

3.18 Taxes and Duties:

3.18.1 Supplier shall be entirely responsible for payment of all taxes, duties and levies, imposed up to/until the delivery point specified in the Contract. If there is a reduction in any of the statutory duties and levies before the despatch of goods, the benefit of the same will be passed on to the Purchaser.

3.19 Limitation of Liablitiy:

The liability of the supplier in respect of all claims under this tender including penality for delay in delivery, services, liquidity damages etc. shall not exceed the aggregate value of the goods and services supplied under this tender. Either party shall not be liable for any claim made for any indirect, consequential or incidental losses and indirect damages, costs or other expenses related thereto.

3.20 Arbitration:

All disputes, differences, claims and demands arising under this tender shall be refered to arbitration of a sole arbitrator to be appointed with mutual consent of both the parties. All arbitration will be held in Shimla. If the parties cannot agree on the appointment of the Arbitrator within a period of one month from the

notification by one party to the other of existence of any dispute and need for appointment of an arbitrator. Further action will be taken in accordance with the provisions of the Arbitration and Conciliation Act, 1996 and the award made under this tender shall be final and binding upon the parties hereto, subject to legal remedies available under the law.

SECTION-4

TECHNICAL SPECIFICATIONS AND MAINTENANCE CONDITIONS

4.1. SCOPE OF THE TENDER:

The successful Bidder(s) will provide the following services:

(i) Manufacture /Import (ii) Testing (iii) Supply (iv) Installation (v) After Sales Service during warranty and Annual Maintenance period.

(i) Manufacture/Import

The OEM/ Bidder can manufacture the Goods in India or import the same (in full or in parts) from any part of the world.

(ii) Testing

Testing/ Benchmarking as per requirement of the Purchaser and in such manner and for such size of sample as may be prescribed subsequently may be got done as a part of the Contract.

(iii) Supply

The Goods need to be supplied F.O.R. as per the list of destinations to be supplied at the time of signing the Contract.

(iv) Installation and Commissioning of networking/ cabling Firewall: The successful bidder of respective Firewall will do installation and ensure that the equipment supplied works/run properly.

4.2 AFTER SALES SERVICES:

4.2.1 Comprehensive Warranty:

The Supplier shall provide Comprehensive OEM warranty (including labour and spares) for 36 calendar months. An undertaking to this effect shall be given by the Bidder in the Compliance Sheets.

4.2.2 Service Centre:

The successful bidder should have a dedicated service centre in the state. The Service Centres in the State shall be manned by qualified Engineers as per Clause 4.1(v) above and one call coordinator. It will be equipped, with sufficient inventory of spares as per ABC Analysis. The supplier will provide prompt after

sales support and shall attend any complaint not later than 24 hours. The minor and major defects shall be rectified not later than 36 hours and 60 hours respectively. If defect is not rectified within the time stipulated as above penalty as prescribed by the Purchaser will be imposed. However, the penalty in such instances shall not exceed 10% of the equipments cost against a non-attendance/ non rectification of defects against a service call. The exact quantum of penalty per day/ week shall be decided at the time of signing the contract. During the warranty period, this penal clause will be enforced by ensuring that the supplier gives a Performance Security by way of Bank Guarantee to the Purchaser.

4.2.3 The amount of non-delivery of products as mentioned in Clause No. 3.15: **Delays in the Supplier's Performance** and Clause No. **4.2: After Sale Services** or any other recoverable amount from bidder(s) may be adjusted/ recovered or set-off against any sum payable to the bidder against any other contract with HPSEDC or with State Government. The amount shown against that shall be withheld to be adjusted against the compensation levied as mentioned above. Recovering or deducting of this amount on failure of delivery/ delay in delivery or not providing services in time bound manner, shall be automatic deducted without any notice to the concerned bidder.

The Managing Director, HPSEDC, will reserve the right to relax/ decrease the penalties or release recovered amount without giving any interest to the bidder(s), after receiving justified/ reasonable reasons from the bidder(s).

4.3 TECHNICAL SPECIFICATIONS & QUANTITIES:

4.3.1 The Technical Specifications have been given in Annexure-I in Section-5. These specifications should be carefully studied by the Bidder, so that the product could be technically evaluated as per the Purchaser's requirement.

4.4. Compliance sheets:

(i) Compliance Sheets as per Annexure-I in Section-5 are to be filled in by the bidders as part of the Bid. These Compliance Sheets should be complete in all respects and should be free from errors and omissions. All required parameters must be replied to in affirmative/ negative.

(ii) The Bidder shall also supply along with the Bid all brochures and authenticated

bulletins carrying latest changes covering the technical aspects of each item appearing in schedule of requirement intended to be supplied by the Bidder. For the purpose of establishing latest changes, printouts downloaded from INTERNET (& duly authenticated) may be acceptable.

5. Acceptance Testing After Notification of Award:

i. The Purchaser may conduct benchmarking & acceptance test, which could involve operation of complete system for at least two consecutive days. The Supplier(s) will provide full assistance in this regard. Partial delivery/ installation/ testing of hardware/ system software will not be permissible for acceptance/ payment. The criteria for benchmarking/ acceptance will be conveyed separately.

PROFORMA- A
(Declaration by the O.E.M.)
[Para 2.8(I) (ii)]

To Date:

The Managing Director,
H.P. State Electronics Development Corporation Ltd.,
1st Floor, IT Bhawan, Mehli, Shimla- 171013.

