भारतीय प्रौद्योगिकीसंस्थानमद्रासचेन्नै 600 036

INDIAN INSTITUTE OF TECHNOLOGY MADRAS Chennai 600 036

भंडार एवं क्रय अनुभाग / STORES & PURCHASE SECTION

Email: adstores@iitm.ac.in

दूरभाष: (044) 2257 8285 / 8287 / 8288 / 8290 फैक्स: (044) 2257 8082
Telephone : (044) 2257 8285/8287/8288/8290 FAX: (044) 2257 8082
GSTIN: 33AAAAI3615G1Z6

P.K. SHEBA SABARI
Assistant Registrar (Stores & Purchase)

Date: 27.02.2024

Tender No. IITM/SPS/Network Firewall/GTE/031/2023-24/SPI

Due Date: 14.03.2024
Before 2.00 p.m.

Dear Sirs,

On behalf of the Indian Institute of Technology Madras, Tenders are invited in two bid system, namely technical and financial bids for:

"Network Firewall"

Conforming to the specifications enclosed.

Tender Documents may be downloaded from Central Public Procurement Portal **https://etenders.gov.in/eprocure/app**. Aspiring Bidders who have not enrolled / registered in e-procurement should enroll/register before participating through the website https://etenders.gov.in/eprocure/app. The portal enrollment is free of cost. Bidders are advised to go through instructions provided at "Help for contractors". [Special instructions to the bidders for the e-submission of the bids online through this e-Procurement Portal"].

Tenderer can access tender documents on the website (For searching in the NIC site, kindly go to Tender Search option and type 'IIT'. Thereafter, Click on "GO" button to view all IIT Madras tenders). Select the appropriate tender and fill them with all relevant information and submit the completed tender document online on the website https://etenders.gov.in/eprocure/app as per the schedule attached.

No manual bids will be accepted. All tender documents including Pre-qualification, Technical and Financial bids should be submitted in the E-procurement portal**.**

1	**LAST DATE for receipt of Tender**	**:**	**14.03.2024 before 02.00 p.m.**
	Pre-bid meeting	**:**	The **Pre-bid Meeting** will be conducted via Google Meet on 05.03.2024 **@ 3.30 p.m.** Please see the below link to join the meeting https://meet.google.com/jqu-bejm-ddc Prospective bidders are requested to register their participation by sending an email to adstores@iitm.ac.in, with name/designation of the representative who will attend the meeting along with queries on or before 04.03.2024
	Date & Time of opening of Tender	**:**	**15.03.2024 @ 3.00 p.m.**

GUIDELINES FOR TENDER SUBMISSION IN CENTRAL PUBLIC PROCUREMENT PORTAL (E-PROCUREMENT MODE)

A	**निविदा की प्रस्तुति /Submission of Tender**	:	As per the directives of Department of Expenditure, this tender document has been published on the Central Public Procurement Portal URL: https://etenders.gov.in/eprocure/app The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal More information useful for submitting online bids on the CPP Portal may be obtained at: https://etenders.gov.in/eprocure/app All tender documents including Technical Bid & Financial Bid should be submitted separately in online CPP portal as per the specified format only. Right is reserved to ignore any tender which fails to comply with the above instructions. **No manual bid submission will be entertained.**
B	**ऑनलाइन बोली जमा के अनुदेश / Instructions for online bid submission**	:	**REGISTRATION** • Bidders are required to enrol on the e-Procurement module of the Central Public Procurement Portal URL: https://etenders.gov.in/eprocure/app by clicking on "Online Bidder Enrolment". Enrolment on the CPP Portal is free of charge. • As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts. • Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal. • Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.) https://eprocure.gov.in/eprocure/app with their profile. • Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse. • Bidder then may log in to the site through the secured log-in by entering their user ID / password and the password of the DSC / eToken.
C	**निविदा दस्तावेज़ की खोज / Searching for tender documents**	:	• There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, organization name, location, date, value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords etc. to search for a tender published on the CPP Portal. • Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective **"My Tender"** folder. This would enable the CPP Portal to intimate the bidders through SMS / email in case there is any corrigendum issued to the tender document. • The bidder should make a note of the **unique Tender ID** assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

	D	**बोली की तैयारी / Preparation of bids**	:	• Bidder should take into account any corrigendum published on the tender document before submitting their bids. • Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid. • Bidder, in advance, should prepare the bid documents to be submitted as indicated in the tender document / schedule and generally shall be in PDF / XLS formats as the case may be. Bid documents may be scanned with 100 dpi with black and white option. • To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GSTIN Details, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use **“My Documents”** area available to them to upload such documents. These documents may be directly submitted from the **“My Documents”** area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.
	E	**बोली की प्रस्तुति / Submission of bids**	:	• Bidder should log into the site well in advance for bid submission so that he/she can upload the bid in time i.e. on or before the bid submission date and time. Bidder will be responsible for any delay due to other issues. • The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document. • A standard BOQ format has been provided in **Annexure-C** with the tender document to be filled by all the bidders. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. Bidders are required to download the BOQ file, open it and complete the detail with their respective financial quotes and other details (such as name of the bidder). If the BOQ file is found to be modified by the bidder, the bid will be rejected. • The server time (which is displayed on the bidders’ dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission. • The **Tender Inviting Authority (TIA)** will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders due to local issues. • The uploaded tender documents become readable only after the tender opening by the authorized bid openers. • Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details. • Kindly add scanned PDF of all relevant documents in a single PDF file of compliance sheet.
	F	**बोलीदाताओं के लिए सहायता / Assistance to bidders**	:	• Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender. • Any queries relating to the process of online bid submission or queries

				relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk. The contact number for the helpdesk is [0120-4200462, 0120-4001002, 0120-4001005]
	G	**बोलीदाताओं के लिए सामान्य अनुदेश** **/ General Instructions to the Bidders**	:	• The tenders will be received online through portal https://etenders.gov.in/eprocure/app. In the Technical Bids, the bidders are required to upload all the documents in single pdf file. • Possession of a Valid Class II/III Digital Signature Certificate (DSC) in the form of smart card/e-token in the company's name is a prerequisite for registration and participating in the bid submission activities through https://etenders.gov.in/eprocure/app • Digital Signature Certificates can be obtained from the authorized certifying agencies, details of which are available in the web site https://etenders.gov.in/eprocure/app under the “Information about DSC”.
	H	बयाना जमा (ईएमडी) / **Earnest Money Deposit (EMD)**	:	**I.** EMD of **INR 6,25,000/-** (Rupees Six Lakhs Twenty Five Thousand only) should be transferred through NEFT/RTGS to the following bank account on or before due date **14.03.2024 before 2:00 p.m.** **a. Name : Registrar IIT Madras** **b. Bank : State Bank of India** **c. Account No. : 10620824305** **d. Branch : IIT MADRAS** **e. IFSC CODE : SBIN0001055** **II.** The EMD will be returned to unsuccessful Bidder(s), after finalization of the tender. The EMD shall be forfeited if any Bidder withdraws the offer before finalization of the tender. **III.** The EMD amount should not be sent through DD. **IV.** Non-submission of EMD details on or before the due date and time will result in rejection of the e-bid. **V.** As per Rule 170 of GFR 2017, exemption of EMD will be given subject to submission of undertaking by the firm seeking such exemption. Copies of relevant orders/ documents regarding such exemption should be submitted along with the tender document. VI. The successful bidder shall submit a **Performance Guarantee of 3%** of the purchase order value by way of DD/Bank Guarantee (including e bank guarantee) / FDR/Insurance surety bonds in favour of **“The Registrar, IIT Madras”** to be obtained from any commercial bank within 14 (Fourteen) days from the date of issue of Order by IIT Madras, which shall be released 60 days after the successful completion of the warranty period after adjustment dues, if any without any interest. VII. In case of successful bidder, the EMD will be adjusted towards the Performance Security Deposit on request, subject to validity. VIII. The amount of EMD is liable to be forfeited, if the bidder withdraws from the offer after submission of the tender or after the acceptance of the offer and fails to remit the Performance Security Deposit.
	I	तकनीकी बोली पर मार्किंग / **Marking on Technical Bid**	:	i. The bidder eligibility criteria (Eligibility Criteria), technical specification of the item for this tender is given in **Annexure A**. The Bidders shall go through the bidder eligibility criteria, technical specification and submit the technical bid in the proforma given in **Annexure B** in the tender document along with the supporting documents. ii. The Technical bid should be submitted **in pdf format only through online (e-tender). No manual submission of bid will be entertained.** iii. The technical bid should have the page-wise **heading as “Technical**

				Bid" and page no. in all pages with seal and signature of authorized signatory. The total no. of pages should be mentioned at the last page of the documents. **iv. The technical bid should consist of** a) Document proof for EMD payment b) Technical Compliance sheet as per proforma given in **Annexure -B** c) Document proof for bidder eligibility criteria, technical details along with catalogue / brochure and other technical, commercial terms and conditions.
	J	**वित्तीय बोली पर मार्किंग / Marking on Financial Bid**	:	Financial bid (BOQ) should be submitted in the prescribed format given **in Annexure- C** in **xls format** through e-tender only. **No manual or other form of submission of Financial Bid will be entertained**.

	TERMS AND CONDITIONS OF TENDER
1	**निनिदा की तैयारी / Preparation of Tender:** • The bids **should be submitted through online only in two bid system i.e. Technical Bid and Financial Bid separately**. • The bidder has to submit the tender document duly signed on all pages by an authorized person and his / her full name and status shall be indicated below the signature along with official seal/stamp of the firm. Submission of wrong / forged information / document will be liable to legal action, and rejection of the bid submitted by the firm. • The bids of the agency/firm/company not in possession of valid statutory license / registrations are liable for rejection. • If any relative of the bidder is an employee of the IIT Madras, the name, designation and relationship of such employee shall be intimated to the Registrar, IIT Madras in writing while submitting the bid. • No bidder will be allowed to withdraw / alter / modify the bid during the bid validity period.
2	निविदा पर हस्ताक्षर **/ Signing of Tender:** • The Tender is liable to be rejected if complete information is not given therein or if the particulars and date (if any) asked for in the schedule to the Tender are not fully filled in or not duly signed/authenticated. Specific attention is drawn to the delivery dates and terms and conditions enclosed herewith. **Each page of the bids required to be signed and bears the official seal of the Bidders.** • If the bid is submitted by a firm in partnership, it shall be signed (with seal) by all the partners of the firm above their full typewritten names and current addresses or alternatively by a partner holding power of attorney for the firm in which case a certified copy of the power of attorney shall accompany the application. A certified copy of the partnership deed along with current addresses of all the partners of the firm shall also accompany the bid. • If a limited company or a corporation makes the application, it shall be signed by a duly authorized person holding power of attorney for signing the application, in which case a certified copy of the power of attorney shall accompany the application. Such limited company or corporation may be required to furnish satisfactory evidence of its existence. The bidder shall also furnish a copy of the Memorandum of Articles of association duly attested by a Notary Public.
3	वह अवधि जिसके लिए ऑफर खुला रहेगा **/ Period for which the offer will remain open:** • The Tender shall remain open for acceptance/validity till: **120 days from the date of opening of the tender.** However, the day up to which the offer is to remain open being declared closed holiday for the Indian Institute of Technology Madras, the offer shall remain open for acceptance till the next working day.
4	कीमत **/Prices:** • The prices quoted must be nett per unit shown in the schedule and must include all packing and delivery charges loading and unloading and other statutory levies considering all scope of work, terms & conditions and as per the Technical bid mentioned in **Annexure A.** • Prices should be inclusive of all.

