



TAMIL UNIVERSITY, THANJAVUR

Tender Document
For

Extension of the Existing Network of the Tamil University
(Supply, Installation and Commissioning for restructuring of Local
Area Network in Tamil University University Campus)

Tender Number: 16/2022-2023/Grant
The Registrar (i/c).,
Tamil University, Thanjavur, Tamilnadu

January - 2023

TENDER NOTICE

Office of Issue	The Registrar (i/c), Tamil University, Thanjavur – 613 010
Tender No.	16/2022-2023/Grant
Date and Time of Issue/Publishing	
Document Download/Sale Start Date & Time	
Tender Submission Start Date & Time	19.01.2023 Time :11.00AM
Tenders Submission Last Date & Time	02.02.2023 Time :5.00PM
Date and Time of opening of Technical bid	03.02.2023 Time :10.30AM
Place of opening of Technical bid	Tamil University, Registrar Section
Date of opening of Price bid	03.02.2023 Time :10.30AM

Sealed Tenders are invited on behalf of Tamil University. Tenders are invited for **the following** for Tamil University from the **Indian Companies of Original Equipment Manufacturers (OEM) or Authorized distributors / Authorized Dealers**. Prices quoted should be F.O.R. Destination, inclusive of all levies and taxes and packing & forwarding charges etc.

S.No.	Particulars
1.	1. Active & Passive Components of Networking Materials

Tenderer shall have to deposit **EMD** as detailed below in the form of Demand Draft issued by any Nationalised or scheduled banks drawn in the favour of **"The Registrar, Tamil University, Thanjavur - 613010"** along with the tender.

S.No.	Particulars	EMD Amount Rs.
1.	Active & Passive Components of Networking Materials	Rs.19,000/-

Tender Document fee is **Rs.500/-** for tender in the form of Demand Draft issued by any Nationalised or scheduled banks drawn in the favour of **"The Registrar, Tamil University, Thanjavur - 613010"** and document is available in Website www.tamiluniversity.ac.in & www.tenders.tn.gov.in **Tender Document to be submitted for the above three items.**

Registrar i/c, Tamil University, Thanjavur.

Part II**TENDER CONDITIONS****1. Introduction**

This tender is for the following for networking of University Campus of Tamil University, Thanjavur, Tamilnadu, India.

No.	Tender No.	Description
1.	16/2022-2023/Grant	1.Active & Passive Components of Networking Materials,

The specification for the above mentioned items is given in Appendix VI.

Applicability of Tamil Nadu Transparency in Tenders Act and Rules: This tender will be governed by the Tamil Nadu Transparency in Tenders Act 1998 and Rules 2000 and Rules 2018 as amended from time to time.

2. Eligibility criteria

A tenderer will be eligible for tendering only if he satisfies the eligibility criteria as given below:

- i. A tenderer should be a manufacturer possessing a valid manufacturing license from the competent authority for manufacturing the items quoted and should have at least three years experience. (Documentary evidence to be furnished)
- ii. The manufacturer should be an ISO:9001 / Equivalent certified company. Documentary evidence should be enclosed.
- iii. Authorized Dealer / Distributor / Supplier can also bid with authorization from the Manufacturer. (Documentary evidence to be furnished). A manufacturer shall not authorize more than one dealer / distributor/supplier for participating in this tender.
- iv. In case a tenderer is participating as an authorized Dealer/Distributor/Supplier, the manufacturer of the item should satisfy the conditions mentioned at (i) and (ii) above.
- v. The tenderer should have a GST Registration. Copy of the Registration Certificate should be enclosed.
- vi. The Tenderer should be an Income Tax assessee. (latest return filed should be enclosed)
- vii. The tenderer should not have been blacklisted or debarred from participating in tenders by any Central / State

- Government agencies or autonomous bodies or universities/ institutions. (An undertaking to this effect should be furnished)
- viii. The tenderer submitting their offer must have supplied/worked for similar items to other Universities or institutions or Government agencies. Copies of such order must be enclosed with the offer.
 - ix. The Tenderer should have recorded and average turnover of **Rs.1.5 Crore during the last Three financial year 2019-2020, 2021-2021, 2021-2022**
 - x. If MSME Certificate is produced EMD will be excepted.

3. Cost of Tendering

- The Tenderer **Document Fee is Rs.500/-** and may download the application format from the University Web Site.
- The Tenderer shall bear all costs associated with the preparation and submission of this Tender and the tender inviting authority will in no way be responsible or liable for these costs.

4. General Instructions

The tenderers are requested to go through the instructions, terms and conditions and specifications given in the tender. Failure to furnish all required information in every aspect will be at the tenderer's risk and may result in the rejection of the tender.

For any queries, tenderer may contact:

The Registrar i/c,
Tamil University,
Thanjavur, – 613 010.
Tamil Nadu, INDIA.

Clarification on the tender

A prospective tenderer requiring any clarification on the tender may request the Office of the Registrar, Tamil University, by a letter or by fax. The Registrar, Tamil University, will respond in writing to any request for clarification in the tender.

Amendments to the Tender

- i. Tender Inviting Authority may amend the tender wherever it is felt that such an amendment is absolutely necessary.
- ii. Amendment to tender may also be given in response to clarifications by prospective tenderers and it is solely the discretion of the Tender Inviting Authority.

Any amendment to the tender will be uploaded on the website <http://www.tamiluniversity.ac.in> and www.tenders.tn.gov.in. It is the responsibility of the tenderer to verify the amendments if any and get the amendment documents before the submission of the tender provided no such change could be effected 48 hours prior to the time fixed for opening of the tender. The Tender document is not transferable under any circumstances.

Earnest Money Deposit (EMD)

The tenderer should furnish **Earnest Money Deposit (EMD) as detailed below** along with the tender by way of Demand Draft/Bankers cheque obtained from any Nationalized/ Scheduled Bank and drawn in favour of “**The Registrar, Tamil University**” payable at **Thanjavur. Tender Document to be submitted for each item.**

S.No.	Particulars	EMD Amount Rs.
1.	Active, Accessories	Rs.19,000

Any tender without required EMD will be considered as NON-RESPONSIVE and will be summarily rejected.

The Tender Inviting Authority will arrange to refund the Earnest Money Deposit to the unsuccessful tenderers after publishing the list of successful tenderers, within a reasonable time.

No interest will be paid on the EMD. The EMD is liable to be forfeited if:

- i. The Tenderer withdraws his tender at any stage after the last date and time fixed for submitting the tender.

- ii. The Tenderer on becoming successful, fails to furnish the required security deposit or sign the agreement, within the stipulated time limit.

Performance Security :

Successful tenderer has to furnish Security Deposit equivalent to 2.5% of the tendered value in the form of Demand Draft drawn in favour of “The Registrar, Tamil University”.

Security Deposit will be released only after the expiry of the warranty period as mentioned in Part – IV - clause 1.5.

Part III

PROCEDURE FOR SUBMISSION OF TENDER

Submission of Tender:

Due Date for Tender Submission

The tender document duly filled in, signed on all pages shall be submitted in sealed cover to **the Registrar, Tamil University, at his office upto 5.00 P.M. on 02.02.2023** as per the procedure laid down herein. The tender can be submitted on all working days upto the above closing date. In the event of this day being declared as a holiday, the tenders can be submitted till 5.00 P.M. on the following working day.