Subject: Authorisation to a distributor for tender No: HPSEDC/RC-FW/2K24-19128
Dear Sir,

Please refer to your Notice Inviting Tenders for Rate Contract for Firewall published in "The Indian Express" and "Amar Ujala".
M/s _____(Bidder), who is our reliable distributor for the last _____years, is hereby authorised to quote on our behalf for this prestigious tender. M/s _____ (Bidder) is likely to continue as our business partner during years to come. We undertake the following regarding the supply of these Firewall etc.

1. The Machines supplied in this tender shall be manufactured by us as per the specifications required by the Purchaser. M/s _____ (Bidder) shall not be allowed to do any hardware integration on our equipment.

2. It will be ensured that in the event of being awarded the contract, Firewall will be delivered by M/s_____ (Bidder) & maintained by M/s _____ (ASP) properly as per the conditions of the contract. For this purpose, we shall provide M/S _____ necessary technical support including technical updates, & spares to the ASP. If M/s _____ fails to maintain the Firewall for any reason what-so-ever, we shall make alternative arrangements for proper maintenance of these components during the warranty period. We shall provide full support back up to the Bidder/ASP. On the whole, it shall be

ensured that the clauses regarding service and maintenance of Machines do not get diluted in implementation due to non-availability of spares and lack of technical inputs from our side even during AMC/extended warranty period.

3. If due to any reason whatsoever, the tie up between our Company & M/s _____ (Bidder) or M/s_____ (ASP) breaks down subsequently, we shall make necessary alternatives arrangements for honouring the terms of the contract.

Yours very truly,

Name : _____
Designation: _____
Company: _____

FORM-B

DECLARATION REGARDING ACCEPTANCE OF TERMS & CONDITIONS CONTAINED IN THE TENDER DOCUMENT

To

The Managing Director,
H.P. State Electronics Development Corporation Ltd.,
1st Floor, IT Bhawan, Mehli, Shimla-171013.

Sir,

I have carefully gone through the Terms & Conditions contained in the Tender Document [No.: HPSEDC/RC-FW/2K24-19128] regarding Rate Contract for Firewall for Tender/Rate Contract by HPSEDC. I declare that all the provisions of this Tender Document contained in this tender and subsequent corrigendum(s)/ clarifications issued from time to time are acceptable to my Company/firm. I further certify that I am an authorised signatory of my company and am, therefore, competent to make this declaration.

Yours very truly,

Name: _____

Designation: _____

Company: _____

Address: _____

Contact No: Email-id:

FORM-C

DECLARATION REGARDING PAST PERFOMANCE

To

The Managing Director,
H.P. State Electronics Development Corporation Ltd.,
1st Floor, IT Bhawan, Mehli, Shimla-13.

Sir,

I have carefully gone through the Terms & Conditions contained in the Tender Document [No. HPSEDC/RC-FW/2K24-19128] regarding Tender/ Rate Contract for Firewall by HPSEDC. I hereby declare that my company has not been debarred/blacklisted by any Government / Semi Government organizations for quality/ service products nor is there any pending dispute regarding short shipment/ installation/service. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours truly,

Name: _____

Designation: _____

Company: _____

Address: _____

Contact No:

Email-id:

# SCHEDULE - I

## SAMPLE OF PRICE SCHEDULE/BOQ

*[Para 2.8 (III) (i)]*

*(to be completed by bidder as per the format available on e-procurement portal https://hptenders.gov.in)*

**PRICE SCHEDULE**

**(DOMESTIC TENDERS - RATES ARE TO GIVEN IN RUPEES (INR) ONLY)**

**(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)**

| Sl. No. | Item Description | Qty | BASIC RATE with installation (if any) and three years warranty In Figures To be entered by the Bidder in Rs. P | GST Amount in percentage (%) | GST amount in Rupees Rs. P | Unit Price with GST Rs. P | TOTAL AMOUNT Without Taxes with three-year warranty Rs. P | Gross Bid Value Inclusive installation and Taxes (for three-year onsite OEM warranty) Rs. P | TOTAL AMOUNT In Words |
|---|---|---|---|---|---|---|---|---|---|
| *1.* | *Item No: 1: Firewall Option 1* | | | | | | | | |
| *2.* | *Item No: 2: Firewall Option 2* | | | | | | | | |
| *3.* | *Item No: 3: Firewall Option 3* | | | | | | | | |
| *4.* | *Item No: 4: Firewall Option 4* | | | | | | | | |
| *5.* | *Item No: 5: Firewall Option 5* | | | | | | | | |
| *6.* | *Item No: 6: Firewall Option 6* | | | | | | | | |
| *7.* | *Item No: 7: Firewall Option 7* | | | | | | | | |
| *8.* | *Item No: 8: Firewall Option 8* | | | | | | | | |
| *9.* | *Item No: 9: Firewall Option 9* | | | | | | | | |
| *10.* | *Item No: 10: Firewall Option 10* | | | | | | | | |

