KENYA BUREAU OF STANDARDS

TENDER DOCUMENT

FOR
SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL

KEBS/T017/2020/2021

KENYA BUREAU OF STANDARDS
P.O. BOX 54974-00200
NAIROBI.
TEL: 020 6948000/605490/605550
E-MAIL: info@kebs.org, procurement@kebs.org
Website: www.kebs.org
FAX: 020 609660/ 604031

Table of Contents

KENYA BUREAU OF STANDARDS

Tel: (020) 6948000/ 605490
Fax: (020) 609660/ 604031

Email: info@kebs.org,
procurement@kebs.org
Website: www.kebs.org

INVITATION TO TENDER

TENDER NO. KEBS/T017/2020/2021: SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL

Kenya Bureau of Standards (KEBS) invites sealed tenders from eligible candidates for the SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL

Interested eligible candidates may obtain further information from and inspect the tender documents from **Procurement Office at KEBS Centre, Popo Road, Off Mombasa Road, Behind Bellevue Cinema Nairobi.** A complete tender document may be obtained by interested candidates on normal working days **between 9.00 a.m. and 4. 00p.m upon payment of a non-refundable fee** of 1,000 as indicated in the tender document, the amount is payable in cash or bankers' cheque **or be downloaded free from KEBS website:**

Completed tender documents in plain sealed envelopes clearly marked "KEBS/T017/2020/2021: SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL

should be addressed and delivered to:

THE MANAGING DIRECTOR,
KENYA BUREAU OF STANDARDS,
POPO ROAD OFF MOMBASA ROAD
P.O. BOX 54974 - 00200
NAIROBI.

Or be deposited in the Tender Box at **KEBS Centre Main Reception** marked "**TENDER BOX**" so as to be received on or before **10.00 am on Tuesday, 30th March 2021.**

Tender opening will be carried out immediately thereafter at the **KEBS Centre Conference Room.** Tenderers or their representatives are free to attend the tender opening.

Tenders must be accompanied by Bid Bond of **2%** of the Tender sum in the format specified in the tender documents.

Tenders will be opened immediately thereafter in the presence of the tenderers representatives who choose to attend the opening at **KEBS Centre Conference Room.**

MANAGING DIRECTOR

Section B. General Information

Introduction

1. Eligible Tenderers

1.1 This Invitation for Tenders is open to all tenderers eligible as described in instructions to tenderers in the tender document. Successful tenderers shall complete the supply of goods by the intended completion date specified in the tender documents.

1.2 Tenderers shall provide the qualification information statement that the tenderer (including all members of a joint venture and subcontractors) is not associated, or have been associated in the past, directly or indirectly, with a firm or any of its affiliates which have been engaged by the Procuring entity to provide consulting services for the preparation of the design, specifications, and other documents to be used for the procurement of the goods under this Invitation for tenders.

1.3 Tenderers shall not be under a declaration of ineligibility for corrupt and fraudulent practices.

2. Eligible Goods

2.1 All goods to be supplied under the contract shall have their origin in eligible source countries.

2.2 For purposes of this clause, “origin” means the place where the goods are mined, grown, or produced. Goods are produced when, through manufacturing, processing, or substantial and major assembly of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

2.3 The origin of goods is distinct from the nationality of the tenderer.

3. Cost of Tendering

3.1 The Tenderer shall bear all costs associated with the preparation and submission of its tender, and the procuring entity, will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.

The Tender Document

4. Contents

4.1 The tender document comprises the documents listed below and addenda issued in accordance with clause 6 of these instructions to tenders.

(i) Invitation for Tenders
(ii) General information
(iii) General Conditions of Contract
(iv) Special Conditions of Contract
(v) Schedule of Requirements
(vi) Technical Specifications
(vii) Tender Form and Price Schedules
(viii) Tender Security Form
(ix) Contract Form
(x) Performance Security Form

4.2 The Tenderer is expected to examine all instructions, forms, terms, and specifications in the tender documents. Failure to furnish all information required by the tender documents or to submit a tender not substantially responsive to the tender documents in every respect will be at the tenderers risk and may result in the rejection of its tender.

5. Clarification of Documents

5.1 A prospective tenderer requiring any clarification of the tender document may notify the Procuring entity in writing or by cable (hereinafter, the term *cable* is deemed to include telex and facsimile) at the entity's address indicated in the Invitation for tenders. The Procuring entity will respond in writing to any request for clarification of the tender documents, which it receives no later than seven (7) days prior to the deadline for the submission of tenders, prescribed by the procuring entity. Written copies of the Procuring entities response (including an explanation of the query but without identifying the source of inquiry) will be sent to all prospective tenderer that have received the tender document.

6. Amendment of Documents

6.1 At any time prior to the deadline for submission of tenders, the Procuring entity, for any reason, whether at its own initiative or in response to a clarification requested by a prospective tenderer, may modify the tender documents by amendment.

6.2 All prospective candidates that have received the tender documents will be notified of the amendment in writing or by cable, and will be binding on them.

6.3 In order to allow prospective tenderers reasonable time in which to take the amendment into account in preparing their tenders, the Procuring entity, at its discretion, may extend the deadline for the submission of tenders.

Preparation of Tenders

7. Language of Tender

7.1 The tender prepared by the tenderer, as well as all correspondence and documents relating to the tender exchanged by the tenderer and the Procuring entity, shall be written in English language, provided that any printed literature furnished by the tenderer may be written in another language provided they are accompanied by an accurate English translation of the relevant passages in which case, for purposes of interpretation of the tender, the English translation shall govern.

8. Documents Comprising the Tender

8.1 The tender prepared by the tenderer shall comprise the following components:

(a) A Tender Form and a Price Schedule completed in accordance with paragraph 9, 10 and 11 below.

(b) Documentary evidence established in accordance with paragraph 12 that the tenderer is eligible to tender and is qualified to perform the contract if its tender is accepted;

(c) Documentary evidence established in accordance with paragraph 13 that the goods and ancillary services to be supplied by the tenderer are eligible goods and services and conform to the tender documents; and

(d) Tender security furnished in accordance with paragraph 14

9. Tender Form

9.1 The tenderer shall complete the Tender Form and the appropriate Price Schedule furnished in the tender documents, indicating the goods to be supplied, a brief description of the goods, their country of origin, quantity, and prices.

10. Tender Prices

10.1 The tenderer shall indicate on the appropriate Price Schedule the unit prices and total tender price of the goods it proposes to supply under the contract.

10.2 Prices indicated on the Price Schedule shall be entered separately in the following manner:

(i) The price of the goods quoted EXW (ex works, ex factory, ex warehouse, ex showroom, or off-the-shelf, as applicable), including all customs duties and sales and other taxes already paid or payable.

(ii) Charges for inland transportation, insurance, and other local costs incidental to delivery of the goods to their final destination.

10.3 Prices quoted by the tenderer shall be fixed during the Tender's performance of the contract and not subject to variation on any account. A tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected, pursuant to paragraph 22.

11. Tender Currencies

11.1 Prices shall be quoted in Kenya shillings

12. Tenderers Eligibility and Qualifications.

12.1 Pursuant to paragraph 1 of section III, the tenderer shall furnish, as part of its tender, documents establishing the tenderers eligibility to tender and its qualifications to perform the contract if it's tender is accepted.

12.2 The documentary evidence of the tenderers eligibility to tender shall establish to the Procuring entity's satisfaction that the tenderer, at the time of submission of its tender, is from an eligible source country as defined under paragraph I of section III.

12.3 The documentary evidence of the tenderers qualifications to perform the contract if its tender is accepted shall establish to the Procuring entity's satisfaction:

(a) That, in the case of a tenderer offering to supply goods under the contract which the tenderer did not manufacture or otherwise produce, the tenderer has been duly authorized by the goods' Manufacturer or producer to supply the goods;

(b) That the tenderer has the financial, technical, and production capability necessary to perform the contract;

(b) That, in the case of a tenderer not doing business within Kenya, the tenderer is or will be (if awarded the contract) represented by an Agent in Kenya equipped, and able to carry out the Tenderer's maintenance, repair, and spare parts-stocking obligations prescribed in the Conditions of Contract and/or Technical Specifications.

13. Goods' Eligibility and Conformity to Tender Document.

13.1 Pursuant paragraph 2 of this section, the tenderer shall furnish, as part of its tender, documents establishing the eligibility and conformity to the tender documents of all goods, which the tenderer proposes to supply under the contract.

13.2 The documentary evidence of the eligibility of the goods shall consist of a statement in the Price Schedule of the country of origin of the goods and services offered which a certificate of origin issued at the time of shipment shall confirm.

13.3 The documentary evidence of conformity of the goods to the tender documents may be in the form of literature, drawings, and data, and shall consist of:

(a) A detailed description of the essential technical and performance characteristics of the goods;

(b) A list giving full particulars, including available sources and current prices of spare parts, special tools, etc., necessary for the proper and continuing functioning of the goods for a period of two (2) years, following commencement of the use of the goods by the Procuring entity; and

(c) A clause-by-clause commentary on the Procuring entity's Technical Specifications demonstrating substantial responsiveness of the goods and services to those specifications, or a statement of deviations and exceptions to the provisions of the Technical Specifications.

13.4 For purposes of the commentary to be furnished pursuant to paragraph 13.3(c) above, the tenderer shall note that standards for workmanship, material, and equipment, as well as references to brand names or catalogue numbers designated by the Procurement entity in its Technical Specifications, are intended to be descriptive only and not restrictive. The tenderer may substitute alternative standards, brand names, and/or catalogue numbers in its tender, provided that it demonstrates to the Procurement entity's satisfaction that the substitutions ensure substantial equivalence to those designated in the Technical Specifications.

14. Tender Security

14.1 The tenderer shall furnish, as part of its tender, a tender security for the amount specified in the Invitation to tender.