	• All conditional tenders will be summarily rejected.
5	**Payment terms : Import:** 90% against shipping documents and 10% against installation. **Local:** 90% against delivery at site and 10% after installation. Advance if any required may be considered against the request of successful vendor by submitting equivalent amount of Bank Guarantee in addition to Performance Security Deposit.
6	सुपुर्दगी **/ Delivery:** Items should be delivered and installed within 30 days from the date of Purchase Order.
7	**वारंटी / Warranty**: 5 years from the date of installation at no cost.
8	**Buy Back Item visit:** The bidder should quote a price separately for buyback. Bidder may visit Computer Centre, IIT Madras if required during the working days (Mon-Fri) between 10am to 5pm, until the bid submission deadline.
8	**Installation:** Installation to be done by the bidder and current setup should be migrated.
9	**Terms and Conditions:** Failure to comply with any of the instructions stated in this document or offering unsatisfactory explanations for non-compliance will likely to lead to rejection of offers.
10	**स्वीकृति का अधिकार / Right of Acceptance:** IIT Madras reserves the right to reject the whole or any part of the Tender without assigning any reason or to accept them in part or full.
11	**स्वीकृति की सूचना/ Communication of Acceptance:** Letter of Intimation and acceptance will be communicated by post /email to the successful bidder to the address indicated in the bid.
12	All information including selection and rejection of technical or financial bids of the prospective bidders will be communicated through CPP portal. In terms of Rule 173(iv) of General Financial Rule 2017, the bidder shall be at liberty to question the bidding conditions, bidding process and/or rejection of bids.
13	**Bidder shall submit along with this Tender:** Name and full address of the Banker and their swift code, PAN No. and GSTIN number.
14	**Jurisdiction:** All questions, disputes, or differences arising under, out of or in connection with the contract, if concluded, shall be subject to the exclusive jurisdiction at the place from which the acceptance of Tender is issued.
15	**Penalty & Liquidated Damages / Force Majeure**: • If the selected Bidder fails to complete the due performance of the contract in accordance with the terms and conditions, Institute reserves the right either to cancel the contract or to accept performance already made by the selected Bidder after imposing Penalty on Selected Bidder. A penalty will be calculated on a per week basis and on the same Rate as applicable to Liquidated Damages (LD). In case of termination of the contract, Institute reserves the right to recover an amount equal to 5% of the Contract value as Liquidated Damages for non-performance. • Both Penalty and Liquidated Damages are independent of each other and are applied separately and concurrently. Penalty and LD are not applicable for reasons attributable to the Institute and Force Majeure. However, it is the responsibility of the selected Bidder to prove that the delay is attributable to the Institute and Force Majeure. The selected Bidder shall submit the proof authenticated by the Bidder and Institute’s official that the delay is attributed to the Institute and/or Force Majeure along with the bills requesting payment.
16	• The bidder shall certify that the tender document submitted by him / her are of the same replica of the tender document as published by IIT Madras and no corrections, additions and alterations made to the same. If any deviation found in the same at any stage and date, the bid / contract will be rejected / terminated and actions will be initiated as per the terms and conditions.
17	• The bidder should study the tender document, bidder eligibility criteria, and technical specification in detail as given in **Annexure A** before submitting the bid.

18 **Bidder Eligibility CRITERIA:**

Eligibility Criteria

1. The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**

2. Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure – E.**

3. The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-F.**

4. MAF - Manufacturer Authorization Form to be attached for the quoted specification **[MAF to be attached for Firewall and Analyzer]**

5. The bidder should have a service centre / local office in Chennai for the past 10 years with experts to handle Installation, Configuration and solving all types of issues in time. **[Self Declaration with proof like Registration Certificate/GST to be submitted]**

6. The firm must have an aggregate turnover of at least Rs.249.6 Lakhs in the last 3 years i.e. 2020-2021, 2021-2022 and 2022-2023 (should enclose the audited financial statement signed by the Chartered Accountant).

7. The vendor (OEM / Bidder) should give at least two references (attach Purchase order copy) in India where they have implemented the similar solution with 2 Gbps Internet Link & 10,000 + users in a single appliance.

19 **Number of Bids and their Submission:**

Bids should be submitted **CPP portal. Two bid system** should be followed as detailed below:

Bid I **Technical Bid**

The bidder should go through the bidder eligibility criteria and technical specification given in **Annexure-A** of the tender document, understand the requirement of IITM and submit their technical bid along with all relevant document proof in the proforma given in **Annexure–B**. **Any tender documents without these shall be invalid and rejected.**

The technical bid should consist of proof of EMD transfer, Bidder Eligibility Criteria, Technical specification and compliance sheet (proforma given in **Annexure – B)** along with all relevant documents proof.

Bid II **Financial Bid**

The financial bid should be submitted as per the proforma (**Annexure C**). The Quoted price should be for supply and installation of the item and inclusive of all cost at IIT Madras.

20 **Evaluation of Bids:**

Bid Evaluation will take place in two stages.

Technical Bid evaluation

1. In the Stage I Bidder will be evaluated first for conformity with bidder Eligibility Criteria and those bidders who have complied with Bidder Eligibility Criteria will be evaluated further for technical specifications.

2. Only those bidders who have fully complied with bidder eligibility Criteria and technical specification will be considered for opening of financial bid.

	Stage II: Financial Bid Evaluation The Lowest financial bid among those who have qualified in the technical bid will be declared as successful bidder (L1) and order will be awarded to the successful bidder (L1). Financial bid prices expressed in multi-currency (USD/EUR) shall be converted to INR as per the prevailing RBI exchange rate on the date of opening of Financial bid for arrival of lowest bid (L1) value. L1 will be arrived including AMC value and after deducting Buyback value.
21.	**'**Class-I local suppliers' and 'Class-II local suppliers', as defined under DIPP, MoCI Order No.P45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein, shall be eligible to bid in this tender. Declaration for Class-I / Class-II local suppliers should be submitted in the prescribed proforma format as per Annexure-E
22	**Selection of successful bidder and Award of Order:** The order will be directly awarded to the technically qualified bidder as per the condition in para 3A of DIPP, MoCI Order No. 45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein.
23	The bidders will not be entertained to participate in opening of Bids. Since the tender is e-tender, the opening of the bids may be checked using the respective logins of the bidders.
24	The pre-bid meetings will be conducted through online. Bidders can submit their queries and doubts to the email id: adstores@iitm.ac.in till the date of the online pre-bid meeting 05.03.2024 @ 3.30 p.m clarification to the queries and doubts raised by the bidders will be issued as a corrigendum/addendum in the e-tenders portal and Institute Website (tenders.iitm.ac.in). For the bidders, submitting bids on downloaded tender document, it is 'bidders' responsibility to check for any amendment/corrigendum on the website of IIT Madras or check for the same CPP Portal before submitting their duly completed bids. **After the pre-bid meeting, queries/clarification if any will not be considered.**
25	In accordance to the Rule 173 of GFR, 2017 and relevant provisions thereof in Procurement Manuals, 2022, IITM reserves the right to carry out the negotiation process through its purchase / technical committee with L1/H1 (as applicable) vendor to ensure price reasonability before final recommendation to the Competent Authority. The negotiation details, if any, on case to case basis shall be recorded in minutes of meetings suitably for records.

Assistant Registrar
Stores & Purchase

ACKNOWLEDGEMENT

It is hereby acknowledged that I/We have gone through all the points listed under **“Specifications, Terms and Conditions”** of tender document, the same is abided and agreed to be executed. In case, if any of the information furnished by me/us is found false, I/We are fully aware that the tender /contract will be rejected / cancelled by IIT Madras and EMD shall be forfeited.

