GEOTHERMAL DEVELOPMENT COMPANY LTD
P.O. Box 100746 – 00101
NAIROBI, KENYA
Tel: 0719715777/8, 0733602260
Website: www.gdc.co.ke

TENDER FOR SUPPLYAND INSTALLATION OF PERIMETER NETWORK FIREWALL

TENDER NO: GDC/ICT/OT/049/2020:2021

CLOSING DATE AND TIME: 11th JUNE 2021 AT 2:00PM

TABLE OF CONTENTS

SECTION I: INVITATION TO TENDER

Date: 25/05/2021

TENDER REF NO: GDC/ICT/OT/049/20:21

TENDER DESCRIPTION: TENDER FOR SUPPLY AND INSTALLATION OF PERIMTER NETWORK FIREWALL

Geothermal Development Company (GDC) invites sealed tenders from eligible candidates for "**SUPPLY AND INSTALLATION OF PERIMETER NETWORK FIREWALL"** whose specifications are detailed in the tender document.

Interested eligible candidates may obtain further information from and inspect the tender documents at the Office of the Manager Supply Chain at GDC Kawi House, South C Office between 9.00am to 4.00pm during weekdays.

An electronic copy of the tender document may be obtained by interested candidates upon payment of a non- refundable fee of **Kshs. 1000** in cash or banker's cheque payable to the GDC **GDC Kawi House, South C Accounts** Office. The documents can also be viewed and downloaded from the website www.gdc.co.ke or tenders. go.ke **free of charge**. Bidders who download the tender document from the website must forward them immediately for records and any further tender clarifications and addenda

The tenderer shall furnish, as part of its tender, a tender security in **the amount of Ksh 200,000** the form of a bank or insurance guarantee as specified in the tender document.

Completed tender documents properly marked with the Tender Reference number and descriptions **"SUPPLY AND INSTALLATION OF PERIMETER NETWORK FIREWALL."** are to be enclosed in plain sealed envelopes, and addressed to: -

The Managing Director & CEO
Geothermal Development Company Limited
P. O. Box 100746-00101
Nairobi, Kenya.

And be deposited in the tender box provided at our **GDC Kawi House, South C** So as to be received on or before **11th June 2021, at 2.00 pm (1400hrs)**.

Tenders will be opened immediately thereafter in the presence of the tenderers representatives who choose to attend at **GDC Kawi House, South C** Offices Boardroom.

Late tenders will NOT be accepted.

MANAGER, SUPPLY CHAIN

SECTION II – INSTRUCTIONS TO TENDERERS

2.1 Eligible tenderers

2.1.1. This Invitation to tender is open to all tenderers eligible as described in the instructions to tenderers. Successful tenderers shall provide the services for the stipulated duration from the date of commencement (hereinafter referred to as the term) specified in the tender documents.

2.1.2. The procuring entity's employees, committee members, board members and their relative (spouse and children) are not eligible to participate in the tender unless where specially allowed under section 131 of the Act.

2.1.3. 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 services under this Invitation for tenders.

2.1.4. Tenderers involved in corrupt or fraudulent practices or debarred from participating in public procurement shall not be eligible.

2.2 Cost of tendering

2.2.1 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.

2.2.2 The price to be charged for the tender document shall not exceed Kshs.1,000/=

2.2.3 The procuring entity shall allow the tenderer to review the tender document free of charge before purchase.

2.3 Contents of tender documents

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

i) Instructions to tenderers
ii) General Conditions of Contract
iii) Special Conditions of Contract

iv) Schedule of Requirements
v) Details of service
vi) Form of tender
vii) Price schedules
viii) Contract form
ix) Confidential business questionnaire form
x) Tender security form
xi) Performance security form
xii) Principal's or manufacturers authorization form

2.3.2. 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.

2.4 Clarification of Documents

2.4.1. A prospective candidate making inquiries of the tender document may notify the Procuring entity in writing or by post, fax or email 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 tenderers who have received the tender documents"

2.4.2. The procuring entity shall reply to any clarifications sought by the tenderer within 3 days of receiving the request to enable the tenderer to make timely submission of its tender

2.5 Amendment of documents

2.5.1. 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 issuing an addendum.

2.5.2. All prospective tenderers who have obtained the tender documents will be notified of the amendment by post, fax or email and such amendment will be binding on them.

2.5.3. 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.

2.6 Language of tender

2.6.1. 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. 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.

2.7 Documents Comprising the Tender

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 Clause 2.11 that the tenderer is eligible to tender and is qualified to perform the contract if its tender is accepted;

(c) Tender security furnished is in accordance with Clause 2.12

(d)Confidential business questionnaire

2.8 Form of Tender

2.8.1 The tenderers shall complete the Form of Tender and the appropriate Price Schedule furnished in the tender documents, indicating the services to be performed.

2.9 Tender Prices

2.9.1 The tenderer shall indicate on the Price schedule the unit prices where applicable and total tender prices of the services it proposes to provide under the contract.

2.9.2 Prices indicated on the Price Schedule shall be the cost of the services quoted including all customs duties and VAT and other taxes payable:

2.9.3 Prices quoted **by** the tenderer shall remain fixed during the term of the contract unless otherwise agreed by the parties. **A** tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected, pursuant to paragraph 2.22.

2.9.4 Contract price variations shall not be allowed for contracts not exceeding one year (12 months)

2.9.5 Where contract price variation is allowed, the variation shall not exceed 10% of the original contract price.

2.9.6 Price variation requests shall be processed by the procuring entity within 30 days of receiving the request.

2.10 **Tender Currencies**

2.10.1 Prices shall be quoted in Kenya Shillings unless otherwise specified in the appendix to in Instructions to Tenderers

2.11 Tenderers Eligibility and Qualifications.

2.11.1 Pursuant to Clause 2.1 the tenderer shall furnish, as part of its tender, documents establishing the tenderers eligibility to tender and its qualifications to perform the contract if its tender is accepted.

2.11.2 The documentary evidence of the tenderers qualifications to perform the contract if its tender is accepted shall establish to the Procuring entity's satisfaction that the tenderer has the financial and technical capability necessary to perform the contract.

2.12 **Tender Security**

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

2.12.2 The tender security shall be in the amount not exceeding 2 per cent of the tender price.

2.12.2 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 2.12.7

2.12.3 The tender security shall be denominated in a Kenya Shillings or in another freely convertible currency and shall be in the form of:

a) A bank guarantees.

b) Cash.

c) Such insurance guarantee approved by the Authority.

d) Letter of credit

2.12.4 Any tender not secured in accordance with paragraph 2.12.1 and 2.12.3 will be rejected by the Procuring entity as non-responsive, pursuant to paragraph 2.20

2.12.5 Unsuccessful tenderer's 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.

2.12.6 The successful tenderer's tender security will be discharged upon the tenderer signing the contract, pursuant to paragraph 2.29, and furnishing the performance security, pursuant to paragraph 2.30.

2.12.7 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 2.26

or

(ii) to furnish performance security in accordance with paragraph 2.27.

(c) If the tenderer rejects, correction of an error in the tender.

2.13 Validity of Tenders

2.13.1 Tenders shall remain valid for **120 days** or as specified in the invitation to tender after date of tender opening prescribed by the Procuring entity, pursuant to paragraph 2.18. A tender valid for a shorter period shall be rejected by the Procuring entity as nonresponsive.

2.13.2 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 2.12 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.

2.14 **Format and Signing of Tender**

2.14.1 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.

2.14.2 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. All pages of the tender, except for unamended printed literature, shall be initialed by the person or persons signing the tender.

2.14.3 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 initialed by the person or persons signing the tender.

2.15 **Sealing and Marking of Tenders**

2.15.1 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.

2.15.2 The inner and outer envelopes shall:

(a) Be addressed to

The Managing Director,
Geothermal Development Company Ltd (GDC)
P.O. Box 100746 – 00101
NAIROBI, KENYA

(b) Bear, "**SUPPLY AND INSTALLATION OF PERIMETER NETWORK FIREWALL",** and the statement: **"DO NOT OPEN BEFORE 11th June 2021 at 2:00pm**

2.15.3 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".

2.15.4 If the outer envelope is not sealed and marked as required by paragraph 2.15.2, the Procuring entity will assume no responsibility for the tender's misplacement or premature opening.

2.16 **Deadline for Submission of Tenders**

2.16.1 Tenders must be received by the Procuring entity at the address specified under paragraph 2.15.2 no later than **11th June 2021 at 2.00pm (1400hrs)**.

2.16.2 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.

2.16.3 Bulky tenders which will not fit in the tender box shall be received by the procuring entity as provided for in the appendix.

2.17 **Modification and withdrawal of tenders**

2.17.1 The tenderer may modify or withdraw its tender after the tender's submission, provided that written notice of the modification, including substitution or withdrawal of the tender's is received by the procuring entity prior to the deadline prescribed for the submission of tenders.

2.17.2 The Tenderer's modification or withdrawal notice shall be prepared, sealed, marked, and dispatched in accordance with the provisions of paragraph 2.15. A withdrawal notice may also be sent by cable, but followed by a signed confirmation copy, postmarked no later than the deadline for submission of tenders.

2.17.3 No tender may be modified after the deadline for submission of tenders.

2.17.4 No tender may be withdrawn in the interval between the deadline for submission of tenders and the expiration of the period of tender validity specified by the tenderer on the Tender Form. Withdrawal of a tender during this interval may result in the Tenderer's forfeiture of its tender security, pursuant to paragraph 2.12.7.

2.17.5 The procuring entity may at any time terminate procurement proceedings before contract award and shall not be liable to any person for the termination.

2.17.6 The procuring entity shall give prompt notice of the termination to the tenderers and on request give its reasons for termination within 14 days of receiving the request from any tenderer.

2.18 Opening of Tenders

2.18.1 The Procuring entity will open all tenders in the presence of tenderers' representatives who choose to attend, on **11th June 2021 at 2.00pm (1400hrs)** and in the location specified in the invitation to tender. The tenderers' representatives who are present shall sign a register evidencing their attendance.

2.18.3 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.

2.18.4 The procuring entity will prepare minutes of the tender opening which will be submitted to the tenderers that signed the tender opening register and will have made the request.

2.19 Clarification of tenders

2.19.1 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 shall be sought, offered, or permitted.

2.19.2 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.

Comparison or contract award decisions may result in the rejection of the tenderers' tender.

2.20 Preliminary Examination and Responsiveness

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

2.20.2 Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If the candidate does not accept the correction of the errors, its tender will be rejected, and its tender security may be

forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.

2.20.3 The Procuring entity may waive any minor informality or nonconformity 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.

2.20.4 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.

2.20.5 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.

2.21 **Conversion to a single currency**

2.21.1 Where other currencies are used, the procuring entity will convert those currencies to Kenya shillings using the selling exchange rate on the date of tender closing provided by the central bank of Kenya.

2.22 **Evaluation and comparison of tenders**.

2.22.1 The procuring entity will evaluate and compare the tenders which have been determined to be substantially responsive, pursuant to paragraph 2.20

2.22.2 The comparison shall be of the price including all costs as well as duties and taxes payable on all the materials to be used in the provision of the services.

2.22.3 The Procuring entity's evaluation of a tender will consider, in addition to the tender price, the following factors, in the manner and to the extent indicated in paragraph 2.22.4 and in the technical specifications:

(a) Operational plan proposed in the tender;

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

2.22.4 Pursuant to paragraph 2.22.3 the following evaluation methods will be applied:

(a) ***Operational Plan.***

The Procuring entity requires that the services under the Invitation for Tenders shall be performed at the time specified in the Schedule of Requirements. Tenderers offering to perform 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 on a schedule outlined in the special conditions of contract. Tenders will be evaluated based on 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.

2.22.5 The tender evaluation committee shall evaluate the tender within 30 days from the date of opening the tender.

2.22.6 To qualify for contract awards, the tenderer shall have the following: -

(a) Necessary qualifications, capability experience, services, equipment and facilities to provide what is being procured.

(b) Legal capacity to enter into a contract for procurement

(c) Shall not be insolvent, in receivership, bankrupt or in the process of being wound up and is not the subject of legal proceedings relating to the foregoing

(d) Shall not be debarred from participating in public procurement.

2.23. **Contacting the procuring entity**

2.23.1 Subject to paragraph 2.19, 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.

2.23.2 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 tenderers tender.

2.24 Award of Contract

a) **Post qualification**

2.24.1 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.

2.24.2 The determination will consider the tenderer's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the tenderer's qualifications submitted by the tenderer, pursuant to paragraph 2.1.2, as well as such other information as the Procuring entity deems necessary and appropriate.

2.24.3 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.

b) **Award Criteria**

2.24.3 Subject to paragraph 2.29 the Procuring entity will award the contract to the successful tenderer 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.

2.24.4 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. If the procuring entity determines that none of the tenderers is responsive; the procuring entity shall notify each tenderer who submitted a tender.

2.24.5 A tenderer who gives false information in the tender document about its qualification or who refuses to enter into a contract after notification of contract award shall be considered for debarment from participating in future public procurement.

2.25 **Notification of award**

2.25.1 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.

2.25.2 The notification of award will signify the formation of the Contract subject to the signing of the contract between the tenderer and the procuring entity pursuant to clause 2.29. Simultaneously the other tenderers shall be notified that their tenders have not been successful.

2.25.3 Upon the successful Tenderer's furnishing of the performance security pursuant to paragraph 2.27, the Procuring entity will promptly notify each unsuccessful Tenderer and will discharge its tender security, pursuant to paragraph 2.12

2.26 **Signing of Contract**

2.26.1 At the same time as the Procuring entity notifies the successful tenderer that its tender has been accepted, the Procuring entity will simultaneously inform the other tenderers that their tenders have not been successful.

2.26.2 Within fourteen (14) days of receipt of the Contract Form, the successful tenderer shall sign and date the contract and return it to the Procuring entity.

2.26.3 The parties to the contract shall have it signed within 30 days from the date of notification of contract award unless there is an administrative review request.

2.26.4 **Performance Security**

2.27.1 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.

2.27.2 Failure of the successful tenderer to comply with the requirement of paragraph 2.29 or paragraph 2.30.1 shall constitute enough 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 or call for new tenders.

2.28 Corrupt or Fraudulent Practices

2.28.1 The Procuring entity requires that tenderers observe the highest standard of ethics during the procurement process and execution of contracts. A tenderer shall sign a declaration that he has not and will not be involved in corrupt or fraudulent practices.

2.28.2 The procuring entity 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;

2.28.3 Further, a tenderer who is found to have indulged in corrupt or fraudulent practices risks being debarred from participating in public procurement in Kenya.

APPENDIX TO INSTRUCTIONS TO THE TENDERERS

The following information for procurement of services shall complement or amend the provisions of 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.