14.2 The tender security is required to protect the Procuring entity against the risk of Tenderer's conduct which would warrant the security's forfeiture, pursuant to paragraph 14.7

14.3 The tender security shall be denominated in Kenya Shillings and shall be in the form of a **bank guarantee** only and should be valid for **thirty (30) days** beyond the validity of the tender.

14.4 Any tender not secured in accordance with paragraph 14.1 and 14.3 will be rejected by the Procuring entity as nonresponsive, pursuant to paragraph 22.

14.5 Unsuccessful Tenderer's tender security will be discharged or returned as promptly as possible as but not later than thirty (30) days after the expiration of the period of tender validity prescribed by the Procuring entity.

14.6 The successful Tenderer's tender security will be discharged upon the tenderer signing the contract, pursuant to paragraph 30, and furnishing the performance security, pursuant to paragraph 31.

14.7 The tender security may be forfeited:

(a) if a tenderer withdraws its tender during the period of tender validity specified by the procuring entity on the Tender Form; or

(b) In the case of a successful tenderer, if the tenderer fails:

(i) To sign the contract in accordance with paragraph 30

Or

(ii) To furnish performance security in accordance with paragraph 31.

15. Validity of Tenders

15.1 Tenders shall remain valid for **180 days** or as specified in the tender documents after date of tender opening prescribed by the Procuring entity, pursuant to paragraph 18. A tender valid for a shorter period shall be rejected by the Procuring entity as nonresponsive.

15.2 In exceptional circumstances, the Procuring entity may solicit the Tenderer's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The tender security provided under paragraph 14 shall also be suitably extended. A tenderer may refuse the request without forfeiting its tender security. A tenderer granting the request will not be required nor permitted to modify its tender.

16. Format and Signing of Tender

16.1 The Tenderer shall prepare two copies of the tender, clearly marking each "ORIGINAL TENDER" and "COPY OF TENDER," as appropriate. In the event of any discrepancy between them, the original shall govern.

16.2 The original and all copies of the tender shall be typed or written in indelible ink and shall be signed by the tenderer or a person or persons duly authorized to bind the tenderer to the contract. Written power-of-attorney accompanying the tender shall indicate the latter authorization. The person or persons signing the tender shall initial all pages of the tender, except for unamended printed literature.

16.3 The tender shall have no interlineations, erasures, or overwriting except as necessary to correct errors made by the tenderer, in which case such corrections shall be initialled by the person or persons signing the tender.

17. Sealing and Marking of Tenders

17.1 The tenderer shall seal the original and each copy of the tender in separate envelopes, duly marking the envelopes as "ORIGINAL" and "COPY." The envelopes shall then be sealed in an outer envelope.

17.2 The inner and outer envelopes shall:

a) Be addressed to the Procuring entity at the following address:

THE MANAGING DIRECTOR
KENYA BUREAU OF STANDARDS
P.O.BOX 54974 – 00200
POPO ROAD
OFF MOMBASA ROAD BEHIND BELLEVUE CINEMA
NAIROBI

Bear the tender no. KEBS/T017/2020/2021: SUPPLY, IMPLEMENTATION AND COMMISSIONING OF KEBS PRIVILEGED ACCESS MANAGEMENT SOLUTION and the words**:** "DO NOT OPEN BEFORE" 10.00 am on **Tuesday 30th March 2021.**

17.3 The inner envelopes shall also indicate the name and address of the tenderer to enable the tender to be returned unopened in case it is declared “late”.

17.4 If the outer envelope is not sealed and marked as required by paragraph 17.2, the Procuring entity will assume no responsibility for the tender’s misplacement or premature opening.

18 Deadline for Submission of Tenders

18.1 Tenders must be received by the Procuring entity at the address specified under paragraph 17.2 no later than **10.00 am on Tuesday 30th March 2021.**

18.2 The Procuring entity may, at its discretion, extend this deadline for the submission of tenders by amending the tender documents in accordance with paragraph 6, in which case all rights and obligations of the Procuring entity and candidates previously subject to the deadline will thereafter be subject to the deadline as extended.

Submission of Tenders

19. Opening of Tenders

19.1 The Procuring entity will open all tenders in the presence of tenderers' representatives who choose to attend, at **10.00 am on Tuesday 30th March 2021** and in the following location:

KENYA BUREAU OF STANDARDS
OFF MOMBASA ROAD
POPO ROAD
BEHIND BELLEVUE CINEMA
CONFERENCE ROOM

The tenderers' representatives who are present shall sign a register evidencing their attendance.

19.2 The tenderers' names, tender modifications or withdrawals, tender prices, discounts, and the presence or absence of requisite tender security and such other details as the Procuring entity, at its discretion, may consider appropriate, will be announced at the opening.

19.3 The Procuring entity will prepare minutes of the tender opening.

20. Clarification of Tenders

20.1 To assist in the examination, evaluation and comparison of tenders the Procuring entity may, at its discretion, ask the tenderer for a clarification of its tender. The request for clarification and the response shall be in writing, and no change in the prices or substance of the tender shall be sought, offered, or permitted.

20.2 Any effort by the tenderer to influence the Procuring entity in the Procuring entity's tender evaluation, tender comparison or contract award decisions may result in the rejection of the tenderers' tender.

21. Preliminary Examination

21.1 The Procuring entity will examine the tenders to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the tenders are generally in order.

21.2 Arithmetical errors shall lead to disqualification of the bid.

21.3 The Procuring entity may waive any minor informality or non-conformity or irregularity in a tender which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any tenderer.

21.4 Prior to the detailed evaluation, pursuant to paragraph 23, the Procuring entity will determine the substantial responsiveness of each tender to the tender documents. For purposes of these paragraphs, a substantially responsive tender is one, which conforms to all the terms and conditions of the tender documents without material deviations. The Procuring entity's determination of a tender's responsiveness is to be based on the contents of the tender itself without recourse to extrinsic evidence.

21.5 If a tender is not substantially responsive, it will be rejected by the Procuring entity and may not subsequently be made responsive by the tenderer by correction of the nonconformity.

22. Evaluation and Comparison of Tenders

22.1 The Procuring entity will evaluate and compare the tenders, which have been determined to be substantially responsive, pursuant to paragraph 22.

22.2 The Procuring entity's evaluation of a tender will exclude and not take into account:

(a) in the case of goods manufactured in Kenya or goods of foreign origin already located in Kenya, sales and other similar taxes, which will be payable on the goods if a contract is awarded to the tenderer; and

(b) Any allowance for price adjustment during the period of execution of the contract, if provided in the tender.

22.3 The comparison shall be of the ex-factory/ex-warehouse/off-the-shelf price of the goods offered from within Kenya, such price to include all costs, as well as duties and taxes paid or payable on components and raw material incorporated or to be incorporated in the goods.

22.4 The Procuring entity's evaluation of a tender will take into account, in addition to the tender price and the price of incidental services, the following factors, in the manner and to the extent indicated in paragraph 23.5 and in the technical specifications:

(a)Delivery schedule offered in the tender;

(b)Deviations in payment schedule from that specified in the Special Conditions of Contract;

(c)The cost of components, mandatory spare parts, and service;

(d)The availability in Kenya of spare parts and after-sales services for the equipment offered in the tender.

22.5 Pursuant to paragraph 23.4 the following evaluation methods will be applied:

(a)*Delivery schedule.*

The Procuring entity requires that the goods under the Invitation for Tenders shall be delivered at the time specified in the Schedule of Requirements. Tenders offering deliveries longer than the procuring entity's required delivery time will be treated as non-responsive and rejected.

(b) Deviation in payment schedule.

Tenderers shall state their tender price for the payment of schedule outlined in the special conditions of contract. Tenders will be evaluated on the basis of this base price. Tenderers are, however, permitted to state an alternative payment schedule and indicate the reduction in tender price they wish to offer for such alternative payment schedule. The Procuring entity may consider the alternative payment schedule offered by the selected tenderer.

(c) Spare parts and after sales service facilities.

Tenderers must offer items with service and spares parts back-up. Documentary evidence and locations of such back- up must be given. Where a tenderer offers items without such back-up in the country, he must give documentary evidence and assurance that he will establish adequate back-up for items supplied.

23. Contacting the Procuring entity

23.1 Subject to paragraph 20, no tenderer shall contact the Procuring entity on any matter relating to its tender, from the time of the tender opening to the time the contract is awarded.

23.2 Any effort by a tenderer to influence the Procuring entity in its decisions on tender evaluation, tender comparison, or contract award may result in the rejection of the Tenderer's tender.

Award of Contract

24. Post-qualification

24.1 In the absence of pre-qualification, the Procuring entity will determine to its satisfaction whether the tenderer that is selected as having submitted the lowest evaluated responsive tender is qualified to perform the contract satisfactorily.

24.2 The determination will take into account the tenderer financial, technical, and production capabilities. It will be based upon an examination of the documentary evidence of the tenderers qualifications submitted by the tenderer, pursuant to paragraph 12.3, as well as such other information as the Procuring entity deems necessary and appropriate.

25.3 An affirmative determination will be a prerequisite for award of the contract to the tenderer. A negative determination will result in rejection of the Tenderer's tender, in which event the Procuring entity will proceed to the next lowest evaluated tender to make a similar determination of that Tenderer's capabilities to perform satisfactorily.

25. Award Criteria

25.1 Subject to paragraph 10, 23 and 28 the Procuring entity will award the contract to the successful tenderer(s) whose tender has been determined to be substantially responsive and has been determined to be the lowest evaluated tender, provided further that the tenderer is determined to be qualified to perform the contract satisfactorily.

26. Procuring entity's Right to Vary quantities

26.1 The Procuring entity reserves the right at the time of contract award to increase or decrease the quantity of goods originally specified in the Schedule of requirements without any change in unit price or other terms and conditions.