Signature of the Bidder Name
& Address of the Bidder with
Office Stamp

SCHEDULE OF TENDER

NETWORK FIREWALL for IIT Madras

Tender No. IITM/SPS/Network Firewall/031/2023-24/SPI

Name of Organization	Indian Institute of Technology Madras
Tender Type (Open/Limited/EOI/Auction/Single)	OPEN
Tender Category (Services/Goods/Works)	Goods
Type/Form of Contract (Work/Supply/Auction/ Service/ Buy/ Empanelment/ Sell)	Supply
Name of the Supply	Network Firewall for IIT Madras
Source of Fund (Institute/Project)	IIT Madras
Is Multi Currency Allowed	Yes / ~~No~~
Date of Issue/Publishing	01.03.2024
Document Download Start Date	01.03.2024
Document Download End Date	14.03.2024
Prebid Meeting via Google Meet	05.03.2024 @ 03.30 p.m.
Bid Submission Start Date	08.03.2024
Last Date and Time for Uploading of Bids	14.03.2024 @ 02.00 p.m.
Date and Time of Tender Opening	15.03.2024 @ 03.00 p.m.
No. of Covers (1/2/3/4)	2
Bid Validity days (180/120/90/60/30)	120 Days
Address for Communication	**For Technical Queries:** Mr. V. Selvaraju Senior Technical Officer (Systems) Computer Centre IIT Madras Chennai - 600 036. Phone No: 044- 2257-4988 Email: selva@iitm.ac.in **For General Queries:** The Assistant Registrar Stores & Purchase Section IIT Madras Chennai – 600 036 Number 044-2257 8287, Email: adstores@iitm.ac.in.
Contact No.	For Queries : 044- 2257 8287/8288

ANNEXURE – A

Tender No. IITM/SPS/Network Firewall/031/2023-24/SPI

Network Firewall for IIT Madras

BIDDER ELIGIBILITY CRITERIA

1. The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**

2. Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure – E.**

3. The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-F.**

4. MAF - Manufacturer Authorization Form to be attached for the quoted specification **[MAF to be attached for Firewall and Analyzer]**

5. The bidder should have a service centre / local office in Chennai for the past 10 years with experts to handle Installation, Configuration and solving all types of issues in time. **[Self Declaration and proof of Registration Certificate/GST to be submitted].**

6. The firm must have an aggregate turnover of at least Rs.124 Lakhs in the last 3 years i.e. 2020-2021, 2021-2022 and 2022-2023 (should enclose the audited financial statement signed by the Chartered Accountant).

7. The vendor (OEM / Bidder) should give at least two references (attach Purchase order copy) in India where they have implemented the similar solution with 2 Gbps Internet Link & 10,000 + users in a single appliance.

TECHNICAL SPECIFICATION:-

S.No.	Technical Specification
1	**Specify the proposed solution Brand name, Model no., Supporting software package details. The quoted product should have minimum life period of 8 years.**
2	The Proposed OEM should be leaders in the gartner magic quadrant for enterprise firewall for consecutively 5 years or more. **[Gartner Certificate to be attached for consecutive years starting from 2018 to till date]**
3	The appliance based security platform should be capable of providing Firewall, Application visibility, IPS, Antivirus / Zero-day protection, Antibot, Antispam, Web filtering, DLP (Data Leak Prevention), IPSEC VPN, SSL VPN and Analyzer on VM as a Bundle.
4	The appliance should be Rack mountable with dual or quad power supply unit for redundancy and the power cord should be C18 / C13 male compatible with two meters length.
5	The Appliance should have Compatibility and interoperability with the existing infrastructure having Fortigate Firewall FG-6301F.
6	The proposed solution should have built in GUI and CLI to make on the go changes in the Firewall policies without any dependency on management for troubleshooting any issues related to network.
7	The Firewall must support Secure SD - WAN feature along with advance routing protocols such as BGP.
8	SD-WAN must be able to link and fail over between various connections such as Internet, MPLS, Leash line and even Routed based VPN interfaces.
9	Built-in SD-WAN must be able to do load balancing of various links based on source address, User group, protocol and applications.
10	SLA for SDWAN must be defined based on packet loss or latency or jitter and combination of all 3 option must be possible.
11	Central management solution for the Firewall must be able to Manage all the SDWAN link centrally and should give clear dashboard showing which links are down and which are up.
12	The proposed solution should support policy routing. Policy routing should work along with SD-WAN and ISP load-balancing.
13	The proposed solution should support identity based routing option allowing traffic to be forced out of specific Internet gateway based on authentication rather than IP address.
14	The proposed system should have integrated Traffic Shaping functionality. This feature should have option to be configured on same firewall policy along with option to configure it separately if required.
15	Built-in GUI on the system should have option to display logical topology of the network about the Firewall is protecting. The display should be able to give security recommendation for the Firewall.
16	The system should support Static routing, RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3 and BGP4+.

17	Appliance should support SFP, SFP+ and QSFP28 ports.
18	The appliance should have atleast 2 x 1G RJ45 for management, 16 x 1/10/25 GE SFP/SFP+/QSFP28 Slots, 4 x 40G QSFP28 Interfaces or more from day one.
19	The appliance should support 25,000 users and 50,000 devices.
20	Proposed platform should have future scalability and capability to deliver minimum of 60 Gbps Threat Protection throughput and 110 Gbps IPS throughput under production environment.
21	The Appliance should support Concurrent sessions (TCP) : 100 millions or more.
22	The Appliance should support New sessions per sec (TCP) : 2 millions or more.
23	The Appliance should support IPSEC VPN throughput : 90 Gbps or more and SSL-VPN throughput : 9 Gbps or more.
24	The Appliance should support 1000 VLANs or more.
25	The Appliance should support 30,000 or more concurrent SSL-VPN users.
26	The Appliance should have built in support IPSec VPN and SSL VPN.
27	IPSec VPN must include gateway to gateway and gateway to client vpn. In case of gateway to client the administrator must have option to assign private IP address to remote user without requiring any additional license.
28	Route based IPSec VPN must be supported along with SD-WAN in case of two or more ISP's.
29	The SSL-VPN should not have any user license and should have option to integrate with local LDAP server.
30	IPSec VPN and SSL VPN must support 2-factor authentication with option to have locally imported tokens on the Firewall appliance itself, if required.
31	Appliance should have 2 TB or more internal storage.
32	Device should support creating access rules with IPv4 & IPv6 objects simultaneously from day 1.
33	Firewall must support NAT policy for multi cast traffic for both IPv4 and IPv6 from day 1.
34	Appliance should support manual NAT.
35	The appliance should support DHCPv6.
36	The appliance should support Multi cast protocols like IGMP, PIM, etc.
37	The system should supports SNMP Versions 1, 2c and 3.
38	The appliance should support security policies based on group names in source or destination fields or both.
39	The appliance should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc..
40	The appliance should support Stateful firewall inspection.
41	The Appliance should support Active/Standby and Active/Active fail over.
42	The Appliance should support FQDN policy based routing. Firewall must support option to configure FQDN server rather than IP address in case server have dynamic IP address or site have multiple IP addresses for single domain.
43	The Appliance should have option to configure wild card FQDN.
44	The Appliance should have support for single sign-on (SSO) and single sign-on using a RADIUS server (RSSO).