INSTRUCTIONS TO TENDERERS	**PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERERS**
2.1.1	The tender is eligible to all tenderers with the capability to Supply and Install a Perimeter Network Firewall. Successful firm will sign a two (2) year contract with GDC.
2.29.1	An electronic copy of the tender document may be obtained by interested candidates upon payment of a non- refundable fee of **Kshs. 1000** in cash or banker's cheque payable to the GDC Kawi House **Accounts** Office. The documents can also be viewed and downloaded from the website www.gdc.co.ke or tenders. go. ke **free of charge**. Bidders who download the tender document from the website must forward their particulars immediately for records and any further tender clarifications and addenda
2.29.2	A prospective tenderer requiring any clarification of the tender document may notify GDC in writing (email in PDF format or by facsimile) at the following address: One copy to: - Manager, Supply Chain Geothermal Development Company Limited, GDC Riverside Office, P.O. Box 100746 – 00101 NAIROBI, KENYA E-mail: dkyaka@gdc.co.ke cc pkapto@gdc.co.ke And one copy to: - Ag. Manager, Information and Communication Technology Geothermal Development Company Limited, GDC Riverside Office, P.O. Box 100746 – 00101 NAIROBI, KENYA E-mail: dlangat@gdc.co.ke GDC will respond in writing (e-mail in PDF format) to any request received at least seven (7) days prior to the deadline

	for the submission of tenders. **NB: Any request for clarification must be in the firm's letterhead and signed and must be about the specific parts of the tender document properly numbered.**
2.29.3	The tender validity period is **120 days** from the date of tender opening. A tender valid for a shorter period shall be considered non-responsive and shall be rejected.
2.29.4	Prices quoted shall be in Kenya Shillings or an easily convertible foreign currency
2.29.5	The tenderer shall furnish, as part of its tender, a tender security in **the amount of Ksh. 200,000.00** the form of a bank or insurance guarantee. The tender security should be **valid for a period of 30 days** beyond the tender validity period. i.e. **150 days from the date of tender opening.**
2.29.6	The tenderer should submit an Original and one (1) copy of the tender.
2.29.7	The Tender Closing date is on 11th June 2021**at 2:00pm (1400hrs)**
Mandatory Requirements.	The evaluation will be based on following stages: **a) PRELIMINARY EVALUATION STAGE** The following Mandatory requirements will be assessed at this stage: - i. Duly filled, signed & stamped Price Schedule ii. Duly filled, Signed & Stamped Tender Form iii. Original Tender Security in the amount of Ksh.200,000.00 in the form of bank or insurance guarantee valid for a period of 150 days from the date of tender opening. The Bank or Insurance guarantee shall be issued by a reputable Bank or Insurance Firm operating in Kenya iv. Attach a copy of Certificate of Incorporation/Registration duly certified by an advocate v. Attach a copy of a Valid Business Permit certified by an advocate vi. Attach a copy of PIN Certificate vii. Attach a copy of the Tax Compliance Certificate valid at

	the time of tender opening. GDC shall confirm the Certificate validity from the KRA tax checker viii. Duly filled, signed and stamped Confidential Business Questionnaire ix. Dully Filled, Signed and Stamped Declaration of Undertaking not to engage in corrupt fraudulent practice x. Attach a valid ICTA accreditation Certificate in ICT Networks Security and/or Information Security. xi. Tenderers to provide audited financial accounts statements for the past three (3) years (2019, 2018 & 2017) duly stamped by the auditing firm and certified by an advocate xii. Provide a Power of Attorney duly signed and witnessed by an advocate giving authority to individual to transact on behalf of the company **NB:** i. Bidders who will not meet the above requirements will be declared non-responsive and their bids will not be evaluated further ii. Please note that the authenticity of the above documents provided <u>SHALL</u> be verified with the relevant authority and any forgery or false presentation in any one of the above shall lead to automatic disqualification and render the tenderers bid non-responsive. iii. In the case of a joint venture, tenderers should submit a duly signed joint venture agreement by both parties clearly defining the roles of each party and highlighting the lead party in the agreement. GDC will sign the contract with the lead partner and channel all contractual matters and financial transactions to the lead party. **b) TECHNICAL EVALUATION STAGE** Only bidders who pass the Preliminary stage will be evaluated at the technical evaluation stage. The technical evaluation is two stage:

	i. Compliance/Responsiveness to Scope of works and fully completed technical specification sheet as per Section VI. ii. Technical evaluation (based on scoring) as per technical evaluation criteria with a cut off score of 75 marks/points. Bids responsive at the technical evaluation stage will be evaluated at the financial stage. **c) FINANCIAL EVALUATION** i. The bids will be checked for costing of all items, services and payment terms. ii. Bidders must quote for completeness of all the price schedules. Incomplete price schedules shall lead to disqualification. <u>No correction of Arithmetic Errors.</u> The tender sum as submitted shall be absolute and final and shall not be subject to correction, adjustment and amendment in anyway by any person. **Award Criteria.** The lowest evaluated tenderer will be recommended for award.
2.30	The performance security shall be 10% of the contract price in the form of a bank guarantee issued by a local Company. The security shall be valid for thirty days beyond the contract completion period.

SECTION III GENERAL CONDITIONS OF CONTRACT

3.1 Definitions

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 services" means services to be provided by the contractor including materials and incidentals which the tenderer is required to provide to the Procuring entity under the Contract.

d) "The Procuring entity" means the organization sourcing for the services under this Contract.

e) "The contractor means the individual or firm providing the services under this Contract.

f) "GCC" means general conditions of contract contained in this section

g) "SCC" means the special conditions of contract

h) "Day" means calendar day

3.2 Application

These General Conditions shall apply to the extent that they are not super ceded by provisions of other part of contract.

3.3 Standards

3.3.1 The services provided under this Contract shall conform to the standards mentioned in the Schedule of requirements

3.5 Patent Right's

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 services under the contract or any part thereof.

3.6 **Performance Security**

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

3.6.2 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.

3.6.3 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) Cash.

b) A bank guarantees.

c) Such insurance guarantee approved by the Authority.

d) Letter of credit.

3.6.4 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 of obligations under the contract, including any warranty obligations under the contract.

3.7 Inspections and Tests

3.7.1 The Procuring entity or its representative shall have the right to inspect and/or to test the services 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.

3.7.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s). 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.

3.7.3 Should any inspected or tested services fail to conform to the Specifications, the Procuring entity may reject the services, and the tenderer shall either

replace the rejected services or make alterations necessary to meet specification requirements free of cost to the Procuring entity.

3.7.4 Nothing in paragraph 3.7 shall in any way release the tenderer from any warranty or other obligations under this Contract.

3.8 **Payment**

3.8.1 The method and conditions of payment to be made to the tenderer under this Contract shall be specified in SCC

3.9 **Prices**

Prices charged by the contractor for services performed under the Contract shall not, except for any Price adjustments authorized in SCC, vary from the prices by the tenderer in its tender or in the procuring entity's request for tender validity extension as the case may be. No variation in or modification to the terms of the contract shall be made except by written amendment signed by the parties.

3.10 **Assignment**

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.

3.10 Termination for Default

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 provide any or all the services 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.

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,

services like those undelivered, and the tenderer shall be liable to the Procuring entity for any excess costs for such similar services.

3.12 Termination of insolvency

The procuring entity may at the anytime terminate the contract by giving written notice to the contractor if the contractor becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the contractor, provided that such termination will not produce or affect any right of action or remedy, which has accrued or will accrue thereafter to the procuring entity.

3.13 Termination for convenience

3.13.1 The procuring entity by written notice sent to the contractor may terminate the contract in whole or in part, at any time for its convenience. The notice of termination shall specify that the termination is for the procuring entity convenience, the extent to which performance of the contractor of the contract is terminated and the date on which such termination becomes effective.

3.13.2 For the remaining part of the contract after termination the procuring entity may elect to cancel the services and pay to the contractor on agreed amount for partially completed services.

3.14 Resolution of disputes

The procuring entity's and the contractor shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute arising between them under or in connection with the contract.

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 that the dispute be referred for resolution to the formal mechanisms specified in the SCC.

3.15 Governing Language

The contract shall be written in the English language. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in the same language.

3.16 Force Majeure

The contractor shall not be liable *for* forfeiture of its performance security, or termination for default if and to the extent that it's delays in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

3.17 Applicable Law.

The contract shall be interpreted in accordance with the laws of Kenya unless otherwise specified in the SCC

3.18 Notices

Any notices given by one party to the other pursuant to this contract shall be sent to the other party by post or by fax or E-mail and confirmed in writing to the other party's address specified in the SCC

A notice shall be effective when delivered or on the notices effective date, whichever is later.

SECTION IV SPECIAL CONDITIONS OF CONTRACT

4.1 Special conditions of contract shall supplement the general conditions of contract, wherever there is a conflict between the GCC and the SCC, the provisions of the SCC herein shall prevail over those in the GCC.

4.2 Special conditions of contract with reference to the general conditions of contract.

GENERAL CONDITIONS OF CONTRACT REFERENCE	SPECIAL CONDITIONS OF CONTRACT
3.1 Definitions	The Purchaser is The Managing Director, Geothermal Development Company Ltd (GDC), KAWI HOUSE, Tel: 0719715777/8, 0733602260, 071903600, 0719037000, P.O Box 100746 – 00101, NAIROBI, KENYA, and includes its legal representatives, successors or assigns.
3.2 Application	The following Special Conditions of Contract shall supplement the General Conditions. Whenever there is a conflict, the provisions herein shall prevail over those in the General Conditions of Contract
3.6 Performance Security	The Performance Security shall be in the amount of 10% of the Contract Price from a Local Bank operating in Kenya. The Performance security will be cashed if the tenderer shall not deliver the materials as per delivery period indicated in the Schedule of Requirements. The performance security shall be valid thirty days beyond the contract lapse period.
3.8 Payment	GDC payment terms are within 60 days upon the receipt of certified invoices and delivery notes confirming that the invoiced services has been delivered and performed in accordance with the contract.
3.9 Prices	Prices shall be fixed during the Supplier's performance of the Contract. Variation if approved will be based on the prevailing consumer price index from the Kenya Bureau of Statistics or the monthly inflation rate issued by the Central Bank of Kenya.
3.14 Resolution of Disputes	If any dispute or difference of any kind arises between the Parties in connection with this Agreement or the breach, termination or validity hereof (a "Dispute") it shall be referred to arbitration under the Arbitration Act, 1995 and it is hereby agreed that; (a) The seat of the arbitration shall be Nairobi, Kenya;

	(b) There shall be a panel of three (3) arbitrators. Each Party shall appoint one arbitrator and the third who shall be the chairman who shall be appointed by the Institute of Chartered Arbitrators Kenya Chapter. Provided that any person who has existing or prior relationship with either Party shall not be eligible for appointment as an arbitrator except with the consent of both Parties. (c)The language of the arbitration shall be English; (d)The award rendered shall apportion the costs of the arbitration; (e)The award shall be in writing and shall set forth in reasonable detail the facts of the Dispute and the reasons for the tribunal's decision
3.18 Notices	For the Purchaser: The Managing Director, Geothermal Development Company Ltd (GDC) KAWI HOUSE – SOUTH C Tel: 0719715777/8, 0733602260 P.O Box 100746 – 00101 NAIROBI, KENYA

SECTION V – SCHEDULE OF REQUIREMENTS

5.1 The scope of work involves:

1. The scope of work shall involve supply and configuring the devices as per the requirements.
2. Successful Bidder shall come up with a detailed project plan for the proposed solution. Bidder shall provide implementation approach and methodology that will be followed along with the Bid response document.
3. Successful Bidder must conduct design workshop with GDC IT team to understand the existing IT environment and come up with the best security design for Customer.
4. The Successful bidder shall supply the hardware and per the defined RFP specifications with Three (3) Years of warranty.
5. The Successful bidder shall understand the traffic flow, IP Addressing, Service provider connectivity and suggest the most appropriate architecture and perform necessary network changes wherever required.
6. GDC is currently running existing perimeter security solution from Sophos/Cyberoam having firewall services, VPN services, IPS services, User Security Control, Antivirus, Repudiation Services, Web Security Services and Malware Protection Services on the existing Firewall solution. Successful bidder shall study the policies and migrate the desired services on the proposed solution and perform necessary fine-tuning wherever required. Details of existing design and firewall configuration will be shared with successful bidder during the design stage.
7. Successful Bidder shall migrate current running services from existing firewall appliances to the new firewall Appliances. GDC will provide necessary support in migration of the business services.
8. Successful Bidder should facilitate Test Criteria and Procedures for UAT of proposed Firewall solution. The Bidder shall conduct UAT test cases with GDC IT team.
9. Successful Bidder shall facilitate necessary knowledge transfer to the GDC team as a part of the project execution.
10. Necessary AS Build document for monitoring and management of the deployed solution will be provided by the successful bidder.
11. Bidder shall provide SLA support for proper operation of deployed solution for a period of 3 years.

NOTE: Nairobi Kawi house and Nakuru polo center are internet entry points while the rest of the branches are served by MPLS links from Nairobi.

NOTE: GDC network comprises of Cisco routers and switches, with Avaya IP PABX operating on H.323 protocol.

Training

Successful bidder shall provide OEM training for eight (8) GDC Technical Staff. The training should be hands on System Administration on the proposed solution, conducted at approved vendor training center in Kenya. The Training should include certification Vouchers for (eight) 8 participants.

SECTION VI: TECHNICAL SPECIFICATIONS

5.2 Specification Details

Tenders must indicate on the specifications sheets whether the services offered comply with the specified requirements.

5.2.1 Any deviation from basic requirements must be explained in detail. GDC reserves the right to reject the services, if such deviations shall be found critical to the use and operation of the services to be offered.

5.2.2 The bidder shall provide a clear technical description of the solution on offer and clearly demonstrate security to GDC Network (traffic and out)

5.2.2 The supplier **MUST** provide **manufacturer's authorization letter** with regards to the line of goods supplied. All products supplied **MUST** be genuine and have genuine licenses that can be verified by the manufacturer of the product. A manufacturer's warranty should be supplied with the product and a warranty certificate provided *(For the bid document the bidders MUST write a commitment letter either on the company letter head or fully signed and stamped by the persons authorized to sign the company documents to offer a valid warranty when their bid is successful).*

5.2.3 No devices should have physical damages/dents neither should the devices be refurbished.

5.2.4 ALL security seals and packaging should not have been tampered with.

5.2.5 The supplier **MUST** have competency to install the services onsite and must have at least three (3) certified technical skill/staff required to deploy and support the solution post implementation.

5.2.6 In case of substandard products or dissatisfaction on the part of GDC, the supplier shall bear costs of replacing the products.

5.2.7 The supplier **MUST** have a local presence and able to offer physical and remote technical support in all the sites.

5.2.8 Manufacturer backed 24x7 Premium Enterprise Support, including advanced device replacement in case of failure for all hardware supplied under this solution - 1 Year

5.2.9 The solution must be supplied with 1 Year License Subscription.

Geothermal Development Company (GDC) seeks to procure Next Generation Firewall with the following general specifications. The Firewall should be future ready and readily scalable to include additional features over and above the currently required modules as listed in the table below.

Nairobi KAWI House Firewall

SN	Component	Specification required including applicable standards	Compliance of specification offered (Fully Comply/Non-Comply)	Description of specifications offered including page no. in Technical literature where specifications is reflected.
1	**NAIROBI GATEWAY FIREWALL (Quantity 1)**			
1.1		Must be support at least 4 x 25GE SFP28 slots		
		Must be support at least 4 x 10GE SFP+ slots		
		Must be support at least 8 x 1GE RJ45 interfaces		
		Must be support at least 8 x 1GE SFP slots		
		Must support at least 7 Million Maximum Concurrent Sessions		
		Must support at least 400,000 New Sessions/Second		
		Must support at least 50Gbps of firewall throughput		
		Must support at least 12 Gbps Enterprise/Production IPS Throughput		
		Must support at least 9 Gbps SSL Inspection Throughput Throughput		
		Must support at least 9 Gbps Enterprise/Production Threat Protection Throughput		
		Must support at least 480GB SSD storage		
		Must be support dual power supplies		
		Must be supplied with at least 1,000 SSL VPN licenses		
		Must have the following licenses included Application Control, IPS, Anti Malware, Web Filtering, DNS Filtering, Mobile Security, IOT Security and Sandbox Cloud		

		The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified		
		It Must be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode		
		The proposed system shall support robust GUI configurations of both IPv4 and IPv6 firewall policies on the same table that include:		
		One-click edit of firewall objects from the policy table panel		
		Drag and drop policy moving		
		Right-Click on one/multiple policy(i.e.) to toggle enabling/disabling and deleting of policies		
		Editing selected policy on GUI or from CLI panel		
		Show matching logs of selected policy		
1.2	**Firewall Features**	The proposed system shall offer a firewall policy table in both views by policy sequence and by interface pairs		
		The proposed system shall allow the administrator to customize the firewall policy table's columns		
		The proposed system shall allow the administrator to view filtered policies by using a search bar		
		The proposed system's firewall policies shall support various types of source objects, including IP address/address range/subnets, users, MAC addresses and dynamic addresses from SaaS and reputation list.		
		The proposed system shall support firewall session helpers and ALGs for FTP, TFTP, RAS, H323, TNS/SQLNET, MMS, SIP, PPTP, RTSP, DNS (UDP), DNS (TCP), PMAP, RSH, DCE/RPC and MGCP		
		The proposed system's firewall policies shall support all protocol types that include TCP, UDP, SCTP, IP, and ICMP		

1.3	**Authentication Features**	The proposed system shall support the following user authentication methods to be applied on a security policy and/or VPN access:		
		Local password authentication		
		Server-based password authentication using LDAP, RADIUS, TACACS+, Windows AD, or POP3 servers		
		Certificate-based authentication for host and endpoints		
		Two-factor authentication for additional security beyond just passwords		
		The proposed system shall support various single sign-on (SSO) techniques so that users to enter their credentials only once, and have those credentials reused when accessing other network resources. These methods include:		
		Agent-based SSO with Windows AD, Citrix, VMware Horizon, Novell eDirectory, and Microsoft Exchange		
		SSO using RADIUS accounting records		
		The proposed system shall support guest access with the following features:		
		Create a guest management administrator which is restricted to guest account provisioning only		
		Guest username and password can be manually specified or auto generated.		
		Guest accounts expiry.		
		Guest login credential can be delivered via an email, SMS message, or a printout		
		Guest login using captive portal authentication		
		The proposed system shall be able to operate as a service provider (SP) in a SAML setup for both firewall and SSL VPN web portal authentication.		
		The proposed system shall have an in-built token server that provisions and manages hard and mobile tokens.		

1.4	**VPN Features**	The system shall support the following IPsec VPN capabilities:		
		Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS		
		Authentication method: Certificate, pre-shared key		
		IPsec Phase 1 mode: Aggressive and main (ID protection) mode		
		Peer acceptance options: Any ID, specific ID, ID in dialup user group		
		Supports IKEv1, IKEv2 (RFC 4306)		
		IKE mode configuration support (as server or client), DHCP over IPsec		
		Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256		
		Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512		
		Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14, 15, 16, 17, 18, 19, 19, 21, 27, 28, 29, 30 and 31		
		XAuth support as client or server mod		
		XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option		
		Configurable IKE encryption key expiry, NAT traversal keepalive frequency		
		Dead peer detection		
		Replay detection		
		Autokey keep-alive for Phase 2 SA		
		The proposed system shall provide IPsec VPN wizards to terminate tunnels to in-house or third-party devices and clients		
		The proposed system shall support SSL VPN portal capabilities that include		
		User portal customization - include color themes, layout, bookmarks, connection tools, and client download location.		