27. Procuring entity’s Right to Accept or Reject Any or All Tenders

27.1 The Procuring entity reserves the right to accept or reject any tender, and to annul the tendering process and reject all tenders at any time prior to contract award, without thereby incurring any liability to the affected tenderer or tenderers or any obligation to inform the affected tenderer or tenderers of the grounds for the Procuring entity’s action.

28. Notification of Award

28.1 Prior to the expiration of the period of tender validity, the Procuring entity will notify the successful tenderer in writing that its tender has been accepted.

28.2 The notification of award will constitute the formation of the Contract.

28.3 Upon the successful Tenderer’s furnishing of the performance security pursuant to paragraph 30, the Procuring entity will promptly notify each unsuccessful Tenderer and will discharge its tender security, pursuant to paragraph 14.

29. Signing of Contract

29.1 At the same time as the Procuring entity notifies the successful tenderer that its tender has been accepted, the Procuring entity will send the tenderer the Contract Form provided in the tender documents, incorporating all agreements between the parties.

29.2 Within thirty (30) days of receipt of the Contract Form, the successful tenderer shall sign and date the contract and return it to the Procuring entity.

30. Performance Security

30.1 Within thirty (30) days of the receipt of notification of award from the Procuring entity, the successful tenderer shall furnish the performance security in accordance with the Conditions of Contract, in the Performance Security Form provided in the tender documents, or in another form acceptable to the Procuring entity.

30.2 Failure of the successful tenderer to comply with the requirement of paragraph 30 or paragraph 31 shall constitute sufficient grounds for the annulment of the award and forfeiture of the tender security, in which event the Procuring entity may make the award to the next lowest evaluated Candidate or call for new tenders.

31. Corrupt Fraudulent Practices

31.1 The Procuring entity requires that tenderers observe the highest standard of ethics during the procurement process and execution of contracts. In pursuance of this policy, the Procuring entity: -

(a) Defines, for the purposes of this provision, the terms set forth below as follows:

(i) “Corrupt practice” means the offering, giving, receiving or soliciting of any thing of value to influence the action of a public official in the procurement process or in contract execution; and

(ii) “Fraudulent practice” means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the

Procuring entity, and includes collusive practice among tenderer (prior to or after tender submission) designed to establish tender prices at artificial non-competitive levels and to deprive the Procuring entity of the benefits of free and open competition;

(b) Will reject a proposal for award if it determines that the tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question;

(c) Will declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded any contract if it at any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing, a contract.

31.2 Furthermore, tenderers shall be aware of the provision stated in the General Conditions of Contract.

Appendix to Instructions to Tenderers

Notes on the Appendix to the Instruction to Tenderers

1. The Appendix to instructions to tenderers is intended to assist the procuring entity in providing specific information in relation to corresponding clause in the instructions to Tenderers included in Section **B** and has to be prepared for each specific procurement.

2. The procuring entity should specify in the appendix information and requirements specific to the circumstances of the procuring entity, the procuring of the procurement, and the tender evaluation criteria that will apply to the tenders.

3. In preparing the Appendix the following aspects should be taken into consideration:

   (a) The information that specifies and complements provisions of Section II to be incorporated.

   (b) Amendments and/or supplements if any, to provisions of Section II as necessitated by the circumstances of the specific procurement to be also incorporated.

4. Section **B** should remain unchanged and can only be amended through the Appendix to instructions to tenders.

5. Any clause to be included in the appendix to instructions to tenderers must be consistent with the applicable public procurement law and regulations

Appendix to instructions to tenders

The following information for the Solution Supply, Implementation and Commissioning of Next Generation Firewall shall complement, supplement, or amend, the provisions on the instructions to tenderers. Wherever there is a conflict between the provisions of the instructions to tenderers and the provisions of the appendix, the provisions of the appendix herein shall prevail over those of the instructions to tenderers.

Instruction to tender reference	***instructions to tenderers***
1	**Eligible tenderers** This Invitation for Tenders is open to all tenderers whose companies are Registered in Kenya.
3	**Cost of tendering** Price for the Hard Copy of the Tender document will be charged Kshs.1000.00. soft copies downloaded will be issued free of charge from KEBS website at **www.kebs.org** 2.3 Clarification of tender document A prospective tenderer requiring any clarification of the tender document may notify KEBS in writing through; 1. procurement@kebs.org 2. info@kebs.org 3. saleria@kebs.org
5	**Clarification of tender document** A prospective tenderer requiring any clarification of the tender document may notify KEBS in writing through procurement@kebs.org saleria@kebs.org Clarification of tenders requested by the tenderer must be received by KEBS not later than seven (7) days prior to the deadline for closing of tenders. KEBS shall reply to any clarifications sought by the tenderer within three (3) working days excluding weekends of receiving the request to enable the tenderer to make timely submission of its tender.
11	Tender Currencies Prices shall be quoted in Kenya Shillings.
14	**Tender Security** Original tender security of **2%** of the Tender sum in form of a **Bank guarantee** from a bank licensed and operating in Kenya, valid for thirty (30) days beyond the validity of the tender (180 days). This shall be in the format provided in the tender document (Section H). Tender Security from an Insurance Company shall NOT be

	acceptable.
15	**Validity of Tenders** The period of tender validity will be **180 days** from the date of opening of the tender.
16	**Format and Signing of Tenders** Bidders Must submit One (1) original and one (1) Copy. The Tenderer shall seal the original and each copy of the tender in separate envelopes, duly marking the envelopes as “ORIGINAL” and “COPY.” The envelopes shall then be sealed in an outer envelope.
17	**Sealing and Marking of Tenders** The tender document shall be properly bound and paginated (each page of the tender submission must have a number and the numbers must be in chronological order), seal and submit two copies (one original and one copy) of the tender, clearly marking each “Original Tender” and “Copy of Tender,” as appropriate. The two shall then be sealed in an outer envelope marked with the words “Do Not Open Before” on or before **Tuesday 30th March 2021 at 1000hrs (East Africa Time).**
22	**EVALUATION AND COMPARISON OF TENDERS** The evaluation shall be carried out in three (3) stages i. Preliminary Evaluation ii. Technical Evaluation and iii. Financial Evaluation Preliminary evaluation shall be based on mandatory requirements and Technical Evaluation shall be rated. For Financial Evaluation the tender with the lowest evaluated price that meets all the requirements shall be considered for award of the contract subject to post qualification.
2.24	**Post qualification** Pursuant to Section 83 of PPADA, 2015, KEBS may conduct post qualification (due diligence) to determine to its satisfaction whether the tenderer that is selected as having submitted the lowest evaluated responsive tender is qualified to perform the contract satisfactorily.
2.25 `	**Award of tender** Subject to submission of the Performance Security, KEBS will award the contract to the successful tenderers whose tender has been determined to be substantially responsive and has been determined to be the tender with the lowest evaluated price, provided further that the tenderer is determined to be qualified to perform the contract satisfactorily.

2.29	**Performance Security** The amount of Performance Security shall be 10% of the contract value in the format of the Performance Security Form provided in the tender document in the form of a **bank guarantee** drawn by a bank licensed by the Central Bank of Kenya.
25	**Award Criteria** ***This is a single award tender where the tender shall be awarded to the lowest evaluated bidder so long as the bidder has passed both the mandatory/preliminary and the technical requirements.***

Section C - General Conditions of Contract

1. Definitions

1.1 In this Contract, the following terms shall be interpreted as indicated:

(a) "The Contract" means the agreement entered into between the Procuring entity and the tenderer, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

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

(c) "The Goods" means all of the equipment, machinery, and/or other materials, which the tenderer is required to supply to the Procuring entity under the Contract.

(d) "The Procuring entity" means the organization purchasing the Goods under this Contract.

(e) "The tenderer" means the individual or firm supplying the Goods under this Contract.

2. Application

2.1 These General Conditions shall apply in all Contracts made by the Procuring entity for the procurement of goods.

3. Country of Origin

3.1 For purposes of this Clause, "origin" means the place where the Goods were mined, grown, or produced.

3.2 The origin of Goods and Services is distinct from the nationality of the tenderer.

4. Standards

4.1 The Goods supplied under this Contract shall conform to the standards mentioned in the Technical Specifications.

5. Use of Contract Documents and Information

5.1 The Candidate shall not, without the Procuring entity's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring entity in connection therewith, to any person other than a person employed by the tenderer in the performance of the Contract.

5.2 The tenderer shall not, without the Procuring entity's prior written consent, make use of any document or information enumerated in paragraph 5.1 above.

5.3 Any document, other than the Contract itself, enumerated in paragraph 5.1 shall remain the property of the Procuring entity and shall be returned (all copies) to the Procuring entity on completion of the Tenderer's performance under the Contract if so required by the Procuring entity.

6. Patent Rights

6.1 The tenderer shall indemnify the Procuring entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof in the Procuring entity's country.

7. Performance Security

7.1 Within thirty (30) days of receipt of the notification of Contract award, the successful tenderer shall furnish to the Procuring entity the performance security in the amount specified in Special Conditions of Contract.

7.2 The proceeds of the performance security shall be payable to the Procuring entity as compensation for any loss resulting from the Tenderer's failure to complete its obligations under the Contract.

7.3 The performance security shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Procuring entity and shall be in the form of a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in Kenya or abroad, acceptable to the Procuring entity, in the form provided in the tender documents.

7.4 The performance security will be discharged by the Procuring entity and returned to the Candidate not later than thirty (30) days following the date of completion of the Tenderer's performance obligations under the Contract, including any warranty obligations, under the Contract.

8. Inspection and Tests

8.1 The Procuring entities or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Contract specifications. The Procuring entity shall notify the tenderer in writing, in a timely manner, of the identity of any representatives retained for these purposes.

8.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s), at point of delivery, and/or at the Goods' final destination. If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring entity.

8.3 Should any inspected or tested Goods fail to conform to the Specifications, the Procuring entity may reject the Goods, and the tenderer shall either replace the rejected Goods or make alterations necessary to meet specification requirements free of cost to the Procuring entity.

