VIRTUAL UNIVERSITY OF PAKISTAN

TENDER NOTICE

Through e_Pak Acquisition and Disposal System (EPADS) v2.0

Sealed Tenders are invited through (EPADS v2.0) **https://epads.gov.pk** from the Firms who are registered with Tax Authorities on Active Taxpayers List (ATL) of FBR, for the following:

Sr. No.	Description	Tender Fee (Rs.)	Tender Opening Date	Tender Receiving / Opening Time
1.	Tender No. VU/26-27/08/897 **Different Items for Electronics Lab (CS)**	1,000/-	September 21, 2026	Receiving: 02:00pm Opening: 02:30pm
2.	Tender No. VU/26-27/08/898 **Network Firewalls(ICT)**	1,000/-	September 22, 2026	Receiving: 02:00pm Opening: 02:30pm

Tender documents for the above-mentioned tender(s) are also available on the Virtual University of Pakistan website **(https://www.vu.edu.pk/Opportunities/Tenders)**. However, bids shall be submitted only **through EPADS v2.0**. Any bid submitted through any other mode shall not be considered.

The complete tendering process shall be carried out through EPADS v2.0.

Interested bidders are required to register themselves on EPADS v2.0 (https://epads.gov.pk) and submit their bids electronically through the EPADS v2.0 portal.

The Bid Security (if applicable), in the amount and form specified in the bidding documents and drawn in favor of the Virtual University of Pakistan, shall be uploaded as a scanned copy on EPADS v2.0. The original Bid Security, along with one hard copy of the sealed bid, must also be submitted physically to the Virtual University of Pakistan at the address provided below on or before the bid closing date and time.

Bids requiring Bid Security that are submitted without the prescribed Bid Security shall be rejected. The bid submission and opening schedule shall be strictly observed.

The University reserves the right to accept or reject any bid, or to annul the procurement process at any stage, in accordance with the provisions of the Public Procurement Rules, 2004.

This Tender Notice is also available on the PPRA website (www.ppra.gov.pk) and the Virtual University of Pakistan website.

PID(I)2061/26

PROCUREMENT DEPARTMENT
DIRECTORATE OF FINANCE VIRTUAL UNIVERSITY OF PAKISTAN
SIR SYED MEMORIAL SOCIETY BUILDING 19-ATATURK AVENUE, G-5/1, ISLAMABAD
Phone No. 051-111-880-880 Extensions: 1354 / 1323 / 2823, 1651
Email: po@vu.edu.pk Website: www.vu.edu.pk
VU NTN: 4388557-8

VIRTUAL UNIVERSITY OF PAKISTAN

Sir Syed Memorial Society Building, 19-Ataturk Avenue, G-5/1, Islamabad

http://www.vu.edu.pk

TENDER DOCUMENT

NETWORK FIREWALLS (ICT)

Tender No. VU/26-27/08/898

This tender will be opened on **September 22, 2026 at 02:30pm** in the Procurement Department, VirtualUniversity of Pakistan, Sir Syed Memorial Society, 19-Ataturk Avenue, G-5/1, Islamabad.

Name of Firm/Company: ______________________________

Office Address: ______________________________

Contact Person: ______________________ Designation: ______________________

Phone No: ____________ Fax No: ____________ Cell No. ______________

GST Reg. No: ____________________ N.Tax Number: ______________________

Active email address (in CAPITAL letters): ______________________________

Status of Firm/Company (Pls. tick appropriate box)

Manufacturer / Authorized Dealer / Distributor ☐

General Supplier / Reseller ☐

ITEMS MARKED WITH (*) MUST BE ATTACHED; OTHERWISE, YOUR BID WILL BE DECLAREDAS NON-RESPONSIVE.

PROCUREMENT METHOD:
"SINGLE STAGE TWO ENVELOPS BIDDING PROCEDURE"

1. Bidding is on the basis of National Competitive Bidding (NCB) in accordance with "Single Stage Two Envelope Bidding Procedure" comprising of "Technical Proposal & Financial Proposal" (Separately Sealed) in single package, as per PPRA-Rules 2004 Clause No. 36(b).
2. No bid shall be considered if;
    - Not uploaded at EPADS v2.0
    - Not provided in shape of hard copy by the given schedule at given location
    - Both uploaded and hard copies of the bids must be with the same bidder name
    - Received without Original Bid Security (if any) and Tender Fee in a single envelop
3. Tender document duly completed should reach the Procurement Department, Directorate of Finance, Virtual University of Pakistan, not later than **02:00 pm on September 22, 2026**. Late Tenders will not be entertained. No telegraphic or faxed bid will be accepted.
4. Technical Proposals shall be opened at **02:30 pm on the same date** in the office of Procurement Department, Directorate of Finance, Virtual University of Pakistan, Islamabad.
5. **VU shall open all bids through EPADS v2.0 as per given schedule and place specified above, in presence of the bidders' representatives who choose to attend the meeting and shall sign an attendance sheet as evidence of their presence.**

6. Sealed Financial Proposals shall be held in safe custody. Financial Proposals will be opened publicly after completing the technical evaluation, in the presence of technically qualified bidder(s), on the date and the timings given afterwards.
7. Financial Proposals of technically non-qualified bidder(s) shall be returned un-opened / not considered.
8. If two or more bidders quote the same price in Financial Proposal, then the contract will be equally divided among all those bidder(s) or will be awarded to the bidder with better technical specification or Virtual University may ask the bidders to submit Financial Proposal again.