		Single-sign-on bookmarks - reuse previous login or predefined credentials to access resources		
		Personal bookmarks management which allows administrators to view and maintain remote client bookmarks		
		One-time login per user options which prevents concurrent logins using the same username		
		The proposed system shall support SSL VPN realms - multiple custom SSL VPN logins associated with user groups (URL paths, design)		
		The proposed system shall support various SSL VPN modes:		
		Web mode: for thin remote clients equipped with a web browser only and support web application, that includes HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix		
		Tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN clients must support MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems		
		Port Forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server		
1.5	**High Availability Features**	The proposed system shall support high availability with industry standard VRRP with the following characteristics:		
		Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP.		
		Be able integrated into a VRRP group with any third-party VRRP devices		

		Supports IPv4 and IPv6 VRRP		
		The proposed system shall support high availability by setting up a cluster with the following characteristics:		
		Supports up to 4 cluster members		
		Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)		
		Cluster units communicate with each other through their heartbeat interfaces		
		Uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit		
		Provides device failover in the event of hardware or software failure		
		Provides link failover when a direct link is not available on one/more monitored interface(s)		
		Provides remote link failover when connectivity with IP addresses of remote network devices, for example, a downstream router is not available		
		In the event of a failover, log messages about the event and can be configured to send log messages to a syslog server. The cluster can also send SNMP traps and alert email messages		
		Supports session failover (also called session pickup) which during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster. during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster.		

		Supports the option to automatically failback in the event the original unit recovers		
		Supports widely separated cluster units installed in different physical locations		
		The proposed system shall support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, similar to normal HA.		
		The proposed system shall support full mesh HA configuration where one can connect an HA cluster consisting of two or more cluster members to the network using 802.3ad Aggregate or Redundant interfaces and redundant switches		
		The proposed system shall support out-of-band management for each cluster member where a management interface is reserved with its own configurations and are not synchronized to other cluster units.		
		The proposed system shall support the upgrade of the firmware without interrupting communication through the cluster		
		In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two to 16 units can be integrated into the load balancing configuration by operating as peers that process traffic and perform configuration synchronization; and session synchronization of connectionless sessions, expectation sessions, and NAT sessions and IPsec tunnels.		
1.6	**Networking**	The proposed system shall support the IEEE standard 802.3ad for physical link aggregation.		
		The proposed system shall be able to send out Gratuitous Address		

		Resolution Protocol (GARP) announcements if the MAC address of a link aggregated interface changes to a new IP pool address due to a link failure or change in ports.		
		Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed system. The interface shall automatically broadcast DHCP requests and then provide IP address, any DNS server addresses, and the default gateway address to clients.		
		Administrators shall be able to configure an interface as a DHCP relay		
		Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed system transmits to improve network performance.		
		A loopback interface is a logical interface that's always up (no physical link dependency) and the attached subnet is always present in the routing table. Administrators shall be able to configure multiple loopback interfaces on the proposed system.		
		Administrators shall be able to configure physical interfaces on the proposed system for one-armed sniffer with the following capabilities:		
		Ability to deploy filters that define a more granular sniff of network traffic. The filter definition shall include hosts, ports, VLANs, and protocol.		
		Ability to sniff IPv6 traffic.		
		Traffic sent to the sniffer interface shall have the option to be logged and examined against security components such as IPS and application control.		

		Administrators shall be able to obtain information of transceivers plugged into the proposed system via CLI command. The output shall include the vendor name, part number, and serial number. It shall also include details about transceiver operation, such as temperature, voltage, and optical transmission power.		
		Administrators shall be able to combine two or more physical interfaces to provide link redundancy. This feature allows administrators to connect to two or more switches to ensure connectivity if one physical interface, or the equipment on that interface, fails. In a redundant interface, traffic travels only over one interface at a time.		
		Administrators shall be able to configure Secondary IP addresses to an interface.		
		Administrators shall be able to group interfaces, both physical and virtual, into zones that simplifies the creation of security policies.		
		The proposed system shall support the creation of native VXLAN interfaces and support for multiple remote IP addresses, which can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast.		
		The proposed system shall support enhanced MAC VLAN which consists of a MAC VLAN with bridge functionality.		
		The proposed system shall support multiple virtual wire pairs that logically bind two physical interfaces so that all traffic from one of the interfaces can exit only through the other interface if allowed by firewall policy.		

		The proposed system shall support wildcard VLANs for a virtual wire pair. Doing this allows all VLAN-tagged traffic to pass through a virtual wire pair if a virtual wire pair firewall policy allows the traffic.		
		The proposed system shall support various enterprise DNS settings, including:		
		Ability to set the number of DNS entries that can be cached		
		Ability to how long entries remain in the cache		
		Ability to define a dedicated IP address for communications with DNS servers		
		The proposed system shall allow organizations to use a dynamic DNS (DDNS) service		
		The proposed system shall provide the ability to run local DNS servers		
		The proposed system shall support static routing with various advanced features:		
		Support for both IPv4 and IPv6 routes		
		Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes.		
		Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database.		
		The proposed system shall support blackhole routing. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator won't discover any information from the target network.		

		The proposed system shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing.		
		The proposed system shall support IPv4 policy routing using the definition of:		
		Protocol type, including SCTP		
		Incoming and outgoing logical interface		
		Source and destination IP addresses/subnets		
		Source and destination firewall address/address group objects		
		Type of Service (ToS)		
		The proposed system shall support IPv6 policy routing		
		The proposed system shall support RIP version 1 (RFC 1058), RIP version 2 (RFC 2453), and the IPv6 version RIPng (RFC 1980) routing protocols		
		The proposed system shall support default information originate option for RIP configuration		
		Administrator shall be able to regulate RIP performance, including specifying update timer, timeout timer, and garbage timer.		
		The proposed system shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols		
		The proposed system shall support BGP4 (IPv4) and BGP4+ (IPv6) routing protocols		
		The proposed system shall support Intermediate System to Intermediate System Protocol (IS-IS) protocol for both IPv4 and IPv6		
		The proposed system shall support the ability to forward multicast traffic in both transparent/bridge and route/NAT mode		
		The proposed system shall be able to operate as a Protocol Independent Multicast (PIM) version 2 router with support for:		

		PIM sparse mode (PIM-SM, RFC 4601)		
		PIM dense mode (PIM-DM, RFC 3973)		
		PIM Source Specific mode (PIM-SSM. RFC 3569)		
		IGMP v1, IGMP v2, IGMP v3 protocols		
		The proposed system shall support the ability to connect 3G/4G modem to its USB port		
1.7	**OS & Management Features**	The proposed OS must:		
		-Be proprietary to prevent inheriting common OS vulnerabilities		
		-Resided on flash disk for reliability over the hard disk		
		-Allow dual booting		
		-Upgradeable via Web UI or TFTP		
		The configurations on the device shall:		
		-Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
		-Provide CLI command configuration file that is readable by Windows Notepad		
		-Have an option to encrypt the backup file		
		-Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision.		
		The proposed system shall minimally provide management access through:		
		-GUI using HTTP or HTTPs access which administration service port can be configured, example via TCP port 8080		
		-CLI console using console port, SSHv2, telnet or from GUI console		
		-The proposed system shall offer the option to automatically redirect HTTP management access to HTTPS		

		-The proposed system shall enforce mandatory default administrator password setup upon the first-time login or after a factory reset.		
		The proposed system shall have the option to implement local administrator password policy enforcement including:		
		-Minimum length		
		-Character requirements - Upper case, lower case, numbers and special character		
		-Disallow password reuse		
		-Password expiration		
		The administrator authentication shall be facilitated by a local database, PKI & remote services such as Radius, LDAP and TACACS+		
		The proposed system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
		The proposed system shall be able to limit remote management access:		
		-From certain trusted network or host with a corresponding administrator account		
		-To certain (virtual) interfaces		
		The proposed system shall be allowed administrators to set administration idle timeout between 1 to 480 minutes		
		The proposed system should be able to facilitate administration audits by logging detailed activities to event log - management access and configuration changes.		
		The proposed solution shall support various zero-touch provisioning options:		
		-Cloud assisted provisioning: When devices at remote locations are plugged in, they automatically obtain an IP address via DHCP. These devices then ‘call home’ to the cloud facility. From there, the device will receive the management related		

		configurations.		
		-DHCP server provisioning: Devices will boot up using the appropriate DHCP server which provides DHCP option 240 and 241 that records manager IP and domain name.		
1.8	**System Integration**	The proposed system shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. The solution should offer the following capabilities:		
		A physical topology view that shows all connected devices, including access layer device and a logical topology view that shows information about the interfaces that each device is connected to.		
		Security best practice checks across various security components in the network to identify potential vulnerabilities and suggest improvements to the configurations.		
		The proposed system shall have in-built automation feature that pairs an event trigger with one or more actions to monitor the network and take the designated actions when a threat or situation change is detected. It should have the followings:		
		Triggers: configuration change, system status, HA failover, event log handler, incoming webhook and schedule		
		Actions: CLI Script, Email, iOS app notification, public cloud functions, slack notification and webhook		
		The proposed system shall allow GUI configurations to external services that include:		
		Public cloud providers - AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud.		
		SDN platforms and private cloud hypervisors - Kubernates, VMware NSX, VMware ESXi, OpenStack,		

		Cisco ACI, and Nuage VSP.		
		Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system and Microsoft Exchange		
		External threat feeds: URL list, IP list, domain name list, and malware file hash		
1.9	**Explicit and Transparent Proxy Features**	The proposed system shall provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic with the following capabilities:		
		-support for the use of multiple ports and port range for proxying		
		-definition of a FQDN, to be entered on browsers		
		-setup of maximum allowed HTTP request and message length		
		-outgoing IP can be selected from an IP pool		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		-create URL match list with URL patterns forward to forwarding servers and/or create a list of URLs that are exempt from web caching		
		The proposed system shall be capable of hosting Proxy Auto-Configuration (PAC) file		
		The proposed system shall support proxy chaining when deployed as an explicit web proxy with these additional capabilities:		
		-monitor the remoter servers periodically and bypass any unavailable servers		
		-load balance traffic to servers using a weighted algorithm or sending new sessions to the server that is processing the fewest sessions		

		The proposed system shall support transparent web proxy whereby the user's client software, such as a browser, is unaware that it is communicating with a proxy.		
		The proposed system shall support transparent web proxy forwarding, without having to reconfigure user browsers or publish a proxy auto-reconfiguration (PAC) file. Explicit web proxy setting is also not required as it shall be implemented as a setting of a firewall policy. Once configured, the system transparently forwards traffic generated by a client to the upstream proxy. The upstream proxy then forwards it to the server.		
		The proposed system shall support explicit FTP Proxy with the following capabilities:		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		The proposed system shall support SaaS (Office 365, G-suite, Dropbox) access control with web proxying by inserting vendor-defined headers that restrict access to the specific accounts.		
1.10	**Intrusion Prevention Features**	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
		Signature based detection using real time updated database		
		Anomaly based detection that is based on thresholds		
		The proposed system shall support One-arm IDS (sniffer mode) and operate in both NAT/route and transparent mode		
		The proposed system's IPS database shall have over 11,000 up-to-date signatures		

		The proposed system shall support custom IPS signatures. In addition, Snort IPS rules can be converted to these signatures using a converter tool		
		The proposed system shall be capable of updating IPS signatures without restarting the systems using the following options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		
		-automatic push update		
		The proposed system shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types, In addition,		
		A signature can be selected by searching for its corresponding CVE-ID (if applicable)		
		The proposed system shall offer one of the following actions when an attack is detected:		
		Allow session		
		Monitor and log session		
		Block session		
		Reset session		
		Quarantine attacker		
1.11	**Advanced Threat Protection**	The proposed system shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs		
		The proposed system shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection using various technologies:		
		Malware signature database		
		Heuristic AV Engine		
		External file analysis with native integration with on-prem system or cloud-based service		
		File checksums query using cloud-based malware database before AV signatures are available		

		File checksums query using external block list/threat feed		
		The proposed system shall be capable of updating AV signatures without restarting the systems using the following options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		
		-automatic push update		
		The proposed system shall also be able to block graywares and mobile malwares		
		The proposed system shall offer the ability to treat Windows Executables in Email Attachments as viruses		
		The antivirus scanning should be supported on various protocols:		
		-HTTP/HTTPS		
		-SMTP/SMTPS		
		-POP3/POP3S		
		-IMAP/IMAPS		
		-MAPI		
		-FTP/SFTP		
		-CIFS		
		The proposed system shall able to scan archive files for malwares		
		The proposed system shall support Content Disarm and Reconstruction (CDR) where exploitable content (within PDF and Microsoft Office files) can be removed and replaced with content that is known to be safe		
		The proposed system shall be capable of blocking Botnet server communications with IPS signatures and IP reputation database		
		The proposed system shall maintain a fingerprint-based certificate blacklist is that useful to block botnet communication that relies on SSL.		
		The proposed system shall be able to automatically ban infected machines from other network segments.		

1.12	**SSL Inspection**	The proposed system shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic.		
		The proposed system shall support certificate inspection on port 443, all ports or a specific non-standard port. In addition, the system should:		
		Have option block sessions with invalid certificates		
		Have option allow sessions with untrusted certificates		
		The proposed system shall provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or using a whitelist.		
1.13	**Web Filter Features**	The proposed system shall allow organizations to implement flow-based, proxy-based and DNS-based web filtering concurrently, depending on the network and security needs		
		The proposed system shall support static web filtering by:		
		-manually-defined URLs using regular expression and wildcards		
		-manually-defined content filter using regular expression and wildcards		
		The proposed system shall support dynamic web filtering by querying real-time cloud-based categorization database.		
		This database should have over 250 million URLs rated into 78 categories and in 70 languages		
		Various actions can be performed when matched to a category: Allow, Block, Monitor (logged), Warning (with message at configurable time interval), (request for) user authentication		
		Customizable replacement page (for warning and blocking)		

		The proposed system shall have pre-configured parental control category-based filter including “G”, ‘PG-13” and “R”		
		The proposed system shall provide ability to use local categories (that override the cloud-based database rating) and remote categories (external URL list) as part of the URL rating function.		
		The proposed system shall have the ability to prevent explicit websites and images from appearing in Google, Yahoo!, Bing and Yandex search results by transparently inserting safe search parameters.		
		The proposed system shall allow implementation of usage quota by category and category group:		
		Allow access for a specified length of time or a specific bandwidth.		
		Calculated separately for each user		
		Reset on daily basis		
		The proposed system shall have the option to allow override blocked categories:		
		By administrative override where administrators can grant temporary access to sites that are otherwise blocked		
		By allowing specified users/user groups/IP addresses		
		The proposed system shall have the ability to limit users' access to YouTube channels, such as in an education environment where users are only able to access YouTube education videos but no other YouTube videos with the following methods:		
		-working with G Suite user access configurations		
		-Manually define allowed channels on the system		
		The proposed system shall offer proxy avoidance prevention capabilities, including:		

		-Proxy site category blocking (via application Control)		
		-Proxy behaviors blocking (via IPS)		
		The proposed system shall provide advanced web filtering options:		
		-Filter Java Applet, ActiveX, and/or cookie		
		-Block HTTP POST		
		-Log search keywords		
		-Allow websites when a rating error occurs		
		-Rate URLs by domain and IP Address		
		-Block invalid URLs		
		-Restrict Google account usage to specific domains (e.g. only corporate accounts only)		
		-Must have configurable policy options to define the URL exempt list		
1.14	**DNS Filter Features**	The proposed system shall provide the ability to apply DNS category filtering to control user access to web resources with the following features:		
		Using cloud-based rating database		
		Botnet C&C domain blocking: blocks the DNS request for the known botnet C&C domains		
		External dynamic category domain filtering: allows manual-definition of domain category		
		DNS safe search: enforces Google, Bing, and YouTube safe addresses for parental controls		
		Local domain filter: allows administrators to define their own domain list to block or allow		
		External IP block list: allows you to define an IP block list to block resolved IPs that match this list.		
		The proposed system shall have the ability to translate a DNS resolved IP address to another IP address that is specified on a per-policy basis		
1.15	**Application Control Features**	The proposed system shall support traffic detection using HTTP protocol (versions 1.0, 1.1, and 2.0)		

		The proposed system shall be able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 1.2		
		The proposed system shall detect over 4,000 applications in 17 categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/ Audio, VoIP, Web Chat and Industrial		
		The proposed system shall support custom application control signatures		
		The proposed system shall allow administrators to apply various actions against the detected traffic, they include monitor, allow, block, reset and quarantine for a defined period of time.		
		The proposed system shall provide ability to group applications dynamically for assignment of actions using various filters:		
		-By Predefined categories		
		-By application behavior (e.g. Evasive, excessive-bandwidth)		
		-By application popularity		
		-By protocols (e.g. HTTP, MODBUS)		
		-By risk level		
		-By technology (e.g. browser-based, peer-to-peer)		
		-By Vendor (e.g. Goggle, Microsoft)		
		The proposed system shall allow administrators to set networking services to defined ports. A violation can be set to block. Organizations shall also be able to block applications detected on non-default ports		
		The proposed system shall offer some application signatures with additional defined parameters to match		
		The proposed system shall support SSH traffic inspection and control various related activities, including:		

		-X server forwarding (X11)		
		-SSH shell		
		-SSH execution (exec)		
		-SSH port-forwarding		
		-SSH Tunnel Forwarding		
		-Unknow channel usage		
		-Administrator-defined commands		
1.16	**SD-WAN Features**	The proposed system shall support aggregation of up to 255 interfaces to create a virtual WAN link.		
		The proposed system shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include:		
		-Predefined performance SLA profiles such as Office 365, AWS and Gmail		
		-Health check probes using IPv4/IPv6 Ping and HTTP		
		-Selection of multiple destinations (or servers) to probe		
		-Interfaces relating to the performance SLA profile		
		The proposed system shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic take. These constraints should include:		
		-Latency threshold		
		-Jitter threshold		
		-Packet loss threshold		
		The proposed system shall provide settings to the characteristic of probes, including check interval, link failure and restoration considerations.		
		The proposed system shall provide option to disable the implicated static route when an interface is inactive.		