8.4 The Procuring entity's right to inspect, test and, where necessary, reject the Goods after the Goods' arrival shall in no way be limited or waived by reason of the Goods having previously been inspected, tested, and passed by the Procuring entity or its representative prior to the Goods' delivery.

8.5 Nothing in paragraph 8 shall in any way release the tenderer from any warranty or other obligations under this Contract.

9. Packing

9.1 The tenderer shall provide such packing of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in theContract.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract.

10. Delivery and Documents

10.1 Delivery of the Goods shall be made by the tenderer in accordance with the terms specified by Procuring entity in its Schedule of Requirements and the Special Conditions of Contract

11. Insurance

11.1 The Goods supplied under the Contract shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery in the manner specified in the Special conditions of contract

12. Payment

12.1 The method and conditions of payment to be made to the tenderer under this Contract shall be specified in Special Conditions of Contract.

12.2 Payments shall be made promptly by the Procuring entity as specified in the contract.

13. Prices

13.1 Prices charged by the tenderer for Goods delivered and Services performed under the Contract shall not, with the exception of any price adjustments authorized in Special Conditions of Contract, vary from the prices by the tenderer in its tender.

14. Assignment

14.1 The tenderer shall not assign, in whole or in part, its obligations to perform under this Contract, except with the Procuring entity’s prior written consent.

15. Subcontracts

15.1 The tenderer shall notify the Procuring entity in writing of all subcontracts awarded under this Contract if not already specified in the tender. Such notification, in the original tender or later, shall not relieve the tenderer from any liability or obligation under the Contract.

16. Termination for Default

16.1 The Procuring entity may, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the tenderer, terminate this Contract in whole or in part:

(a) If the tenderer fails to deliver any or all of the Goods within the period(s) specified in the Contract, or within any extension thereof granted by the Procuring entity.
(b) If the tenderer fails to perform any other obligation(s) under the Contract.

(c) If the tenderer, in the judgment of the Procuring entity has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

16.2 In the event the Procuring entity terminates the Contract in whole or in part, it may procure, upon such terms and in such manner, as it deems appropriate, Goods similar to those undelivered, and the tenderer shall be liable to the Procuring entity for any excess costs for such similar Goods.

17. Liquidated Damages

17.1 If the tenderer fails to deliver any or all of the goods within the period(s) specified in the contract, the procuring entity shall, without prejudice to its other remedies under the contract, deduct from the contract prices liquidated damages sum equivalent to 0.5% of the delivered price of the delayed goods up to a maximum deduction of 10% of the delayed goods. After this the tenderer may consider termination of the contract.

18. Resolution of Disputes

18.1 The procuring entity and the tenderer shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the Contract.

18.2 If, after thirty (30) days from the commencement of such informal negotiations both parties have been unable to resolve amicably a contract dispute, either party may require adjudication in an agreed national or international forum, and/or international arbitration.

19. Language and Law

19.1 The language of the contract and the law governing the contract shall be English language and the Laws of Kenya respectively unless otherwise stated.

20. Force Majeure

20.1 The tenderer shall not be liable for forfeiture of its performance security, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

Section D. Special Conditions of Contract

1. Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the General Conditions of Contract.

2. General conditions of the contract clause 7.1 performance security.
The performance security shall be in the amount of 10% of the contract price and shall remain valid for **30 days** beyond the last date of installation and commissioning of the system.

3. The tender price shall be in Kenya shillings

Section E. Schedule of Requirements

Number	Description	Quantity	Delivery schedule Start: End:
	SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL		

(Shipment) In weeks/months from ______________________

Indicate your Delivery schedule for the goods/service after receipt of a confirmed Purchase Order from the Kenya Bureau of Standards.

Section F. Technical Specifications

TERMS OF REFERENCE: SUPPLY, IMPLEMENTATION AND COMMISSIONING OF NEXT GENERATION FIREWALL

1.0 Introduction and Background

The Kenya Bureau of Standards (KEBS) has remained the premier government agency for the provision of Standards, Metrology and Conformity Assessment (SMCA) services since its inception in 1974. Over that period its main activities have grown from the development of standards and quality control for a limited number of locally made products in the 1970s to the provision of more comprehensive Standards development, Metrology, Conformity Assessment, Training and Certification services. With the re-establishment of the East African Community (EAC) and Common Market for Eastern and Southern Africa (COMESA), KEBS activities now include participation in the development and implementation of SMCA activities at the regional level where it participates in the harmonization of standards, measurements and conformity assessment regimes for regional integration. KEBS operates the National Enquiry Point in support of the WTO Agreement on Technical Barriers to Trade (TBT). As part of overall digital strategy in implementing secure and industry standard technology, security management processes and supporting ICT management applications, KEBS is looking to procure a Next Generation firewalls to be deployed on premise for securing the network against internal and external threats.

The successful bidder is expected to supply, deliver, implement and test/commission the next generation firewall solution. The specifications listed in the specifications list the desired features of these firewalls which the bidders must adhere to. The bidder will also offer technical maintenance and support for a period of three (3) years.

1.1 Scope of Works/Service

1. Supply, Installation & commissioning of Next Generation Firewall and Firewall Management Appliance Solution.
2. Provision of initial and extended warranties and technical support services (including detailed initial acquisition costs and on-going support for three (3) years.
3. On-site installation and setup, software configuration and user settings
4. Migration of the security settings and policies from existing firewall i.e. Fortigate and Fortimail Appliances.
5. Knowledge Transfer Training for software configuration for Next Generation Firewalls to at least 5 ICT staff
6. Provide local Vendor Training for 2 ICT staff to be trained to configure, operate, and maintain the proposed solution.
7. The Bidder will be responsible for any upgrades and patches of the proposed solution during the contract period.

1.2 Project Management:

1. Bidders shall provide a project management methodology.
2. A project manager shall be assigned to handle the project.
3. Throughout the life cycle of the project, project manager must provide regular and on-request status and progress reports on the achievement of the project.
4. Throughout the life cycle of the project, KEBS representatives will have the right to request regular and non-regular meetings to follow up with the project manager on the achievements of the project.

1.3 Delivery, Installation, Configuration, Testing and Commissioning:

1. The Successful Bidder must assess the existing setup before implementing the solution.
2. Testing and commissioning criteria shall be developed during the project plan.
3. All software, documentation, manuals, instructions, labels shall be in Standard English.

2.0 EVALUATION CRITERIA

STAGE 1: MANDATORY EVALUATION CRITERIA STAGE

(Required to proceed to the Technical Evaluation Stage): Failure to provide any of the below-mentioned documents will lead to automatic disqualification of the firm at the mandatory evaluation stage. The bidders that will meet the mandatory requirements above will qualify to proceed to mandatory technical compliance evaluation stage.

No	**Requirements**	Indicate page submitted in the tender document
MR 1	Submit 1 (one) Original and 1 (one) copy of the tender document and be addressed as stated in the invitation to tender	
MR 2	Bidding documents must be paginated. All bidders are required to submit their documents paginated in a continuous ascending order from the first page to the last in this format; (i.e. 1,2,3. . n) w h ere n is the last page	
MR 3	Submit a copy of company‘s Valid Certificate of Registration Incorporation/Business name	
MR 4	Provide copy of the company's current KRA Tax Compliance Certificate **(To be verified on the KRA TCC Checker)**	
MR 5	Submit Valid CR 12 Form	
MR 6	Submit Valid County Government Business Permit	
MR 7	Original Bid Bond of 2% of the Total tender sum and valid for **180 days** from date of tender opening	
MR 8	Duly filled, signed and stamped Business Questionnaire	
MR 9	Duly completed Tender form signed and Stamped	
MR 10	Duly completed Anti-Corruption Declaration signed and stamped	
MR 11	Must Provide proof of Valid Current Certified Manufacturer's Authorization Form signed by the manufacturer to sell/service the product on the proposed **NEXT GENERATION FIREWALL (To be Verified).**	
MR 12	Must Provide proof of Valid Current Certified Manufacturer's Authorization Form signed by the manufacturer of the existing appliances to be migrated. **(To be Verified).**	
MR 13	Provide Certified Copies of audited accounts for the company for the last three years 2017 & 2018 & 2019	
MR 14	Submit with tender a valid ICT Authority Accredited Certificate in Network Security. **(To be Verified)**	
MR15	Provide original datasheet for the proposed solution from OEM (Original Equipment Manufacturer)	
MR16	Duly completed signed and stamped NON-DEBARMENT Declaration Form	

STAGE 2: TECHNICAL COMPLIANCE EVALUATION STAGE

2.1 Mandatory Technical Compliance Evaluation Stage

(a) Compliance to Technical Specifications

Bidders are expected to demonstrate compliance to the systems specifications in the bidder response column. The response should be comprehensive to demonstrate understanding of KEBS requirements.

“Yes”, “No” or “To comply” responses will not be accepted. Any bidder who gives this kind of response shall be assessed as “NO” in the Technical Compliance Evaluation column and consequently failed in this stage of evaluation.

Technical Compliance Evaluation Criteria

- Yes – Response satisfactory and demonstrates compliance to the specification.
- No – Response does not demonstrate compliance to the specification

A “NO” assessment in any of the specifications leads to automatic disqualification from the next stage of evaluation.

NOTE

The bidders **MUST give Reference to both** Technical proposal and Data sheet that the proposed solution meets these requirements. A reference to the technical proposal and datasheet must be provided with clear page and paragraph numbers in the bidder’s response column. When the page and paragraph reference on the datasheet and Technical proposal is not given, the bidder’s solution will be considered not meeting the mandatory requirements and therefore Non-responsive.