The tender inviting authority will not be held responsible for any delay in the receipt of the Bank Draft or any delay in the receipt of the document by the tenderer including loss of the document in transit or delay in obtaining any document / certificate or on any other account. No extension of the date and time for the submission of the documents will be given for any such delay.

The tender inviting authority may extend the due date for submission of tender by issuing an amendment, in which case, all the rights and obligations of the Tender Inviting Authority and the Tenderers previously subject to the original due date for submission will then be subject to the new date for submission.

Any tender received by the Tender Inviting Authority **after the due date and time will not be considered and will be returned to the tenderer.**

Procedure for Submission of Tender

Tenderers are advised to go through the tender documents and understand all the provisions and stipulations contained therein before submitting the tender.

The tender shall be submitted as per the procedures and requirements stipulated herein.

Tender submitted by fax will not be accepted and will be summarily rejected.

The Commercial bid should be neatly typed. Hand written offers will be rejected. Any deviation in the offer shall lead to rejection.

The tenderer who are supplying imported material, must be registered with the Competent Authority/Department of the Government of India.

The purchaser shall not be responsible for any postal delay in receipt of the offer. Any bid received by the Purchaser which does not fulfil the required terms and conditions shall be rejected outrightly and no communication in this regard shall be sent. Delayed/Late bids will not be accepted, at any circumstances.

All the bids will be opened in the presence of bidders representatives, who, choose to attend the same as per the date and time specified in the Tender Document.

This tender is based on two-cover systems i.e. Technical bid and price bid. Therefore, the tender shall be submitted in two parts viz. Cover A and Cover B. Each part shall be placed in an independent sealed envelope and shall be superscribed as follows

Cover-A "TECHNICAL BID COVER"

1. **"TENDER FOR SUPPLY OF ACTIVE & PASSIVE COMPONENTS OF NETWORKING MATERIALS TO TAMIL UNIVERSITY"**

Cover-B “PRICE BID COVER”

1. “TENDER FOR SUPPLY OF ACTIVE & PASSIVE COMPONENTS OF NETWORKING MATERIALS TO TAMIL UNIVERSITY”

TENDER No.: 16/2022-2023/Grant

The contents of each of the two covers shall be as described in the subsequent clauses. For all other references, these covers will be referred to briefly as “**Technical Bid Cover**” and “**Price Bid Cover**”.

Both the covers i.e. Cover-A and Cover-B, shall be placed inside an outer cover and shall be superscribed as follows:

1 “TENDER FOR SUPPLY OF ACTIVE & PASSIVE COMPONENTS OF NETWORKING MATERIALS TO TAMIL UNIVERSITY”

TENDER No.: 16/2022-2023/Grant

The sealed tender envelope shall be addressed to
The Registrar i/c, Tamil University, Thanjavur – 613 010,

The tender envelope shall carry the name and address of the Tenderer prominently with Phone No. / email ID / and FAX No.

The **Technical Bid Cover (Cover-A)** shall contain the following as per the sequence indicated below.

1.	Tender Document Fee of Rs.500/- as per clause- 3 of the Tender Document
2.	Earnest Money Deposit (EMD) of as per clause-5 of the Tender document
3.	Application form for supply of equipment as per Appendix-1
4.	Documentary evidence for payment of income tax (latest income tax return should be furnished)
5.	Letter of Tender as per Appendix-2
6.	Documentary evidence for registration under GST
7.	Documentary evidence for ISO:9001 / equivalent certified company

8.	A copy of Manufacturing license/Registration Certificate
9.	Authorization from Manufacturer incase of Authorized Dealers/Distributors/Suppliers
10.	Documentary evidence of supplying similar items to other Universities/Institutions/Govt. agencies.
11.	In addition to the above any document or certificates, etc., mentioned anywhere in the tender document shall also be a part of the technical tender requirements.
12	Annual turnover of last three financial year

The **PRICE BID COVER (Cover-B)** shall contain the Price Bid as per the format given in Appendix – III.

The tenderer shall not carry out any alteration in the format prescribed for Price Bid. The tenderer shall not enclose any other document or statement that will influence the price. In such an event, the tender inviting authority shall summarily reject the tender.

1.3. Signing of the Tender

The tender shall be signed by a person or persons duly authorized to sign on behalf of the Tenderer. All pages of the tender shall be signed by the person or persons signing the tender. The tenderer shall enclose a certified copy of the power of attorney authorizing the signatory or signatories to sign the tender document. This certification shall be from the Managing Director or the Legal Manager of the firm.

The tender shall contain no alterations or additions, except those to comply with instructions issued by the Tender Inviting Authority, or as necessary to correct errors made by the tenderer, in which case such corrections shall be signed by the person or persons signing the tender.

All the pages in the tender document should be signed by the tenderer, after filling the prices in figures & words.

GENERAL TERMS AND CONDITIONS**Delivery Schedule:****The Price Quoted should be FOR Tamil University**

- Materials should be door delivered at Tamil University, Thanjavur, Tamilnadu.
- Delivery must be made within a period of 30 days from the issue of the order either directly or through their dealer network unless otherwise specified.
- If the supplier fails to deliver the equipment ordered within the allotted delivery period as specified above, the Purchaser may procure goods or services similar to those un-delivered upon such terms and in such manner as it deems appropriate from any other firm at the risk and cost of the supplier.

Payment Terms:

- Payment will be made within 30 days from the date of delivery, installations, commissioning and demonstration of the equipment and acceptance by concerned Department/ Section.
- Payment shall be made by Cheque/ PFMS or such other mode/ electronic fund transfer offered by the Bank.

Taxes & Duties :

- (DSIR) GST may be charged as applicable. Any statutory variation will be paid to supplier on documentary evidence. Supplier should clearly indicate the percentage of GST applicable.
- Clearing & forwarding charges should also be mentioned

Loss, Damage & shortage:

- Tamil University shall not be responsible for any loss, damages and shortage during transit. Payment shall be made for the ordered material received in good condition only.

Warranty

- The equipment supplied under the contract shall carry a warranty for at least Five years. Supplier shall extend free maintenance service during the warranty period.

Commissioning and Demonstration

- The Supplier shall be responsible for commissioning of the equipment. Supplier should also arrange for demonstration and Training of the equipment to the Staff of the University.

Annual Maintenance

- The University reserves the right to entrust Annual Maintenance of the equipment supplied under this tender to the concerned supplier. Therefore the tenderer shall mention the annual maintenance charges AMC/SMC in the price schedule after warranty period. Tenderer should also give a brief write up about the services to be covered under the Annual Maintenance.

General

- The acceptance of the offer will rest with the Tamil University who reserves the right to reject/accept partially or wholly the tenders received, without assigning any reason.
- Mere submission of tender/ proposal does not imply acceptance of the same at this end and the firms will be finalised only after meeting the laid down qualifying parameters for which decision of the Tender Inviting Authority / Tender Accepting Authority shall be final and binding on the parties.
- Printed terms and conditions of the applicant on their quotation Form/ Literature/ Letter etc. if any, will not be binding on the University.
- Piece-based work / extension of existing network should also be carried out as specified by the designated authorities of Tamil University as per the materials quoted.