		The proposed system shall allow organizations to define SD-WAN rules that are used to control how sessions are distributed to SD-WAN interfaces. The definition of these rules shall include:		
		-Source: address and/or user group		
		-Destination: address, applications and/or dynamic IP database		
		-Path control strategies		
		The proposed system shall provide the following path control strategies:		
		-Manual: Interfaces are manually assigned a priority		
		-Best Quality: Interface are assigned a priority based on the quality of the interface. Quality criteria may be latency, jitter, packet loss, available bandwidth (for upstream, downstream, or both) or custom with a cocktail of weighted criteria		
		-Lowest Cost (SLA): Interface is selected based on the lowest cost defined on SD-WAN interfaces that meets selected SLA settings		
		-Maximize Bandwidth (SLA): Traffic is distributed among all available links that satisfies selected SLA profile based on a round-robin load balancing algorithm		
		The proposed system shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces:		
		-Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path		
		-Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces.		

		-Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces.		
		-Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path.		
		-Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface.		
		The proposed system shall support per-packet load-balancing among IPSec tunnels.		
		The proposed system shall support forward error correction (FEC) on VPN overlay networks.		
		The proposed system shall support SD-WAN rules with Border Gateway Protocol (BGP) learned routes as dynamic destinations.		
		The proposed system shall provide Dual VPN tunnel wizard that is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.		
		The proposed system shall support integration with a cloud-based solution to simplify IPsec VPN setup.		
1.17	**Additional Requirements**	The vendor must attain ISO 9001:1900 certification that covers the scope of the Quality Management System which includes the design, development, and manufacturing of network security products and the delivery of associated security services and support		

		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations		
		The proposed solution must be listed in the latest Gartner Leaders MQ for Network Firewalls		
		The device should be from a family of products that attains ICSA Labs Certifications for Antivirus, Corporate Firewall, IPsec, NIPS, SSL-TLS.		
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
		The proposed system shall support unlimited IP addresses license		
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
		The proposed solution must be from a family of products that achieves Common Criteria FWcPP (V2.0) + IPS (V2.11) and VPN (V2.1) Certification		

Nakuru Firewall Specifications

SN	Component	Specification required including applicable standards	Compliance of specification offered (Fully Comply/Non-Comply)	Description of specifications offered including page no. in Technical literature where specifications is reflected.
2	**NAKURU GATEWAY FIREWALL (Quantity 1)**			
2.1		Must be support at least 2 x 10GE SFP+ slots		
		Must be support at least 8 x 1GE RJ45 interfaces		
		Must be support at least 8 x 1GE SFP slots		
		Must support at least 7 Million Maximum Concurrent Sessions		
		Must support at least 400,000 New Sessions/Second		

		Must support at least 30Gbps of firewall throughput		
		Must support at least 10 Gbps Enterprise/Production IPS Throughput		
		Must support at least 7 Gbps SSL Inspection Throughput Throughput		
		Must support at least 7 Gbps Enterprise/Production Threat Protection Throughput		
		Must support at least 480GB SSD storage		
		Must be support dual power supplies		
		Must be supplied with at least 1,000 SSL VPN licenses		
		Must have the following licenses included Application Control, IPS, Anti Malware, Web Filtering, DNS Filtering, Mobile Security, IOT Security and Sandbox Cloud		
2.2	**Firewall Features**	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified		
		It Must be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode		
		The proposed system shall support robust GUI configurations of both IPv4 and IPv6 firewall policies on the same table that include:		
		-One-click edit of firewall objects from the policy table panel		
		-Drag and drop policy moving		
		-Right-Click on one/multiple policy(ies) to toggle enabling/disabling and deleting of policies		
		-Editing selected policy on GUI or from CLI panel		
		-Show matching logs of selected policy		
		The proposed system shall offer a firewall policy table in both views by policy sequence and by		

		interface pairs		
		The proposed system shall allow the administrator to customize the firewall policy table's columns		
		The proposed system shall allow the administrator to view filtered policies by using a search bar		
		The proposed system's firewall policies shall support various types of source objects, including IP address/address range/subnets, users, MAC addresses and dynamic addresses from SaaS and reputation list.		
		The proposed system shall support firewall session helpers and ALGs for FTP, TFTP, RAS, H323, TNS/SQLNET, MMS, SIP, PPTP, RTSP, DNS (UDP), DNS (TCP), PMAP, RSH, DCE/RPC and MGCP		
		The proposed system's firewall policies shall support all protocol types that include TCP, UDP, SCTP, IP, and ICMP		
2.3	**Authentication Features**	The proposed system shall support the following user authentication methods to be applied on a security policy and/or VPN access:		
		Local password authentication		
		Server-based password authentication using LDAP, RADIUS, TACACS+, Windows AD, or POP3 servers		
		Certificate-based authentication for host and endpoints		
		Two-factor authentication for additional security beyond just passwords		
		The proposed system shall support various single sign-on (SSO) techniques so that users to enter their credentials only once, and have those credentials reused when accessing other network resources. These methods include:		

		Agent-based SSO with Windows AD, Citrix, VMware Horizon, Novell eDirectory, and Microsoft Exchange		
		SSO using RADIUS accounting records		
		The proposed system shall support guest access with the following features:		
		Create a guest management administrator which is restricted to guest account provisioning only		
		Guest username and password can be manually specified or auto generated		
		Guest accounts expiry		
		Guest login credential can be delivered via an email, SMS message, or a printout		
		Guest login using captive portal authentication		
		The proposed system shall be able to operate as a service provider (SP) in a SAML setup for both firewall and SSL VPN web portal authentication.		
		The proposed system shall have an in-built token server that provisions and manages hard and mobile tokens		
2.4	**VPN Features**	The system shall support the following IPsec VPN capabilities:		
		Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS		
		Authentication method: Certificate, pre-shared key		
		IPsec Phase 1 mode: Aggressive and main (ID protection) mode		
		Peer acceptance options: Any ID, specific ID, ID in dialup user group		
		Supports IKEv1, IKEv2 (RFC 4306)		
		IKE mode configuration support (as server or client), DHCP over IPsec		
		Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128.		

		AES192, AES256		
		Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512		
		Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14, 15, 16, 17, 18, 19, 19, 21, 27, 28, 29, 30 and 31		
		XAuth support as client or server mod		
		XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option		
		Configurable IKE encryption key expiry, NAT traversal keepalive frequency		
		Dead peer detection		
		Replay detection		
		Autokey keep-alive for Phase 2 SA		
		The proposed system shall provide IPsec VPN wizards to terminate tunnels to in-house or third-party devices and clients		
		The proposed system shall support SSL VPN portal capabilities that include		
		User portal customization - include color themes, layout, bookmarks, connection tools, and client download location.		
		Single-sign-on bookmarks - reuse previous login or predefined credentials to access resources		
		Personal bookmarks management which allows administrators to view and maintain remote client bookmarks		
		One-time login per user options which prevents concurrent logins using the same username		
		The proposed system shall support SSL VPN realms - multiple custom SSL VPN logins associated with user groups (URL paths, design)		

		The proposed system shall support various SSL VPN modes:		
		Web mode: for thin remote clients equipped with a web browser only and support web application, that includes HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix		
		Tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN clients must support MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems		
		Port Forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server		
2.5	**High Availability Features**	The proposed system shall support high availability with industry standard VRRP with the following characteristics:		
		Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP		
		Be able integrated into a VRRP group with any third-party VRRP devices		
		Supports IPv4 and IPv6 VRRP		
		The proposed system shall support high availability by setting up a cluster with the following characteristics:		
		Supports up to 4 cluster members		
		Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)		
		Cluster units communicate with each other through their heartbeat interfaces		

		Uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit		
		Provides device failover in the event of hardware or software failure		
		Provides link failover when a direct link is not available on one/more monitored interface(s)		
		Provides remote link failover when connectivity with IP addresses of remote network devices, for example, a downstream router is not available		
		In the event of a failover, log messages about the event and can be configured to send log messages to a syslog server. The cluster can also send SNMP traps and alert email messages		
		Supports session failover (also called session pickup) which during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster. during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up-to-date with the traffic currently being processed by the cluster.		
		Supports the option to automatically failback in the event the original unit recovers		
		Supports widely separated cluster units installed in different physical locations		

		The proposed system shall support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, like normal HA.		
		The proposed system shall support full mesh HA configuration where one can connect an HA cluster consisting of two or more cluster members to the network using 802.3ad Aggregate or Redundant interfaces and redundant switches		
		The proposed system shall support out-of-band management for each cluster member where a management interface is reserved with its own configurations and are not synchronized to other cluster units.		
		The proposed system shall support the upgrade of the firmware without interrupting communication through the cluster		
		In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two to 16 units can be integrated into the load balancing configuration by operating as peers that process traffic and perform configuration synchronization; and session synchronization of connectionless sessions, expectation sessions, and NAT sessions and IPsec tunnels.		
2.6	**Networking**	The proposed system shall support the IEEE standard 802.3ad for physical link aggregation		

		The proposed system shall be able to send out Gratuitous Address Resolution Protocol (GARP) announcements if the MAC address of a link aggregated interface changes to a new IP pool address due to a link failure or change in ports		
		Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed system. The interface shall automatically broadcast DHCP requests and then provide IP address, any DNS server addresses, and the default gateway address to clients		
		Administrators shall be able to configure an interface as a DHCP relay		
		Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed system transmits to improve network performance		
		A loopback interface is a logical interface that's always up (no physical link dependency) and the attached subnet is always present in the routing table. Administrators shall be able to configure multiple loopback interfaces on the proposed system		
		Administrators shall be able to configure physical interfaces on the proposed system for one-armed sniffer with the following capabilities:		
		Ability to deploy filters that define a more granular sniff of network traffic. The filter definition shall include hosts, ports, VLANs, and protocol		
		Ability to sniff IPv6 traffic		
		Traffic sent to the sniffer interface shall have the option to be logged and examined against security components such as IPS and application control.		

		Administrators shall be able to obtain information of transceivers plugged into the proposed system via CLI command. The output shall include the vendor name, part number, and serial number. It shall also include details about transceiver operation, such as temperature, voltage, and optical transmission power.		
		Administrators shall be able to combine two or more physical interfaces to provide link redundancy. This feature allows administrators to connect to two or more switches to ensure connectivity if one physical interface, or the equipment on that interface, fails. In a redundant interface, traffic travels only over one interface at a time.		
		Administrators shall be able to configure Secondary IP addresses to an interface		
		Administrators shall be able to group interfaces, both physical and virtual, into zones that simplifies the creation of security policies.		
		The proposed system shall support the creation of native VXLAN interfaces and support for multiple remote IP addresses, which can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast.		
		The proposed system shall have interfaces compromising of both physical interfaces and VLANs		
		The proposed system shall support enhanced MAC VLAN which consists of a MAC VLAN with bridge functionality.		
		The proposed system shall support multiple virtual wire pairs that logically bind two physical interfaces so that all traffic from one of the interfaces can exit only through the other interface if allowed by firewall policy.		

		The proposed system shall support wildcard VLANs for a virtual wire pair. Doing this allows all VLAN-tagged traffic to pass through a virtual wire pair if a virtual wire pair firewall policy allows the traffic.		
		The proposed system shall support various enterprise DNS settings, including:		
		Ability to set the number of DNS entries that can be cached		
		Ability to how long entries remain in the cache		
		Ability to define a dedicated IP address for communications with DNS servers		
		The proposed system shall allow organizations to use a dynamic DNS (DDNS) service		
		The proposed system shall provide the ability to run local DNS servers		
		The proposed system shall support static routing with various advanced features:		
		Support for both IPv4 and IPv6 routes		
		Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes.		
		Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database.		

		The proposed system shall support blackhole routing. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator won't discover any information from the target network.		
		The proposed system shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing.		
		The proposed system shall support IPv4 policy routing using the definition of:		
		Protocol type, including SCTP		
		Incoming and outgoing logical interface		
		Source and destination IP addresses/subnets		
		Source and destination firewall address/address group objects		
		Type of Service (ToS).		
		The proposed system shall support IPv6 policy routing		
		The proposed system shall support RIP version 1 (RFC 1058), RIP version 2 (RFC 2453), and the IPv6 version RIPng (RFC 1980) routing protocols		
		The proposed system shall support default information originate option for RIP configuration		
		Administrator shall be able to regulate RIP performance, including specifying update timer, timeout timer, and garbage timer.		
		The proposed system shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols		
		The proposed system shall support BGP4 (IPv4) and BGP4+ (IPv6) routing protocols		

		The proposed system shall support Intermediate System to Intermediate System Protocol (IS-IS) protocol for both IPv4 and IPv6		
		The proposed system shall support the ability to forward multicast traffic in both transparent/bridge and route/NAT mode		
		The proposed system shall be able to operate as a Protocol Independent Multicast (PIM) version 2 router with support for:		
		PIM sparse mode (PIM-SM, RFC 4601)		
		PIM dense mode (PIM-DM, RFC 3973)		
		PIM Source Specific mode (PIM-SSM. RFC 3569)		
		IGMP v1, IGMP v2, IGMP v3 protocols		
		The proposed system shall support the ability to connect 3G/4G modem to its USB port		
2.7	**OS & Management Features**	The proposed OS must:		
		-Be proprietary to prevent inheriting common OS vulnerabilities		
		-Resided on flash disk for reliability over the hard disk		
		-Allow dual booting		
		-Upgradeable via Web UI or TFTP		
		The configurations on the device shall:		
		-Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
		-Provide CLI command configuration file that is readable by Windows Notepad		
		-Have an option to encrypt the backup file		

		-Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision.		
		The proposed system shall minimally provide management access through:		
		-GUI using HTTP or HTTPs access which administration service port can be configured, example via TCP port 8080		
		-CLI console using console port, SSHv2, telnet or from GUI console		
		The proposed system shall offer the option to automatically redirect HTTP management access to HTTPS		
		The proposed system shall enforce mandatory default administrator password setup upon the first-time login or after a factory reset.		
		The proposed system shall have the option to implement local administrator password policy enforcement including:		
		-Minimum length		
		-Character requirements - Upper case, lower case, numbers and special character		
		-Disallow password reuse		
		-Password expiration		
		The administrator authentication shall be facilitated by a local database, PKI & remote services such as Radius, LDAP and TACACS+		
		The proposed system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
		The proposed system shall be able to limit remote management		

		access:		
		-From certain trusted network or host with a corresponding administrator account		
		-To certain (virtual) interfaces		
		The proposed system shall be allowed administrators to set administration idle timeout between 1 to 480 minutes		
		The proposed system should be able to facilitate administration audits by logging detailed activities to event log - management access and also configuration changes.		
		The proposed solution shall support various zero-touch provisioning options:		
		Cloud assisted provisioning: When devices at remote locations are plugged in, they automatically obtain an IP address via DHCP. These devices then 'call home' to the cloud facility. From there, the device will receive the management related configurations.		
		DHCP server provisioning: Devices will boot up using the appropriate DHCP server which provides DHCP option 240 and 241 that records manager IP and domain name.		
2.8	**System Integration**	The proposed system shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. The solution should offer the following capabilities:		
		A physical topology view that shows all connected devices, including access layer device and a logical topology view that shows information about the interfaces that each device is connected to.		