45	Firewall policy should be single policy where all the feature get applied such as IPS, Application control , URL filtering , Antivirus , SSL inspection , Logging and NAT.
46	The appliance should be capable of tuning IDS/IPS, AV, URL Filtering (ie., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
47	The Firewall should allow policy based on port or service to protect attack at L3 not just application based policy which might be vulnerable to L3 attacks.
48	The Firewall should support Geo-based IP address blocking.
49	DNS translation option must be available in Firewall to change only the specific DNS reply from public to private IP. This is required for allowing user to access local resources using Private IP rather than there public IP address.
50	Built-in GUI/CLI support option to configure firewall policy which allow packet capture for troubleshooting purposes.
51	The security appliance should be having configurable option to quarantine attack generating source address for a defined duration.
52	There must be option to configure the said Firewall policy from GUI without requiring any Management solution.
53	The appliance Should be capable of automatically providing appropriate inspections and protections for traffic sent over non-standard communications ports.
54	The appliance should be able to link Active Directory and LDAP user names to IP addresses related to suspected security events.
55	The appliance should have inbuilt antivirus detection and should be able to quarantine the IP for a defined duration and display the preset message and should be able to restrict access of infected host. The Solution should prevent malware based threats.
56	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation IP addresses determined by the proposed security vendor.
57	The appliance must support URL and DNS threat feeds to protect against threats.
58	The appliance should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 65 categories from day one.
59	The appliance should support more than 2500 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
60	The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.
61	The detection engine should have the capability of detecting and preventing a wide variety of threats (ex., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
62	The appliance should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
63	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided and it must support scalability to 200 Virtual Firewalls.
64	Virtualization must be for every feature which are IPS , Application control, Antivirus/Anti-malware , URL filtering , SSL inspection , SSL VPN, IPSec VPN, Traffic

	shaping and user authentication.
65	Enabling Virtualization shouldn't require any kind of downtime or reboot. It must be done seamless even if the FW is live in the network.
III	**Intrusion Prevention System**
1	The IPS detection methodologies shall consist of: a) Signature based detection using real time updated database. b) Anomaly based detection that is based on thresholds.
2	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available.
3	In the event of IPS cease to function, network traffic should not be blocked. It should be configurable. This means that crucial network traffic should not be blocked and the Firewall will continue to operate till the problem is resolved.
4	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. It should have flexibility to configure IPv4 and IPv6 Rate based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/ port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding. Threshold settings must be customizable for different sources, destinations & services.
5	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident.
6	Signatures should have a severity level defined to it. It helps the administrator to understand and decide which signatures to be enabled for what traffic (e.g. for severity level: high, medium, low).
IV	**Antivirus**
1	Firewall should have integrated Antivirus solution.
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy or based on firewall authenticated user groups with configurable selection of the following services: a) HTTP, HTTPS b) SMTP, SMTPS c) POP3, POP3S d) IMAP, IMAPS e) FTP, FTPS
3	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
V	**Web Content Filtering**
1	The proposed system should have integrated Web Content Filtering solution without external solution / devices / hardware modules.
2	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
3	The proposed system should provide the following web content filtering features: a) blocking web plug-ins such as ActiveX, Java Applet and Cookies. b) Shall include Web URL block. c) Shall include score based web keyword block. d) Shall include Web Exempt List.

VI	**Application Control**
1	The proposed system shall have the ability to detect, log and take action against network traffic based on over 4,000 application signatures.
2	The application signatures shall be manual or automatically updated.
3	The administrator shall be able to define application control list based on selectable application group or list and its corresponding actions.
4	Application control and URL filtering must work independent of each other.
5	The proposed solution should support AAA solution for user authentication
6	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection and behavioral anomaly detection techniques. Support to Identify and explain each type of detection mechanism.
7	The device should have inbuilt antibot and should prevent clients from contacting C&C.
8	The appliance should not allow clients contacting malware infected domains.
9	Appliance should be able to share threat intelligence with other security components in the network natively.
10	Solution should have inbuilt application control.
11	Solution should support scanning the files for threats with file size starting from KB to 500 MB.
12	The appliance should support interface based polices and should have policy for multiple interfaces bundled together.
13	Should have inbuilt DNS filter to provide DNS based security.
14	Should have integration for Domain and IP Reputation based protection.
15	Solution should be able to exchange threat intelligence with other components like WAF/NAC/SIEM etc..
16	Solution should support device based / IP based restriction.
17	Proposed solution should have SSL/SSH inspection.
18	Should be able to download and update firmware from the firewall.
19	The management must be accessible via web-based interface without any additional client software.
VII	**High Availability**
1	The proposed system shall have built-in high availability (HA) features without extra cost/license.
2	The device shall support stateful session maintenance in the event of fail-over to a standby unit.
3	High Availability Configurations should support Active/Active or Active/ Passive.
VIII	**Centralized Logging & Reporting Solution (Analyzer)**
1	The solution should deliver complete security oversight with granular graphical reporting.
2	The solution should provide centralized security event analysis, forensic research, reporting, content archiving, data mining and malicious file quarantining.
3	The solution should provide streamlined graphical network-wide reporting of events, activities and trends occurring on UTM / FW.
4	The solution should provide centralized logging of multiple record types including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.

5	The solution be able to provide real-time and historical logs with filtering and search capabilities.
6	The solution should be able to displays a map of the world that shows the top traffic destination country by colour.
7	The solution should provide predefined templates for building / generating reports.
8	The solution should be able to collect logs from multiple devices and push it to backup server automatically based on predefined settings.
9	The solution should be able to support threshold values to generate alerts and send it through emails.
10	The solution should be able to manually generate the report or schedule the same.
11	The solution should be able to generate report based on user name, IP Address, source / destination ports.
12	The solution should be able to process 100 GB logs per day.
13	The solution must be licensed to support minimum of 16 TB storage capacity.
14	The Centralized Logging & Reporting architecture should be software based appliance on VMWare based solution and VM hardware will be provided by IIT Madras.
15	The analyzer / reporting solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.
16	The analyzer / reporting solution must have reporting function to perform a detailed search on User Account with Downloadable format in PDF, HTML, CSV. It should support search options (User name, IP Address, Time zone).
17	The solution must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
18	The solution must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
19	The solution must provide risk reports like advanced malware attacks
20	Appliance Should support REST/API to support API integration
21	Appliance should have inbuilt web management for configuring polices, objects etc..
22	All performance numbers mentioned in the data sheet should be arrived by: 1) Enabling scan of all packets by IPS & Antivirus/zero-day protection. 2) IPS to scan all parts of session in both direction. 3) AV to scan the complete payload. 4) Complete Threat Prevention signatures to be enabled.
23	Data sheet should be submitted as proof for all specifications
24	Product supplied should be directly installed by OEM professionals / OEM Certified professionals.
25	Supplied products and licenses should be supported for 5 years warranty from the date of Installation completion by OEM.