Liquidated Damages

- Timely delivery is essence of the contract and hence should any consignment be delayed, liquidated damages at the rate 0.5% of the value of the delayed consignment, for each week or part there of shall be levied and recovered subject to maximum of 5% of total order value.

Acceptance / Rejection:

- The Tender Accepting Authority reserves the right to accept a quotation in part or in full or to reject all quotations or any of the quotations received, for non-compliance of any of the above items, conditions or instructions or for any other reason without assigning any reason thereof.

Part V**OPENING OF TENDER****Tender Opening**

- Tender will be opened in the presence of the tenderers or their authorized representative who choose to be present and the **tender scrutiny committee at 10.30 A.M. on 03.02.2023** The representative of tenderer who attend the tender opening must produce their identification proof and authorization letter from the companies / tenderer.
- In the event of the specified date of Tender opening being declared a holiday, the tenders will be opened at the same time on the next working day.
- Cover-A containing “Technical Bid” shall be opened first.
- On opening the tender, the details such as name of the tenderer, address, Tender Document Fee, EMD details, etc., will be read out.
- Tenders found without the Tender Document Fee and EMD or with an invalid or insufficient Tender Document Fee and EMD, will be summarily rejected. Unopened tenders will be returned to such tenderers.
- On verifying the Tender Document Fee and EMD, the Technical bids will be examined to decide their service suitability for the said work. Tenderers whose Technical bids are not found acceptable will be advised of the same and their sealed covers containing the respective Financial Bids will not be opened. Their EMD will also be returned to them.
- Price bids of only those tenderers whose Technical bids are substantively responsive, will be opened.

Process to be Confidential

- Information relating to the examination, clarification, evaluation and comparison of tenders and recommendations for the award of contract shall not be disclosed to tenderers or any other persons not officially concerned with such process until the award to the successful tenderer has been announced.
- **Any effort by a tenderer to influence the tender accepting authority, scrutiny / evaluation committee or its members in the processing of tenders or award decisions may result in the rejection of his tender.**

Criteria for Technical Evaluation (Evaluation of Technical Bid)

- The tender accepting authority will determine whether the tenderer has fulfilled all the tender conditions as stipulated in the tender document and whether the tender is substantially responsive or not.

- A responsive tender is one which conforms to all the terms, conditions and specifications of the tender documents without material deviation or reservation. A material deviation or reservation is one:
 - Which affects in any substantial way the scope, quality or performance of the contract.
 - Which is a substantial way is inconsistent with the Tender conditions, the tender accepting authority's rights or the Tenderers obligations under the Contract, or
 - Whose rectification would affect unfairly the competitive position of other Tenderers presenting substantively responsive Tenders.
- Tenderers who have not fulfilled the tender conditions shall be a non-responsive tender and will not be taken up for further evaluation and Price Bid opening.
- To assist the examination, evaluation and comparison of Tenders, the tender accepting authority may at its discretion, ask any tenderer for clarification on his Tender. The request for clarification and the response shall be in writing or by fax but no change in the substance of the Tender shall be so sought, offered, or permitted
- When a tender fails to be responsive, it will be rejected by the tender accepting authority and may not subsequently be made responsive by correction or addition / withdrawal of the non-conforming deviation or reservation.

Price Bid Opening and Evaluation of Price Bid

- The Tender inviting Authority will then proceed with opening of Cover-B, i.e., "PRICE BID COVER" of those tenderers whose technical bid has been found substantively responsive. The opening of the "Price Bid cover" will be done in the presence of those tenderers or their representatives who choose to be present. The Tender Inviting Authority will inform such tenderers in advance about the acceptance of their technical tender and the date and time of opening of the "Price Bid Cover".
- The tender will be evaluated based on the prices offered by the tenders for the concerned equipments/work.
- The tender who has bid the lowest evaluated price will be determined considering the following factors:-
 - the quoted price shall be corrected for arithmetical errors;
 - in cases of discrepancy between the prices quoted in words and in figures, lower of the two shall be considered;
- The evaluation shall include all central duties such as customs duty (for the imported items), central excise duty , GST, as a part of the price, as detailed below:-

- In evaluation of the price of an imported item, the price has to be determined inclusive of the customs duty;
- In evaluation of the price of articles which are subject to excise duty, the price has to be determined inclusive of such excise duty.
- **Annual Maintenance charges will not be included while evaluating the tender.**

Award of Tender

- The award of the tender shall be made strictly in accordance with the “Tamil Nadu Transparency in Tenders Act 1998 and Rules 2000 and Rules 2018 / and no deviation will be made.
- Notwithstanding anything that is said herein, the Tender Accepting Authority reserves the right to accept or reject any tender or all tenders, and to cancel the tendering process and reject all tenders, at any time prior to the award of tender, without thereby incurring any liability to the affected tenderer or tenderers or any obligation to inform the affected tenderer or tenderers on the grounds for the tender accepting authority’s action.

Notification of Award

- The tenderer whose tender has been accepted will be notified by the Tender Accepting Authority, in writing.
- Upon furnishing the security deposit by the successful tenderer or tenderers and upon signing the Agreement (Appendix-4), the EMD will be returned to the unsuccessful tenderer within a reasonable time period.

Disputes and Jurisdiction:

- Any legal disputes arising out of any breach of contract pertaining to this tender process shall be settled in the court of competent jurisdiction located within the town of Thanjavur in Tamil Nadu.

Acknowledgement:

It is hereby acknowledged that we have gone through all the conditions mentioned above and we agree to abide by them.

Date:

Signature of Tenderer

Place:

Official seal and address

Appendix-I**APPLICATION FORM FOR SUPPLY OF EQUIPMENT****NAME OF THE EQUIPMENT:****TENDER NUMBER:**

S. NO.	VENDOR DETAILS	
1	Name and Address of the Manufacturer/Firm/Vendor	
	Phone Number	
	Fax	
	E-Mail	
	Contact Person Name	
	Mobile Number	
2	Name and Address of the Local Authorized Dealer/Distributors/Supplier	
	Phone Number	
	FAX	
	E-Mail	
	Contact Person Name	
	Mobile Number	
3	GST No. of the Firm/Dealer (copy to be enclosed)	
4	PAN	
5	Tender Document Fee (DD No., Date & Amount and issuing Bank)	
6	EMD (DD No., Date & Amount and issuing Bank)	

7	Name of the University/ Government Institutes who have purchased similar equipments from your concern (attach copies)	
---	--	--

Declaration by the tenderer.

We hereby declare that all the particulars given in this application are true and complete to the best of our knowledge and belief and we will produce all the relevant documents promptly, if necessary or as and when asked for by Tamil University, Thanjavur.

We understand that information provided by us will serve as Prequalification Criteria for supply of equipment under this tender and in the event of any information being found false or incorrect or ineligibility being detected even after the award of Contract, our contract may be cancelled and all our claims may be forfeited by the Tamil University, Thanjavur.

We have read and understood all the terms and conditions of the tender and we fully agree to it.

We also declare that we will not sell our products at a lesser price to other parties than those supplied to Tamil University, Thanjavur and in the event of happening of such situation, we will be bound to refund the difference and our contract may also be cancelled at the discretion of Tamil University, Thanjavur.