		Security best practice checks across various security components in the network to identify potential vulnerabilities and suggest improvements to the configurations.		
		The proposed system shall have in-built automation feature that pairs an event trigger with one or more actions to monitor the network and take the designated actions when a threat or situation change is detected. It should have the followings:		
		Triggers: configuration change, system status, HA failover, event log handler, incoming webhook and schedule		
		Actions: CLI Script, Email, iOS app notification, public cloud functions, slack notification and webhook		
		The proposed system shall allow GUI configurations to external services that include:		
		Public cloud providers - AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud		
		SDN platforms and private cloud hypervisors - Kubernates, VMware NSX, VMware ESXi, OpenStack, Cisco ACI, and Nuage VSP		
		Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system and Microsoft Exchange		
		External threat feeds: URL list, IP list, domain name list, and malware file hash		
2.9	**Explicit and Transparent Proxy Features**	The proposed system shall provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic with the following capabilities:		
		-support for the use of multiple ports and port range for proxying		

		-definition of a FQDN, to be entered into browsers		
		-setup of maximum allowed HTTP request and message length		
		-outgoing IP can be selected from an IP pool		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		-create URL match list with URL patterns forward to forwarding servers and/or create a list of URLs that are exempt from web caching		
		The proposed system shall be capable of hosting Proxy Auto-Configuration (PAC) file		
		The proposed system shall support proxy chaining when deployed as an explicit web proxy with these additional capabilities:		
		-monitor the remoter servers periodically and bypass any unavailable servers		
		-load balance traffic to servers using a weighted algorithm or sending new sessions to the server that is processing the fewest sessions		
		The proposed system shall support transparent web proxy whereby the user's client software, such as a browser, is unaware that it is communicating with a proxy.		
		The proposed system shall support transparent web proxy forwarding, without having to reconfigure user browsers or publish a proxy auto-reconfiguration (PAC) file. Explicit web proxy setting is also not required as it shall be implemented as a setting of a firewall policy. Once configured, the system transparently forwards traffic generated by a client to the upstream proxy. The upstream		

		proxy then forwards it to the server.		
		The proposed system shall support explicit FTP Proxy with the following capabilities:		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		The proposed system shall support SaaS (Office 365, G-suite, Dropbox) access control with web proxying by inserting vendor-defined headers that restrict access to the specific accounts.		
2.10	**Intrusion Prevention Features**	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
		Signature based detection using real time updated database		
		Anomaly based detection that is based on thresholds		
		The proposed system shall support One-arm IDS (sniffer mode) and operate in both NAT/route and transparent mode		
		The proposed system's IPS database shall have over 11,000 up-to-date signatures		
		The proposed system shall support custom IPS signatures. In addition, Snort IPS rules can be converted to these signatures using a converter tool		
		The proposed system shall be capable of updating IPS signatures without restarting the systems using the following		

		options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		
		-automatic push update		
		The proposed system shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types, In addition,		
		A signature can be selected by searching for its corresponding CVE-ID (if applicable)		
		The proposed system shall offer one of the following actions when an attack is detected:		
		Allow session		
		Monitor and log session		
		Block session		
		Reset session		
		Quarantine attacker		
2.11	**Advanced Threat Protection**	The proposed system shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs		
		The proposed system shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection using various technologies:		
		Malware signature database		
		Heuristic AV Engine		
		External file analysis with native integration with on-prem system or cloud-based service		
		File checksums query using cloud-based malware database before AV signatures are available		
		File checksums query using external block list/threat feed		

		The proposed system shall be capable of updating AV signatures without restarting the systems using the following options:		
		manual database upload (without system internet access)		
		periodically scheduled pull update		
		automatic push update		
		The proposed system shall also be able to block graywares and mobile malwares		
		The proposed system shall offer the ability to treat Windows Executables in Email Attachments as viruses		
		The antivirus scanning should be supported on various protocols:		
		-HTTP/HTTPS		
		-SMTP/SMTPS		
		-POP3/POP3S		
		-IMAP/IMAPS		
		-MAPI		
		-FTP/SFTP		
		-CIFS		
		The proposed system shall able to scan archive files for malwares		
		The proposed system shall support Content Disarm and Reconstruction (CDR) where exploitable content (within PDF and Microsoft Office files) can be removed and replaced with content that is known to be safe		
		The proposed system shall be capable of blocking Botnet server communications with IPS signatures and IP reputation database		
		The proposed system shall maintain a fingerprint-based certificate blacklist is that useful to block botnet communication that relies on SSL		
		The proposed system shall be able to automatically ban infected machines from other network		

		segments		
2.12	**SSL Inspection**	The proposed system shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic		
		The proposed system shall support certificate inspection on port 443, all ports or a specific non-standard port. In addition, the system should:		
		Have option block sessions with invalid certificates		
		Have option allow sessions with untrusted certificates		
		The proposed system shall provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or using a whitelist.		
2.13	**Web Filter Features**	The proposed system shall allow organizations to implement flow-based, proxy-based and DNS-based web filtering concurrently, depending on the network and security needs		
		The proposed system shall support static web filtering by:		
		-manually-defined URLs using regular expression and wildcards		
		-manually-defined content filter using regular expression and wildcards		
		The proposed system shall support dynamic web filtering by querying real-time cloud-based categorization database.		
		This database should have over 250 million URLs rated into 78 categories and in 70 languages		

		Various actions can be performed when matched to a category: Allow, Block, Monitor (logged), Warning (with message at configurable time interval), (request for) user authentication		
		Customizable replacement page (for warning and blocking)		
		The proposed system shall have pre-configured parental control category-based filter including “G”, ‘PG-13” and “R”		
		The proposed system shall provide ability to use local categories (that override the cloud-based database rating) and remote categories (external URL list) as part of the URL rating function.		
		The proposed system shall have the ability to prevent explicit websites and images from appearing in Google, Yahoo!, Bing and Yandex search results by transparently inserting safe search parameters		
		The proposed system shall allow implementation of usage quota by category and category group:		
		Allow access for a specified length of time or a specific bandwidth		
		Calculated separately for each user		
		Reset on daily basis		
		The proposed system shall have the option to allow override blocked categories:		
		By administrative override where administrators can grant temporary access to sites that are otherwise blocked		
		By allowing specified users/user groups/IP addresses		

		The proposed system shall have the ability to limit users' access to YouTube channels, such as in an education environment where users are only able to access YouTube education videos but no other YouTube videos with the following methods:		
		-working with G Suite user access configurations		
		-Manually define allowed channels on the system		
		The proposed system shall offer proxy avoidance prevention capabilities, including:		
		-Proxy site category blocking (via application Control)		
		-Proxy behaviors blocking (via IPS)		
		The proposed system shall provide advanced web filtering options:		
		-Filter Java Applet, ActiveX, and/or cookie		
		-Block HTTP POST		
		-Log search keywords		
		-Allow websites when a rating error occurs		
		-Rate URLs by domain and IP Address		
		-Block invalid URLs		
		-Restrict Google account usage to specific domains (e.g. only corporate accounts only)		
		-Must have configurable policy options to define the URL exempt list		
2.14	**DNS Filter Features**	The proposed system shall provide the ability to apply DNS category filtering to control user access to web resources with the following features:		
		Using cloud-based rating database		
		Botnet C&C domain blocking: blocks the DNS request for the known botnet C&C domains		
		External dynamic category domain filtering: allows manual-definition of domain category		

		DNS safe search: enforces Google, Bing, and YouTube safe addresses for parental controls		
		Local domain filter: allows administrators to define their own domain list to block or allow		
		External IP block list: allows you to define an IP block list to block resolved IPs that match this list.		
		The proposed system shall have the ability to translate a DNS resolved IP address to another IP address that is specified on a per-policy basis		
2.15	**Application Control Features**	The proposed system shall support traffic detection using HTTP protocol (versions 2.0, 2.1, and 2.0)		
		The proposed system shall be able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 2.2		
		The proposed system shall detect over 4,000 applications in 17 categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/ Audio, VoIP, Web Chat and Industrial		
		The proposed system shall support custom application control signatures		
		The proposed system shall allow administrators to apply various actions against the detected traffic, they include monitor, allow, block, reset and quarantine for a defined period.		
		The proposed system shall provide ability to group applications dynamically for assignment of actions using various filters:		
		-By Predefined categories		
		-By application behavior (e.g. Evasive, excessive-bandwidth)		

		-By application popularity		
		-By protocols (e.g. HTTP, MODBUS)		
		-By risk level		
		-By technology (e.g. browser-based, peer-to-peer)		
		-By Vendor (e.g. Goggle, Microsoft)		
		The proposed system shall allow administrators to set networking services to defined ports. A violation can be set to block. Organizations shall also be able to block applications detected on non-default ports		
		The proposed system shall offer some application signatures with additional defined parameters to match		
		The proposed system shall support SSH traffic inspection and control various related activities, including:		
		X server forwarding (X11)		
		SSH shell		
		SSH execution (exec)		
		SSH port-forwarding		
		SSH Tunnel Forwarding		
		Unknow channel usage		
		Administrator-defined commands		
2.16	**SD-WAN Features**	The proposed system shall support aggregation of up to 255 interfaces to create a virtual WAN link.		
		The proposed system shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include:		
		-Predefined performance SLA profiles such as Office 365, AWS and Gmail		

		-Health check probes using IPv4/IPv6 Ping and HTTP		
		-Selection of multiple destinations (or servers) to probe		
		-Interfaces relating to the performance SLA profile		
		-The proposed system shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic take. These constraints should include:		
		Latency threshold		
		Jitter threshold		
		Packet loss threshold		
		The proposed system shall provide settings to the characteristic of probes, including check interval, link failure and restoration considerations.		
		The proposed system shall provide option to disable the implicated static route when an interface is inactive.		
		The proposed system shall allow organizations to define SD-WAN rules that are used to control how sessions are distributed to SD-WAN interfaces. The definition of these rules shall include:		
		-Source: address and/or user group		
		-Destination: address, applications and/or dynamic IP database		
		-Path control strategies		
		The proposed system shall provide the following path control strategies:		
		-Manual: Interfaces are manually assigned a priority		
		-Best Quality: Interface are assigned a priority based on the quality of the interface. Quality criteria may be latency, jitter, packet loss, available bandwidth (for upstream, downstream, or both) or custom with a cocktail of weighted criteria		

		-Lowest Cost (SLA): Interface is selected based on the lowest cost defined on SD-WAN interfaces that meets selected SLA settings		
		-Maximize Bandwidth (SLA): Traffic is distributed among all available links that satisfies selected SLA profile based on a round-robin load balancing algorithm		
		The proposed system shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces:		
		-Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path		
		-Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces.		
		-Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces.		
		-Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path.		
		-Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface.		
		The proposed system shall support per-packet load-balancing among IPSec tunnels.		

		The proposed system shall support forward error correction (FEC) on VPN overlay networks.		
		The proposed system shall support SD-WAN rules with Border Gateway Protocol (BGP) learned routes as dynamic destinations.		
		The proposed system shall provide Dual VPN tunnel wizard that is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.		
		The proposed system shall support integration with a cloud-based solution to simplify IPsec VPN setup.		
2.17	**Additional Requirements**	The vendor must attain ISO 9001:1900 certification that covers the scope of the Quality Management System which includes the design, development, and manufacturing of network security products and the delivery of associated security services and support		
		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations		
		The proposed solution must be listed in the latest Gartner Leaders MQ for Network Firewalls		
		The device should be from a family of products that attains ICSA Labs Certifications for Antivirus, Corporate Firewall, IPsec, NIPS, SSL-TLS.		
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		

		The proposed system shall support unlimited IP addresses license		
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
		The proposed solution must be from a family of products that achieves Common Criteria FWcPP (V2.0) + IPS (V2.11) and VPN (V2.1) Certification		

Menengai and Paka Firewall Specifications

SN	Component	Specification required including applicable standards	Compliance of specification offered (Fully Comply/Non-Comply)	Description of specifications offered including page no. in Technical literature where specifications is reflected.
3	**MENENGAI & PAKA GATEWAY FIREWALL (Quantity 2)**			
3.1		Must be support at least 2 x 10GE SFP+ slots		
		Must be support at least 8 x 1GE RJ45 interfaces		
		Must be support at least 4 x 1GE SFP slots		
		Must support at least 1 Million Maximum Concurrent Sessions		
		Must support at least 50,000 New Sessions/Second		
		Must support at least 10Gbps of firewall throughput		
		Must support at least 2 Gbps Enterprise/Production IPS Throughput		
		Must support at least 1 Gbps SSL Inspection Throughput Throughput		
		Must support at least 1 Gbps Enterprise/Production Threat Protection Throughput		
		Must support at least 480GB SSD storage		
		Must be support dual power supplies		

		Must be supplied with at least 100 SSL VPN licenses		
		Must have the following licenses included Application Control, IPS, Anti Malware, Web Filtering, DNS Filtering, Mobile Security, IOT Security and Sandbox Cloud		
3.2	**Firewall Features**	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified		
		It Must be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode		
		The proposed system shall support robust GUI configurations of both IPv4 and IPv6 firewall policies on the same table that include:		
		-One-click edit of firewall objects from the policy table panel		
		-Drag and drop policy moving		
		-Right-Click on one/multiple policy(ies) to toggle enabling/disabling and deleting of policies		
		Editing selected policy on GUI or from CLI panel		
		Show matching logs of selected policy		
		The proposed system shall offer a firewall policy table in both views by policy sequence and by interface pairs		
		The proposed system shall allow the administrator to customize the firewall policy table's columns		
		The proposed system shall allow the administrator to view filtered policies by using a search bar		
		The proposed system's firewall policies shall support various types of source objects, including IP address/address range/subnets, users, MAC addresses and dynamic addresses from SaaS and reputation list.		

		The proposed system shall support firewall session helpers and ALGs for FTP, TFTP, RAS, H323, TNS/SQLNET, MMS, SIP, PPTP, RTSP, DNS (UDP), DNS (TCP), PMAP, RSH, DCE/RPC and MGCP		
		The proposed system's firewall policies shall support all protocol types that include TCP, UDP, SCTP, IP, and ICMP		
3.3	**Authentication Features**	The proposed system shall support the following user authentication methods to be applied on a security policy and/or VPN access:		
		Local password authentication		
		Server-based password authentication using LDAP, RADIUS, TACACS+, Windows AD, or POP3 servers		
		Certificate-based authentication for host and endpoints		
		Two-factor authentication for additional security beyond just passwords		
		The proposed system shall support various single sign-on (SSO) techniques so that users to enter their credentials only once, and have those credentials reused when accessing other network resources. These methods include:		
		Agent-based SSO with Windows AD, Citrix, VMware Horizon, Novell eDirectory, and Microsoft Exchange		
		SSO using RADIUS accounting records		
		The proposed system shall support guest access with the following features:		
		Create a guest management administrator which is restricted to guest account provisioning only		
		Guest username and password can be manually specified or auto generated		
		Guest accounts expiry		

		Guest login credential can be delivered via an email, SMS message, or a printout		
		Guest login using captive portal authentication		
		The proposed system shall be able to operate as a service provider (SP) in a SAML setup for both firewall and SSL VPN web portal authentication.		
		The proposed system shall have an in-built token server that provisions and manages hard and mobile tokens		
3.4	**VPN Features**	The system shall support the following IPsec VPN capabilities:		
		Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS		
		Authentication method: Certificate, pre-shared key		
		IPsec Phase 1 mode: Aggressive and main (ID protection) mode		
		Peer acceptance options: Any ID, specific ID, ID in dialup user group		
		Supports IKEv1, IKEv2 (RFC 4306)		
		IKE mode configuration support (as server or client), DHCP over IPsec		
		Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256		
		Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512		
		Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14, 15, 16, 17, 18, 19, 19, 21, 27, 28, 29, 30 and 31		
		XAuth support as client or server mod		
		XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option		
		Configurable IKE encryption key expiry, NAT traversal keepalive frequency		

		Dead peer detection		
		Replay detection		
		Autokey keep-alive for Phase 2 SA		
		The proposed system shall provide IPsec VPN wizards to terminate tunnels to in-house or third-party devices and clients		
		The proposed system shall support SSL VPN portal capabilities that include		
		User portal customization - include color themes, layout, bookmarks, connection tools, and client download location.		
		Single-sign-on bookmarks - reuse previous login or predefined credentials to access resources		
		Personal bookmarks management which allows administrators to view and maintain remote client bookmarks		
		One-time login per user options which prevents concurrent logins using the same username		
		The proposed system shall support SSL VPN realms - multiple custom SSL VPN logins associated with user groups (URL paths, design)		
		The proposed system shall support various SSL VPN modes:		
		Web mode: for thin remote clients equipped with a web browser only and support web application, that includes HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix		
		Tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN clients must support MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems		

		Port Forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server		
3.5	**High Availability Features**	The proposed system shall support high availability with industry standard VRRP with the following characteristics:		
		Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP		
		Be able integrated into a VRRP group with any third-party VRRP devices		
		Supports IPv4 and IPv6 VRRP		
		The proposed system shall support high availability by setting up a cluster with the following characteristics:		
		Supports up to 4 cluster members		
		Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)		
		Cluster units communicate with each other through their heartbeat interfaces		
		Uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit		
		Provides device failover in the event of hardware or software failure		
		Provides link failover when a direct link is not available on one/more monitored interface(s)		

		Provides remote link failover when connectivity with IP addresses of remote network devices, for example, a downstream router is not available		
		In the event of a failover, log messages about the event and can be configured to send log messages to a syslog server. The cluster can also send SNMP traps and alert email messages		
		Supports session failover (also called session pickup) which during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster. during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up-to-date with the traffic currently being processed by the cluster.		
		Supports the option to automatically failback in the event the original unit recovers		
		Supports widely separated cluster units installed in different physical locations		
		The proposed system shall support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, like normal HA.		