TERMS AND CONDITIONS:

1. The notice published in the media shall be considered an integral part of this tender document.
2. The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding Documents carefully. Failure to furnish the required information may result in the rejection of the Bid.
3. Tender shall be opened on the given date, time and venue. In the case of holiday on given tender opening date, same shall be opened on next working day.
4. Tender should be addressed to the Director Finance, Virtual University of Pakistan.
5. VU takes no responsibility for delay, loss or non-receipt of bids sent by post/courier.
6. Original tender Document, along with item specifications must be attached. All pages must be signed and stamped. **(*)**
7. Technical evaluation shall be carried out by the Technical Evaluation Committee and finalized according to the recommendations of the Committee.
8. Please attach financial soundness certificate / Account Maintenance Certificate issued by your bank which should not be older than 03 months. **(*)**
9. The bidder must submit an “Affidavit” on Rs.100/- Stamp Paper that the Bidder/Firm/Company/Contractor is not Blacklisted from Public Procurement Regulatory Authority (PPRA). Draft is given herewith in the document. **(*)**
10. The bidder submit the list of Directors/Partners/Owners along with the bid.
11. The bidder must be a registered taxpayer with FBR on Active Taxpayer List (ATL) and certificatemust be attached for NTN and GST. (If GST is exempted, please provide necessary evidence). **(*)**
12. GST should be exclusively/separately indicated in the Tender document and bill/invoice.
13. Bidder(s) should quote their rates (including all applicable taxes & duties at the prevailing rates) clearly on the Tender Document for each item both in figures and words.
14. The bid shall remain valid for a period of three (3) months from the date of opening of the bid. Validity of bid for a shorter period shall be rejected as non-responsive. **(*)**
15. To submit a tender with the Virtual University of Pakistan, bidders are required to deposit **Rs.1,000/- online in any branch of Allied Bank Limited in Account No. PK58ABPA0010061279710055 (Virtual University of Pakistan). (*)**
16. The original deposit slip must be attached with the bid. This amount is a non-refundable tender fee and is mandatory. Cash, crossed/open cheques, Pay Orders, or Demand Drafts are not acceptable.
17. Bids submitted without the tender fee shall not be accepted. (*)
18. **The bidder shall furnish, as part of its bid, a Bid Security(ies) (Earnest Money) as mentioned in the bidding documents uploaded at EPADS v2.0 in the form of Demand Draft (DD), Pay Order (PO), Call Deposit Receipt (CDR), or Bank Guarantee only. Cheques shall not be accepted. (*)**
19. Bids without bid security shall not be entertained, even if the bidder is technically qualified. (*)
20. A scanned copy of the bid security must be uploaded on EPADS V2.0, and the original hard copy must be submitted physically along with the bidding documents on the closing date. (*)
21. The deposit slip/proof of online transfer of the Tender Fee and Bid Security(ies) must be submitted in the required form, in a separate envelope placed inside the main envelope. (*)
22. The bid security shall be refundable to unsuccessful bidders after finalization of the tender.
23. Bid security of successful bidder (in which warranty is applicable) will be retained till providing

the Performance Security in shape of a Bank Guarantee as per detail given ahead.

24. The successful bidder shall have to furnish within **Twenty one (21) days** after the execution / signing of the contract / issuance of Purchase Order, a performance security to the amount of **5% of the contract price / value of the Purchase Order** to VU. The proceeds of the performance security shall be payable to VU as compensation for any loss resulting from the Supplier's failure to complete its obligations under the contract / order. The performance securityshall be denominated in the currency of the contract and shall be in the following form.

    a. A Bank Guarantee issued by any Commercial Bank located in Pakistan ("A" rated or above).

    b. The performance bond will be discharged by VU not later than **15 days** following the date of expiry of the warranty, under the contract / purchase order.

25. If the Performance security is not submitted to VU within the specified period or its amount is less than 5% of the contract price / purchase order value, VU reserves the right to cancel the award of contract / purchase order and forfeit the Bid Security.

26. Items must be delivered to the Virtual University of Pakistan's Head Office at the address mentioned below or as instructed by the university within **Sixty (60) days** from receipt of the Purchase Order.

    a. No extensions will be allowed unless granted by Purchase committee on solid grounds.
    b. Delay in provision of goods/item(s)/services by the bidder(s)/supplier(s) in accordance with the time schedule prescribed in the General Terms and Conditions (GTC) shall not be tolerated and in such default, penalty for delaying goods/item(s) shall be imposed @ 0.1% per day of the total contract / order amount or value of the items / services delivered after due date, which will be capped to maximum of 10% of the total value of the Contract / purchase order / undelivered items/services.
    c. The penalty on the value of goods/item(s) not delivered in time will be imposed which may lead to cancellation of order without any liability to the university and the said bidder/supplier/firm/company may also be blacklisted.
    d. Moreover, any penalty may be imposed by the VU in case of any default by the bidder/supplier, in addition to initiating legal action against such defaulter. Virtual University has also the right to stop its pending payment or forfeit its guarantee/security submitted to the Virtual University of Pakistan in this procurement or any other contract.