We also undertake that all the terms such as Product Range, Price, Discount, Delivery/other charges, Terms of Payment and also the name/s of the Dealer/ Distributor will remain unchanged during the contract period and no alteration will be done without the approval of Tamil University, Thanjavur.

Date : Signature :

Place : Name :

Designation :

Seal of the firm :

**TENDER FOR SUPPLY OF NETWORKING MATERIALS TOTAMIL
UNIVERSITY**

LETTER OF TENDER

To

The Registrar (i/c),
Tamil University,
Thanjavur – 613 010

Sir,

Sub: Tender for Supply of Active & Passive Components of Networking Materials (or) Digging and Laying of OFC Cables (or) Accessories for the structuring materials.

- i. I / We, the undersigned do hereby tender and undertake to Supply of _____ equipment (or) ----- work to Tamil University in strict accordance with and subject to the terms and conditions set forth or mentioned in the Tender documents and appendices.
- ii. I / We have gone through the instructions in the tender and carefully read all the conditions of tender and agree to abide by all the conditions mentioned there in.
- iii. I / We hereby state that I/we have remitted (Rupees only) in the form of Demand Draft/Bankers Cheque No. Dated --- --- drawn on Bank Branch, in favour of the “Registrar, Tamil University”, as Earnest Money Deposit and agree to have it forfeited by the Tamil University in case of my / our failure to supply the equipment.
- iv. I / We hereby certify that the price offered is final and I / We will not come forward for any revision or alteration in rates quoted subsequently due to hike in prices or any other reasons. However I/We are aware of the University’s right to negotiate the discount rate while evaluating the tender.
- v. I / We confirm that our Tender is in conformity with the technical specifications and commercial terms & conditions as stipulated in the Tender Document and without any deviations whatsoever. I am / We are aware that our Tender is liable for disqualification in the event of technical and commercial deviations observed by the Tender Accepting Authority at a later date during the process of evaluation of our Tender.
- vi. I / We further declare that the information and documents furnished in the Tender submitted by us are correct and genuine. I am/We are

aware of the Tender Inviting Authority's right to forfeit the Earnest Money Deposit and / or Security Deposit and blacklisting me/us if, any information furnished by us proved to be false at the time of inspection and not complying with the tender conditions.

- vii. I/We state that I/We have not been blacklisted or debarred from participating in tenders by any Central/State Government agencies or autonomous bodies or universities / institutions.
- viii. In the event of my/our tender becoming successful, I/We undertake and agree to forward to the Registrar, Tamil University, in ten (10) days, after the notification of the acceptance of this tender has been received by us.
- ix. We undertake and agree that we will not withdraw this Tender during the period that will be required for intimation of acceptance or non-acceptance as stipulated in clause 10 of the Tender document. If I/We do so withdraw, I/We shall forfeit the Earnest Money Deposit to Tamil University. I/We agree to execute at our cost the Agreement in ten (10) days after the notification of the acceptance of our Tender has been received by us. In the event of our failing to make the Security Deposit or to execute the Agreement in the said manner, the Earnest Money Deposit accompanying this Tender shall be forfeited to the Tamil University and this concluded Contract shall in such case be considered as having been cancelled or terminated and I/We agree to be liable, irrespective of the forfeiture aforesaid for all damages, losses, costs, charges and expenses arising from or by reason of such failure and arrangements.

As witness our hand this.....day of.....of 2023.

Signature of the Tenderer :

Name & Address :

Company Seal :

Appendix – III (A)COMMERCIAL QUOTE

Name of the Work: Supply, Installation and Commissioning of Firewall and
Network Accessories

S. No.	Material Description	Technical Details	Qty	Rate/ Unit	Total Cost
1.	Firewall	Firewall Security Appliance - IN power cord equivalent to existing CYberoam CR300ING	1 No		
2.	Router	Layer 2 or Layer 3 Switch. Should have 2x100/1000 Base X/SFP/ WAN Ports, min 2 Lan Port	1 No		
3.	Core Switch	Layer 3 Core switch with min 6 1/10G SFP+ ports and Min 6 Copper ports	1 No		
4.	Distribution switch	Layer 2 Distribution switch with Min 12 1/10G SFP+ ports uplink supporting 10G/40 G	1 No		
5.	24 port Edge Access Switch	Edge switch containing 24 port copper port with min 2 SFP uplink ports supporting 1 G/10G ports	30 No's		
6.	LX Copper Modules	10G/1G LX Copper Modules that suits the Above L2 & L3 Switches	10 No's		
7.	LX Fiber Modules	10G/1G LX SFP Modules that suits the Above L2 & L3 Switches	60 No's		
8.	OFC Patch	AMP SC-SC OFC Patch Cord	10 No's		
9.	OFC Patch	AMP LC-LC OFC Patch Cord	5 No's		
10.	OFC Patch	AMP SC-LC OFC Patch Cord	60 No's		

Name of the Work: Supply, Installation and Commissioning of Firewall and Network Accessories

Technical Specification :

General Requirements

Proposed NGFW OEM must be Leader in Gartner Magic Quadrant for Enterprise Network NGFW's in last 3 years and must have achieved at least 95% of security effectiveness in NSS Labs Breach Prevention Systems report 2019.

1. Firewall with Xstream protection with throughput 1.4GBPS

Sl No	Features	Compliance (Yes/No)
1	The proposed solution shouldn't use any proprietary ASIC hardware for any kind of performance Improvement. The solution should be completely based on multi-core CPU for effective use of compute.	
2	The solution must have Firewall, Application visibility and control, IPS, Anti-virus, Anti-malware, Anti-bot and URL filtering capabilities from day one. The operating system of the solution proposed must not have any backdoor vulnerability identified in last 3 years.	
3	Licensing should be a per device and not user/IP based (should support unlimited users)	
4	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	
5	The Proposed solution must be in HA mode from Day one.	
Hardware and Interface Requirements		
6	The proposed solution must be supplied with minimum 8 X 1G RJ 45 ports and 4 X 10G SFP+. The proposed solution should be highly scalable and should be able to scale up if needed without replacing the existing appliances. The 10G ports must either be populated with 10GBaseSR SFP+ optics or 10GBase SFP+ DAC cables having 3 meters length.	
7	The appliance must be supplied with minimum	

	240 GB internal SSD based storage	
8	Proposed appliances must be supplied with minimum 16 GB RAM from day one and should be scalable to double in future.	
Performance Requirements		
9	NGFW (IPS with Bi-Directional Scan + Application Control+ Firewall features enabled) Throughput must be minimum 5 Gbps tested under an enterprise traffic condition with protocol mix of multiple packet sizes and not just one particular packet size. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance	
10	The proposed solution should be provided at least 2.5 Gbps of throughput after enabling anti-virus, URL filtering and Malware Inspection under an enterprise traffic condition with protocol mix of multiple packet sizes and not just one particular packet size. The proposed solution must have the capability of linearly increasing the throughput to at least 5 times in future in case additional compute is procured in future to enhance the performance. In case of scalability with multiple appliances, the solution framework should be configurable with N + 1 Redundancy.	
11	The proposed appliance must provide at least 2 Gbps of VPN throughput	
12	The proposed appliance must support at least 4 Million concurrent connection from day one and should be scalable to double. The solution must support at least 80,000 new connections per second.	
Architecture Features		
13	Proposed appliance must support configuration minimum 2 nos. virtual firewall/contexts from day one and should be scalable to support at least 20 virtual instances in future.	
14	NGFW system should support virtual tunnel interfaces to provision Route-Based IPsecVPN	
15	It should support the system authentication with RADIUS and local authentication. Both should work simultaneously.	