		The proposed system shall support full mesh HA configuration where one can connect an HA cluster consisting of two or more cluster members to the network using 803.3ad Aggregate or Redundant interfaces and redundant switches		
		The proposed system shall support out-of-band management for each cluster member where a management interface is reserved with its own configurations and are not synchronized to other cluster units.		
		The proposed system shall support the upgrade of the firmware without interrupting communication through the cluster		
		In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two to 16 units can be integrated into the load balancing configuration by operating as peers that process traffic and perform configuration synchronization; and session synchronization of connectionless sessions, expectation sessions, and NAT sessions and IPsec tunnels.		
3.6	**Networking**	The proposed system shall support the IEEE standard 803.3ad for physical link aggregation		
		The proposed system shall be able to send out Gratuitous Address Resolution Protocol (GARP) announcements if the MAC address of a link aggregated interface changes to a new IP pool address due to a link failure or change in ports		

		Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed system. The interface shall automatically broadcast DHCP requests and then provide IP address, any DNS server addresses, and the default gateway address to clients		
		Administrators shall be able to configure an interface as a DHCP relay		
		Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed system transmits to improve network performance		
		A loopback interface is a logical interface that's always up (no physical link dependency) and the attached subnet is always present in the routing table. Administrators shall be able to configure multiple loopback interfaces on the proposed system		
		Administrators shall be able to configure physical interfaces on the proposed system for one-armed sniffer with the following capabilities:		
		Ability to deploy filters that define a more granular sniff of network traffic. The filter definition shall include hosts, ports, VLANs, and protocol		
		Ability to sniff IPv6 traffic		
		Traffic sent to the sniffer interface shall have the option to be logged and examined against security components such as IPS and application control.		
		Administrators shall be able to obtain information of transceivers plugged into the proposed system via CLI command. The output shall include the vendor name, part number, and serial number. It shall also include details about transceiver operation, such as temperature, voltage, and optical		

		transmission power.		
		Administrators shall be able to combine two or more physical interfaces to provide link redundancy. This feature allows administrators to connect to two or more switches to ensure connectivity if one physical interface, or the equipment on that interface, fails. In a redundant interface, traffic travels only over one interface at a time.		
		Administrators shall be able to configure Secondary IP addresses to an interface		
		Administrators shall be able to group interfaces, both physical and virtual, into zones that simplifies the creation of security policies.		
		The proposed system shall support the creation of native VXLAN interfaces and support for multiple remote IP addresses, which can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast.		
		The proposed system shall support and compromise both physical interfaces and VLANs		
		The proposed system shall support enhanced MAC VLAN which consists of a MAC VLAN with bridge functionality.		
		The proposed system shall support multiple virtual wire pairs that logically bind two physical interfaces so that all traffic from one of the interfaces can exit only through the other interface if allowed by firewall policy.		
		The proposed system shall support wildcard VLANs for a virtual wire pair. Doing this allows all VLAN-tagged traffic to pass through a virtual wire pair if a virtual wire pair firewall policy allows the traffic.		

		The proposed system shall support various enterprise DNS settings, including:		
		Ability to set the number of DNS entries that can be cached		
		Ability to how long entries remain in the cache		
		Ability to define a dedicated IP address for communications with DNS servers		
		The proposed system shall allow organizations to use a dynamic DNS (DDNS) service		
		The proposed system shall provide the ability to run local DNS servers		
		The proposed system shall support static routing with various advanced features:		
		Support for both IPv4 and IPv6 routes		
		Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes.		
		Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database.		
		The proposed system shall support blackhole routing. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator won't discover any information from the target network.		

		The proposed system shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing.		
		The proposed system shall support IPv4 policy routing using the definition of:		
		Protocol type, including SCTP		
		Incoming and outgoing logical interface		
		Source and destination IP addresses/subnets		
		Source and destination firewall address/address group objects		
		Type of Service (ToS)		
		The proposed system shall support IPv6 policy routing		
		The proposed system shall support RIP version 1 (RFC 1058), RIP version 2 (RFC 2453), and the IPv6 version RIPng (RFC 1980) routing protocols		
		The proposed system shall support default information originate option for RIP configuration		
		Administrator shall be able to regulate RIP performance, including specifying update timer, timeout timer, and garbage timer.		
		The proposed system shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols		
		The proposed system shall support BGP4 (IPv4) and BGP4+ (IPv6) routing protocols		
		The proposed system shall support Intermediate System to Intermediate System Protocol (IS-IS) protocol for both IPv4 and IPv6		
		The proposed system shall support the ability to forward multicast traffic in both transparent/bridge and route/NAT mode		

		The proposed system shall be able to operate as a Protocol Independent Multicast (PIM) version 2 router with support for:		
		PIM sparse mode (PIM-SM, RFC 4601)		
		PIM dense mode (PIM-DM, RFC 3973)		
		PIM Source Specific mode (PIM-SSM. RFC 3569)		
		IGMP v1, IGMP v2, IGMP v3 protocols		
		The proposed system shall support the ability to connect 3G/4G modem to its USB port		
3.7	**OS & Management Features**	The proposed OS must:		
		-Be proprietary to prevent inheriting common OS vulnerabilities		
		-Resided on flash disk for reliability over the hard disk		
		-Allow dual booting		
		-Upgradeable via Web UI or TFTP		
		The configurations on the device shall:		
		-Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
		-Provide CLI command configuration file that is readable by Windows Notepad		
		-Have an option to encrypt the backup file		
		-Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision.		
		The proposed system shall minimally provide management access through:		
		-GUI using HTTP or HTTPs access which administration service port can be configured, example via TCP port 8080		

		-CLI console using console port, SSHv2, telnet or from GUI console		
		-The proposed system shall offer the option to automatically redirect HTTP management access to HTTPS		
		-The proposed system shall enforce mandatory default administrator password setup upon the first-time login or after a factory reset.		
		The proposed system shall have the option to implement local administrator password policy enforcement including:		
		-Minimum length		
		Character requirements - Upper case, lower case, numbers and special character		
		-Disallow password reuse		
		-Password expiration		
		The administrator authentication shall be facilitated by a local database, PKI & remote services such as Radius, LDAP and TACACS+		
		The proposed system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
		The proposed system shall be able to limit remote management access:		
		From certain trusted network or host with a corresponding administrator account		
		To certain (virtual) interfaces		
		The proposed system shall be allowed administrators to set administration idle timeout between 1 to 480 minutes		
		The proposed system should be able to facilitate administration audits by logging detailed activities to event log - management access and also		

		configuration changes.		
		The proposed solution shall support various zero-touch provisioning options:		
		Cloud assisted provisioning: When devices at remote locations are plugged in, they automatically obtain an IP address via DHCP. These devices then ‘call home’ to the cloud facility. From there, the device will receive the management related configurations.		
		DHCP server provisioning: Devices will boot up using the appropriate DHCP server which provides DHCP option 240 and 241 that records manager IP and domain name.		
3.8	**System Integration**	The proposed system shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. The solution should offer the following capabilities:		
		A physical topology view that shows all connected devices, including access layer device and a logical topology view that shows information about the interfaces that each device is connected to.		
		Security best practice checks across various security components in the network to identify potential vulnerabilities and suggest improvements to the configurations.		
		The proposed system shall have in-built automation feature that pairs an event trigger with one or more actions to monitor the network and take the designated actions when a threat or situation change is detected. It should have the followings:		

		Triggers: configuration change, system status, HA failover, event log handler, incoming webhook and schedule		
		Actions: CLI Script, Email, iOS app notification, public cloud functions, slack notification and webhook		
		The proposed system shall allow GUI configurations to external services that include:		
		Public cloud providers - AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud		
		SDN platforms and private cloud hypervisors - Kubernates, VMware NSX, VMware ESXi, OpenStack, Cisco ACI, and Nuage VSP		
		Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system and Microsoft Exchange		
		External threat feeds: URL list, IP list, domain name list, and malware file hash		
3.9	**Explicit and Transparent Proxy Features**	The proposed system shall provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic with the following capabilities:		
		-support for the use of multiple ports and port range for proxying		
		-definition of a FQDN, to be entered into browsers		
		-setup of maximum allowed HTTP request and message length		
		-outgoing IP can be selected from an IP pool		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		

		-create URL match list with URL patterns forward to forwarding servers and/or create a list of URLs that are exempt from web caching		
		The proposed system shall be capable of hosting Proxy Auto-Configuration (PAC) file		
		The proposed system shall support proxy chaining when deployed as an explicit web proxy with these additional capabilities:		
		-monitor the remoter servers periodically and bypass any unavailable servers		
		-load balance traffic to servers using a weighted algorithm or sending new sessions to the server that is processing the fewest sessions		
		The proposed system shall support transparent web proxy whereby the user's client software, such as a browser, is unaware that it is communicating with a proxy.		
		The proposed system shall support transparent web proxy forwarding, without having to reconfigure user browsers or publish a proxy auto-reconfiguration (PAC) file. Explicit web proxy setting is also not required as it shall be implemented as a setting of a firewall policy. Once configured, the system transparently forwards traffic generated by a client to the upstream proxy. The upstream proxy then forwards it to the server.		
		The proposed system shall support explicit FTP Proxy with the following capabilities:		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		

		The proposed system shall support SaaS (Office 365, G-suite, Dropbox) access control with web proxying by inserting vendor-defined headers that restrict access to the specific accounts.		
3.10	**Intrusion Prevention Features**	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
		Signature based detection using real time updated database		
		Anomaly based detection that is based on thresholds		
		The proposed system shall support One-arm IDS (sniffer mode) and also operate in both NAT/rout and transparent mode		
		The proposed system's IPS database shall have over 11,000 up-to-date signatures		
		The proposed system shall support custom IPS signatures. In addition, Snort IPS rules can be converted to these signatures using a converter tool		
		The proposed system shall be capable of updating IPS signatures without restarting the systems using the following options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		
		-automatic push update		
		The proposed system shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types, In addition,		
		A signature can be selected by searching for its corresponding CVE-ID (if applicable)		
		The proposed system shall offer one of the following actions when an attack is detected:		
		Allow session		

		Monitor and log session		
		Block session		
		Reset session		
		Quarantine attacker		
3.11	**Advanced Threat Protection**	The proposed system shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs		
		The proposed system shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection using various technologies:		
		Malware signature database		
		Heuristic AV Engine		
		External file analysis with native integration with on-prem system or cloud-based service		
		File checksums query using cloud-based malware database before AV signatures are available		
		File checksums query using external block list/threat feed		
		The proposed system shall be capable of updating AV signatures without restarting the systems using the following options:		
		manual database upload (without system internet access)		
		periodically scheduled pull update		
		automatic push update		
		The proposed system shall also be able to block graywares and mobile malwares		
		The proposed system shall offer the ability to treat Windows Executables in Email Attachments as viruses		
		The antivirus scanning should be supported on various protocols:		
		HTTP/HTTPS		
		SMTP/SMTPS		
		POP3/POP3S		

		IMAP/IMAPS		
		MAPI		
		FTP/SFTP		
		CIFS		
		The proposed system shall able to scan archive files for malwares		
		The proposed system shall support Content Disarm and Reconstruction (CDR) where exploitable content (within PDF and Microsoft Office files) can be removed and replaced with content that is known to be safe		
		The proposed system shall be capable of blocking Botnet server communications with IPS signatures and IP reputation database		
		The proposed system shall maintain a fingerprint-based certificate blacklist is that useful to block botnet communication that relies on SSL		
		The proposed system shall be able to automatically ban infected machines from other network segments		
3.12	**SSL Inspection**	The proposed system shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic		
		The proposed system shall support certificate inspection on port 443, all ports or a specific non-standard port. In addition, the system should:		
		Have option block sessions with invalid certificates		
		Have option allow sessions with untrusted certificates		
		The proposed system shall provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or		

		using a whitelist.		
3.13	**Web Filter Features**	The proposed system shall allow organizations to implement flow-based, proxy-based and DNS-based web filtering concurrently, depending on the network and security needs		
		The proposed system shall support static web filtering by:		
		-manually-defined URLs using regular expression and wildcards		
		-manually-defined content filter using regular expression and wildcards		
		The proposed system shall support dynamic web filtering by querying real-time cloud-based categorization database.		
		This database should have over 250 million URLs rated into 78 categories and in 70 languages		
		Various actions can be performed when matched to a category: Allow, Block, Monitor (logged), Warning (with message at configurable time interval), (request for) user authentication		
		Customizable replacement page (for warning and blocking)		
		The proposed system shall have pre-configured parental control category-based filter including “G”, ‘PG-13” and “R”		
		The proposed system shall provide ability to use local categories (that override the cloud-based database rating) and remote categories (external URL list) as part of the URL rating function.		
		The proposed system shall have the ability to prevent explicit websites and images from appearing in Google, Yahoo!, Bing and Yandex search results by transparently inserting safe search parameters		

		The proposed system shall allow implementation of usage quota by category and category group:		
		Allow access for a specified length of time or a specific bandwidth		
		Calculated separately for each user		
		Reset on daily basis		
		The proposed system shall have the option to allow override blocked categories:		
		By administrative override where administrators can grant temporary access to sites that are otherwise blocked		
		By allowing specified users/user groups/IP addresses		
		The proposed system shall have the ability to limit users' access to YouTube channels, such as in an education environment where users are only able to access YouTube education videos but no other YouTube videos with the following methods:		
		-working with G Suite user access configurations		
		-Manually define allowed channels on the system		
		The proposed system shall offer proxy avoidance prevention capabilities, including:		
		-Proxy site category blocking (via application Control)		
		-Proxy behaviors blocking (via IPS)		
		The proposed system shall provide advanced web filtering options:		
		-Filter Java Applet, ActiveX, and/or cookie		
		-Block HTTP POST		
		-Log search keywords		
		-Allow websites when a rating error occurs		
		-Rate URLs by domain and IP Address		

		-Block invalid URLs		
		-Restrict Google account usage to specific domains (e.g. only corporate accounts only)		
		-Must have configurable policy options to define the URL exempt list		
3.14	**DNS Filter Features**	The proposed system shall provide the ability to apply DNS category filtering to control user access to web resources with the following features:		
		Using cloud-based rating database		
		Botnet C&C domain blocking blocks the DNS request for the known botnet C&C domains		
		External dynamic category domain filtering allows manual-definition of domain category		
		DNS safe search enforces Google, Bing, and YouTube safe addresses for parental controls		
		Local domain filter allows administrators to define their own domain list to block or allow		
		External IP block list allows you to define an IP block list to block resolved IPs that match this list.		
		The proposed system shall have the ability to translate a DNS resolved IP address to another IP address that is specified on a per-policy basis		
3.15	**Application Control Features**	The proposed system shall support traffic detection using HTTP protocol (versions 3.0, 3.1, and 3.0)		
		The proposed system shall be able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 3.2		
		The proposed system shall detect over 4,000 applications in 17 categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/		

		Audio, VoIP, Web Chat and Industrial		
		The proposed system shall support custom application control signatures		
		The proposed system shall allow administrators to apply various actions against the detected traffic, they include monitor, allow, block, reset and quarantine for a defined period of time.		
		The proposed system shall provide ability to group applications dynamically for assignment of actions using various filters:		
		-By Predefined categories		
		-By application behavior (e.g. Evasive, excessive-bandwidth)		
		-By application popularity		
		-By protocols (e.g. HTTP, MODBUS)		
		-By risk level		
		-By technology (e.g. browser-based, peer-to-peer)		
		-By Vendor (e.g. Goggle, Microsoft)		
		The proposed system shall allow administrators to set networking services to defined ports. A violation can be set to block. Organizations shall also be able to block applications detected on non-default ports		
		The proposed system shall offer some application signatures with additional defined parameters to match		
		The proposed system shall support SSH traffic inspection and control various related activities, including:		
		X server forwarding (X11)		
		SSH shell		
		SSH execution (exec)		
		SSH port-forwarding		
		SSH Tunnel Forwarding		
		Unknow channel usage		

		Administrator-defined commands		
3.16	**SD-WAN Features**	The proposed system shall support aggregation of up to 255 interfaces to create a virtual WAN link.		
		The proposed system shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include:		
		-Predefined performance SLA profiles such as Office 365, AWS and Gmail		
		-Health check probes using IPv4/IPv6 Ping and HTTP		
		-Selection of multiple destinations (or servers) to probe		
		-Interfaces relating to the performance SLA profile		
		The proposed system shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic take. These constraints should include:		
		Latency threshold		
		Jitter threshold		
		Packet loss threshold		
		The proposed system shall provide settings to the characteristic of probes, including check interval, link failure and restoration considerations.		
		The proposed system shall provide option to disable the implicated static route when an interface is inactive.		
		The proposed system shall allow organizations to define SD-WAN rules that are used to control how sessions are distributed to SD-WAN interfaces. The definition of these rules shall include:		

		-Source: address and/or user group		
		-Destination: address, applications and/or dynamic IP database		
		-Path control strategies		
		The proposed system shall provide the following path control strategies:		
		-Manual: Interfaces are manually assigned a priority		
		-Best Quality: Interface are assigned a priority based on the quality of the interface. Quality criteria may be latency, jitter, packet loss, available bandwidth (for upstream, downstream, or both) or custom with a cocktail of weighted criteria		
		-Lowest Cost (SLA): Interface is selected based on the lowest cost defined on SD-WAN interfaces that meets selected SLA settings		
		-Maximize Bandwidth (SLA): Traffic is distributed among all available links that satisfies selected SLA profile based on a round-robin load balancing algorithm		
		The proposed system shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces:		
		-Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path		
		-Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces.		