TECHNICAL COMPLIANCE

TECHNICAL AND PERFORMANCE SPECIFICATIONS FOR NEXT GENERATION FIREWALLS		
NEXT GENERATION FIREWALLS – QUANTITY TWO (2)		
Requirements	**Bidder’s Remarks and References. Indicate page number and section where the specific item is addressed**	**Technical Compliance Yes/No**
1. General requirements		
The Vendor of the Firewall software must have at least 20 years of experience in the security market		
The vendor must exclusively provide Internet security solutions.		

The vendor must provide evidence of year over year leadership positions in enterprise firewall, UTM firewalls and intrusion prevention based on independent security industry data.		
The vendor must be capable of serving the entire scope of security Firewall requirements, including throughput, connection rate and next generation security application enablement for all network deployments, from small office to data center in a single hardware appliance.		
The vendor must have a security Firewall solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, Sand-boxing & Scrubbing (Threat Emulation and Threat Extraction) all managed from a central platform.		
The next generation Firewall must be capable of supporting these next generation security applications on a unified platform.		
a. Stateful Inspection Firewall		
b. Intrusion Prevention System		
c. User Identity Acquisition		
d. Application Control and URL filtering		
e. Anti – Bot and Anti – Virus		
f. Threat Emulation (Sandboxing)		
g. Threat Extraction (scrubbing)		
h. HTTPS Inspection		
i. Identity Awareness		
j. Anti – Spam and Email Security		
k. IPsec VPN		
l. Data Loss Prevention		
m. Mobile Access		
n. Security Policy Management		

o. Monitoring and Logging		
p. Logging and Status		
q. Event Correlation and Reporting		
r. Networking & Clustering		
s. Virtual Systems		
The vendor must supply all industry certifications of the solution.		
Vendor must have the capability to provide a solution to mitigate Distributed Denial of Service attacks.		
2. Requirements for Next Generation Firewall		
The Firewall must use Stateful Inspection based on granular analysis of communication and application state to track and control the network flow.		
The Firewalls must be capable of supporting throughputs, connection rates and concurrent connections requirements as below: Real World Enterprise Testing Conditions: a. 9 Gbps of Threat Prevention. b. 22 Gbps of NGFW c. 25 Gbps IPS. d. 47 Gbps of firewall throughput Lab Conditions: e. 11.0 Gbps IPsec Throughput f. 75Gbps Firewall Throughput (1518B UDP). g. 310,000 connections/second. h. Minimum - 6 million concurrent connections.		
Solution must support access control for at least 150 predefined /services/protocols		
Must provide security rule hit count statistics to the management application.		
Must allow security rules to be enforced within time intervals to be configured with an expiry date/time.		
The communication between the management servers and the security firewalls must be encrypted and authenticated with PKI Certificates.		
The firewall must support user, client and session authentication methods.		

The following user authentication schemes must be supported by the firewall and VPN module: tokens (ie - SecureID), TACACS, RADIUS and digital certificates		
Solution must include a local user database to allow user authentication and authorization without the need for an external device		
Solution must support DCHP, server and relay		
Solution must support HTTP & HTTPS proxy.		
Solution must include the ability to work in Transparent/Bridge mode.		
Solution must support Firewall high availability and load sharing with state synchronization		
IPv6 Support		
Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface		
Solution must support IPv6 traffic handling on IPS and APP module, Firewall, Identity Awareness, URL Filtering, Antivirus and Anti-Bot		
Solution must Support 6 to 4 NAT, or 6 to 4 tunnels		
Solution must support AD integration using ipv6 traffic		
Solution must support Smart view tracker / smart log able to show ipv6 traffic		
Platform shall support ability to display IPv6 routing table (separated per customer security context in CLI and GUI (EMS/Portal)		
Solution shall support the following Ipv6 RFCs:		
RFC 1981 Path Maximum Transmission Unit Discovery for IPv6		
RFC 2460 IPv6 Basic specification		
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
RFC 3596 DNS Extensions to support IPv6		

RFC 4007 IPv6 Scoped Address Architecture		
RFC 4193 Unique Local IPv6 Unicast Addresses		
RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.		
RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)		
RFC 4443 ICMPv6		
RFC 4861 Neighbor Discovery		
RFC 4862 IPv6 Stateless Address Auto-configuration		
Intrusion Prevention System		
Vendor must provide evidence of year over year leadership position of Gartner Magic Quadrant for Intrusion Prevention solutions and/or Enterprise network Firewall Gartner Magic Quadrant		
IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection		
IPS and firewall module must be integrated on one platform.		
The administrator must be able to configure the inspection to protect internal hosts only		
IPS must have options to create profiles for either client or server based protections, or a combination of both		
IPS must provide at least two pre-defined profiles/policies that can be used immediately		
IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage		
IPS must provide an automated mechanism to activate or manage new signatures from updates		
IPS must support network exceptions based on source, destination, service or a combination of the three		

IPS must include a troubleshooting mode which sets the in use profile to detect only, with one click without modifying individual protections		
IPS application must have a centralized event correlation and reporting mechanism		
The administrator must be able to automatically activate new protections, based on configurable parameters (performance impact, threat severity, confidence level, client protections, server protections)		
IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts and generic attack types without predefined signatures		
For each protection the solution must include protection type (server-related or client related), threat severity, performance impact, confidence level and industry reference		
IPS must be able to collect packet capture for specific protections		
IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)		
Vendor must supply evidence of leadership in protecting Microsoft vulnerabilities		
IPS and/or Application Control must include the ability to detect and block P2P & evasive applications		
The administrator must be able to define network and host exclusions from IPS inspection		
Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses		
Solution must provide VOIP protocols protections		
IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic		
IPS must have SCADA protections		

IPS must have a mechanism to convert SNORT signatures		
Solution must enforce Citrix protocol enforcement		
Solution must allow the administrator to easily block inbound and/or outbound traffic based on countries, without the need to manually manage the IP ranges corresponding to the country		
User Identity Acquisition		
Must be able to acquire user identity by querying Microsoft Active Directory based on security events		
Must have a browser based User Identity authentication method for non-domain users or assets		
Must have a dedicated client agent that can be installed by policy on users' computers that can acquire and report identities to the Security Gateway		
Must support terminal server environments		
The solution should integrate seamlessly with directory services, IF-MAP and Radius		
Impact on the domain controllers must be less than 3%.		
The identity solution should support terminal and citrix servers		
The Solution should allow identification through a proxy (example: X-forwarded headers)		
Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers		
Must support Kerberos transparent authentication for single sign on		
Must support the use of LDAP nested groups		
Must be able share or propagate user identities between multiple security gateways		
Must be able to create identity roles to be used across all security applications		
Application Control and URL Filtering		
Application control database must contain more than 8,000 known applications.		

Solution must have a URL categorization that exceeds 200 million URLs and covers more than 85% of Alexa’s top 1M sites		
Solution must be able to create a filtering rule with multiple categories.7		
Solution must be able to create a filtering for single site being supported by multiple categories.		
Solution must have users and groups granularity with security rules		
The security gateway local cache must give answers to 99% of URL categorization requests within 4 weeks in production		
The solution must have an easy to use, searchable interface for applications and URLs		
The solution must categorize applications and URLs by Risk Factor		
The application control and URLF security policy must be able to be defined by user identities		
The application control and URLF database must be updated by a cloud based service		
The solution must have unified application control and URLF security rules		
The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy		
The solution must provide a mechanism to limit application usage based on bandwidth consumption		
The solution must allow network exceptions based on defined network objects		
The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page		
Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category		
Solution must have a configurable bypass mechanisms		
Solution must provide an override mechanism on the categorization for the URL database		
The application control and URLF security policy must report on the rule hit count		

Anti-Bot and Anti-Virus		
Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall		
Anti-bot application must be able to detect and stop suspicious abnormal network behavior		
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		
Anti-Bot protections must be able to scan for bot actions		
The solution should support detection & prevention of Cryptors & ransomware viruses and variants (e.g. Wannacry, Cryptlocker , CryptoWall…) through use of static and/or dynamic analysis		
The solution should have mechanisms to protect against spear phishing attacks		
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		
The solution should have detection and prevention capabilities for DNS tunneling attacks		
Anti-Bot and Anti-Virus policy must be administered from a central console		
Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism		
Anti-virus application must be able to prevent access to malicious websites		
Anti-virus application must be able to inspect SSL encrypted traffic		
Anti-Bot and Anti-Virus must be have real time updates from a cloud based reputation services		
Anti-Virus must be able to stop incoming malicious files		
Anti-Virus must be able to scan archive files		
Anti-Virus and Anti-Bot policies must be		

centrally managed with granular policy configuration and enforcement		
The Anti-Virus should support more than 50 cloud based AV engines		
The Solution should support scanning for links inside emails		
The Anti-Virus should Scan files that are passing on CIFS protocol		
SSL Inspection (inbound / outbound)		
The Solution offers support for SSL Inspection/Decryption with leading performance across all threat mitigation technologies		
The solution should support Perfect Forward Secrecy (PFS , ECDHE cipher suites)		
The solution should support AES-NI,AES-GCM for improved throughput		
Threat emulation/sandboxing should be integrated with SSL Inspection		
The Solution should leverage the URL filtering data base to allow administrator to create granular https inspection policy		
The Solution can inspect HTTPS based URL Filtering without requiring SSL decryption		
Sandboxing and Emulation		
The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created		
1 Real-Time Prevention-unknown malware patient-0 in web browsing		
2 Real-Time Prevention-unknown malware patient-0 in email		
Deployment topologies:		
The solution should be part of a complete multi-layered threat prevention architecture (with IPS,AV,AB,URLF,APP FW)		
The solution should support Network based Threat emulation		
The solution should support Host based Threat emulation		
The solution should provide both onsite and cloud based implementations		
Pure cloud solution		
The solution should support 3rd party integration (public API)		
The solution should support deployment in inline mode		