ANNEXURE – B

PROFORMA FOR TECHNICAL COMPLIANCE SHEET

Tender No. IITM/SPS/ Network Firewall/031/2023-24/SPI

Network Firewall for IIT Madras

1. BIDDER ELIGIBILITY CRITERIA

S. No.	Description	Compliance (Yes / NO)	Reference
1	The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**		
2.	Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure –E.**		
3.	The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-F.**		
4.	MAF - Manufacturer Authorization Form to be attached for the quoted specification **[MAF to be attached for Firewall and Analyzer]**		
5.	The bidder should have a service centre / local office in Chennai for the past 10 years with experts to handle Installation, Configuration and solving all types of issues in time. **[Self Declaration and proof of Registration Certificate/GST to be submitted]**		
6.	The firm must have an aggregate turnover of at least Rs.124 Lakhs in the last 3 years i.e. 2020-2021, 2021-2022 and 2022-2023 (should enclose the audited financial statement signed by the Chartered Accountant).		
7.	The vendor (OEM / Bidder) should give at least two references (attach Purchase order copy) in India where they have implemented the similar solution with 2 Gbps Internet Link & 10,000 + users in a single appliance.		

3. TECHNICAL SPECIFICATION

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
1.	Specify the proposed solution Brand name, Model no., Supporting software package details The quoted product should have minimum life period of 8 years.		
2.	The Proposed OEM should be leaders in the gartner magic quadrant for enterprise firewall for consecutively 5 years or more. [Gartner Certificate to be attached for consecutive years starting from 2018 to till date]		
3.	The appliance based security platform should be capable of providing Firewall, Application visibility, IPS, Antivirus / Zero-day protection, Antibot, Antispam, Web filtering, DLP (Data Leak Prevention), IPSEC VPN, SSL VPN and Analyzer on VM as a Bundle.		
4.	The appliance should be Rack mountable with dual or quad power supply unit for redundancy and the power cord should be C18 / C13 male compatible with two meters length.		
5.	The Appliance should have Compatibility and interoperability with the existing infrastructure having Fortigate Firewall FG-6301F.		
6.	The proposed solution should have built in GUI and CLI to make on the go changes in the Firewall policies without any dependency on management for troubleshooting any issues related to network.		
7.	The Firewall must support Secure SD - WAN feature along with advance routing protocols such as BGP.		
8.	SD-WAN must be able to link and fail over between various connections such as Internet, MPLS, Leash line and even Routed based VPN interfaces.		
9.	Built-in SD-WAN must be able to do load balancing of various links based on source address, User group, protocol and applications.		
10.	SLA for SDWAN must be defined based on packet loss or latency or jitter and combination of all 3 option must be possible.		
11.	Central management solution for the Firewall must be able to Manage all the SDWAN link centrally and should give clear dashboard showing which links are down and which are up.		
12.	The proposed solution should support policy routing. Policy routing should work along with SD-WAN and ISP load-balancing.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
13.	The proposed solution should support identity based routing option allowing traffic to be forced out of specific Internet gateway based on authentication rather than IP address.		
14.	The proposed system should have integrated Traffic Shaping functionality. This feature should have option to be configured on same firewall policy along with option to configure it separately if required.		
15.	Built-in GUI on the system should have option to display logical topology of the network about the Firewall is protecting. The display should be able to give security recommendation for the Firewall.		
16.	The system should support Static routing, RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3 and BGP4+.		
17.	Appliance should support SFP, SFP+ and QSFP28 ports.		
18.	The appliance should have atleast 2 x 1G RJ45 for management, 16 x 1/10/25 GE SFP/SFP+/QSFP28 Slots, 4 x 40G QSFP28 Interfaces or more from day one.		
19.	The appliance should support 25,000 users and 50,000 devices.		
20.	Proposed platform should have future scalability and capability to deliver minimum of 60 Gbps Threat Protection throughput and 110 Gbps IPS throughput under production environment.		
21.	The Appliance should support Concurrent sessions (TCP) : 100 millions or more.		
22.	The Appliance should support New sessions per sec (TCP) : 2 millions or more.		
23.	The Appliance should support IPSEC VPN throughput : 90 Gbps or more and SSL-VPN throughput : 9 Gbps or more.		
24.	The Appliance should support 1000 VLANs or more.		
25.	The Appliance should support 30,000 or more concurrent SSL-VPN users.		
26.	The Appliance should have built in support IPSec VPN and SSL VPN.		
27.	IPSec VPN must include gateway to gateway and gateway to client vpn. In case of gateway to client the administrator must have option to assign private IP address to remote user without requiring any additional license.		
28.	Route based IPSec VPN must be supported along with SD-		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
	WAN in case of two or more ISP's.		
29.	The SSL-VPN should not have any user license and should have option to integrate with local LDAP server.		
30.	IPSec VPN and SSL VPN must support 2-factor authentication with option to have locally imported tokens on the Firewall appliance itself, if required.		
31.	Appliance should have 2 TB or more internal storage.		
32.	Device should support creating access rules with IPv4 & IPv6 objects simultaneously from day 1.		
33.	Firewall must support NAT policy for multi cast traffic for both IPv4 and IPv6 from day 1.		
34.	Appliance should support manual NAT.		
35.	The appliance should support DHCPv6.		
36.	The appliance should support Multi cast protocols like IGMP, PIM, etc.		
37.	The system should supports SNMP Versions 1, 2c and 3.		
38.	The appliance should support security policies based on group names in source or destination fields or both.		
39.	The appliance should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc..		
40.	The appliance should support Stateful firewall inspection.		
41.	The Appliance should support Active/Standby and Active/Active fail over.		
42.	The Appliance should support FQDN policy based routing. Firewall must support option to configure FQDN server rather than IP address in case server have dynamic IP address or site have multiple IP addresses for single domain.		
43.	The Appliance should have option to configure wild card FQDN.		
44.	The Appliance should have support for single sign-on (SSO) and single sign-on using a RADIUS server (RSSO).		
45.	Firewall policy should be single policy where all the feature get applied such as IPS, Application control , URL filtering , Antivirus , SSL inspection , Logging and NAT.		
46.	The appliance should be capable of tuning IDS/IPS, AV, URL Filtering (ie., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
47.	The Firewall should allow policy based on port or service to protect attack at L3 not just application based policy which might be vulnerable to L3 attacks.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
48.	The Firewall should support Geo-based IP address blocking.		
49.	DNS translation option must be available in Firewall to change only the specific DNS reply from public to private IP. This is required for allowing user to access local resources using Private IP rather than there public IP address.		
50.	Built-in GUI/CLI support option to configure firewall policy which allow packet capture for troubleshooting purposes.		