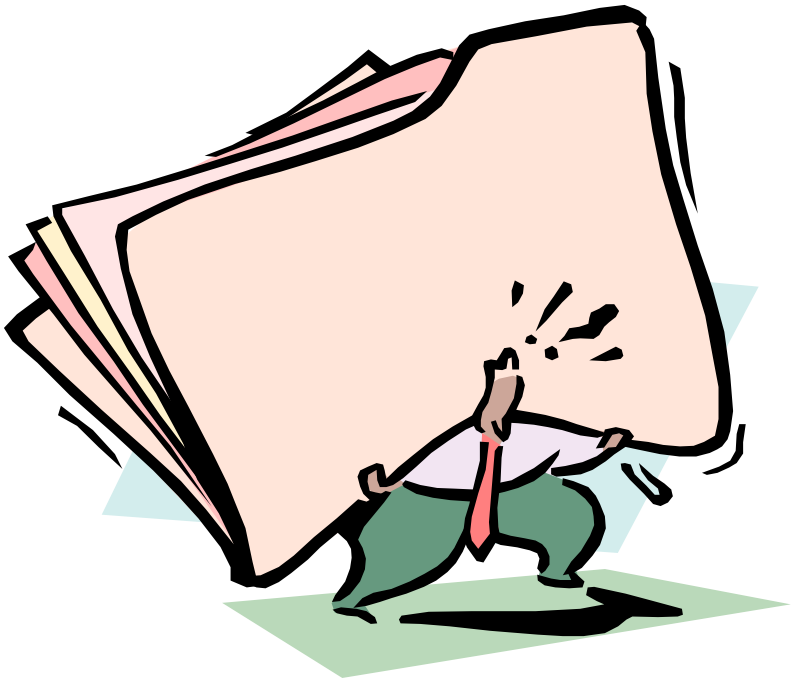
**SECTION- 5**

TECHNICAL SPECIFICATIONS

ANNEXURES

Tender Document No:

HPSEDC/RC-FW/2K24-19128



*NB: Final specifications uploaded after pre-bid meeting. Please visit our websites www.hpsedc.in & https://hptenders.gov.in for latest amendments or notices in reference to this tender.*

**** The quoted product should not be end of life at the time of bid submission. The support shall be provided by the bidder/ OEM for next three years, an undertaking for the same shall be provided by the OEM.***

---

ANNEXURE-I

## SECTION – V

TECHNCIAL SPECIFICATIONS AND COMPLIANCE SHEETS ANNEXURES

The specification mentioned hereunder are bare minimum requirement. Bidders are encouraged to offer better specifications in this bid or subsequently during the period of tender/rate contract. Technical compliance to be provided on OEMs letterhead with signatures, name, email, contact number of Authorized signatory.

**Item No: 1: Firewall Option 1**

| Sl. No | Item Description | Technical Specification | Compliance (Yes/No) |
|---|---|---|---|
| 1 | **Make** | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 24 x 1G Copper ports, 6 x 10G SFP+ port and 4x5G SFP+ from day 1. | |
| | | Appliance should have minimum 128 GB or more SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 5.5 Gbps or more Firewall throughput & 3.8 Gbps or more IPS throughput. | |
| | | Appliance shall support 3.5 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 2 Million or higher & New connection/Sec: 22,000 or higher | |

| | | | |
|---|---|---|---|
| | | Firewall shall support at least 2.2 Gbps or more IPSec VPN throughput and 3000 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 650 Mbps or more & 500 or more remote access/SSL VPN(Concurrent) Users support. | |
| | | Firewall shall support 1000 or more IPSec VPN clients. | |
| | | Firewall shall support 500 or more Access points. | |
| | | Firewall Should support 850 Mbps or more SSL throughput and 150K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Route-based VPN over OSPF, RIP, BGP. | |
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |

| | | | |
|---|---|---|---|
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 500+ Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat | |

| | | | |
|---|---|---|---|
| | | found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | The Firewall should Support for TLS 1.3 to improve overall security on the firewall. | |
| | | Should support more than 7300+ IPS signatures from day1 | |
| | | Should support 80 million Cloud AV signatures and 3400+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting | The management platform must be accessible via a web-based interface and without any additional client software | |

| | | | |
|---|---|---|---|
| | Feature | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises or on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc. | |
| | | The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019). | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

## Item No: 2: Firewall Option 2

| Sl. No | Item Description | Technical Specification | Compliance (Yes/No) |
|---|---|---|---|
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cup's based architecture to protect latest security threats. | |
| 5 | Performance & Scalability | Appliance must have one Console port, dedicated one management Port, two USB port and redundant power supply | |
| | | The device should have 6 x 10G/5G/2.5G/1G (SFP+); 24 x 1GbE Cu from day 1. | |
| | | Appliance should have 128 GB or more Built in Storage from day 1 and should be expandable to 1 TB | |
| | | Appliance should support 18 Gbps or more Firewall throughput & 10 Gbps or more IPS throughput. | |
| | | Appliance should support 9 or 10 Gbps or more Threat Protection throughput | |
| | | The device should have Concurrent Sessions: 4 Million or higher & New connection/Sec: 115,000 or higher | |
| | | Firewall Should support at least 11 Gbps or more Ipsec VPN throughput and 4000 IPSec Site-to-Site VPN tunnels & 3000 IPSec VPN clients. | |
| | | Firewall Should support at least 5 Gbps or more TLS/SSL inspection & decryption throughput and 1000 SSL VPN clients. The appliance should have 350,000 SSL DPI connections. | |
| 6 | General Firewall Features | Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode. Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Application Control : The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500 application | |

| | | | |
|---|---|---|---|
| | | signatures | |
| | | The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found. The Firewall should Support for TLS 1.3 to improve overall security on the firewall. This should be implemented in Firewall Management, SSL VPN and DPI. | |
| | | Firewall should support clientless SSL VPN technology or an easy to manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms. | |
| | | Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate based authentication connection tunnel. | |
| | | Solution should support User identification and activity available through seamless AD/LDAP Services SSO integration combined with extensive information obtained through Deep Packet Inspection. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.. | |
| | | Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and | |

| | | | |
|---|---|---|---|
| | | vulnerabilities. Should have at least 7300+ IPS Signatures and 80 million Could AV signatures. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify. URL database should have at least 15-20 million sites and 55 + categories. | |
| | | Firewall should support HTTP Request tempering protection, Directory traversal prevention, SQL injection Protection, Cross site scripting Protection (XSS) & DNS security | |
| | | The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration. Firewall Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. | |