Solution Filtering Requirements		
16	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with custom ports	
17	the solution must have an Internal CA and External third-party CA must be supported	
18	Solution must support 3DES and AES-256 cryptographic for IKE Phase I and II IKEv2 plus "" and "Suite-B-GCM-256" for phase II	
19	Solution must support at least the following Diffie-Hellman Groups: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20	
20	Solution must support data integrity with md5, sha1 SHA-256, SHA-384 and AES-XCBC	
21	The NGFW should have no limit for firewall policies	
22	The IPS should scan all parts of the session in both directions and should be able to scan the complete file during the transit.	
23	The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.	
24	IPS should have the functionality of GeoProtection to Block the traffic country wise in incoming direction, outgoing direction or both. IPS also should alert through Mail if any IPS traffic/event detected from Specific Country.	
25	NGFW Should support Identity Access for Granular user, group and machine-based visibility and policy enforcement	
26	IPS should be able to detect and prevent imbedded threats within in SSL traffic.	
27	The solutions should support automated machine learning based detection engines	
28	The solution should allow for third party signature import such as Snort	
29	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	

30	IPS must have a software-based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
31	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
32	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
33	Solution must provide VOIP protocols protections	
34	IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunnelling over HTTP traffic.	
35	Solution must be able to create a filtering rule with multiple categories.7	
36	Solution must be able to create a filtering for single site being supported by multiple categories.	
37	Solution must have users and groupsgranularity with security rules	
38	The solution must have an easy to use, searchable interface for applications and URLs	
39	The solution must categorize applications and URLs. In addition, the solution should also support applications by Risk Factor	
40	The application control and URLF security policy must be able to be defined by user identities	
41	The application control and URLF database must be updated by a cloud-based service	
42	The solution must have unified application control and URLF security rules	
43	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
44	The solution must allow network exceptions based on defined network objects	
45	The solution must provide the option to modify the Blocking Notification and to redirect the userto a remediation page	
46	Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category	
47	Solution must have a configurable bypass mechanism	
48	Solution must provide an override mechanismon the categorization for the URL database	

49	The application control and URLF security policy must report on the rule hit count	
50	DNS based attacks: The solution should have detection and prevention capabilities for C&C DNS hide outs: -Look for C&C traffic patterns, not just at their DNS destination -Reverse engineer malware in order to uncover their DGA (Domain Name Generation) -DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	
51	The solution should have detection and prevention capabilities for DNS tunnelling attacks	
52	Anti-Bot and Anti-Virus policy must be administered from a central console	
53	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
54	Anti-virus application must be able to prevent access to malicious websites	
55	Anti-virus application must be able to inspect SSL encrypted traffic	
56	Anti-Bot and Anti-Virus must be having real time updates from a cloud-based reputation service	
57	Anti-Virus must be able to stop incoming malicious files	
58	Anti-Virus must be able to scan archive files	
59	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement	
60	The Solution offers support for SSL Inspection/Decryption with leading performance across all threat mitigation technologies	
61	The solution should support Perfect Forward Secrecy (PFS , ECDHE cipher suites)	
62	The solution should support AES-NI, AES-GCM for improved throughput	
63	Internal CA and External third-party CA must be supported	
64	Solution must support 3DES and AES-256 cryptographic for IKE Phase I and II IKEv2 plus "" and "Suite-B-GCM-256" for phase II	
	Solution must support at least the following	

65	Diffie-Hellman Groups: Group 1 (768 bit), Group2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20	
66	Solution must support data integrity with md5, sha1 SHA-256, SHA-384 and AES-XCBC	
	Solution must include support for site-to-site VPN in the following topologies:	
67	Full Mesh (all to all),	
68	Star (remote offices to central site)	
69	Hub and Spoke (remote site through central site to another remote site)	
70	Solution must support the VPN configuration with a GUI using drag and drop object to VPN communities	
71	Solution must support clientless SSL VPNs for remote access.	
72	Solution must support L2TP VPNs, including support for iPhone L2TP client	
73	Solution must allow the administrator to apply security rules to control the traffic inside the VPN	
74	Solution must include the ability to establish VPNs with gateways with dynamic public IPs	
75	The solution should support future integration with on-premise or cloud-based sandbox for prevention of APT attacks	
76	The solution should detect the attack at the exploitation stage	
77	The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created	
78	The solution must provide Real-Time Prevention-unknown malware in web and mail traffic	
79	Solution must include a Zero-hour protection mechanism for new viruses spread without relying solely in heuristic or content inspection	
80	The solution should have a real-time capability to eliminate unknown threats and remove exploitable content, including active content and embedded objects and deliver safe content to the users.	
81	Solution must include IP compression for client- to-site and site-to-site VPNs	

Management, logging and reporting		
82	The management solution should be appliance based centralized management dashboard along with correlated logging and reporting.	
83	Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant segment	
84	Solution must be able to segment the rule base in favour of delegation of duties in which changes in one segment will not affect other segments	
85	Solution must be able to segment the rule base in a layered structure	
86	Security management application must support role-based administrator accounts. For instance, roles for firewall policy management only or role for log viewing only. The log Viewer should support text-based log search for easier operation.	
87	Solution must combine policy configuration and log analysis in a single pane, in order to avoid mistakes and achieve confidence of the change.	
88	The proposed solution should have complete customization of overviews and reports generation for every logged event in every security field	
89	Solution must include an automatic packet capture mechanism for IPS events to provide better forensic analysis	
90	Solution must support adding exceptions to IPS enforcement from the log record	
91	Solution must include a graphical monitoring interface that provides an easy way to monitor gateways status	
92	Solution must provide the following system information for each gateway: OS, CPU usage, memory usage, all disk partitions and % of free hard disk space	
93	Solution must include a tool to correlate events from all the gateway features	
94	Solution must allow the creation of filters based on any characteristic of the event such as security application, source and destination IP, service, event type, event severity attack name, country of origin and destination, etc.	

95	Upon malicious files detection, a detailed report should be generated for each one of the malicious files. The details report should include but not limited to Screen Shots, timelines, registry key creation/modifications, file and process creation, network activity detected	
96	The application must support a mechanism to assign these filters to different graph lines that are updated in regular intervals showing all events that matches that filter. Allowing the operator to focus on the most important events	
97	The event correlation application must support a graphical view events based on time	
98	Solution must show the distribution of events per country on a map	
99	Solution must allow the administrator to group events based on any of its characteristics, including many nesting levels and export to PDF	
100	Solution must include the option to search inside the list of events, drill down into details for research and forensics.	
101	It the event list view Solution must include the option to automatically generate small graphs or tables with the event, source and destination distribution	
102	Solution must detect Denial of Service attacks correlating events from all sources	
103	Solution must detect an administrator login at irregular hour	
104	Solution must detect credential guessing attacks	
105	Solution must report on all security policy installations	
106	Solution must include predefined hourly, daily, weekly and monthly reports. Including at least Top events, Top sources, Top destinations, Top services, Top sources and their top events, Top destinations and their top events and Top services and their top events	
107	Solution must support automatic reports scheduling for information that need to extract on regular basis (daily, weekly, and monthly). Solution must also allow the administrator to define the date and time that reporting system begins to generate the scheduled report	
108	Solution must support the following reports formats: PDF & Excel	

109	Solution must support automatic report distribution by email, upload to FTP/Web server and an external custom report distribution script	
110	Upon malicious files detection, a detailed report should be generated for each one of the malicious files. The details report should include but not limited to Screen Shots, timelines, registry key creation/modifications, file and process creation, network activity detected	
Services and Support		
111	The complete solution should be provided with comprehensive warranty, subscription and support for 3 years.	