51.	The security appliance should be having configurable option to quarantine attack generating source address for a defined duration.		
52.	There must be option to configure the said Firewall policy from GUI without requiring any Management solution.		
53.	The appliance Should be capable of automatically providing appropriate inspections and protections for traffic sent over non-standard communications ports.		
54.	The appliance should be able to link Active Directory and LDAP user names to IP addresses related to suspected security events.		
55.	The appliance should have inbuilt antivirus detection and should be able to quarantine the IP for a defined duration and display the preset message and should be able to restrict access of infected host. The Solution should prevent malware based threats.		
56.	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation IP addresses determined by the proposed security vendor.		
57.	The appliance must support URL and DNS threat feeds to protect against threats.		
58.	The appliance should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 65 categories from day one.		
59.	The appliance should support more than 2500 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
60.	The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
61.	The detection engine should have the capability of detecting and preventing a wide variety of threats (ex., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
62.	The appliance should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
63.	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided and it must support scalability to 200 Virtual Firewalls.		
64.	Virtualization must be for every feature which are IPS , Application control, Antivirus/Anti-malware , URL filtering , SSL inspection , SSL VPN, IPSec VPN, Traffic shaping and user authentication.		
65.	Enabling Virtualization shouldn't require any kind of downtime or reboot. It must be done seamless even if the FW is live in the network.		
III	Intrusion Prevention System		
1	The IPS detection methodologies shall consist of: a) Signature based detection using real time updated database. b) Anomaly based detection that is based on thresholds.		
2	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available.		
3	In the event of IPS cease to function, network traffic should not be blocked. It should be configurable. This means that crucial network traffic should not be blocked and the Firewall will continue to operate till the problem is resolved.		
4	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. It should have flexibility to configure IPv4 and IPv6 Rate based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/ port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding. Threshold settings must be customizable for different sources, destinations & services.		
5	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
6	Signatures should have a severity level defined to it. It helps the administrator to understand and decide which signatures to be enabled for what traffic (e.g. for severity level: high, medium, low).		
IV	Antivirus		
1	Firewall should have integrated Antivirus solution.		
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy or based on firewall authenticated user groups with configurable selection of the following services: a) HTTP, HTTPS b) SMTP, SMTPS c) POP3, POP3S d) IMAP, IMAPS e) FTP, FTPS		
3	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
V	Web Content Filtering		
1	The proposed system should have integrated Web Content Filtering solution without external solution / devices / hardware modules.		
2	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.		
3	The proposed system should provide the following web content filtering features: a) blocking web plug-ins such as ActiveX, Java Applet and Cookies. b) Shall include Web URL block. c) Shall include score based web keyword block. d) Shall include Web Exempt List.		
VI	Application Control		
1	The proposed system shall have the ability to detect, log and take action against network traffic based on over 4,000 application signatures.		
2	The application signatures shall be manual or automatically updated.		
3	The administrator shall be able to define application control list based on selectable application group or list and its corresponding actions.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
4	Application control and URL filtering must work independent of each other.		
5	The proposed solution should support AAA solution for user authentication		
6	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection and behavioral anomaly detection techniques. Support to Identify and explain each type of detection mechanism.		
7	The device should have inbuilt antibot and should prevent clients from contacting C&C.		
8	The appliance should not allow clients contacting malware infected domains.		
9	Appliance should be able to share threat intelligence with other security components in the network natively.		
10	Solution should have inbuilt application control.		
11	Solution should support scanning the files for threats with file size starting from KB to 500 MB.		
12	The appliance should support interface based polices and should have policy for multiple interfaces bundled together.		
13	Should have inbuilt DNS filter to provide DNS based security.		
14	Should have integration for Domain and IP Reputation based protection.		
15	Solution should be able to exchange threat intelligence with other components like WAF/NAC/SIEM etc..		
16	Solution should support device based / IP based restriction.		
17	Proposed solution should have SSL/SSH inspection.		
18	Should be able to download and update firmware from the firewall.		
19	The management must be accessible via web-based interface without any additional client software.		
VII	High Availability		
1	The proposed system shall have built-in high availability (HA) features without extra cost/license.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
2	The device shall support stateful session maintenance in the event of fail-over to a standby unit.		
3	High Availability Configurations should support Active/Active or Active/ Passive.		
VIII	Centralized Logging & Reporting Solution (Analyzer)		
1	The solution should deliver complete security oversight with granular graphical reporting.		
2	The solution should provide centralized security event analysis, forensic research, reporting, content archiving, data mining and malicious file quarantining.		
3	The solution should provide streamlined graphical network-wide reporting of events, activities and trends occurring on UTM / FW.		
4	The solution should provide centralized logging of multiple record types including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.		
5	The solution be able to provide real-time and historical logs with filtering and search capabilities.		
6	The solution should be able to displays a map of the world that shows the top traffic destination country by colour.		
7	The solution should provide predefined templates for building / generating reports.		
8	The solution should be able to collect logs from multiple devices and push it to backup server automatically based on predefined settings.		
9	The solution should be able to support threshold values to generate alerts and send it through emails.		
10	The solution should be able to manually generate the report or schedule the same.		
11	The solution should be able to generate report based on user name, IP Address, source / destination ports.		
12	The solution should be able to process 100 GB logs per day.		
13	The solution must be licensed to support minimum of 16 TB storage capacity.		
14	The Centralized Logging & Reporting architecture should be software based appliance on VMWare based solution and VM hardware will be provided by IIT Madras.		
15	The analyzer / reporting solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.		