The solution should support deployment in MTA (Mail Transfer Agent) mode, inspect TLS & SSL		
The solution should support deployment in TAP/SPAN port mode		
The solution should not require separate infrastructure for email protection & web protection		
Device must support cluster installation.		
Files supported:		
The solution should be able to emulate executable, archive files ,documents, JAVA and flash specifically:		
Threat Emulation supports these file types:		
File Extension		
.bz2		
.CAB		
.csv		
.com		
.cpl		
.doc		
.docx		
.dot		
.dotx		
.dotm		
.docm		
.exe		
.gz		
.hwp		
.iso		
.jar		
.js /.jse (*)		
.PIF		
.pdf		
.ppt		
.pptx		
.pps		
.pptm		
.potx		
.potm		
.ppam		
.ppsx		
.ppsm		
.rar		
.rtf		
.scr		

.Seven-Z		
.sldx		
.sldm		
.swf		
.tar		
.tbz2 .tbz .tb2		
.tgz		
.vbs (*)		
.vba (*)		
.vbe (*)		
.wsf (*)		
.wsh (*)		
*.xz		
Protocols		
The solution should be able to emulate executable, archive files ,documents, JAVA and flash specifically within various protocols:		
HTTP		
HTTPS		
SMTP		
SMTP TLS		
PO3		
FTP		
CIFS (SMB)		
OS support:		
The emulation engine should support multiple OS's such as XP and Windows7, 8,10 32/64bit including customized images		
The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft		
The engine should detect API calls, file system changes, system registry, network connections, system processes		
The solution should support static analysis for windows, mac OS-X, Linux or any x86 platform		
Sandboxing Technology:		
The emulation engine should be able to inspect, emulate, prevent and share the results of the sandboxing event into the anti-malware infrastructure		
The solution should be able to perform pre-emulation static filtering		

the solution would enable emulation of file sizes larger than 10 Mb in all types it supports		
The solutions should support automated machine learning based detection engines		
The solution should detect the attack at the exploitation stage – i.e. before the shell-code is executed and before the malware is downloaded/executed.		
The solution should be able to detect ROP and other exploitation techniques (e.g. privilege escalation) by monitoring the CPU flow		
The solution must be able to support scanning links inside emails for 0-days & unknown malware		
- scan history URLs recorded from emails last X days and check if rating changed (example: from clean to malicious rating)		
Average Emulation time of a suspected malware verdict as benign should be no more than 1 minute		
Average Emulation time of a suspected malware verdict as malware should be no more than 3 minutes		
The threat emulation solution should allow for 'Geo Restriction' which enables emulations to be restricted to a specific country		
The solution must provide the ability to Increase security with automatic sharing of new attack information with other gateways in means of signature updates etc.		
The emulation engine should exceed 90% catch rate on Virus Total tests where known malicious pdf's and exe's are modified with 'unused' headers in order to demonstrate the solutions capability to detect new, unknown malware		
The solution should detect C&C traffic according to dynamic ip/url reputation		
The solution should be able to emulate and extract files embedded in documents		
The solution should be able to scan documents containing URLs		
System Activity Detection:		
The solution should monitor for suspicious activity in:		
API calls		
File system changes		
System registry		
Network connections		

System processes		
File creation and deletion		
File modification		
Kernel code injection		
Detect Privilege escalation attempts		
Kernel modifications (memory changes performed by kernel code, not the fact that a driver is loaded - this is covered by the item above)		
Kernel code behavior (monitor activity of non-user-mode code)		
Direct physical CPU interaction		
UAC(user access control) bypass detection		
Anti-Evasion Technology:		
The solution should have anti-evasion capabilities detecting sandbox execution		
Solution should be resilient to cases where the shell-code or malware would not execute if they detect the existence of virtual environment. (proprietary hypervisor)		
time delays		
Solution should be resilient to delays implemented at the shell code or malware stages.		
shut-down, re-start		
Solution should be resilient to cases where the shell-code or malware would execute only upon a restart or a shutdown of the end point.		
User interaction		
Human Emulation: Solution should emulate real user activities such as mouse clicks, key strokes etc.		
Icon similarity: the solution should be able to identify icon that are similar to popular application documents		
evasion within flash file (swf)		
Management & Reporting		
The solution must provide the ability to be centrally managed		
Upon malicious files detection, a detailed report should be generated for each one of the malicious files.		
The detailed report must include:		
screen shots,		
time lines,		
registry key creation/modifications,		
file and processes creation,		
Network activity detected.		

Extraction of Malicious File Content (File Scrubbing/Flattening)		
The solution should Eliminate threats and remove exploitable content, including active content and embedded objects		
the solution should be able to Reconstruct files with known safe elements		
the solution should Provide ability to convert reconstructed files to PDF format		
the solution should Maintain flexibility with options to maintain the original file format and specify the type of content to be removed		
Anti-Spam & Email Security		
Anti-Spam and Email security application must be content and language agnostic		
Anti-Spam and Email security application must have real-time classification and protections based on detected spam outbreaks which are based on patterns and not content		
The Anti-Spam and Email security application must include IP reputation blocking based on an online service to avoid false positives		
Solution must include a Zero-hour protection mechanism for new viruses spread through email and spam without relying solely in heuristic or content inspection		
IPsec VPN		
Internal CA and External third party CA must be supported		
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 Diffie-Hellman Groups: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20	-	
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:		
Full Mesh (all to all),		
Star (remote offices to central site)		
Hub and Spoke (remote site through central site to another remote site)		

Solution must support the VPN configuration with a GUI using drag and drop object addition to VPN communities		
Solution must support clientless SSL VPNs for remote access.		
Solution must support L2TP VPNs, including support for iPhone L2TP client		
Solution must allow the administrator to apply security rules to control the traffic inside the VPN		
Solution must support domain based VPNs and route based VPNs using VTI's and dynamic routing protocols	-	
Solution must include the ability to establish VPNs with gateways with dynamic public IPs	-	
Solution must include IP compression for client-to-site and site-to-site VPNs		
FIREWALL MANAGEMENT APPLIANCE – QUANTITY ONE		
Requirements	**Bidder's Remarks and References**	**Technical Compliance Yes/No**
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		
Solution must be able to segment the rule base in favor of delegation of duties in which changes in one segment will not affect other segments		
Solution must be able to segment the rule base in a layered structure		
Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks		
Solution must be able to re-use segment of the rule base (e.g. use same segment of rules on different policy packages)		
Solution must have the granularity of administrators that works on parallel on same policy without interfering each other		
Solution must integrate logs, audit logs in one console to have context while working on the security policy		
Solution must be able to install threat related protections and access related rules separately in order to allow managing it by separate teams		
Security management application must be able to co-exist on the security gateway as an option.		
Security management application must support role based administrator		

accounts. For instance roles for firewall policy management only or role for log viewing only		
Solution must include a Certificate-based encrypted secure communications channel among all vendor distributed components belonging to a single management domain		
Solution must include an internal x.509 CA (Certificate Authority) that can generate certificates to gateways and users to allow easy authentication on VPNs		
Solution must include the ability to use external CAs, that supports PKCS#12, CAPI or Entrust standards		
All security applications must be managed from the central console		
The management must provide a security rule hit counter in the security policy		
Solution must include a search option to be able to easily query which network object contain a specific IP or part of it		
Solution must include the option to segment the rule base using labels or section titles to better organize the policy		
Solution must provide the option to save the entire policy or specific part of the policy		
Solution must have a security policy verification mechanism prior to policy installation		
Solution must have a security policy revision control mechanism		
Solution must provide the option to add management high availability, using a standby management server that is automatically synchronized with the active one, without the need for an external storage device		
Solution must include the ability to centrally distribute and apply new gateway software versions		
Solution must include a tool to centrally manage licenses of all gateways controlled by the management station		
Solution must have the capabilities for multi-domain management and support the concept of global security policy across domains		
The management GUI should have the ability to easily exclude IP address from the IPS signature definition		

The Log Viewer should have the ability to easily exclude IP address from the IPS logs when detected as false positive		
The management GUI should have the ability to easily get to IPS signature definition from the IPS logs		
The Log Viewer should have the ability view all of the security logs (fw,IPS ,urlf...) in one view pane (helpful when troubleshooting connectivity problem for one IP address)		
The Log Viewer should have the ability in the log viewer to create filter using the predefined objects (hosts ,network, groups, users...)		
The Log Viewer should have the ability in the log viewer to create custom multiple "saved filter" for use at a later time		
Solution must combine policy configuration and log analysis in a single pane, in order to avoid mistakes and achieve confidence of the change.		
Policy management solution must provide logs of similar rules to the user as he creates or modifies rules (= content logs)		
Solution GUI must provide easy navigation between hundreds of policies, each containing up to 1 million objects. Jumps between sub-policies and section titles must be provided as well as comprehensive search.		
Policy management must provide search of rules by packets, even without having logs of that packet in the system. Search should be integrated in the same pane as the policy configuration and return all results within few seconds.		
Security management solution must provide lookup of all references to any given network object in all of its policies and settings (= where used).		
Solution must provide built-in ticket management. A set of changes on the security policy must be automatically associated to a session in order to achieve proper accountability and documentation.		
Security management server must self-contain all validations, triggers and business processes in order to provide stable and reliable service for any user-defined client that is operating through its API.		