27. Notwithstanding anything contrary provided in the provisions of General Terms and Conditions (GTC) Clauses, the Bidder/Supplier shall not be liable for forfeiture of its performance security, liquidated damages, late delivery charges, or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of the Force Majeure.

    a. For purposes of this clause, "Force Majeure" means an event beyond the control of the Bidder/Supplier and not involving the Bidder/Supplier's fault or negligence and not foreseeable. such as, acts of God, perils of navigation, floods, storms, earthquakes, fire, hostilities, war (declared), terrorism, Port closure, Impositions of restrictions or regulations by any Government or Government Agency, illegality arising from applicable domestic or foreign laws or regulations, blockage and strikes that is politically motivated strikes and is widespread or nationwide, insurrection.

    b. A change in economic/market circumstances or unexpected hike in prices affecting the profitability of a contract or the ease with which parties' obligations can be performed, is not a force majeure event."

    c. If a Force Majeure situation arises, the Bidder/Supplier shall promptly notify the Virtual University in writing within five days from the date of such event of such condition and the cause thereof along with evidence, moreover take all steps that are reasonably necessary to mitigate or remove the consequences of force majeure. Where such notice of Force Majeure is not served by the Party claiming Force Majeure within the period prescribed herein then that Party's right to claim Force Majeure for that event would stand irrevocably waived.

    d. Unless otherwise directed by the Virtual University in writing, the Bidder/Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. The benefit of Force Majeure shall be in favor of the client (VU), if it happened anytime.

28. Virtual University requires Contractors/Bidders, to the highest standard of ethics during the procurement and execution of contracts. For the purposes of this provision, the terms set forth in PPRA Rules /Act shall be applicable:

   a. VU will bar a firm/company/individual bidders/Contractors /consultant or whatsoevernamed, in accordance with Blacklisting procedures under Public Procurement Rules 2004 in any case if deems so.
   b. Furthermore, the Contractor/ Bidder(s) shall be aware of the provision stated in the General Terms & Conditions of the Contract.

29. Virtual University may, under the applicable Law (s) for a specified period, debar a bidder/ Contractor from participating in any public procurement process of VU, if the bidder or Contractor has

   a. Acted in a manner detrimental to the public interest or good practices.
   b. Consistently failed to perform its obligation under the contract.
   c. Not performed the contract up to the mark.
   d. Indulged in any corrupt practice.

   If VU debars a bidder/Contractor, the procuring agency:

   a. The said bidder/firm/company may also be blacklisted for a period of at least three (03) years.
   b. May forward the decision to the Public Procurement Regulatory Authority (PPRA) for publication on the website of the PPRA; and
   c. May request the PPRA to debar the bidder or c ontractor for procurement of allprocuring agencies.

30. Virtual University has the right to take any legal action against the bidder/supplier/firm/company, in addition to blacklisting, if it is found involved in corrupt practices.

31. Virtual University reserves the right to increase or decrease the quantity of goods specified ahead at the time of award of tender as per PPRA Rules. VU also reserves the right to place the order on a partial shipment basis.

32. The supplied items should conform to the standard specifications, must be brand new and be free from defects in all respects.

33. Income tax and GST shall be withheld as per Government rules.

34. Payment shall be released after submission of the Commercial invoice & Sales Tax Invoice, duly verified by the technical department. The payment will be made in accordance with SRO 660(I) 2007.

35. Virtual University reserves the right to accept or reject any bid or annul the procurement process a tany time as prescribed under PPRA Rules.

36. A bidder requiring any clarification in the bidding document shall contact the VU in writing within **Five (05) days through EPADS v2.0 or through given email**. The VU will respond in writing to respond to any clarification provided that such request is received within time. Should the clarification result in changes to the essential elements of the bidding documents, the VU shall amend the bidding documents at any time prior to the deadline for the submission of bids. The VU may amend the bidding documents by issuing addenda. Any addendum issue shall be part of the bidding document and shall be communicated in writing to all who obtained the bidding document from the VU. The VU shall also promptly publish the addendum to the Bidder on the VU website and EPADS v2.0.

37. To assist in the examination, evaluation, comparison of the Bids, and qualification of the Bidders, the VU may, at its discretion, ask any Bidder for a clarification of its Bid. Any clarification submitted by a Bidder in respect to its Bid and that is not in response to a request by the VU shall not be considered. The VU request for clarification and the response shall be in writing. No change, including any voluntary increase or decrease, in the prices or substance of the Bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the VU in the evaluation of the Bids. If a Bidder does not provide clarifications of its Bid by the

date and time set in the VU request for clarification, its Bid may be rejected.

38. Provided that the Bid is substantially responsive, the VU shall correct arithmetical errors on the following basis:

   a. if there is a discrepancy between the unit price and the line-item total that is obtained by multiplying the unit price by the quantity, the unit price shall prevail and the line-item total shall be corrected, unless in the opinion of the VU there is an obvious misplacement of the decimal point in the unit price, in which case the line-item total as quoted shall govern and the unit price shall be corrected.

   b. if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.

   c. if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to (a) and (b) above.

39. Bidders shall be requested to accept correction of arithmetical errors. Failure to accept the corrections shall result in the rejection of the Bid.

40. Amicable Settlement

    VU and the Supplier shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with this contract.

    Except as otherwise provided in the contract, any difference, dispute or question arising out of or with reference to this contract which cannot be settled amicably, shall within **(30) thirty days** from the date that either party informs the other in writing that such difference, dispute or question exists, be referred to arbitration.

    Within 30 days of the said notice, one arbitrator shall be nominated in writing by VU and one arbitrator shall be nominated in writing by the Supplier. The two arbitrators shall initiate arbitration proceedings at Islamabad. In case the two arbitrators do not reach any agreement, a third arbitrator shall be selected by the two arbitrators.