		-Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces.		
		-Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path.		
		-Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface.		
		The proposed system shall support per-packet load-balancing among IPSec tunnels.		
		The proposed system shall support forward error correction (FEC) on VPN overlay networks.		
		The proposed system shall support SD-WAN rules with Border Gateway Protocol (BGP) learned routes as dynamic destinations.		
		The proposed system shall provide Dual VPN tunnel wizard that is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.		
		The proposed system shall support integration with a cloud-based solution to simplify IPsec VPN setup.		
3.17	**Additional Requirements**	The vendor must attain ISO 9001:1900 certification that covers the scope of the Quality Management System which includes the design, development, and manufacturing of network security products and the delivery		

		of associated security services and support		
		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations		
		The proposed solution must be listed in the latest Gartner Leaders MQ for Network Firewalls		
		The device should be from a family of products that attains ICSA Labs Certifications for Antivirus, Corporate Firewall, IPsec, NIPS, SSL-TLS.		
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
		The proposed system shall support unlimited IP addresses license		
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
		The proposed solution must be from a family of products that achieves Common Criteria FWcPP (V3.0) + IPS (V3.11) and VPN (V3.1) Certification		

Kapkerwa/Suswa/Kabarak Firewall Specifications

SN	Component	Specification required including applicable standards	Compliance of specification offered (Fully Comply/Non-Comply)	Description of specifications offered including page no. in Technical literature where specifications is reflected.
4	**KAPKERWA/SUSWA/KABARAK GATEWAY FIREWALL (Quantity 1 each)**			
4.1		Must be support at least 8 x 1GE RJ45 interfaces		
		Must support at least 1 Million Maximum Concurrent Sessions		
		Must support at least 50,000 New Sessions/Second		

		Must support at least 5Gbps of firewall throughput		
		Must support at least 1 Gbps Enterprise/Production IPS Throughput		
		Must support at least 700 Mbps SSL Inspection Throughput Throughput		
		Must support at least 700 Mbps Enterprise/Production Threat Protection Throughput		
		Must support at least 128GB SSD storage		
		Must be supplied with at least 100 SSL VPN licenses		
		Must have the following licenses included Application Control, IPS, Anti Malware, Web Filtering, DNS Filtering, Mobile Security, IOT Security and Sandbox Cloud		
4.2	**Firewall Features**	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified		
		It Must be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode		
		The proposed system shall support robust GUI configurations of both IPv4 and IPv6 firewall policies on the same table that include:		
		-One-click edit of firewall objects from the policy table panel		
		-Drag and drop policy moving		
		-Right-Click on one/multiple policy(ies) to toggle enabling/disabling and deleting of policies		
		Editing selected policy on GUI or from CLI panel		
		Show matching logs of selected policy		
		The proposed system shall offer a firewall policy table in both views by policy sequence and by interface pairs		

		The proposed system shall allow the administrator to customize the firewall policy table's columns		
		The proposed system shall allow the administrator to view filtered policies by using a search bar		
		The proposed system's firewall policies shall support various types of source objects, including IP address/address range/subnets, users, MAC addresses and dynamic addresses from SaaS and reputation list.		
		The proposed system shall support firewall session helpers and ALGs for FTP, TFTP, RAS, H323, TNS/SQLNET, MMS, SIP, PPTP, RTSP, DNS (UDP), DNS (TCP), PMAP, RSH, DCE/RPC and MGCP		
		The proposed system's firewall policies shall support all protocol types that include TCP, UDP, SCTP, IP, and ICMP		
4.3	**Authentication Features**	The proposed system shall support the following user authentication methods to be applied on a security policy and/or VPN access:		
		Local password authentication		
		Server-based password authentication using LDAP, RADIUS, TACACS+, Windows AD, or POP3 servers		
		Certificate-based authentication for host and endpoints		
		Two-factor authentication for additional security beyond just passwords		
		The proposed system shall support various single sign-on (SSO) techniques so that users to enter their credentials only once, and have those credentials reused when accessing other network resources. These methods include:		
		Agent-based SSO with Windows AD, Citrix, VMware Horizon, Novell eDirectory, and Microsoft		

		Exchange		
		SSO using RADIUS accounting records		
		The proposed system shall support guest access with the following features:		
		Create a guest management administrator which is restricted to guest account provisioning only		
		Guest username and password can be manually specified or auto generated		
		Guest accounts expiry		
		Guest login credential can be delivered via an email, SMS message, or a printout		
		Guest login using captive portal authentication		
		The proposed system shall be able to operate as a service provider (SP) in a SAML setup for both firewall and SSL VPN web portal authentication.		
		The proposed system shall have an in-built token server that provisions and manages hard and mobile tokens		
4.4	**VPN Features**	The system shall support the following IPsec VPN capabilities:		
		Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS		
		Authentication method: Certificate, pre-shared key		
		IPsec Phase 1 mode: Aggressive and main (ID protection) mode		
		Peer acceptance options: Any ID, specific ID, ID in dialup user group		
		Supports IKEv1, IKEv2 (RFC 4306)		
		IKE mode configuration support (as server or client), DHCP over IPsec		
		Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256		

		Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512		
		Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14, 15, 16, 17, 18, 19, 19, 21, 27, 28, 29, 30 and 31		
		XAuth support as client or server mod		
		XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option		
		Configurable IKE encryption key expiry, NAT traversal keepalive frequency		
		Dead peer detection		
		Replay detection		
		Autokey keep-alive for Phase 2 SA		
		The proposed system shall provide IPsec VPN wizards to terminate tunnels to in-house or third-party devices and clients		
		The proposed system shall support SSL VPN portal capabilities that include		
		User portal customization - include color themes, layout, bookmarks, connection tools, and client download location.		
		Single-sign-on bookmarks - reuse previous login or predefined credentials to access resources		
		Personal bookmarks management which allows administrators to view and maintain remote client bookmarks		
		One-time login per user options which prevents concurrent logins using the same username		
		The proposed system shall support SSL VPN realms - multiple custom SSL VPN logins associated with user groups (URL paths, design)		
		The proposed system shall support various SSL VPN modes:		

		-Web mode: for thin remote clients equipped with a web browser only and support web application, that includes HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix		
		-Tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN clients must support MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems		
		-Port Forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server		
4.5	**High Availability Features**	The proposed system shall support high availability with industry standard VRRP with the following characteristics:		
		-Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP		
		-Be able integrated into a VRRP group with any third-party VRRP devices		
		-Supports IPv4 and IPv6 VRRP		
		The proposed system shall support high availability by setting up a cluster with the following characteristics:		
		Supports up to 4 cluster members		
		Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)		
		Cluster units communicate with each other through their heartbeat interfaces		

		Uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit		
		Provides device failover in the event of hardware or software failure		
		Provides link failover when a direct link is not available on one/more monitored interface(s)		
		Provides remote link failover when connectivity with IP addresses of remote network devices, for example, a downstream router is not available		
		In the event of a failover, log messages about the event and can be configured to send log messages to a syslog server. The cluster can also send SNMP traps and alert email messages		
		Supports session failover (also called session pickup) which during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster. during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up to date with the traffic currently being processed by the cluster.		
		Supports the option to automatically failback in the event the original unit recovers		
		Supports widely separated cluster units installed in different physical locations		

		The proposed system shall support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, like normal HA.		
		The proposed system shall support full mesh HA configuration where one can connect an HA cluster consisting of two or more cluster members to the network using 804.3ad Aggregate or Redundant interfaces and redundant switches		
		The proposed system shall support out-of-band management for each cluster member where a management interface is reserved with its own configurations and are not synchronized to other cluster units.		
		The proposed system shall support the upgrade of the firmware without interrupting communication through the cluster		
		In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two to 16 units can be integrated into the load balancing configuration by operating as peers that process traffic and perform configuration synchronization; and session synchronization of connectionless sessions, expectation sessions, and NAT sessions and IPsec tunnels.		
4.6	**Networking**	The proposed system shall support the IEEE standard 804.3ad for physical link aggregation		

		The proposed system shall be able to send out Gratuitous Address Resolution Protocol (GARP) announcements if the MAC address of a link aggregated interface changes to a new IP pool address due to a link failure or change in ports		
		Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed system. The interface shall automatically broadcast DHCP requests and then provide IP address, any DNS server addresses, and the default gateway address to clients		
		Administrators shall be able to configure an interface as a DHCP relay		
		Administrators shall be able to adjust the maximum transmission unit (MTU) of the packets that the proposed system transmits to improve network performance		
		A loopback interface is a logical interface that's always up (no physical link dependency) and the attached subnet is always present in the routing table. Administrators shall be able to configure multiple loopback interfaces on the proposed system		
		Administrators shall be able to configure physical interfaces on the proposed system for one-armed sniffer with the following capabilities:		
		Ability to deploy filters that define a more granular sniff of network traffic. The filter definition shall include hosts, ports, VLANs, and protocol		
		Ability to sniff IPv6 traffic		
		Traffic sent to the sniffer interface shall have the option to be logged and examined against security components such as IPS and application control.		

		Administrators shall be able to obtain information of transceivers plugged into the proposed system via CLI command. The output shall include the vendor name, part number, and serial number. It shall also include details about transceiver operation, such as temperature, voltage, and optical transmission power.		
		Administrators shall be able to combine two or more physical interfaces to provide link redundancy. This feature allows administrators to connect to two or more switches to ensure connectivity if one physical interface, or the equipment on that interface, fails. In a redundant interface, traffic travels only over one interface at a time.		
		Administrators shall be able to configure Secondary IP addresses to an interface		
		Administrators shall be able to group interfaces, both physical and virtual, into zones that simplifies the creation of security policies.		
		The proposed system shall support the creation of native VXLAN interfaces and support for multiple remote IP addresses, which can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast.		
		The proposed system shall support and compromise for both physical interfaces and VLANs		
		The proposed system shall support enhanced MAC VLAN which consists of a MAC VLAN with bridge functionality.		
		The proposed system shall support multiple virtual wire pairs that logically bind two physical interfaces so that all traffic from one of the interfaces can exit only through the other interface if allowed by firewall policy.		

		The proposed system shall support wildcard VLANs for a virtual wire pair. Doing this allows all VLAN-tagged traffic to pass through a virtual wire pair if a virtual wire pair firewall policy allows the traffic.		
		The proposed system shall support various enterprise DNS settings, including:		
		Ability to set the number of DNS entries that can be cached		
		Ability to how long entries remain in the cache		
		Ability to define a dedicated IP address for communications with DNS servers		
		The proposed system shall allow organizations to use a dynamic DNS (DDNS) service		
		The proposed system shall provide the ability to run local DNS servers		
		The proposed system shall support static routing with various advanced features:		
		Support for both IPv4 and IPv6 routes		
		Ability to define static routes with administrative distance and priority. Priority, which will artificially weight the route during route selection. The higher the priority number, the less likely the route is to be selected over other routes.		
		Ability to define destinations in static routes using IP subnet, firewall address (including FQDN type) objects, and Internet service objects. Internet service objects are IP lists mapped to popular Internet services and are residing on a dynamically updated database.		

		The proposed system shall support blackhole routing. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator won't discover any information from the target network.		
		The proposed system shall support reverse path lookup (anti-spoofing). This feature can be disabled to enable asymmetric routing.		
		The proposed system shall support IPv4 policy routing using the definition of:		
		Protocol type, including SCTP		
		Incoming and outgoing logical interface		
		Source and destination IP addresses/subnets		
		Source and destination firewall address/address group objects		
		Type of Service (ToS)		
		The proposed system shall support IPv6 policy routing		
		The proposed system shall support RIP version 1 (RFC 1058), RIP version 2 (RFC 2453), and the IPv6 version RIPng (RFC 1980) routing protocols		
		The proposed system shall support default information originate option for RIP configuration		
		Administrator shall be able to regulate RIP performance, including specifying update timer, timeout timer, and garbage timer.		
		The proposed system shall support Open Shortest Path First (OSPF), OSPFv2 and OSPFv3 routing protocols		
		The proposed system shall support BGP4 (IPv4) and BGP4+ (IPv6) routing protocols		

		The proposed system shall support Intermediate System to Intermediate System Protocol (IS-IS) protocol for both IPv4 and IPv6		
		The proposed system shall support the ability to forward multicast traffic in both transparent/bridge and route/NAT mode		
		The proposed system shall be able to operate as a Protocol Independent Multicast (PIM) version 2 router with support for:		
		PIM sparse mode (PIM-SM, RFC 4601)		
		PIM dense mode (PIM-DM, RFC 3973)		
		PIM Source Specific mode (PIM-SSM. RFC 3569)		
		IGMP v1, IGMP v2, IGMP v3 protocols		
		The proposed system shall support the ability to connect 3G/4G modem to its USB port		
4.7	**OS & Management Features**	The proposed OS must:		
		-Be proprietary to prevent inheriting common OS vulnerabilities		
		-Resided on flash disk for reliability over the hard disk		
		-Allow dual booting		
		-Upgradeable via Web UI or TFTP		
		The configurations on the device shall:		
		-Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
		-Provide CLI command configuration file that is readable by Windows Notepad		
		-Have an option to encrypt the backup file		

		-Have revisions listed on GUI for ease of use. The display shall allow revert to selected revision and configuration diff between 2 selected revisions. Administrators shall be able to add comments for each revision.		
		The proposed system shall minimally provide management access through:		
		-GUI using HTTP or HTTPs access which administration service port can be configured, example via TCP port 8080		
		-CLI console using console port, SSHv2, telnet or from GUI console		
		The proposed system shall offer the option to automatically redirect HTTP management access to HTTPS		
		The proposed system shall enforce mandatory default administrator password setup upon the first-time login or after a factory reset.		
		The proposed system shall have the option to implement local administrator password policy enforcement including:		
		-Minimum length		
		-Character requirements - Upper case, lower case, numbers and special character		
		-Disallow password reuse		
		-Password expiration		
		The administrator authentication shall be facilitated by a local database, PKI & remote services such as Radius, LDAP and TACACS+		
		The proposed system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
		The proposed system shall be able to limit remote management		

		access:		
		From certain trusted network or host with a corresponding administrator account		
		To certain (virtual) interfaces		
		The proposed system shall be allowed administrators to set administration idle timeout between 1 to 480 minutes		
		The proposed system should be able to facilitate administration audits by logging detailed activities to event log - management access and also configuration changes.		
		The proposed solution shall support various zero-touch provisioning options:		
		Cloud assisted provisioning: When devices at remote locations are plugged in, they automatically obtain an IP address via DHCP. These devices then 'call home' to the cloud facility. From there, the device will receive the management related configurations.		
		DHCP server provisioning: Devices will boot up using the appropriate DHCP server which provides DHCP option 240 and 241 that records manager IP and domain name.		
4.8	**System Integration**	The proposed system shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. The solution should offer the following capabilities:		
		A physical topology view that shows all connected devices, including access layer device and a logical topology view that shows information about the interfaces that each device is connected to.		