Security management must provide set of built-in security best practices which provide automatic score for various security regulations (= compliance blade).		
Security management must have option to alert users on possible misconfiguration in a central place, while still provide them a way to add exceptions to these possible misconfigurations (= compliance blade)		
User should provide NAT details for a network object in the scope of the network object. The inferred NAT rules should be added automatically to the NAT policy.		
User should be able to seamlessly treat IPV4, IPV6 and dynamic network objects in the same policy (criticism against Fortinet…)		
Security gateway should inspect network traffic, application context and data & content within 1 rule.		
IPS system should provide automatic actions on IPS Protections based on the user's definitions of his critical assets (= IPS tags)		
IPS system should provide intelligent profiles in three levels in the axis of security vs. throughput. User can choose to enable granular protections or instead to choose one of the intelligent profiles.		
Security management GUI must have same design language and capabilities in its single-domain as well as its multi-domain deployment.		
Security management must support automatic live synchronizations of its domains in high-availability deployment.		
Built-in SIEM system should have complete customization of overviews and reports generation for every logged event in every security field (access, threat prevention). (= Smart Event)		
Built-in SIEM system must have drill-down from the high-level security event to the granular logs that composed it. (= Smart Event)		
Threat Prevention Updates		
Vendor must provide the details of its threat prevention update mechanism and its ability to handle zero day attacks across all next generation threat prevention applications including IPS, Application Control, URL filtering, Anti-Bot and Anti-Virus		

Vendor must provide details on the re-categorization of URL, under the circumstances that a website has been comprised and possibly distributing malware		
Vendor should have the capability to provide incident handling		
Logging & Monitoring		
The central logging must be part of the management system. Alternatively administrators can install dedicated Log Servers		
Solution must provide the option to run on the management server or on a dedicated server		
Solution must be able to run on an X86 based open servers listed on a hardware compatibility list		
Solution must have the ability to log all rules (+30k logs/sec)		
Log viewer must have an indexed search capability		
Solution must have the ability to log all integrated security applications on the Firewall and including IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti – Spam, User Identity, Data Loss Prevention, Mobile Access		
Solution must include an automatic packet capture mechanism for IPS events to provide better forensic analysis		
Solution must provide different logs for regular user activity and management related logs		
Solution must be able to move from security log record to the policy rule with one mouse click.		
For each match rule or type of event Solution must provide at least the following event options: Log, alert, SNMP trap, email and execute a user defined script		
The logs must have a secure channel to transfer logging to prevent eavesdropping, Solution must be authenticated and encrypted		
The logs must be securely transferred between the Firewall and the management or the dedicated log server and the log viewer console in the administrator’s PC		
Solution must include the option to dynamically block an active connection from the log graphical interface without the need to modify the rule base		

Solution must support exporting logs in database format		
Solution must support automatic switch of the log file, based on a scheduled time or file size		
Solution must support adding exceptions to IPS enforcement from the log record		
Solution must be able to associate a username and machine name to each log record		
Solution must include a graphical monitoring interface that provides an easy way to monitor Firewalls status		
Solution must provide the following system information for each Firewall: OS, CPU usage, memory usage, all disk partitions and % of free hard disk space		
Solution must provide the status of each Firewall components (i.e. firewall, vpn, cluster, antivirus, etc)		
Solution must include the status of all VPN tunnels, site-to-site and client-to-site		
Solution must include customizable threshold setting to take actions when a certain threshold is reached on a Firewall. Actions must include: Log, alert, send an SNMP trap, send an email and execute a user defined alert		
Solution must include preconfigured graphs to monitor the evolution in time of traffic and system counters: top security rules, top P2P users, vpn tunnels, network traffic and other useful information. Solution must provide the option to generate new customized graphs with different chart types		
Solution must include the option to record traffic and system views to a file for later viewing at any time		
Solution must be able to recognize malfunctions and connectivity problems, between two points connected through a VPN, and log and alert when the VPN tunnel is down		
Event Correlation and Reporting		
Solution must be fully integrated in the management application		
Solution must include a tool to correlate events from all the Firewall features and third party devices		
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.		
The application must have 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		
The event correlation application must supply a graphical view events based on time		
Solution must show the distribution of events per country on a map		
Solution must allow the administrator to group events based on any of its characteristics, including many nesting levels and export to PDF		
Solution must include the option to search inside the list of events, drill down into details for research and forensics.		
It the event list view Solution must include the option to automatically generate small graphs or tables with the event, source and destination distribution		
Solution must detect Denial of Service attacks correlating events from all sources		
Solution must detect an administrator login at irregular hour		
Solution must detect credential guessing attacks		
Solution must report on all security policy installations		
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		
The reporting tool must support at least 25 filters that allow to customize a predefined report to be closest to administrator's needs		
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		

Solution must support the following reports formats: PDF & Excel		
Solution must support automatic report distribution by email, upload to FTP/Web server and an external custom report distribution script		
The reporting system must provide consolidated information about:		
The volume of connections that were blocked by security rule.		
Top sources of blocked connections, their destinations and services		
Top Rules used by the security policy		
Top security attacks detected by enforcement point (perimeter) determining their the top sources and destinations		
Number of installed and uninstalled policies in the enforcement point		
Top networking services		
Web activity by user detailing the top visited sites and top web users		
Top services that created most load for encrypted traffic		
Top VPN users performing the longest duration connections		
Management Portal		
Solution must include a browser based access to view in read-only the security policies, manage firewall logs and users providing access to managers and auditors without the need to use the management application		
Solution must include SSL support and configurable port		
Data Loss Prevention (DLP)		
Vendor must have an option to add a fully integrated Data Loss Prevention application		
DLP policy must be centrally managed with all other security applications		
DLP application must have a mechanism for end user self-incident handling		
DLP application must have over 500 pre-defined data types		
DLP must have an open scripting language to create customer data types relevant to any organization		
DLP must alert the data type owner when an incident occurs		
DLP application must cover transport		

types SMTP, HTTP/HTTPS, and FTP TCP protocols		
Mobility		
The vendor should have an option to provide a fully integrated secure mobility solution on the next generation firewall		
The solution must support both managed and unmanaged access devices, such as BYOD		
Best Practice Governance Risk and Compliance (GRC)		
Vendor must have an option to provide a fully integrated Governance Risk and Compliance application		
Vendor must have an option for Real Time Compliance Monitoring across all security services in the product		
Vendor must have an option to Deliver real-time assessment of compliance with major regulations (PCI-DSS,HiPPA,SOX...)		
Vendor must have an option for Instant notification on policy changes impacting compliance		
Vendor must have an option to Provide actionable recommendations to improve compliance		
Vendor must have an option to recommend Security Best Practices		
Vendor must have an option to Translate regulatory requirements into actionable security best practices		
Vendor must have an option to Monitor constantly Firewall configuration with the security best practices		
Vendor must have an option to Generate automated assessment reports for compliance rating with top regulations		
Vendor must have an option to Fully Integrate into Software Architecture & Management infrastructure		
Vendor must have an option to Check compliance with every policy change for all Network Security Software Blades		
Firewall Sizing and Recommendations		
Vendor must have a dedicated hardware solution to meet all next generation requirements of the customer		

Vendor must be able to supply a recommended hardware configuration based on the criteria of real world traffic and next generation security applications provided by the customer. Vendor must be able to supply the recommended platform for any combination of these next generation firewall application, with supporting evidence that the appliance will perform as expected.		
Enablement of next generation firewall applications		
Firewall		
Intrusion Prevention		
Application Control and URL filtering		
Anti-Bot		
Anti-Virus		
Threat Emulation & Extraction		
IPsec VPN		
Data Loss Prevention		
Anti-Spam		
Centralized security management		
Clustering or high availability.		
Physical Firewall Requirements – (Mandatory): • 10x1GbE copper. • Memory (RAM) 32 GB • 4 x 10 GB SFP+ ports. • 10G SFP+ Transceivers for the SFP+ ports + LC Connectors. **(Quantity 4 per firewall).** • Sync port. • USB 3.0 ports. • RJ45 console port. • Lights-out Management port. • Network card expansion slots. • USB Type-C console port • Management Port • 480GB SSD RAID1 Storage **(Two for redundancy).** • (Dual) Redundant hot-swap power supplies.		
Firewall Management Appliance Requirements (Mandatory)		
a. Appliance based.		
b. Managed Firewalls – 10.		
c. Peak Logs per Sec – 40,000		
d. Peak Indexed Logs per Sec – 6,000.		
e. Sustained Indexed Logs per Sec – 3,000		

f. GB per Day of Logs - 88		
g. Default Network s - 5x Copper GbE		
h. Memory (RAM) – 16GB		
i. Storage (HDD) Hot-Swappable – 1TB		

STAGE 3: TECHNICAL CAPACITY EVALUATION STAGE

2.2 Technical Capacity Evaluation

NO	Criteria Description	Weight	Indicate page submitted in the tender document
	EXPERIENCE OF THE FIRM		
1	Provide at least three (3) Contracts/LSO of similar/related assignments on Next Generation Firewall Solution within the last five years **(5 marks each to a maximum of 15 Marks) To be verified** Provide at least three (3) Contracts/LSO of similar/related assignments to the KEBS existing Firewall Solution to be migrated within the last five years **(5marks each to a maximum of 15 Marks) To be verified**	15 15	
2	Submit three (3) Recommendation Letters in official client letterheads from reputable organizations/clients listed references above (requirement No.1) addressed to Managing Director KEBS. **(5 Marks each recommendation letters to a maximum of 15 Marks) To be verified** Submit three (3) Recommendation Letters in official client letterheads from reputable organizations/clients listed references of the KEBS existing Firewall Solution to be migrated addressed to Managing Director KEBS. **(5 Marks each recommendation letters to a maximum of 15 Marks) To be verified**	15 15	
3	Minimum of Five (5) years' experience in a similar/related assignment **5 or more years of experience – 5 Marks** **Less than 5 years – 0 Mark**	5	
	KEY STAFF QUALIFICATIONS		
4	**<u>Project Manager/Team Lead</u>** **Qualifications** – Bachelor's Degree in related field – Attach Certificate **(2 Marks)** Three years' and above experience in Project planning and Management – Project Management Certification for the project manager. (Prince2 or PMP). **Attach Certificate (4 Marks)**	2 4	
5	**<u>Team Members (Two Engineers)</u>** **Qualifications –** Certified Professionals on the proposed Next Generation Firewall Solution. **(Attach Certifications) To be Verified** **(5 Marks Each Engineer to a maximum of 10 Marks)**	10	

	<u>**Team Members (Two Engineers)**</u> **Qualifications –** Certified Professionals on the KEBS existing Firewall Solution to be migrated **(Attach Certifications) To be Verified** **(5 Marks Each Engineer to a maximum of 10 Marks)**	10	
6	Provide a Technical proposal with detailed design of the proposed Next Generation Firewall solution	5	
7	Bidders Must attach a Project Implementation Plan which must contain at least: (i) Detailed activities and milestones (i) Timelines (ii) Resources required	2	
8	Draft SLA on the maintenance of the proposed Next Generation Firewall Solution	2	
	TOTAL	**100**	

NB: (Mandatory, Technical Compliance Evaluation and Technical Capacity Evaluation stage) and a pass score of 80 score and above qualifies for financial evaluation.