    The arbitration shall be conducted in accordance with the rules of procedure set forth in the Arbitration Act 1940 or as subsequently amended. The contract of the majority of the arbitrators shall be final and binding on both Parties. Each party shall bear the cost of its own arbitrator and the cost of the third arbitrator shall be borne equally by both parties. In the event of an arbitrator resigning or becoming incapable or unable to act, the party nominating such arbitrator shall be entitled to appoint another one in the place of the outgoing arbitrator. Proceedings shall continue without recommencing as if such arbitrator had been originally nominated.

    An abnormally Low Bid is one where the Bid price, in combination with other constituent elements of the Bid, appears unreasonably low to the extent that the Bid price raises material concerns with the Procuring Agency as to the capability of the Bidder to perform the Contract for the offered Bid price. In the event of identification of a potentially abnormally Low Bid, the VU shall seek written clarification from the Bidder, including a detailed price analysis of its Bid price in relation to the subject matter of the contract, scope, delivery schedule, allocation of risks and responsibilities and any other requirements of the bidding document. After evaluation of the price analysis, in the event that the VU determines that the Bidder has failed to demonstrate its capability to perform the contract for the offered Bid price, the VU shall reject the Bid.

41. The University reserves the right to accept or reject any bid or annul the procurement process at any time in accordance with PPRA Rules.

42. Payment shall be made as per actual verified quantity after submission of the Sales Tax Invoice, duly verified by the concerned department, in accordance with SRO 660(I) 2007. Income tax and GST shall be withheld as per Government rules.

43. Delivered items must conform to standard specifications and VU requirements and free from any defect(s) in all respect.

MANDATORY DOCUMENTS REQUIRED

(MUST BE ATTACHED WITH THE TECHNICALPROPOSAL ON TOP OF ALL DOCUMENTS AND TO BE SUBMITTED AT THE TIME OF OPENING OF TECHNICALS BID(S):

Sr. No	Description	Attached (Yes / No)
	General	
1	Bid Security in the shape of DD/PO/CDR or a Bank Guarantee amounting to Rs. 800,000/-	
2	Tender document duly filled, signed & stamped by the bidder	
3	Tender Fee Rs. 1,000/- in shape of paid Bank Deposit Slip	
4	Financial soundness certificate / Account Maintenance Certificate issued by Bidder's bank (not older than 03 months)	
5	Affidavit on Rs.100 stamp paper that the bidder/firm/company is not Blacklisted from PPRA	
6	Copy of NTN & GST certificate	
7	Copies of Last Three Tax Return of both Income Tax and Sales Tax	
8	Validity of the bid for a period of three (3) months (Confirmation required)	
9	Delivery of ordered items within given Days (Confirmation required on Letterhead)	
	Technical (Certificate(s) required issued by the Principal/Manufacturer of quoted brand)	
1	The bidder must be authorized partner of the quoted brand.	
2	The bidder must submit a current/valid Authorization certificate to participate in this tender issued by the Principal/Manufacturer of the quoted items.	
3	The brand should be established since a minimum of five (05) years.	
4	Local partner representation should be at least three (03) years.	
5	Warranty and support Coverage from Principal/Manufacturer through its authorized distributor/dealer.	
	Technical (Others)	
1	The bidder must have offices/workshop at 03 major cities, i.e., Lahore, Islamabad/Rawalpindi, Karachi (Please mention the current addresses in the bid)	

NOTE:

- Your bid will be rejected if any of the above documents are not attached with the bid.
- Warranty certificate on the supplier(s) letterhead shall be provided in original by the successful bidder(s)/supplier(s) upon delivery along with the invoice.

Bidder's Name:____________________________________

Sign & Stamp of Bidder: ______________________________

EVALUATION CRITERIA:

i. Initial scrutiny of tender documents/bids
ii. Technical Evaluation as per BOQ
iii. Evaluation of Demo / sample Unit(s) **if needed**
iv. Selection of technically compliant bidder(s)
v. Financial Evaluation of compliant bidders(s)
vi. Award of tender to the Most advantageous bidder(s)

Procurement Department
Directorate of Finance
Virtual University of Pakistan
Sir Syed Memorial Society Building,
19-Ataturk Avenue, G-5/1, Islamabad
UAN: 051-111-880-880
Technical Queries Ext 1651
Financial Queries 1323, 1354
VU NTN: 4388557-8
Email: po@vu.edu.pk

Declaration by the Bidder
Should be on Rs.100/- stamp paper

I, being the owner/proprietor/director/authorized representative of the firm/company, hereby certify that I have read and understood all the terms and conditions of this office and accept the same without any reservation.

I further confirm that all items and/or services provided shall be of the best quality, strictly in accordance with the prescribed standards, specifications, and requirements. I undertake to replace or redo, at my own cost, any item or service found to be substandard, unsatisfactory, or defective, without any claim whatsoever against the Virtual University of Pakistan (VU).

In case of failure to comply with the above, I understand and agree that VU shall have the right to impose penalties, confiscate the earnest money and blacklist the firm/company in accordance with applicable rules.

I hereby also confirm to provide on-site warranty including service & support with parts for complete unit(s) (where applicable) from the date of delivery.

I further declare that, as of the date of this undertaking, the firm/company is not blacklisted by the Public Procurement Regulatory Authority (PPRA) or any other government organization.