**Item No: 3: Firewall Option 3**

| Sl. No | Item Description | Technical Specification | Compliance (Yes/No) |
|---|---|---|---|
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 16 x 1G Copper ports, 3 x 10G SFP+ port with pre populated transceiver from day 1. | |
| | | Appliance should have minimum 64 GB and expendable up to 256 GB or more SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 5.2 Gbps or more Firewall throughput & 3.4 Gbps or more IPS throughput. | |
| | | Appliance shall support 3.0 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 1.5 Million or higher & New connection/Sec: 21,000 or higher | |
| | | Firewall shall support at least 2.1 Gbps or more IPsec VPN throughput and 2000 IPsec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 800 Mbps or more & 500 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 1000 or more IPsec VPN clients. | |
| | | Firewall shall support 512 or more Access points. | |
| | | Firewall Should support 800 Mbps or more SSL throughput and 125K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |

| | | | |
|---|---|---|---|
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, and Route-based VPN over OSPF, RIP, BGP. | |
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |

| | | | |
|---|---|---|---|
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |

| | | | |
|---|---|---|---|
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support min 20K DPI signatures, 80 million Cloud AV signatures and 3500+ Application Signatures from day one. | |
| | | Solution should have more than 7300+ IPS signature from day 1 | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multiservice firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |

| | | | |
|---|---|---|---|
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc | |
| | | The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019). | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

**Item No: 4: Firewall Option 4**

| Sl. No | Item Description | Technical Specification | Compliance (Yes/No) |
|---|---|---|---|
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 6x10G/5G/2.5/1G SFP+, 2x10G/5G/2.5G/1G (Cu); 24x1GbE (Cu) with pre populated transceiver from day 1. | |

| | | | |
|---|---|---|---|
| | | Appliance should have minimum 128 GB or more SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 28 Gbps or more Firewall throughput & 15 Gbps or more IPS throughput. | |
| | | Appliance shall support 15 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 5 Million or higher & New connection/Sec: 228K or higher | |
| | | Firewall shall support at least 15 Gbps or more IPSec VPN throughput and 6000 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 8 Gbps or more & 1500 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 4000 or more IPSec VPN clients. | |
| | | Firewall shall support 512 or more Access points. | |
| | | Firewall Should support 7 Gbps or more SSL throughput and 350K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, and Route-based VPN over OSPF, RIP, and BGP. | |

| | | | |
|---|---|---|---|
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled.. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |

| | | | |
|---|---|---|---|
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support 80 million Cloud AV signatures and 3400+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |

| | | | |
|---|---|---|---|
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc. | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

## Item No: 5: Firewall Option 5

| Technical Specifications for Firewall | | | |
|---|---|---|---|
| **Sl. No** | **Item Description** | **Technical Specification** | **Compliance (Yes/No)** |
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 2x40G; 8x25G, 4 x10G/5G/2.5/1G SFP+, 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 Mgmt. port from day 1. | |
| | | Appliance should have minimum 256 GB or more SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 36 Gbps or more Firewall throughput & 20 Gbps or more IPS throughput. | |
| | | Appliance shall support 19 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 8 Million or higher & New connection/Sec: 228K or higher | |
| | | Firewall shall support at least 19 Gbps or more IPSec VPN throughput and 6000 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 9 Gbps or more & 1500 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 6000 or more IPSec VPN clients. | |
| | | Firewall shall support 512 or more Access points. | |
| | | Firewall Should support 9 Gbps or more SSL throughput and 750K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and | |

| | | | |
|---|---|---|---|
| | | control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, and Route-based VPN over OSPF, RIP, BGP. | |
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 512 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |

| | | | |
|---|---|---|---|
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |

| | | | |
|---|---|---|---|
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support min 20K DPI signatures, 80 million Cloud AV signatures and 3500+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability | |

| | | | |
|---|---|---|---|
| | | & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution must be ICSA certified (As per ICSA Report of Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc. | |
| | | The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019). | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

**Item No: 6: Firewall Option 6**

| | **Technical Specification of Firewall :-** | **Compliance (Yes/No)** |
|---|---|---|
| **SL No** | **Specifications** | |
| **A.** | **Security Features** | |
| 1 | Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware, Application Control and Geo-IP protection. The firewall should also support anti-Spam services integrated as a license in the firewall. | |
| 2 | The device should be IPv6 ready (Both phase 1 and Phase2), and should support multi-core architecture and not proprietary ASIC based architecture. | |
| 3 | Appliance should support IPSec NAT traversal, OSPF, RIP V1 and V2 routing protocol and NAT without degrading the performance of the firewall. | |