S.No.	Technical Specification	Compliance YES/NO	Reference (URL Address with page no. / data sheet with page no.)
16	The analyzer / reporting solution must have reporting function to perform a detailed search on User Account with Downloadable format in PDF, HTML, CSV. It should support search options (User name, IP Address, Time zone).		
17	The solution must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
18	The solution must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
19	The solution must provide risk reports like advanced malware attacks		
20	Appliance Should support REST/API to support API integration		
21	Appliance should have inbuilt web management for configuring polices, objects etc..		
22	All performance numbers mentioned in the data sheet should be arrived by: 1) Enabling scan of all packets by IPS & Antivirus/zero-day protection. 2) IPS to scan all parts of session in both direction. 3) AV to scan the complete payload. 4) Complete Threat Prevention signatures to be enabled.		
23	Data sheet should be submitted as proof for all specifications		
24	Product supplied should be directly installed by OEM professionals / OEM Certified professionals.		
25	Supplied products and licenses should be supported for 5 years warranty from the date of Installation completion by OEM.		

**** Reference page number is mandatory and should be mentioned in the technical compliance***

SIGNATURE OF TENDERER ALONG WITH SEAL OF THE COMPANY WITH DATE

ANNEXURE – C

PROFORMA FOR FINANCIAL BID (BoQ)

Tender No. IITM/SPS/ Network Firewall/031/2023-24/SPI

Network Firewall for IIT Madras

S. No.	Detailed Description as per Annexure-B	Unit	Qty	Quoted Currency in INR/USD/EUR	Unit Rate in Figures, to be entered by the Bidder in INR (or) Ex-works rate for USD/EUR	GST/CIP Chennai charges	Total Amount incl.of GST/CIP Chennai charges*
					(A)	(B)	
1	**Network Firewall with supported Analyzer on VM as a bundle with 5 years warranty**		**1**				
2	**10 Gbps SFP+ or compatible Transceiver module Short Range should be Firewall OEM brand**		**4**				
3	**10 Gbps SFP+ Transceiver module Short Range compatible to WS-C6807 – should be SFP – 10G-SR-S Module.**		**4**				
4	AMC for 6th year for serial no. 1 and 2 including failed hardware replacement with 8x5xNBD support				**ENTER AND SUBMIT THE FINANCIAL BID IN THE CPP(e-PROCURMENT PORTAL)**		
5	AMC for 7th year for serial no. 1 and 2 including failed hardware replacement with 8x5xNBD support						
6	AMC for 8th year for serial no. 1 and 2 including failed hardware replacement with 8x5xNBD support						
7	LESS: Buyback of Fortigate Firewall FW-3200D		1				
Total Cost after deducting buyback value							

NOTE:

*The rate should be inclusive of transporting, loading and unloading.

* The value including AMC and after deducting Buyback value will be considered for arriving L1.

Place:
Date:

SIGNATURE OF TENDERER ALONG WIT
SEAL OF THE COMPANY WITH DATE

ANNEXURE D

(To be given on the letter head of the bidder)

Tender No. IITM/SPS/ Network FIREWALL/GTE/031/2023-24/SPI

Dated: ________________

CERTIFICATE

(Bidders from India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I am not from such a country.

OR

(Bidders from Country which shares a land border with India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I am from ___________________ (Name of Country) and have registered with the Competent Authority. I also certify that I fulfil all the requirements in this regard and am eligible to be considered. *(Copy/ evidence of valid registration by the Competent Authority is to be attached)*

Place:	**Signature of the Bidder**
Date:	**Name & Address of the**
	Bidder with Office Stamp

ANNEXURE - E

(To be given on the letter head of the bidder)

Self-Declaration that the Service Provider has not been Black listed

I …… S/o …………………………………………………………

R/o …………………………… police station ……………… District …………………………. ……………………………………… Director

/ Partner/ sole proprietor (Strike out whichever is not applicable) of ……………………………………………………………….………

………………………………………. (Firm or Company) do hereby declare and solemnly affirm:

I. That the Firm …………………………………………………………………… ……………………. has not been Blacklisted or declared insolvent by any of the Union or State Government / Organization.

II. That none of the individual / firm / Company Blacklisted or any partners or shareholder thereof has any connection directly or indirectly with or has any subsistence interest in the deponent business / firm company.

III. That neither the Firm nor any of its partner has been involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police.

Place:
Date:

Signature of the Tenderer
Name & Address of the
Tenderer with Office Stamp

ANNEXURE –F

OEM CERTIFICATION FORM

(in Original Letter Head of OEM)

Tender No: .... Dated: ....

We are Original Equipment Manufacturers (OEM) of... (Name of the company)

Ms.. (Name of the vendor) is one of our Distributors/Dealers/Resellers/Partners (tick one) for the ………………………………………………………………… and is participating in the above mentioned tender by offering our product model..(Name of the product with model number).

………………………………………………………………. is authorized to bid, sell and provide service support warranty for our product as mentioned above.

Name and Signature of the authorized

signatory of OEM along with

seal of the company with Date

ANNEXURE – G

FORMAT FOR AFFIDAVIT OF SELF-CERTIFICATION UNDER PUBLIC PROCUREMENT POLICY (PREFERENCE TO MAKE IN INDIA) 2017

Tender No. Tender No. IITM/SPS/ Network FIREWALL /GTE/031/2023-24/SPI

Name of the item / Service: Network FIREWALL at IIT Madras

Date: ___________

I/We ____S/o, D/o, W/o, _______________________________
Resident of ____
Hereby solemnly affirm and declare as under:

That I will agree to abide by the terms and conditions of the Public Procurement (Preference to Make in India) Policy vide GoI Order no. P-45021/2/2017-PP (B.E.-II) dated 15.06.2017 (subsequently revised vide orders dated 28.05.2018, 29.05.2019and 04.06.2020) MOCI order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P-45021/102/2019-BE-II-Part (1) (E-50310) Dt.4th March 2021 and any subsequent modifications/Amendments, if any and

That the local content for all inputs which constitute the said item/service/work has been verified by me and I am responsible for the correctness of the claims made therein.

Tick (✓) and Fill the Appropriate Category	
□	I/We______________________[name of the supplier] hereby confirm in respect of quoted items thatLocal Content is equal to or more than 50% and come under **“Class-I Local Supplier”** category.
□	I/We______________________[name of the supplier] hereby confirm in respect of quoted items that Local Content is equal to or more than 20% but less than 50% and come under **“Class-II Local Supplier”** category.

The details of the location (s) at which the local value addition is made and the proportionate value of local content in percentage

Percentage of Local content : _________ %**

Location at which value addition done : ____

____

____

For and on behalf of.. (Name of firm/entity)

Authorized signatory (To be duly authorized by the Board of Directors)
<Insert Name, Designation and Contact No.>

[Note: In case of procurement for a value in excess of Rs. 10 Crores, the bidders shall provide this certificate from statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.]

This letter should be on the letterhead of the quoting firm and should be signed by a competent authority.

*** Services such as transportation, insurance, installation, commissioning, and training and after sales service support like AMC/CMC cannot be claimed as local value addition*