SIGNATURE & STAMP

Name: __________________

Designation: _____________

TECHNICAL PORTION

TECHNICAL TERMS AND CONDITIONS:

1. The bidder must have offices/workshop at 03 major cities, i.e., Lahore, Islamabad/Rawalpindi, Karachi (Please mention the current addresses in the bid) **(*)** in order to ensure timely repair/maintenance of the supplied items. The bidder should clearly indicate the cities where they will be able to arrange effective after-sales service and how the service will be offered/provided.
2. The bidder will arrange a demo according to the specifications quoted in the bid, as and when required by the university.
3. The bid should clearly indicate the Manufacturer's warranty for the period mentioned against each item. The bidder shall be responsible to provide free installation, commissioning, and free comprehensive on-site replacement warranty (VU, Head Office and/or any of its Campuses in other cities of Pakistan) including service & support with parts for the said warranty period from the date of delivery. If the bidder fails to provide the warranty as per tender terms and conditions the firm may be blacklisted for a period of three (03) years.

MANDATORY DOCUMENTARY REQUIREMENT (TECHNICAL) (MUST BE ATTACHED WITH TECHNICAL PROPOSAL):

Sr. No	Vendor Qualification	Document Needed	Attached (Yes / No)
1	The bidder must be authorized partner of the quoted brand.	Certificate required issued by the Principal/Manufacturer of quoted brand.	
2	The bidder must submit a current/valid Authorization certificate to participate in this tender issued by the Principal/Manufacturer of the quoted items.		
3	The brand should be established since a minimum of five (05) years.		
4	Local partner representation should be at least three (03) years.		
5	Warranty and support Coverage from Principal/Manufacturer through its authorized distributor/dealer.		

NOTE:

- Your bid will be rejected if any of the above documents are not attached to the bid.
- Warranty certificate, on the supplier(s) letterhead shall be provided in original by the successful bidder(s)/supplier(s) upon delivery along with the invoice.

TERMS AND CONDITIONS OF CONTRACT FOR SUCCESSFUL BIDDER:

TERMS AND CONDITIONS OF CONTRACT FOR THE SUCCESSFUL BIDDER

1. **Implementation and Deployment**

The OEM/Successful Bidder shall be responsible for the complete implementation, deployment, configuration, integration, testing, and commissioning of the proposed Network Firewalls (NGFW + WAF). The scope shall include:

- Installation and configuration
- Performance tuning and optimization
- Configuration of NGFW and WAF security policies in accordance with OEM recommendation.
- Functional and operational testing prior to handover.

2. **Installation Schedule**

All installation, configuration and maintenance activities shall be planned to minimize disruption to the University's normal operations. The Successful Bidder shall coordinate implementation activities with the University and provide an implementation schedule indicating the timeline for deployment. Any planned service interruption shall only be carried out with the prior approval of Virtual University (VU).

3. **Documentation**

Upon successful implementation, the Successful Bidder shall provide comprehensive technical documentation in both hard and soft copy, including but not limited to:

- Next Generation Firewall configuration documentation.
- Web application Firewall configuration documentation.
- Security policies and exceptions.
- System architecture and deployment diagram.
- Administrative and operational manuals.
- Backup and restoration procedures (where applicable).

4. **Software Updates and Upgrades**

During the entire subscription/support period, the Successful Bidder shall provide, at no additional cost:

- Software version upgrades.
- Security patches.
- Signature and threat intelligence updates.
- Detection engine updates.
- Feature enhancements released by the OEM.

5. **Technical Support**

The Successful Bidder shall provide comprehensive OEM-backed technical support for Network Firewalls (NGFW + WAF) throughout the subscription/support period, including:

- Remote and on-site support, whenever required.
- Troubleshooting and fault rectification.
- Configuration assistance.
- OEM escalation support for critical issues.

6. Training

OEM recommended trainings with respect to quoted solution will be arranged by the OEM/successful bidder for the quoted solution with certification track for at least three (03) VU resources through certified trainer/professional.

7. Implementation Timeline

The Successful Bidder shall complete the deployment, configuration, integration, testing, and commissioning of the complete solution within fifteen (15) calendar days from the date of delivery.

8. Acceptance Testing

Final acceptance of the solution shall be subject to successful completion of installation, configuration, integration, functional testing, training and demonstration that all specified features are operating satisfactorily. The project shall be considered complete only after issuance of an Acceptance Certificate by Virtual University.

9. Warranty and Support

The Successful Bidder shall provide comprehensive on-site hardware replacement warranty including service and support and complete security features licensing cost for Five (05) years. The Successful Bidder shall provide comprehensive OEM-backed support and subscription services from the date of deployment of complete solution. The support shall include software updates and support, technical assistance, and replacement or reactivation of licenses, where applicable.

10. Failure to Provide warranty and Support

Failure of the Successful Bidder to fulfill the contractual warranty, subscription, or support obligations may result in action under the applicable procurement rules and the terms of the contract, including forfeiture of performance security, imposition of penalties, termination of the contract, and blacklisting for a period of three (03) years.

11. Integrity Pact

The Successful Bidder shall execute an Integrity Pact in the prescribed format, affirming that no official or employee of Virtual University has any direct or indirect interest in the contract or any benefit arising therefrom. Any violation of the Integrity Pact shall render the contract liable to cancellation and may result in legal or administrative action in accordance with the applicable laws and procurement regulations.

SLA AGREEMENT FOR SUCCESSFUL BIDDER

The Successful Bidder shall provide comprehensive OEM-backed technical support and maintenance services for the supplied Network Firewalls (NGFW + WAF) throughout the subscription/support period. The support shall cover all hardware, software, subscriptions, licenses, security services, and associated components supplied under the purchase order.