| | | |
|---|---|---|
| 4 | Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix | |
| 5 | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| 6 | Dual WAN/ISP Support : Should support automatic ISP failover as well as ISP load balancing for outbound traffic | |
| 7 | Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. | |
| 8 | Should proactively detect and block mass market, zero-day threats and unknown malware by inspecting directly in memory | |
| 9 | Product Support should be (24 x 7) with Advanced replacement | |
| 10 | Should have capability to look deep inside every packet (the header and data) searching for protocol non-compliance, threats, zero days, intrusions, and even defined criteria. The firewall should support stream/flow based inspection only without compromising/missing any security features like AV, Windows File Sharing (CIFS), email filter, web filter, VOIP etc. | |
| 11 | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| 12 | Should allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements. | |
| 13 | Vendor & OEM should support the appliance with all necessary upgrade for at least 5 years from the date of purchase installation along with 5 years security software subscription. | |
| 14 | Should scan for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside. | |
| 15 | Should provide real-time monitoring and visualization provides a graphical representation of applications, users and bandwidth usage for granular insight into traffic across the network. | |
| 16 | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| 17 | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. | |
| 18 | Should have H.323 gatekeeper and SIP proxy support to block spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy. | |
| 19 | Should support mobile device authentication such as (biometric authentication) fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access | |

| | | |
|---|---|---|
| 20 | The proposed solution should be scalable and offer fault tolerance to safeguard against hardware failures. The failover should be capable of taking over the traffic without any manual intervention and session loss. | |
| 21 | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| 22 | Should have TLS/SSL decryption and inspection engine that decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic. | |
| 23 | Should have deep packet inspection of SSH to decrypt and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH. | |
| 24 | Should have IPv6 and should support filtering and wire mode implementations. | |
| 25 | Should support REST APIs that allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransom ware and advanced persistent threats. | |
| 26 | Should have Bi-directional raw TCP inspection. The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports. | |
| 27 | Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decode payloads for malware inspection, even if they do not run on standard, well-known ports. | |
| 28 | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| 29 | Should have secure SD-WAN feature that enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public internet services. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| 30 | Should control applications, or individual application features, that are identified by the security engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity. Should control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network. | |

| | | |
|---|---|---|
| 31 | The firewall should support traffic management option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| 32 | Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. Appliance should protect against DOS & DDOS attacks. | |
| 33 | Should have anti-evasion technology by using extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7 | |
| 34 | Should not buffer traffic before scanning for IPS and must support inbound and outbound IPS scanning. It should scan the entire traffic and not few specific kilobyte of the session. | |
| 35 | The device should be featured with Gateway Antivirus and DPI SSl Scanning | |
| 36 | The OEM should have regular update of its attack signature database and the same should be configurable to update the signatures automatically without manual intervention. The new attack signatures and new major software releases should be available in OEM website for free download. | |
| 37 | Should not buffer traffic before scanning for virus. Should have capacity to scan unlimited file size without buffering them. | |
| 38 | Should be an unlimited user based appliance. Firewall must support inbound and outbound Antimalware/Antispyware scanning. Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. | |
| 39 | Should enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client. | |
| 40 | Should block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups. | |
| 41 | Should have more than 7300 IPS signature from Day 1 | |
| 42 | URL database should have at least 20 million sites and 55 + categories. | |
| 43 | There should be a proposed sandboxing solution which should be cloud based or appliance based and employ sandboxing engine for effective scanning | |
| 44 | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. | |
| 45 | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |

| | | |
|---|---|---|
| 46 | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| 47 | Should have ability to prevent potentially malicious files from entering the network. Should have support for files sent to the proposed on-premise sandbox for analysis to be held at the gateway until a verdict is determined. | |
| 48 | Should have continuously updated database of tens of millions of threat signatures residing in the sandbox servers and referenced to augment the capabilities of the on-board signature database, providing deep packet inspection with extensive coverage of threats. Should support min 20K DPI signatures, and 3500+ Application Signatures from day 1. | |
| | **Hardware and Interface Requirements** | |
| 1 | The product should have minimum of 8x1GbE, 2 USB 3.0, 1 Console | |
| 2 | Should have built-in storage (SSD) of at least 32 GB | |
| C | Firewall Performance Requirement | |
| 1 | Threat prevention throughput of 750 Mbps or higher which should include Firewall, Gateway Anti-Virus, AntiSpyWare, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and URL & Reputation service from Advance Threat Prevention/Protection/sandboxing services. | |
| 2 | The Firewall should have at least 1 Gbps of IPS throughput | |
| 3 | Firewall inspection throughput at least 2 Gbps | |
| 4 | The Firewall should support at least 6K new sessions/connections per second. | |
| 5 | The Firewall should support at least 750000 Connections and 25K maximum DPI SSL sessions/connections. | |
| 6 | Should support at least 50 IPSec Site-to-Site VPN tunnels and 200 no of IPSec Client Remote access VPN | |
| 7 | Should support at least 50 SSL VPN users | |
| 8 | Solution should support IPSEC & SSL VPN and Layer 2 Tunnelling protocol (L2TP)over IPSEC | |
| D | **Licensing and Certification** | |
| 1 | The devices should not have license restriction on number of users. The license should the following subscriptions from day 1 - Firewall, Gateway Anti-Virus, Anti Spyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and Advance Threat Prevention/Protection including advance sandboxing. | |
| 2 | The OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Security Effectiveness in the last NSS Lab for NGFW report (2019) | |
| 4 | The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc. | |
| 5 | The device should be IPv6 Ready (Both phase 1 and Phase2) | |

| E | **Logging and reporting** | |
|---|---|---|
| 1 | Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. | |
| 2 | Logging and reporting solution should be supported. | |
| 3 | Should have options to generate reports in different formats | |
| 4 | The solution should have configurable options to schedule the report generation. | |
| 5 | The solution should support Offline management thereby enabling scheduling of configurations and firmware updates on managed appliances to minimize service disruptions. | |