2. Router

Router		
Sl.No.	Description	Whether Complied (Yes/No)
		Model
1	<i>Hardware and interface requirements</i>	
1.1	The Router should be a Layer 3 or layer 2 switch with all required hardware and software to meet below specifications	
1.2	should have 2 x 100/1000BaseX /SFP WAN ports and minimum 2 Lan port additional free slots for future expansion in a single switch	
1.3	should have minimum 512 mb DRAM and 2/4 gb Maximum	
1.4	should support Compact External Flash	
2	<i>Performance requirements</i>	
2.1	Should support wirespeed switching throughput of minimum 912 Mbps	
2.2	Should support distributed Layer 2 and Layer 3 forwarding	
3	<i>Quality of Service (QoS) requirements</i>	
3.1	should support Layer 2 IEEE 802.1p (class of service [CoS])	
3.2	Should have minimum 12 hardware queues per port	
3.3	Should support Layer 2 classification based on Interface, MAC address, Ethertype, 802.1p and VLAN	
3.4	should support tail drop ,WRED for congestion avoidance	
4	<i>System Management and Administration</i>	

4.1	Switch management using 10/100/1000-Mbps management or console ports	
4.2	CLI-based console to provide detailed out-of-band management	
4.3	Switch should support DHCP server and relay for both IPv4 and v6	
4.4	Switch should support Configuration rollback and image rollback	
4.5	Switch should support Secure Shell Version 2 (SSHv2) & Telnet	
4.6	Switch should support Authentication, authorization, and accounting (AAA) via TACACS+ and RADIUS	
4.7	Switch should have Syslog	
4.8	Switch should support SNMPv1, v2, and v3 and have Enhanced SNMP MIB support	
4.9	Should support remote performance monitoring	
5	Security features	
5.1	Switch should support Ingress & Egress ACLs (standard and extended)	
5.2	Standard and extended Layer 2 ACLs: MAC addresses, protocol type	
5.3	Standard and extended Layer 3 and 4 ACLs: IPv4 and IPv6, Internet Control Message Protocol (ICMP and ICMPv6), TCP, User Datagram Protocol (UDP)	
5.4	Should support 802.1AE - MACsec on all user ports and also on the 25G ports	
5.5	Should support IPv4 and IPv6 source guard, Dynamic ARP Inspection and DHCPv4 and v6 Snooping	
6	High Availability	
6.1	Should support Ethernet ring protection - G.8032	
6.2	Switch should support Active/Active cluster of two core switches to provide sub-second failover and full utilization of all links connected to the Core Switches	
6.3	Primary and Backup Routing Engines in a cluster should be kept synchronized at all times to enable rapid stateful routing engine failover and Non-Stop Forwarding in case of Routing Engine failures	
6.4	Should support Hot-swappable field-replaceable power supplies and fan modules with N + 1 redundancy	

7	Certifications and compliances	
7.1	Should be ROHS 6.6 compliant	
7.2	The equipment shall be manufactured in accordance with the international standards ISO 9000:2008 or later for which the manufacturer shall be duly accredited.	
7.3	The OEM must be placed as Leaders in the latest Gartner Magic Quadrant for Data Center Networking and Wired & Wireless Access Infrastructure for the last 2 years.	
7.4	IPv6 feature should be ready from day 1 and IPv6 Ready Logo approved	
8	Environmental and power parameters	
8.1	Switch should be able to operate at environments :min 0° to 45°C (32° to 113 °F)	
8.2	Switch model should be rack mountable and should support both AC and DC power supply options. AC power supply to be proposed for the current requirement.	
9	Warranty	
9.1	Switch should be provided with hardware replacement warranty and ongoing software upgrades for all major and minor releases for a period of 3 years.	

3. Core Switch

Sr.No.	Specification	Compliance (Yes/No)
1.	The Core Switch should be high-performance switches that feature high port density, routing, and ultra-low latency, designed to be deployed as TOR switch.	
2.	Non-Blocking architecture. Switch should be EMI Certificates FCC, CE and Safety Certifications CUL/UL, CB.	
3.	Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
4.	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
5.	All the specified features/parameters/certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered.	

6.	Switch should support VXLAN, ONIE / OpenFlow v1.3, Data Center Bridging Exchange (DCBX)	
7.	Should supports 8-port 1GbE/10GbE and 4-port 40GbE/100GbE	
8.	The switch should have min 1200G stacking bandwidth with nine devices functioning together as a single unit.	
9.	All Switches and Fiber Modules should be from Same OEM	
10.	The Switch have 800 GBPS Switching Capacity, and forwarding rate 1607.4Mpps, for Higher switching functionality.	
11.	MAC Address Table - Min 250K, MTBF - 90K hours Min	
12.	Min 4K static VLAN groups and Min 4K VLANs	
13.	Switch should support STP/MSTP/RSTP and ERPS for support less than 50 Millisecond convergence (G.8032 v1/v2) Protocol support	
14.	802.1AX Link Aggregation, Multi-Chassis Link Aggregation Group (MLAG)	
15.	At least 8 nos of 802.1p Priority Queues per port, IEEE 802.1Qbb Priority-based Flow Control (PFC)	
16.	IGMP & MLD Snooping, Multicast Table Size: Up to 16K, PIM-SM IPv4/IPv6, PIM-DM, MSDP, PIM-SMD, PIM-SSM, DVMRP v3	
17.	Port Mirroring, Flow Mirroring, RSPAN mirroring	
18.	The switch shall have hardware based forwarding for IPv4 & IPv6.	
19.	Following protocols shall be supported with IPV4: Static routing, PBR, RIPv2, OSPFv2, BGPv4, PIM, VRRP from day one, MPLS/BGP L3 VPN, MP-BGP, VRF aware application, Graceful Restart (GR) Helper	
20.	IPV6: PBR, Static routing, OSPFv3, Bidirectional Forwarding Detection (BFD), BGP/MPLS VPN, BGP v4/v4+, IS-ISv6, IP Directed Broadcast.	
21.	The switch shall have Dual stack mode to run both IPv4 & IPv6, IPv4/IPv6 Routing Table - Min 16K, IPv4/IPv6 Forwarding Table - Min 120K	
22.	Shall support VRRP for IPV4 and IPV6.	
23.	MAC and 802.1X based Login must be available, Supports 802.1X NAP	