The support services shall include, but shall not be limited to, incident management, troubleshooting, software/firmware updates, security signature updates, configuration assistance, bug fixes, performance optimization, security policy configuration, vulnerability remediation, license/subscription management, and escalation to the OEM where required.

Scope of Services

- SLA time period = 05 Years
- The Successful Bidder agrees to provide comprehensive technical support for the Network Firewalls (NGFW + WAF) as specified in the Purchase Order and technical specifications.
- The bidder shall ensure that all required OEM licenses, subscriptions, security updates, firmware/software updates, patches, signatures, and security services remain valid and operational throughout the SLA period.

Support Availability

- **Critical Incidents:** 24x7x365 support.
- **Non-Critical Incidents:** Monday to Friday during normal business hours (excluding public holidays), unless otherwise agreed.
- Support shall be available through telephone, email, remote access, and on-site visits whenever required.

1. Service Levels

Severity	Description	Initial Response Time	Resolution / Workaround Time
Critical (Severity-1)	Complete failure or unavailability of the Network Firewalls (NGFW + WAF); Network Firewalls (NGFW + WAF) becoming inaccessible; complete loss of network or web application protection; major security incident, ransomware attack, active exploitation, or security incident affecting production services with no available workaround.	Within 30 minutes	Within 4 hours
High (Severity-2)	Major functionality impaired; significant degradation of Network Firewall (NGFW + WAF) security functions; failure of IPS/IDS, application control, URL filtering, VPN, threat protection, SSL inspection, WAF protection, or other critical security features affecting systems/services.	Within 1 hour	Within 8 hours
Medium (Severity-3)	Partial functionality affected; isolated Network Firewall (NGFW + WAF) policy issues; configuration problems; policy deployment failure; reporting/logging issues; performance degradation; or malfunction of non-critical security features.	Within 4 hours	Within 1 business days

Low (Severity-4)	General technical queries, configuration assistance, policy optimization, reporting assistance, documentation requests, minor issues, or enhancement/guidance requests.	Within 1 business day	Within 3 business days

2. Penalties

2.1 **Failure to Meet SLAs**: In the event that the bidder fails to meet the specified response time or resolution time outlined above, penalties shall be applied as follows:

- For the delay beyond the agreed response time, a penalty of Rs. 5,000/hour shall be applicable.
- For the delay beyond the agreed resolution time, a penalty of Rs. 10,000/day shall be applicable.
- If the bidder does not provide resolution within time VU reserves the right to blacklist the bidder for the period of three (03) years.

3. Miscellaneous

Any modifications or amendments to this SLA must be made in writing and signed by both parties.

4. Signatures

This SLA is executed in duplicate originals, each of which shall be deemed an original and all of which shall constitute together but one and the same agreement.

Client Signature: ___________________________ Date: ______________

Bidder Signature: __________________________ Date: ______________

BOQ / SPECIFICATIONS OF REQUIRED ITEMS

Network Firewalls (NGFW + WAF) (Quantity:2)

NGFW Features

Technical Specifications	
Firewall Throughput	≥ 50 Gbps
NGFW Throughput	≥ 14 Gbps
Application Control Throughput	≥ 25 Gbps
Concurrent Connections	≥ 1,000,000
New Connections/ Second	≥ 500,000
Internal Storage Capacity	≥ 500 GB SSD
1G RJ45 Interface	≥ 4
1G Fiber SFP Interface	≥ 4
10G Fiber SFP+ Interface	≥ 6
Network Module/interface Slot(s)	≥ 1

1. The proposed solution shall support a minimum of 500 concurrent Site-to-Site IPsec VPN tunnels/connections.
2. The proposed solution must include a minimum of 1,500 concurrent-user licenses for SSL VPN.
3. The proposed solution must include:
   - Intrusion Prevention System (IPS)
   - Anti-Virus & Anti-Malware
   - Email Security Protection
   - Cloud-Based Security Sandbox
   - URL Filtering
   - Anti-Brute Force Attack
   - Application Control
   - Botnet Protection
   - Traffic Shaper
4. The proposed solution shall provide account/user security capabilities to detect and report authentication behavior, compromised accounts, and weak or vulnerable authentication practices.
5. The proposed solution must support automatic/manual configuration backups, including scheduled daily backups with internal storage and the capability to back up configuration files to FTP, TFTP, and SFTP servers.
6. The proposed solution must have a connection limitation feature to limit connections by source, destination, or bidirectional traffic and block IPs or discard sessions whenever the configured threshold is violated.

7. The proposed solution must provide global blacklist and whitelist options to block or allow any domain or IP address globally.
8. The proposed solution shall support SSL/TLS inspection for both outbound Internet traffic and inbound traffic destined for protected application servers, subject to applicable security policies and performance requirements.
9. The proposed solution shall support TLS 1.3 inspection/decryption.
10. The proposed solution must provide centralized monitoring of device status, CPU/RAM/disk utilization, traffic, and sessions by device, application, IP address, and interface, Servers & Client Threat dashboards for comprehensive security visibility.
11. The proposed solution should manage bandwidth by:
    - Application
    - User/group
    - IP address
    - Schedule
    - Country/region
    - Sub-interface
    - VLAN interface
    - VPN tunnel
12. Bandwidth Control shall support:
    - Bandwidth guarantee
    - Bandwidth limit
    - Upload/download speed control
    - Speed control for individual IP addresses
13. The proposed solution must support Stateful Packet Inspection.
14. The proposed solution must support Deep Packet Inspection (DPI) to identify applications for allowing or denying access.
15. The proposed solution must support Geolocation blocking to allow/deny access from specified countries/regions.
16. The proposed solution must support authentication with LDAP, RADIUS, and POP3, including user import through CSV files.
17. The proposed solution shall support Single Sign-On (SSO) through integration with Microsoft Active Directory/LDAP, RADIUS, and other supported identity/authentication mechanisms. The bidder shall specify the supported SSO methods.
18. The proposed solution must provide DoS/DDoS attack protection for both the network and the device itself.
19. The proposed solution must provide protection against:
    - SYN Flood
    - ICMP Flood
    - ICMPv6 Flood