**Item No: 7: Firewall Option 7**

| **Technical Specifications for Firewall** | | | |
|---|---|---|---|
| **Sl. No** | **Item Description** | **Technical Specification** | **Compliance (Yes/No)** |
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G). | |
| | | The device should have 8 x 1G Copper ports with pre populated transceiver from day 1. | |
| | | Appliance should have minimum 64 GB or more SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 3 Gbps or more Firewall throughput & 1.5 Gbps or more IPS throughput. | |
| | | Appliance shall support 1 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 900 K or higher & New connection/Sec: 9000 or higher | |
| | | Firewall shall support at least 1.3 Gbps or more IPSec VPN throughput and 100 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 500 Mbps or more & 100 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 200 or more IPSec VPN clients. | |
| | | Firewall shall support 30 or more Access points. | |

| | | | |
|---|---|---|---|
| | | Firewall Should support 500 Mbps or more SSL throughput and 30K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, and Route-based VPN over OSPF, RIP, BGP. | |
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |

| | | | |
|---|---|---|---|
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |

| | | | |
|---|---|---|---|
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support min 20K DPI signatures, 60 million Cloud AV signatures and 3500+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH ,GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |

| | | | |
|---|---|---|---|
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution offered must be ICSA certified for Network Firewall, Anti-virus, Advanced Threat Defence, Common Criteria NDPP (Firewall and IPS) – Certification etc. | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

**Item No: 8: Firewall Option 8**

| **Technical Specifications for Firewall** | | | |
|---|---|---|---|
| **Sl. No** | **Item Description** | **Technical Specification** | **Compliance (Yes/No)** |
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should be desktop form Factor. | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G). | |
| | | The device should have 8 x 1G & 2 X 2.5G Copper ports with pre populated transceiver from day 1. | |

| | | | |
|---|---|---|---|
| | | Appliance should have minimum 4 GB or more & Optional up to 256GB SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 3.5 Gbps or more Firewall throughput & 2 Gbps or more IPS throughput. | |
| | | Appliance shall support 1.5 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled. | |
| | | The device shall support Concurrent Sessions: 1M or higher & New connection/Sec: 12000 or higher | |
| | | Firewall shall support at least 1.5 Gbps or more IPSec VPN throughput and 150 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 600 Mbps or more & 150 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 200 or more IPSec VPN clients. | |
| | | Firewall shall support 30 or more Access points. | |
| | | Firewall Should support 600 Mbps or more SSL throughput and 35K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, and Route-based VPN over OSPF, RIP, BGP. | |

| | | | |
|---|---|---|---|
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |

| | | | |
|---|---|---|---|
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support min 20K DPI signatures, 60 million Cloud AV signatures and 3500+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |

| | | | |
|---|---|---|---|
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution offered must be ICSA certified for Network Firewall, Anti-virus, Advanced Threat Defence, Common Criteria NDPP (Firewall and IPS) – Certification etc. | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

## Item No: 9: Firewall Option 9

| Technical Specifications for Firewall | | | |
|---|---|---|---|
| **Sl. No** | **Item Description** | **Technical Specification** | **Compliance (Yes/No)** |
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country **of Origin** | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware **Architecture** | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 8x1GbE, 2x5G SFP+ port with pre populated transceiver from day 1. | |
| | | Appliance should have minimum 256 GB SSD Storage from day 1 | |
| 5 | Performance & Scalability | Appliance shall support 4.0 Gbps or more Firewall throughput & 2.0 Gbps or more IPS throughput. | |
| | | Appliance shall support 2.5 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 1.2 Million or higher & New connection/Sec: 16000 or higher | |
| | | Firewall shall support at least 1.8 Gbps or more IPSec VPN throughput and 200 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 560 Mbps or more & 200 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 500 or more IPSec VPN clients. | |
| | | Firewall shall support 30 or more Access points. | |
| | | Firewall Should support 750 Mbps or more SSL throughput and 50K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |

| | | | |
|---|---|---|---|
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, and Route-based VPN over OSPF, RIP, BGP. | |
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |

| | | | |
|---|---|---|---|
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |

| | | | |
|---|---|---|---|
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support 80 million Cloud AV signatures and 3400+ Application Signatures from day one. | |
| | | Should support more than 7000 IPS signatures | |
| | | Should have more than 50 Categories for URL Filtering | |
| | | The Firewall should Support for TLS 1.3 to improve overall security on the firewall. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |

| | | | |
|---|---|---|---|
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defence & IPv6/USGv6 - Certification etc | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