24.	MAC Address based Lockdown and Limited Learning,	
25.	L2/L3/L4 IP based, Source port, destination port,MAC based, Time based	
26.	AAA using RADIUS must be available, Identity-driven Policy (VLAN/ACL/QoS) Assignment, Guest VLAN	
27.	Secure Web based management (On https) through NMS or Full featured CLI, TELNET Access.	
28.	SSH based management (SSH v2). IEEE 802.3ah Ethernet link OAM, IEEE 802.1ag, ITU-T Y.1731	
29.	Serial console port, Alarm Port, USB Port, Management Ethernet port - Dedicated OOB port	
30.	The switch shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges.	
31.	The switch should support SNMP V2c and V3, and SDN with Open flow and ONIE for an open network support and RMONv1 and RMONv2 Support	
32.	Syslog shall be supported with multiple syslog destinations.	
33.	Shall support Netflow/IPFIX/sflow for flow exports.	
34.	Time synchronization using Network time protocol must be available.	
35.	The switch shall have feature of backing up the configuration & restoring a backed- up configuration. Multiple Configuration files must be supported.	
36.	Config/image upload and download from TFTP/FTP server shall be available.	
37.	Switch should be supplied with the all necessary hardware accessories like PSU, FAN, Power cord (full load front-to-back AC PSUs - 2 Min, and 4 front-to back fan modules), Stacking Cable (QSFP28 to QSFP28), Rack-mount bracket, Installation Guide, etc. and necessary software image file to fulfill all above mention feature set from day 1.	
38.	Power Supply & FAN - Switch should support Internal Hot swappable PSU and Field replicable FAN module.	

39.	Safety certification - The switch shall conform to IEC-60950/CSA-60950/EN-60950/UL-60950 standard for safety requirements of information technology equipment.	
40.	Environmental conditions- The offered equipment must be able to operate in the following environmental conditions	
41.	Operating temperature: 0°C to 45 °C and Relative Humidity: 10% to 95% Non-condensing	
42.	Warranty : Three years comprehensive onsite warranty	

4. Distribution switch

Sr.No.	Specifications	Compliance (Yes/No)
1.	Proposed Switch should have 12 10/100/1000BASESFP ports 4 Combo 10/100/1000BASE-T/SFP ports and 4 SFP+ ports	
2.	Switch should Support Internal/External Redundant Power Supply.	
3.	Switch shall have SD Card slot/USB/External flash for easy file store & restoration like firmware, configuration file, boot image, syslog etc.	
4.	Switching Capacity should be 128 Gbps & Packet Forwarding rate should be 95 Mpps.	
5.	The Switch shall support Min. 48K Mac address	
6.	Switch should support Physical Stacking up to 9 units per stack. Stacking bandwidth should be up to 80G and up to 32 devices per virtual stack.	
7.	Switch should support ARP, Proxy ARP and Gratuitous ARP.	
8.	The LAN switch shall have IEEE 802.1Q VLAN encapsulation and should support 4k Vlan.	
9.	It shall have support for Detection of Unidirectional links and to disable them to avoid problems such as spanning tree loops	
10.	It shall support 802.1v Protocol-based VLAN	
11.	Should support MAC based Vlan	
12.	Should support GVRP or equivalent, Private Vlan or equivalent, Subnet Vlan or equivalent, Voice Vlan and QinQ (port based qinq and selective qinq).	

13.	Multicast VLAN to allow multiple VLANs to receive the same multicast traffic	
14.	Should have 802.1D STP, 802.1w RSTP and 802.1s MSTP Spanning Tree Protocol and ERPS as per standard ITU-T G.8032 to provide protection for Ethernet traffic in ring topology.	
15.	The Switch should have 802.1AX Link Aggregation Up to 30 groups per device.	
16.	Port Mirroring One to one/Many to One, Flow based mirroring & VLAN Mirroring	
17.	Switch shall support ITU-T G.8032 Ethernet Ring Protection Switching to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer	
18.	The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment	
19.	Switch should support Static routing for IPv4 and IPv6, RIP for IPv4 and RIPng for IPv6, VRRP v2 & V3, OSPF, OSPF v3, BGP4, BGP4+ IS-IS v4/V6 and MPLS from day 1	
20.	Switch should support PIM-SM, PIM-DM, PIM-SDM, PIM-SMv6, DVMRP v3 and MSDP	
21.	IPv6 Tunnelling: Tunnel types should be supported are Static, 6to4, ISATAP and GRE.	
22.	Should support URPF, ECMP, Bidirectional Forwarding Detection, policy based routing, Route Redistribution support	
23.	Switch should support 802.1p priority queuing with 8 queues per port.	
24.	Queue Handling mode: WRR & Strict Mode, Strict +WRR and Weighted Deficit Round Robin (WDRR)	
25.	Granular Rate Limiting functions on per port & flow based to guarantee bandwidth in increments shall be as low as 8 Kilobits per Second.	
26.	Class of service shall be based on Switch port, DSCP, Vlan ID, TCP/UDP port, Protocol type, 802.1p queues, IPv4/v6 address, IPv6 flow label & User defined packet content	
27.	Broadcast and Multicast traffic/storm control	
28.	Weighted Random Early Detection (WRED) for congestion control	

29.	Switch shall support ITU-T Y.1731, 802.3ah Ethernet Link OAM, 802.1ag Connectivity Fault Management (CFM), Optical Transceiver Digital Diagnostic Monitoring (DDM) & Dying gasp	
30.	IEEE 802.1X Port Based Access control and Host based Access control and Guest Vlan	
31.	It shall support RADIUS/TACACS+ authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.	
32.	It shall have IP-MAC-Port binding and Safeguard Engine	
33.	Switch should be able to authenticate and access control based on MAC and web (Http or Https)	
34.	BPDU Attack Protection, ARP protection, IP Source Guard, Dynamic ARP Inspection and DOS Attack Prevention	
35.	It shall support for SSHv2, SNMPv3 to provide network security by encrypting administrator traffic	
36.	Switch shall support 802.1Qbb Priority-based Flow Control (PFC).	
37.	Able to manage through Web-GUI, Fully functional CLI interface and Telnet.	
38.	Should support sFlow for monitoring traffic in data networks, SNMP v1, v2c, v3 and SNMP Traps and RMON.	
39.	Switch should be EMI Certificates FCC, CE and Safety Certifications cUL/UL, CB.	
40.	Switch should be supplied with the all necessary hardware accessories like Power cord, Rack-mount bracket, Installation Guide, etc. and necessary software image file to fulfill all above mentioned feature set from day 1.	
41.	Warranty : Three years comprehensive onsite warranty	

5. 24 port Edge Access Switch

Sr.No.	Specifications	Compliance (Yes/No)
1.	Switch Should Support 24port 100/1000BASE-T PoE, 4 SFP/ SFP+ ports and RJ-45 console port. All Gigabit Ethernet ports support IEC 61000-4-5 surge protection (6KV)	
2.	switch should support Operating Temperature -5 to 50 °C (23 to 122 °F)	
3.	Switch Should Support Min. 56 Gbps Switching Capacity and Maximum 64 Byte Packet Forwarding Rate is 41.7 MPPS, 16K MAC address table.	
4.	The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment. Dying Gasp for quick trouble shooting during power failures or system shut downs	
5.	Switch Should Support IEEE 802.3af & at compliance (for PoE ports) and 193W Power Budget.	
6.	Switch Should Support IGMP Snooping v1, v2 and MLD snooping v1/v2	
7.	Switch shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) & LLDP-MED.	
8.	Switch Should Support IEEE 802.3az Energy Efficient Ethernet (EEE) Power saving Technology, Power Saving by Link Status, Time-based PoE, System hibernation, Port shut off, Cablelength detection Etc.	
9.	Switch Should Support 4K VLAN ID's, Min 256static VLAN , Multicast VLAN and Auto Voice & Video VLAN	
10.	Switch Should Support Port Mirroring One to one/Many to One,	
11.	Switch should support Quality of Service (QoS), 802.1p, Strict, Weighted Round Robin (WRR), Bandwidth Control.	
12.	Switch Should Support IP interfaces, Staticrouting for inter-VLAN Communication	
13.	Switch should support Access Control List (ACL), Port Base, MAC Base, IP Based, L2 & L3 ACL (IPv4 and IPv6) ITU-T G.8032 ERPS sub-50 ms protection and recovery.	