- UDP Flood
- DNS Flood
- ARP Flood

20. The proposed solution must provide IP scan and port scan prevention.
21. The proposed solution must support file filtering for both upload and download directions, including pictures, text files, compressed files, and executable files.
22. The proposed solution shall provide malware inspection and detection capabilities for commonly used network, web, file-transfer, messaging, and application protocols supported by the proposed platform. The bidder shall clearly identify the supported protocols and inspection capabilities.
23. The proposed solution shall support malware inspection of commonly used file formats, including executable, document, compressed, script, image, and other commonly transferred file types. The bidder shall provide details of supported file types/formats.
24. The proposed solution must support Malicious Domain & URL Detection.
25. The proposed solution shall provide detection and prevention of malware-related command-and-control communications, including remote-access Trojan (RAT) activity.
26. The proposed solution shall provide detection of anomalous and suspicious network traffic, including abnormal protocol/port usage and communication patterns.
27. The proposed solution shall provide protection against known and emerging vulnerability exploitation attempts targeting network services, operating systems, applications, databases, middleware, and other protected resources.
28. The proposed solution shall provide configurable brute-force and credential-attack protection for commonly used authentication and remote-access protocols and services.
29. The proposed solution must support Botnet Detection, including detection of:
    - DNS tunneling
    - ICMP tunneling
    - HTTP tunneling
    - DGA communication
    - Other botnet client communications
30. The proposed solution shall provide centralized security visibility and reporting for protected servers and endpoints, including:
    - Threat severity
    - Threat category/type
    - Affected assets
    - Security events
    - Threat progression/attack indicators
31. The proposed solution shall provide capabilities to detect, identify, monitor, and report ransomware-related activities, indicators of compromise, and associated security risks within the protected environment.

32. The proposed solution shall provide centralized monitoring and reporting of account-related security events, including abnormal login activity, brute-force attempts, suspicious authentication behavior, and potentially compromised accounts.
33. The proposed solution shall record logs to local disk, including:
    - Access control logs
    - Session logs
    - Traffic audit logs
    - User authentication logs
    - Admin operation logs
    - SSL VPN logs
    - Local ACL logs
34. The proposed solution shall display traffic rankings by:
    - User/IP
    - Group
    - Application type
    - Application category
35. The proposed solution shall support security reports in PDF format.
36. The proposed solution shall support centralized logging and monitoring through industry-standard mechanisms, including Syslog and SNMP, with support for multiple log/monitoring destinations. The bidder shall specify the supported Syslog formats and SNMP versions.
37. The proposed solution shall support management through:
    - WebUI
    - SSH
    - CLI
    - Serial port
    - Other standard management interfaces
38. The proposed solution must support administrator authentication through:
    - Local authentication
    - TACACS server
    - RADIUS server
39. The proposed solution must support Out-of-Band Management (OOBM).
40. The proposed solution must support firmware version rollback.
41. The proposed solution must provide troubleshooting capabilities through WebUI, including identification of packet-drop reasons by policy, interface, etc.
42. The proposed solution shall provide logging and reporting capabilities with a minimum retention period of one (01) month, either locally or through an integrated/centralized management and logging platform. All hardware, software, licenses, subscriptions and components required to provide the specified log retention shall be included in the quoted solution.

43. The proposed solution must be a Hardware Appliance.
44. Complete licensing, including all licenses, subscriptions, and features required for Active/Active High Availability (HA), automatic failover, and seamless failback, shall be quoted with each hardware appliance. No additional license or subscription cost shall be applicable for HA, failover, or failback functionality during the quoted license/subscription period.
45. The proposed solution must operate within a temperature range of 0°C to 45°C.
46. The proposed solution must have dual power supplies with hot-swapping capability.
47. The proposed solution must be listed in any year Gartner Magic Quadrant for Next Generation Firewall
48. The proposed solution must be listed in any year ICSA Labs Certified Next Generation Firewall.
49. The proposed solution must be listed in any year CyberRatings for Enterprise Firewall.

WAF Features

1. The proposed solution must be listed in any year of NSS Labs for Web Application Firewall.
2. The proposed solution must provide a minimum 7 Gbps Web Application Firewall (WAF) throughput or higher.
3. The proposed solution shall provide advanced, automated, and/or machine-learning-based capabilities for detection of anomalous and emerging web application threats. The bidder shall describe the underlying detection capabilities and applicable licensing requirements.
4. The proposed solution must support IP Geolocation based access control.
5. The proposed solution must support Data Leak Prevention (DLP) for web applications.
6. The proposed solution must provide Brute Force Protection.
7. The proposed solution must provide DoS Prevention for web applications.
8. The proposed solution must support HTTP Header Security.
9. The proposed solution must support Custom Error Messages.
10. The proposed solution must support Error Code Handling and Local Report Center.
11. The proposed solution must provide Application Attack Protection, including protection against the OWASP Top 10.
12. The proposed solution must provide protection against Cross-Site Scripting (XSS) attacks.
13. The proposed solution must provide protection against SQL Injection (SQLi) attacks.
14. The proposed solution must provide protection against Cross-Site Request Forgery (CSRF) attacks.
15. The proposed solution must provide protection against Session Hijacking.
16. The proposed solution must have a built-in vulnerability scanner.
17. The proposed solution must support file upload scanning with Anti-Virus.
18. The proposed solution shall provide dedicated and purpose-built Web Application Firewall (WAF) inspection and protection capabilities, independently configurable from general network IPS policies.