2.3 PRICE SCHEDULE

Description	**Qty**	**Unit Price**	**TOTAL PRICE (16% VAT inclusive)**
Next Generation Firewalls **(HA Cluster for 3 Years)** with; Sandboxing, Antivirus, Anti-bot, IPS, Application Control, URL Filtering, Identity Awareness, Antispam and Email Security	2		
Firewall Management Appliance with; Report, Firewall administration, Firewall Management, Correlation and Compliance Features. **(3 years)**	1		
Total Cost of Migration, Delivery, Implementation and Commissioning of Next Generation Firewalls	LOT		
Total Cost of Support and Maintenance Services **(3 Years)**	LOT		
Local Vendor Training of Staff	2		
		Sub-Total	
		Applicable Taxes	

		Grand Total (3 Years)	

Section G. Tender Form and Price Schedules

(i) Form of Tender

Date:______________________
Tender Nº: __________________

To: ……………………………
…………………………...
[Name and address of procuring entity]

Gentlemen and/or Ladies:

1. Having examined the tender documents including Addenda Nos..*[Insert numbers],*
The receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver*……………………………………………… ………….*
[Description of services] In conformity with the said tender documents for the sum of .... *[Total tender amount in words and figures]*

2. We undertake, if our Tender is accepted, to provide the services in accordance with the services schedule specified in the Schedule of Requirements.

3. If our Tender is accepted, we will obtain the guarantee of a bank in a sum equivalent to 10 percent of the Contract Price for the due performance of the Contract, in the form prescribed by ……………………………………………(Procuring entity).

4. We agree to abide by this Tender for a period of...................[*number]* days from the date fixed for tender opening of the Instructions to tenderers, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

5. Until a formal Contract is prepared and executed, this Tender, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

6. We understand that you are not bound to accept the lowest or any tender you may receive.

Dated this________________day of________________20________.

______________________ ________________________________
[Signature] *[In the capacity of]*

Duly authorized to sign tender for and on behalf of ___________________

CONFIDENTIAL BUSINESS QUESTIONNAIRE

You are requested to give the particulars indicated in Part 1 and either Part 2 (a), 2(b) or 2(c) whichever applied to your type of business.

You are advised that it is a serious offence to give false information on this form.

Part 1 General

Business Name ....
Location of Business Premises ....
Plot No,..Street/Road ....
Postal address .... Tel No. .... Fax Email.........................
Nature of Business ....
Registration Certificate No...
Maximum value of business which you can handle at any one time – Kshs.....
Name of your bankers ....

Part 2 (a) – Sole Proprietor
Your name in full……………………….Age………………………………………….
Nationality…………………………Country of Origin……………………………..
Citizenship details
…………………………………………………..

Part 2 (b) – Partnership
Given details of partners as follows

Name	Nationality	Citizenship details	Shares

1. ……………………………………………………………………………………
2. ……………………………………………………………………………………
3. ……………………………………………………………………………………
4. ………………………………………………………………………………

Part 2 (c) – Registered Company
Private or Public
State the nominal and issued capital of company
Nominal Kshs.
Issued Kshs.
Given details of all directors as follows

Name	Nationality	Citizenship details	Shares

1. ……………………………………………………………………………………
2. ……………………………………………………………………………………
3. ……………………………………………………………………………………
4. ……………………………………………………………………………………

Date .... Signature of Candidate………………………..

Section H. Tender Security Form (From Bank)

Whereas…..*[Name of the tenderer]*
(Hereinafter called "the tenderer") has submitted its tender dated ....*[Date of submission of tender]* for the supply of……………………………………….
……………… .. *[Name and/or description of the goods]*
(Hereinafter called "the Tender")……………………………………………………………….
KNOW ALL PEOPLE by these presents that WE……………………………………………
Of.. Having our registered office at
……………………… (Hereinafter called "the Bank"), are bound
unto.. *[Name of procuring entity]* (Hereinafter called "the Procuring entity") in the sum of
………………….
For which payment well and truly to be made to the said Procuring entity, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this______day of_________20____.

THE CONDITIONS of this obligation are:

1. If the tenderer withdraws its Tender during the period of tender validity specified by the tenderer on the Tender Form; or

2. If the tenderer, having been notified of the acceptance of its Tender by the Procuring entity during the period of tender validity:

(a) Fails or refuses to execute the Contract Form, if required; or
(b) Fails or refuses to furnish the performance security, in accordance with the Instructions to tenderers;

We undertake to pay to the Procuring entity up to the above amount upon receipt of its first written demand, without the Procuring entity having to substantiate its demand, provided that in its demand the Procuring entity will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including thirty (30) days after the period of tender validity, and any demand in respect thereof should reach the Bank not later than the above date.

[Signature of the bank]

Section I. Contract Form

THIS AGREEMENT made the______day of____________20______ between............ *[name of Procurement entity)* of .... *[Country of Procurement entity]* (Hereinafter called "the Procuring entity") of the one part and.................................. *[Name of tenderer]* of….............. *[City and country of tenderer]* (Hereinafter called "the tenderer") of the other part:

WHEREAS the Procuring entity invited tenders for certain goods, viz., ... *[Brief description of goods]* and has accepted a tender by the tenderer for the supply of those goods in the sum of.. *[Contract price in words and figures]* (Hereinafter called "the Contract Price").

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 Contract referred to.
2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:
   (a) The Tender Form and the Price Schedule submitted by the tenderer;
   (b)The Schedule of Requirements;
   (c)The Technical Specifications;
   (d)The General Conditions of Contract;
   (e)The Special Conditions of Contract; and
   (f)The Procuring entity's Notification of Award.
3. In consideration of the payments to be made by the Procuring entity to the tenderer as hereinafter mentioned, the tenderer hereby covenants with the Procuring entity to provide the goods and to remedy defects therein in conformity in all respects with the provisions of the Contract
4. The Procuring entity hereby covenants to pay the tenderer in consideration of the provision of the goods and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

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

Signed, sealed, delivered by___________the_________ (for the Procuring entity)

Signed, sealed, delivered by___________the_______________(for the tenderer)

In the presence of_______________

Section J. Performance Security Form (From bank)

To:.. *[Name of procuring entity]*

WHEREAS ....*[Name of tenderer]*
(Hereinafter called "the tenderer") has undertaken, in pursuance of Contract
No ____________ [*reference number of the contract]* dated_____________20_____
to supply………………………………………..…………………………………………
*[Description of goods] (*Hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the tenderer shall furnish you with a bank guarantee by a reputable bank for the sum specified therein as security for compliance with the Tenderer's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the tenderer a guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the tenderer, up to a total of .... *[Amount of the guarantee in words and figures],* and we undertake to pay you, upon your first written demand declaring the tenderer to be in default under the Contract and without cavil or argument, any sum or sums within the limits of……………………………………
[Amount of guarantee] as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the______day of___________20_.

Signature and seal of the Guarantors

____
[Name of bank or financial institution]

____
[Address]

____
[Date]

LETTER OF NOTIFICATION OF AWARD

Address of Procuring Entity

____

____

To:_____________________

____

____

____

RE: Tender No._______________________

Tender Name_____________________

This is to notify that the contract/s stated below under the above mentioned tender have been awarded to you.

____

____

1. Please acknowledge receipt of this letter of notification signifying your acceptance.
2. The contract/contracts shall be signed by the parties within 30 days of the date of this letter but not earlier than 14 days from the date of the letter.
3. You may contact the officer(s) whose particulars appear below on the subject matter of this letter of notification of award.

*(FULL PARTICULARS)*____

____

SIGNED FOR ACCOUNTING OFFICER

SELF DECLARATION THAT THE PERSON/TENDERER WILL NOT ENGAGE IN ANY CORRUPT OR FRAUDULENT PRACTICE.

I, ……………………………………. of P. O. Box....................................... being a resident of………………………………….. in the Republic of .... do hereby make a statement as follows: -

1. THAT I am the Chief Executive/Managing Director/Principal Officer/Director of ……….... ……………………………….. (insert name of the Company) who is a Bidder in respect of **Tender No. KEBS/T017/2020/2021** for Supply, Implementation and Commissioning of Supply, Implementation and Commissioning of Next Generation Firewall and duly authorized and competent to make this statement.

2. THAT the aforesaid Bidder, its servants and/or agents /subcontractors will not engage in any corrupt or fraudulent practice and has not been requested to pay any inducement to any member of the Board, Management, Staff and/or employees and/or agents of the **KEBS** which is the procuring entity.

4. THAT the aforesaid Bidder will not engage /has not engaged in any corrosive practice with other bidders participating in the subject tender

5. THAT what is deponed to hereinabove is true to the best of my knowledge information and belief.

…………………………………………..…………………………….. ………………………

(Title)

(Signature)

(Date)

Bidder's Official Stamp

NON-DEBARMENT DECLARATION

We (insert the name of the company/ supplier) … ....declares and guarantees that no director or any person who has any controlling interest in our organization has been debarred from participating in a procurement proceeding.

Name……………………………..Signature……….................

Date……………………………

Company Seal/Business Stamp