**Item No: 10: Firewall Option 10**

| **Technical Specifications for Firewall** | | | |
|---|---|---|---|
| **Sl. No** | **Item Description** | **Technical Specification** | **Compliance (Yes/No)** |
| 1 | Make | To be mentioned by the bidder/ Vendor | |
| 2 | Model No. | To be mentioned by the bidder/ Vendor | |
| 3 | Country of Origin | To be mentioned by the bidder/ Vendor | |
| 4 | Hardware Architecture | The proposed hardware based firewall should not consume more than 1RU Rack-mountable space | |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core cpu's based architecture to protect latest security threats. | |
| | | The proposed firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet | |
| | | Appliance must have one Console port, dedicated one GbE management Port, two USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support dual power supply. | |
| | | The device should have 8x1GbE, 2x10GbE, port with pre populated transceiver from day 1. | |
| | | Appliance should have minimum 256 GB SSD Storage from day 1 | |

| | | | |
|---|---|---|---|
| 5 | Performance & Scalability | Appliance shall support 5 Gbps or more Firewall throughput & 3 Gbps or more IPS throughput. | |
| | | Appliance shall support 2.5 Gbps or more Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled | |
| | | The device shall support Concurrent Sessions: 1.5 Million or higher & New connection/Sec: 25000 or higher | |
| | | Firewall shall support at least 2.1 Gbps or more IPSec VPN throughput and 250 IPSec Site-to-Site VPN tunnels | |
| | | Shall support SSL VPN throughput 800 Mbps or more & 250 or more remote access/SSL VPN (Concurrent) Users support. | |
| | | Firewall shall support 500 or more IPSec VPN clients. | |
| | | Firewall shall support 30 or more Access points. | |
| | | Firewall Should support 800 Mbps or more SSL throughput and 75K SSL connections. | |
| 6 | General Firewall Features | Solution must support unified threat policy, Bandwidth management, policy based routing & SDWAN. | |
| | | Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2). | |
| | | Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration | |
| | | Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode | |
| | | Should support Zero-Touch registration & provisioning using mobile App. | |
| | | Solution should support policy based routing, Application based routing and also Multi Path routing. | |
| | | Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. | |
| | | Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. | |
| | | Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of | |
| | | Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. | |
| | | Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Route-based VPN over OSPF, RIP, BGP. | |

| | | | |
|---|---|---|---|
| | | Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. | |
| | | Proposed Appliance should support SD WAN features without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support at least 32 Wireless Access Points from day 1. Necessary licenses, if required, need to be provisioned from day 1. | |
| | | Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP. | |
| | | Firewall should have Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled. | |
| 7 | Firewall Security Features | Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. | |
| | | The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port. | |
| | | Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations. | |
| | | The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. | |
| | | Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. | |
| | | Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting. | |
| | | Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify | |

| | | | |
|---|---|---|---|
| | | Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. | |
| | | Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. | |
| | | Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. | |
| | | The firewall must support cloud & appliance based Sandbox technology and OEM must have own Advanced Threat Protection solutions. | |
| | | The cloud or appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. | |
| | | The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Port smash etc. | |
| | | Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. | |
| | | Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. | |
| | | Should support min 20K DPI signatures, 60 million Cloud AV signatures and 3500+ Application Signatures from day one. | |
| 8 | High Availability | Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention. | |
| | | Proposed solution should support Active/Passive with State Sync or Active/Active. | |
| | | The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance. | |
| 9 | Visibility and Monitoring | Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. | |

| | | | |
|---|---|---|---|
| | | The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status. | |
| | | Solution should support granular network visibility of network topology along with host info. | |
| | | Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. | |
| 10 | Management & Reporting Feature | The management platform must be accessible via a web-based interface and without any additional client software | |
| | | Firewall should support management via Cli, SSH, GUI and support for SNMPv2/3. | |
| | | The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on premises and on cloud. | |
| | | The Centralize management platform should support multi device firmware upgrade, certificate management, and global policy template to push config across multiple firewall in single click. | |
| | | The Centralize management platform should support account lockout security & account access control through whitelisted IPs. | |
| | | The on premises Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator. | |
| | | The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address | |
| | | Analytics platform support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem | |
| | | The solution should support Cloud-based configuration backup. | |
| | | The solution should support IPFIX or Net Flow protocols for real-time and historical monitoring and reporting | |
| 11 | Certification, Warranty, Installation, Testing and Commissioning | The Firewall solution offered must be ICSA certified for Network Firewall, Anti-virus, Advanced Threat Defence, Common Criteria NDPP (Firewall and IPS) – Certification etc. | |
| | | Proposed Solution should support 24x7 telephone, email and web-based technical support. | |
| | | OEM should have TAC and R&D center in INDIA. | |
| | | Manufacturer's warranty should be mentioned minimum 03 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade. | |
| | | Bidder must carry out on site installation, testing and commissioning. | |

## Annexure-II

Performance Bank Guarantee Template

[Date]

To,

The Managing Director,
H.P. State Electronics Development Corporation Ltd.,
First Floor, IT Bhawan, Mehli, Shimla-171013.

Dear Sir,

**1.** Whereas M/s _____ (hereinafter called "CONTRACTOR") has supplied _____ (as per Bill of Material Specified in this Document) as per agreement/supply order No._____ dated _____ signed between the HPSEDC (hereinafter called "Client") and them and as per the agreement/supply order the M/s. _____ is supposed to furnish Performance Security for supply of _____ and maintain the same for a period of _____years.

**2.** NOW THEREFORE KNOW ALL THE MAN THESE PRESENTS THAT WE, __(Bank Name)_____ having its Head Office at _____(hereinafter called "the Bank") are bound up to the Client in the sum of Rs._____/- (Rs._____ _____) only) for which payment will and truly to be made to the said Client, the Bank binds itself, its successors and assignees by these presents.

**3.** The Bank further undertakes to pay to the purchaser up to the above amount on receipt of its first written demand, without the Client having to substantiate its demand. The Client's decision in this regard shall be final and shall not be called upon to question under any circumstances. The Bank Guarantee will remain in force up to _____. However, its validity can be got extended before _____ solely at the instance of the Purchaser. This clause shall remain valid not withstanding anything else contained to the contrary in this document.