14.	Switch Should Support Security Features like Broadcast/Multicast/Unicast Storm Control, Traffic segmentation, TLS, DoS attack prevention, 802.1X Port-based Access Control , Port Security, ARP Spoofing Prevention, DHCP Server Screening, IP-MAC-Port Binding, ARP Inspection, DHCP Snooping.	
15.	Switch Should Support 802.1X Authentication local/RADIUS database (IPv4 & IPv6), port-based access control, EAP, OTP, TLS, TTLS, PEAP and Support MD5 authentication	
16.	Switch Should Support features Cable diagnostics, IPv4 & IPv6 Inspection, SSH v2 feature, 802.3x Flow Control and HOL Blocking Prevention	
17.	Switch Should Support Management thru Web-based and CLI.	
18.	Switch Should Support SNMP v1/v2c/v3, SNTP, ICMP v6, IPv4/v6 Dual Stack, Dual image, Dual configuration	
19.	Switch should have EMI CERTIFICATE as per EN/FCC/IC/CE.	
20.	Switch should have SAFETY CERTIFICATE as per UL/IEC/EN 60950	
21.	Switch should be supplied with the all necessary components like Power supply, Power cord, Console Cable, Rack-mount kit, Installation Guide, etc. and necessary software image file to fulfil all above mention feature set from day 1.	
22.	Warranty : Three years comprehensive onsite warranty	

6. LX Copper Transceivers (10G/1G)

SI No	Minimum Technical Specifications	Complied (Yes/No)
	All the following transceivers required for this project should be from the same OEM as	

1	<p>switches, Wireless Controller & AP:</p> <ul style="list-style-type: none"> • 1000BaseT SFP, 1000BaseLX SFP, <ul style="list-style-type: none"> ○ 1000Base SX SFP, 1000BaseLX SFP • 10GBaseLR SFP+, 10GBaseSR SFP+, <ul style="list-style-type: none"> ○ 10/25GBASE-SR SFP28, 10/25GBASE- LR SFP28, 10/25GBASE SFP28 DAC cables, 10G DAC SFP+ (passive/copper cable with minimum 3m length and SFP+ transceivers at both end) • 3rd party or local/Chinese made transceivers shall not be acceptable. <p>Bidder shall submit certified declaration specific to this tender that all Copper as well as optical transceivers offered for this project will be from the switching + WLAN + NMS OEM</p>	
---	---	--

7. LX Fiber Modules

Sr.No	Specifications	Compliance (Yes/ No)
1.	Description: 1GBASE-LR SFP Transceiver	
2.	Fiber Module should be Hot Pluggable, MSA Compliant and RoHS Compliant	
3.	Wavelength: 1310 nm	
4.	Fiber Module should support 10KM Distance	
5.	Certification - CE, FCC, UL, LVD, TUV, VCCI. (Should Enclosed with bid)	
6.	Warranty : Three years comprehensive onsite warranty	

8. 10 OFC Patch LC-LC / SC-SC / SC - LC

Sr.No.	Specifications	Compliance (Yes/No)
1.	Adopts high precision ceramic ferrule with good concentricity	
2.	Fiber corning single mode G652D,G657A,G657B	
3.	Cable Type 0.9mm	

4.	Mechanical specification Apex Offset :-< 50 um	
5.	Mechanical specification Fiber Height +(-)100 nm	
6.	End-face radius of Curvature 7mm < R <25mm	
7.	Repeatability <(-) 0.2 db	
8.	Working Temperature :- -4 0 c ~ +85 o C	
9.	Storage Temperature:- 40 o C ~ + 85 o C	
10.	Length -- 2Mtr	
11.	Type -- LC-LC / SC-SC / SC - LC	
12.	Warranty : Three years comprehensive onsite warranty	

** Additional Technical details for Sl.no: 01, 02, 03 & 04

IMPORTANT NOTE:

- The price quoted above shall be inclusive of all taxes and charges except GST.
- GST shall be mentioned separately.
- FOR; Destination as given in the purchase order.
- Warranty period for the above items must be at least 5 years from the date of installation.
- Annual Maintenance Charges (after expiry of warranty period)
- Certified Training must be provided to the faculty members and research scholars after the successful installation of the Equipment.

Signature:

Name:

Designation:

Seal of the Firm:

Appendix – IV**CONTRACT AGREEMENT**

THIS AGREEMENT made on the day of 2023 between The Registrar, Tamil University, Thanjavur – 613 010, (Herein after “the Purchaser”) of the one part and (Name of Supplier) of (Address of the Supplier) (herein after called “the Supplier) of the other part:

WHEREAS the Purchaser is desirous of procuring-----equipment as per the tender reference No -----and has accepted a bid by the Supplier for the above said equipment, the price offered by the Supplier is Rs.----- (Rupees in words).

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Tender referred to, and they shall be deemed to form and be read and construed as part of this agreement.
2. The following documents shall be deemed to form, be read and construed as part of this Agreement, viz;
 - a) The letter of Acceptance issued by the purchaser.
 - b) The Notice Inviting Tender.
 - c) The supplier’s bid including enclosures, appendixes, documents, Price Catalogue etc.
 - d) The Tender Document including various Terms and Conditions.
 - e) Any other document listed in the Tender document.
3. In consideration of the payments to be made by the Purchaser to the Supplier within thirty (30) days from the date of delivery and acceptance by concerned department/ section.
4. The warranty period is-----years.
5. The AMC/SMC for the subsequent year after the warranty period will be as follows.

For the First year after the expiry of the warranty	
For the Second year after the expiry of the warranty	
For the Third year after the expiry of the warranty	
For the Fourth year after the expiry of the warranty	
For the Fifth year after the expiry of the warranty	

IN WITNESS whereof the parties here to have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the Said
(For the Supplier) in the presence of

Signature

Name & Address

Signed, Sealed and Delivered by the Said (For the Purchaser) in the presence of

Signature

Name & Address

Appendix – V

TENDER NO.: 16/2022-2023/Grant
EQUIPMENT: ACTIVE & PASSIVE COMPONENTS OF
NETWORKING MATERIALS

SPECIFICATION

DETAILED SPECIFICATION FOR Firewall

DETAILED SPECIFICATION FOR ROUTER

DETAILED SPECIFICATION FOR CORE SWITCH

DETAILED SPECIFICATION FOR DISTRIBUTION SWITCH

**DETAILED SPECIFICATION FOR ACCESS SWITCH and
other Accessories Prescribed above**

Signature of the Tenderer