19. The proposed solution must support custom WAF rules.
20. The proposed solution must provide protection against buffer overflow attacks, including:
    - URL length overflow
    - HTTP header overflow
    - POST entity overflow
21. The proposed solution must provide CC (Challenge Collapsar) attack prevention.
22. The proposed solution must provide XXE (XML External Entity) attack prevention.
23. The proposed solution must detect HTTP request anomalies.
24. The proposed solution must provide protection against cookie-based attacks.
25. The proposed solution shall support reputation-based threat intelligence services for identification and blocking of malicious IP addresses, domains, URLs, and other known indicators of compromise.
26. The proposed solution shall provide web application vulnerability assessment/scanning capabilities, preferably including passive assessment, with the ability to generate detailed vulnerability reports in commonly used electronic formats.
27. The proposed solution must support Application Hiding to prevent targeted attacks based on feedback information from applications.
28. The proposed solution must support weak password detection and brute-force attack prevention.
29. The proposed solution must support restriction of uploads of blacklisted file types.
30. The proposed solution must allow administrators to specify access privileges for sensitive URLs, including administrative pages.
31. The proposed solution must be a Hardware Appliance.
32. Complete licensing, including all licenses, subscriptions, and features required for Active/Active High Availability (HA), automatic failover, and seamless failback, shall be quoted with each hardware appliance. No additional license or subscription cost shall be applicable for HA, failover, or failback functionality during the quoted license/subscription period.

Management and Reporting

1. Graphical Analysis and reporting Tool
2. User/device tracking
    - Realtime Dashboard
    - OWASP Top 10 attack Categorization
    - Geo IP Analytics
3. Must quote Training & Product advanced Certification for three (03) Participants
4. Five (05) Years comprehensive on-site hardware replacement warranty including complete security features licensing cost for Five (05) years.
5. Five (05) Years Software Upgrade & 24x7 Technical Support
6. Must quote onsite deployment & configurations.

Note: The NGFW and WAF capabilities may be provided as an integrated solution or through separate purpose-built appliances from the same or different OEMs, provided that the proposed solution meets all stated technical, performance, integration, licensing, support, and security requirements.

The proposed solution shall be equipped with a minimum of six (06) 10GbE SFP+ interfaces per firewall appliance. The bidder shall provide all required 10GbE SFP+ optical transceiver modules for the proposed firewalls as well as compatible 10GbE SFP+ optical transceiver modules for the University's existing Huawei CloudEngine CE6863E-48S6CQ-B core switches, along with all necessary multimode fiber-optic cables, patch cords, connectors, and other accessories required for complete connectivity.

Each firewall appliance shall have at least two (02) independent 10GbE links to each of the two (02) existing core switches, providing a minimum of four (04) 10GbE links per firewall appliance for redundant core-network connectivity. The connectivity shall be designed such that failure of any single link, SFP+ transceiver, or cable does not result in loss of connectivity with the core network.

The remaining available 10GbE interfaces shall be utilized, where required, to provide a minimum of two (02) independent physical HA/synchronization links between the two firewall appliances, ensuring redundancy of HA connectivity and continued synchronization/failover capability in the event of failure of any single HA link, transceiver, or cable.

All required SFP+ transceivers, including those required at the Huawei CloudEngine CE6863E-48S6CQ-B core-switch side, and all necessary cables and accessories for the specified redundant core and HA connectivity shall be included in the quoted price without any additional cost.

Where NGFW and WAF functionality is proposed through separate appliances, the bidder shall provide all additional interfaces, SFP+ optical transceiver modules, fiber-optic cables, HA/synchronization links, inter-appliance connectivity, and other required hardware/accessories necessary to implement the complete, redundant, and fully operational NGFW and WAF solution. Such additional requirements shall be included in the quoted price and shall not be charged separately.

All SFP+ transceivers, including those required at the Huawei CloudEngine CE6863E-48S6CQ core-switch side, and all cables, connectors, and accessories required for the specified core-network, HA, and, where applicable, inter-appliance NGFW-WAF connectivity shall be included in the quoted price. The bidder shall be responsible for ensuring complete compatibility with the proposed solution and the University's existing network infrastructure.

Where NGFW and WAF functionality is delivered through separate appliances, the bidder shall provide HA for each security function as required to ensure that failure of a single appliance does not result in loss of the respective security service."

The solution shall support multi-factor authentication (MFA) for administrative access, either natively or through integration with a supported external identity provider.

FINANCIAL PORTION

(Must be placed in separate sealed envelope marked as "FINANCIAL PROPOSAL"
Items List as Per Specifications Given In Technical Portion

Sr. No.	Description	Unit Price Rs.	GST (If applicable)	Total Unit Price Rs.	Qty	Total Amount Rs.
Item# 1	Network Firewalls (NGFW + WAF)				02	
	Grand Total Amount Rs.					

Grand Total Amount in words (Rs.): ____

____

Rate of GST applied: __________ %