**4.** Our responsibility under this guarantee is restricted to Rs._____/- (Rupees _____) only and it will remain enforce up to _____ unless a demand in writing is received by the bank on or before _____, all your rights under the said guarantee shall be forfeited and we shall be released and discharged from all the liabilities thereunder.

**5.** This guarantee will remain in force up to <date of validity> and any demand in respect thereof should reach the Bank not later than the specified date/dates. However, notwithstanding anything else contained to the contrary in this Guarantee, if the implementing agency does not submit the fresh performance bank guarantee (as per required schedule and amount) till 15 days before expiry of this performance bank guarantee, the Purchaser may either forfeit the PBG or ask the Bank to extend validity of the Bank Guarantee for a further period not exceeding six months. In the latter situation, the Bank shall comply with such a request of extension.

**6.** Sealed with the Common Seal of the said Bank this _____ day of _____, 2024. In witness whereof the Bank, through its authorized officer, has set its hand and stamp on this _____ day of _____, 2024 for Bank _____

Witness

Signature

Name

M/s._____ (complete address)

Note: This guarantee will attract stamp duty as a security bond.

A duly certified copy of the requisite authority conferred on the official/s to execute the Guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence.

Annexure-III

Bank Guarantee (BG) Format for EMD

Date _____

To

The Managing Director,
H.P. State Electronics Development Corporation Ltd., First Floor, IT Bhawan, Mehli, Shimla-171013.

Dear Sir,

**1.** Whereas M/s. _____ (hereinafter called "Bidder") has quoted against the Tender No: HPSEDC/RC-FW/2K24-19128

**2.** Invited by M/s H.P. State Electronics Development Corporation Ltd. (HPSEDC) towards supply of _____is supposed to furnish Bank Guarantee the same valid for a period of 180 days.

**3.**NOW THEREFORE KNOW ALL THE MAN THESE PRESENTS THAT WE, __ (Bank Name)_____ having its Head Office at _____(hereinafter called "the Bank") are bound up to the Client in the sum of Rs._____/- (Rs._____ _____) only) for which payment will and truly to be made to the said Client, the Bank binds itself, its successors and assignees by these presents.

**4.** The Bank further undertakes to pay to the purchaser up to the above amount on receipt of its first written demand, without the Client/ HPSEDC having to substantiate its demand. The Client's decision in this regard shall be final and shall not be called upon to question under any circumstances. The Bank Guarantee will remain in force up to 180 days. However, its validity can be got extended before expiry of its validity solely at the instance of the HPSEDC. This clause shall remain valid not withstanding anything else contained to the contrary in this document.

**5.** Our responsibility under this guarantee is restricted to Rs._____/- (Rupees _____) only and it will remain enforce up to _____ unless a demand in writing is received by the bank on or before _____, all your rights under the said guarantee shall be forfeited and we shall be released and discharged from all the liabilities thereunder.

**6.** This guarantee will remain in force up to <date of validity> and any demand in respect thereof should reach the Bank not later than the specified date/dates. However, notwithstanding anything else contained to the contrary in this Guarantee, if the bidder does not submit the fresh bank guarantee or extend the existing Bank Guarantee till 15 days before expiry of this bank guarantee, the Purchaser/ HPSEDC may either forfeit the BG or ask the Bank to extend validity of the Bank Guarantee for a further period not exceeding six months. In the latter situation, the Bank shall comply with such a request of extension.

**7.** Sealed with the Common Seal of the said Bank this _____ day of _____, 2024. In witness whereof the Bank, through its authorized officer, has set its hand and stamp on this _____ day of _____, 2024 for Bank _____

Witness

Signature

Name

M/s._____ (complete address)

Note: This guarantee will attract stamp duty as a security bond.

A duly certified copy of the requisite authority conferred on the official/s to execute the Guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence.

**Latest instructions for bidders:**

I. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority.

II. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process.

III. "Bidder from a country which shares a land border with India" for the purpose of this Order means: -

a. An entity incorporated, established, or registered in such a country; or

b. A subsidiary of an entity incorporated, established, or registered in such a country; or

c. An entity substantially controlled through entities incorporated, established, or registered in such a country; or

d. An entity whose beneficial owner is situated in such a country; or

e. An Indian (or other) agent of such an entity; or

f. A natural person who is a citizen of such a country; or

g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

IV. The beneficial owner for the purpose of (III) above will be as under:

1. In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation—

a. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent. of shares or capital or profits of the company.

b. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

2. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has

ownership of entitlement to more than fifteen percent of capital or profits of the partnership.

3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals.
4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
5. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

V. An Agent is a person employed to do any act for another, or to represent another in dealings with third person.

VI. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority.

The Bidder has to provide following declarations (duly signed and stamped):

**Declaration 1 of Latest instructions to bidders**

"I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; I hereby certify that this bidder is not from such a country and is eligible to be considered."

**Declaration 2 of Latest instructions to bidders**

"I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India. I certify that this bidder is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]

**Declaration 3 of Latest instructions to bidders**

"I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that this bidder is not from such a country or if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached"

In case bidder is Himachal based company/ firm/ entity then the bidder should submit a self-declaration certificate regarding above mentioned Declaration 1, 2 and 3.

Note: Interested bidder may refer to Office Memorandum (F. No. 6/18/2019-PPD) dated 23.07.2020 of Department of Expenditure, Ministry of Finance, Govt. of India for further details and all the requirements will be in accordance with this memorandum.