		Security best practice checks across various security components in the network to identify potential vulnerabilities and suggest improvements to the configurations.		
		The proposed system shall have in-built automation feature that pairs an event trigger with one or more actions to monitor the network and take the designated actions when a threat or situation change is detected. It should have the followings:		
		Triggers: configuration change, system status, HA failover, event log handler, incoming webhook and schedule		
		Actions: CLI Script, Email, iOS app notification, public cloud functions, slack notification and webhook		
		The proposed system shall allow GUI configurations to external services that include:		
		Public cloud providers - AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud		
		SDN platforms and private cloud hypervisors - Kubernates, VMware NSX, VMware ESXi, OpenStack, Cisco ACI, and Nuage VSP		
		Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system and Microsoft Exchange		
		External threat feeds: URL list, IP list, domain name list, and malware file hash		
4.9	**Explicit and Transparent Proxy Features**	The proposed system shall provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic with the following capabilities:		
		-support for the use of multiple ports and port range for proxying		

		-definition of a FQDN, to be entered in to browsers		
		-setup of maximum allowed HTTP request and message length		
		-outgoing IP can be selected from an IP pool		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		-create URL match list with URL patterns forward to forwarding servers and/or create a list of URLs that are exempt from web caching		
		The proposed system shall be capable of hosting Proxy Auto-Configuration (PAC) file		
		The proposed system shall support proxy chaining when deployed as an explicit web proxy with these additional capabilities:		
		-monitor the remoter servers periodically and bypass any unavailable servers		
		-load balance traffic to servers using a weighted algorithm or sending new sessions to the server that is processing the fewest sessions		
		The proposed system shall support transparent web proxy whereby the user's client software, such as a browser, is unaware that it is communicating with a proxy.		
		The proposed system shall support transparent web proxy forwarding, without having to reconfigure user browsers or publish a proxy auto-reconfiguration (PAC) file. Explicit web proxy setting is also not required as it shall be implemented as a setting of a firewall policy. Once configured, the system transparently forwards traffic generated by a client to the upstream proxy. The upstream		

		proxy then forwards it to the server.		
		The proposed system shall support explicit FTP Proxy with the following capabilities:		
		-security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		The proposed system shall support SaaS (Office 365, G-suite, Dropbox) access control with web proxying by inserting vendor-defined headers that restrict access to the specific accounts.		
4.10	**Intrusion Prevention Features**	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
		Signature based detection using real time updated database		
		Anomaly based detection that is based on thresholds		
		The proposed system shall support One-arm IDS (sniffer mode) and operate in both NAT/route and transparent mode		
		The proposed system's IPS database shall have over 11,000 up-to-date signatures		
		The proposed system shall support custom IPS signatures. In addition, Snort IPS rules can be converted to these signatures using a converter tool		
		The proposed system shall be capable of updating IPS signatures without restarting the systems using the following options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		
		-automatic push update		

		The proposed system shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types, In addition,		
		A signature can be selected by searching for its corresponding CVE-ID (if applicable)		
		The proposed system shall offer one of the following actions when an attack is detected:		
		Allow session		
		Monitor and log session		
		Block session		
		Reset session		
		Quarantine attacker		
4.11	**Advanced Threat Protection**	The proposed system shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs		
		The proposed system shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection using various technologies:		
		Malware signature database		
		Heuristic AV Engine		
		External file analysis with native integration with on-prem system or cloud-based service		
		File checksums query using cloud-based malware database before AV signatures are available		
		File checksums query using external block list/threat feed		
		The proposed system shall be capable of updating AV signatures without restarting the systems using the following options:		
		-manual database upload (without system internet access)		
		-periodically scheduled pull update		

		-automatic push update		
		The proposed system shall also be able to block graywares and mobile malwares		
		The proposed system shall offer the ability to treat Windows Executables in Email Attachments as viruses		
		The antivirus scanning should be supported on various protocols:		
		HTTP/HTTPS		
		SMTP/SMTPS		
		POP3/POP3S		
		IMAP/IMAPS		
		MAPI		
		FTP/SFTP		
		CIFS		
		The proposed system shall able to scan archive files for malwares		
		The proposed system shall support Content Disarm and Reconstruction (CDR) where exploitable content (within PDF and Microsoft Office files) can be removed and replaced with content that is known to be safe		
		The proposed system shall be capable of blocking Botnet server communications with IPS signatures and IP reputation database		
		The proposed system shall maintain a fingerprint-based certificate blacklist is that useful to block botnet communication that relies on SSL		
		The proposed system shall be able to automatically ban infected machines from other network segments		
4.12	**SSL Inspection**	The proposed system shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic		

		The proposed system shall support certificate inspection on port 443, all ports or a specific non-standard port. In addition, the system should:		
		Have option block sessions with invalid certificates		
		Have option allow sessions with untrusted certificates		
		The proposed system shall provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or using a whitelist.		
4.13	**Web Filter Features**	The proposed system shall allow organizations to implement flow-based, proxy-based and DNS-based web filtering concurrently, depending on the network and security needs		
		The proposed system shall support static web filtering by:		
		-manually-defined URLs using regular expression and wildcards		
		-manually-defined content filter using regular expression and wildcards		
		The proposed system shall support dynamic web filtering by querying real-time cloud-based categorization database.		
		This database should have over 250 million URLs rated into 78 categories and in 70 languages		
		Various actions can be performed when matched to a category: Allow, Block, Monitor (logged), Warning (with message at configurable time interval), (request for) user authentication		
		Customizable replacement page (for warning and blocking)		
		The proposed system shall have pre-configured parental control category-based filter including “G”, ‘PG-13” and “R”		

		The proposed system shall provide ability to use local categories (that override the cloud-based database rating) and remote categories (external URL list) as part of the URL rating function.		
		The proposed system shall have the ability to prevent explicit websites and images from appearing in Google, Yahoo!, Bing and Yandex search results by transparently inserting safe search parameters		
		The proposed system shall allow implementation of usage quota by category and category group:		
		Allow access for a specified length of time or a specific bandwidth		
		Calculated separately for each user		
		Reset on daily basis		
		The proposed system shall have the option to allow override blocked categories:		
		By administrative override where administrators can grant temporary access to sites that are otherwise blocked		
		By allowing specified users/user groups/IP addresses		
		The proposed system shall have the ability to limit users' access to YouTube channels, such as in an education environment where users are only able to access YouTube education videos but no other YouTube videos with the following methods:		
		-working with G Suite user access configurations		
		-Manually define allowed channels on the system		
		The proposed system shall offer proxy avoidance prevention capabilities, including:		

		-Proxy site category blocking (via application Control)		
		-Proxy behaviors blocking (via IPS)		
		The proposed system shall provide advanced web filtering options:		
		-Filter Java Applet, ActiveX, and/or cookie		
		-Block HTTP POST		
		-Log search keywords		
		-Allow websites when a rating error occurs		
		-Rate URLs by domain and IP Address		
		-Block invalid URLs		
		-Restrict Google account usage to specific domains (e.g. only corporate accounts only)		
		-Must have configurable policy options to define the URL exempt list		
4.14	**DNS Filter Features**	The proposed system shall provide the ability to apply DNS category filtering to control user access to web resources with the following features:		
		Using cloud-based rating database		
		Botnet C&C domain blocking: blocks the DNS request for the known botnet C&C domains		
		External dynamic category domain filtering: allows manual-definition of domain category		
		DNS safe search: enforces Google, Bing, and YouTube safe addresses for parental controls		
		Local domain filter: allows administrators to define their own domain list to block or allow		
		External IP block list: allows you to define an IP block list to block resolved IPs that match this list.		
		The proposed system shall has the ability to translate a DNS resolved IP address to another IP address that is specified on a per-policy basis		

		The proposed system shall support traffic detection using HTTP protocol (versions 4.0, 4.1, and 4.0)		
		The proposed system shall be able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 4.2		
		The proposed system shall detect over 4,000 applications in 17 categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/ Audio, VoIP, Web Chat and Industrial		
		The proposed system shall support custom application control signatures		
4.15	**Application Control Features**	The proposed system shall allow administrators to apply various actions against the detected traffic, they include monitor, allow, block, reset and quarantine for a defined period of time.		
		The proposed system shall provide ability to group applications dynamically for assignment of actions using various filters:		
		-By Predefined categories		
		-By application behavior (e.g. Evasive, excessive-bandwidth)		
		-By application popularity		
		-By protocols (e.g. HTTP, MODBUS)		
		-By risk level		
		-By technology (e.g. browser-based, peer-to-peer)		
		-By Vendor (e.g. Goggle, Microsoft)		
		The proposed system shall allow administrators to set networking services to defined ports. A violation can be set to block. Organizations shall also be able to block applications detected on		

		non-default ports		
		The proposed system shall offer some application signatures with additional defined parameters to match		
		The proposed system shall support SSH traffic inspection and control various related activities, including:		
		X server forwarding (X11)		
		SSH shell		
		SSH execution (exec)		
		SSH port-forwarding		
		SSH Tunnel Forwarding		
		Unknow channel usage		
		Administrator-defined commands		
4.16	**SD-WAN Features**	The proposed system shall support aggregation of up to 255 interfaces to create a virtual WAN link.		
		The proposed system shall support performance SLA (also known as health checks) settings which are used to monitor WAN interfaces link quality and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. The settings should include:		
		-Predefined performance SLA profiles such as Office 365, AWS and Gmail		
		-Health check probes using IPv4/IPv6 Ping and HTTP		
		-Selection of multiple destinations (or servers) to probe		
		-Interfaces relating to the performance SLA profile		
		The proposed system shall allow SLA targets to be created. These are a set of constraints that are used in SD-WAN rules to control the paths that traffic take. These constraints should include:		
		Latency threshold		

		Jitter threshold		
		Packet loss threshold		
		The proposed system shall provide settings to the characteristic of probes, including check interval, link failure and restoration considerations.		
		The proposed system shall provide option to disable the implicated static route when an interface is inactive.		
		The proposed system shall allow organizations to define SD-WAN rules that are used to control how sessions are distributed to SD-WAN interfaces. The definition of these rules shall include:		
		-Source: address and/or user group		
		-Destination: address, applications and/or dynamic IP database		
		-Path control strategies		
		The proposed system shall provide the following path control strategies:		
		-Manual: Interfaces are manually assigned a priority		
		-Best Quality: Interface are assigned a priority based on the quality of the interface. Quality criteria may be latency, jitter, packet loss, available bandwidth (for upstream, downstream, or both) or custom with a cocktail of weighted criteria		
		-Lowest Cost (SLA): Interface is selected based on the lowest cost defined on SD-WAN interfaces that meets selected SLA settings		
		-Maximize Bandwidth (SLA): Traffic is distributed among all available links that satisfies selected SLA profile based on a round-robin load balancing algorithm		

		The proposed system shall provide implicit an SD-WAN rule for sessions that do not meet the conditions of defined rules. This implicit rule shall offer the following load balancing algorithms with the ability to assign weight on each member interfaces:		
		-Source IP: The system divides traffic equally between the interfaces. However, sessions that start at the same source IP address use the same path		
		-Sessions: The system distributes the workload based on the number of sessions that are connected through the interfaces.		
		-Spillover: If the amount of traffic bandwidth on an interface exceeds the ingress or egress thresholds that organization set for that interface, the system sends additional traffic through one of the other member interfaces.		
		-Source-Destination IP: Sessions that start at the same source IP address and go to the same destination IP address use the same path.		
		-Volume: The system uses the weight that is assigned to each interface to calculate a percentage of the total bandwidth that's allowed to go through each interface.		
		The proposed system shall support per-packet load-balancing among IPSec tunnels.		
		The proposed system shall support forward error correction (FEC) on VPN overlay networks.		
		The proposed system shall support SD-WAN rules with Border Gateway Protocol (BGP) learned routes as dynamic destinations.		

		The proposed system shall provide Dual VPN tunnel wizard that is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.		
		The proposed system shall support integration with a cloud-based solution to simplify IPsec VPN setup.		
4.17	**Additional Requirements**	The vendor must attain ISO 9001:1900 certification that covers the scope of the Quality Management System which includes the design, development, and manufacturing of network security products and the delivery of associated security services and support		
		The bidder must provide evidence of the latest NSS Labs NGFW, SSL/TLS and DCIPS security and performance test recommendations		
		The proposed solution must be listed in the latest Gartner Leaders MQ for Network Firewalls		
		The device should be from a family of products that attains ICSA Labs Certifications for Antivirus, Corporate Firewall, IPsec, NIPS, SSL-TLS.		
		The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
		The proposed system shall support unlimited IP addresses license		
		The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		

		The proposed solution must be from a family of products that achieves Common Criteria FWcPP (V4.0) + IPS (V4.11) and VPN (V4.1) Certification		

Central Management Appliances Specifications

SN	Component	Specification required including applicable standards	Compliance of specification offered (Fully Comply/Non-Comply)	Description of specifications offered including page no. in Technical literature where specifications is reflected.
5	**Central Management Appliances (Quantity 2)**			
3.1	**Management, NOC & SOC Features**	Must be a virtual appliance supporting VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer 6.0+ and Open Source Xen, KVM on Redhat and Ubuntu, Nutanix AHV, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud)		
		Must support at least 5GB/Day of logging		
		Must support at least 10 Managed devices		
		Must support at least the following SDN connectors:		
		VMWare vCenter		
		Aruba ClearPass		
		Cisco PxGrid		
		Symantec Endpoint Protection		
		VMWare NSX-T		
		Must support an SD-WAN Orchestrator		
		Must support an SD-WAN monitoring interface		
		Must support automated Indicators of Compromise (IOC)		
		Must Support role-based administrator		

		Must support Network Operation Center (NOC) and Security Operation Center (SOC) dashboards		
		Must support the creation of automation playbooks		
		Must support default playbook templates		
		Must have Built in report templates		
		Allow Comprehensive alert builders		
		Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network.		

5.3 Description of services.

To secure its operations against modern-day cyber-attacks, GDC is seeking for an integrated cybersecurity solution that secures against both known and unknown (zero-day) attacks/ exploits.

This tender document specifies the requirements for supply, configuration and management of the following security components:

i. Network Perimeter Security at GDC internet entry points, Head office at Kawi House, Nairobi and Nakuru office at Polo Center.
ii. Centralized Management appliances for Security Gateways
iii. Network security for five (5) remote offices/sites (Menengai, Kapkerwa, Paka, Kabarak and Suswa)
iv. Licensing, support and warranty for three years,

The winning service bidder would plan for and implement a solution that incorporates the above including any other recommendations deemed necessary for full effectiveness of the solution in compliance to Network Security best practices. Due to the nature of this project implementation must be handled by staffs that are certified in the proposed vendor's product. The service provider is also required to ensure the transfer of knowledge to GDC staff in addition to certification training so that they can understand and maintain the solution.

6.4 TECHNICAL EVALUATION CRITERIA

The technical proposal from each bidder must address all the following critical areas,

	The bidders shall meet the mandatory requirements listed under "**APPENDIX TO INSTRUCTIONS TO THE TENDERERS"** to qualify for this stage. The bidder **Must** provide evidence of each of the following requirements listed below.	
Item	**Criteria**	**Maximum Score**
1	**Partnership with proposed Original Equipment Manufacturer (OEM)** Bidder Must be an authorized partner with the proposed OEM. (Bidder must submit OEM accreditation / Authorization Letter) i. Gold/Platinum - 5 marks ii. Silver/Bronze/Premier – 3 marks	5
2	**Firewall Requirements** For all the below critical requirements highlight on the brochure and provide a technical write up how the proposed solution meets the requirements. The firewall solution MUST meet the following: - a) The security gateway MUST use stateful inspection based on granular analysis of communication and application state to track and control the network flow. *(2 Marks)* b) The security gateway MUST be capable of supporting throughput, connection rate, concurrent connections requirements of the customer. *(3 Marks)* *c)* MUST provide security rule hit count statistics to the management application. *(2 Marks)* d) MUST allow security rule to be enforced within time intervals to be configured with an expiry date/time. *(2 marks)* e) The communication between the management servers and the security gateways MUST be encrypted and authenticated with PKI certificates. *(2 marks)* f) The firewall MUST support user, client and session authentication methods. *(1 mark)*	25

	g) The following user authentication schemes MUST be supported by the security gateway and VPN module: tokens (i.e. SecurID), TACAS, RADIUS and digital certificates. *(2 Marks)* h) Solution MUST include a local user database to allow user authentication without the need for an external device. *(1 Mark)* i) Integrated sandboxing MUST support CPU-level and OS-level emulation of files for zero-day malware. *(attach evidence*) *(5 Marks)* j) Integrated File scrubbing should be able to reconstruct files with known safe elements. *(attach evidence*) *(5 Marks)*	
3	**Industry Rating** For all the below requirements highlight on the brochure and attach the relevant verified reports from Gartner and NSS labs. Intrusion prevention system (IPS). The solution should meet the following IPS capabilities. i. Vendor MUST provide evidence of year over year leadership position of Intrusion Prevention Solutions (IPS) and / or Enterprise Network Firewall (ENF) Gartner Magic Quadrant. For the last five (5) years (2015 to 2019) years. *(1 mark per year)* *ii.* Vendor MUST provide evidence of leadership approval of the proposed firewall by NSS labs for the last five (5) years (2015 -2019) *(1 Mark per year)* iii. IPS MUST be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection. *(2 Marks)* iv. IPS and firewall module should be integrated on one platform. *(3 Marks)* *v.* IPS application should have a centralized event correlation and reporting mechanism. *(1 Mark)* *vi.* Vendor MUST supply evidence of leadership in protecting Microsoft vulnerabilities. *(2 Marks)* vii. IPS and /or Application Control MUST include the ability to detect and block peer to peer traffic using evasion techniques. *(2 Marks)*	20
4	**Proof of Established Organization**	10

	Bidder should; Be an established IT organization in Kenya with at least five (5) years of experience. i. Provide a list of at least five (5) major clientele/customers in which the bidder has undertaken similar services/assignments in the last five (5) years, detailing the nature of the assignment, the value of the contract, contact person including contact addresses. – 2.5 Marks *0.5 Marks for each Clientele/Customer provided* *ii.* For the above list, provide copies of LPOs and/or Contracts where similar assignments have been undertaken in the last five (5) years – 2.5 Marks. 0.5 *Marks for each LPO/Contract* iii. Provide signed and stamped recommendation letters from the above listed major clientele/customers in which the bidder has undertaken similar services/assignments in the last five (5) years – 5 Marks (*1 Mark for each signed and stamped recommendation letter)*	
5	**Adequacy of the proposed Work Plan & Methodology in responding to the requirements.** The bidder shall provide his proposed maintenance work plans and methodology to reflect the following: a) **Timelines.** Clearly indicate the timelines for deploying the proposed solution with specific dates within six (6) weeks. *(4 Marks)* b) **Escalation Matrix.** Clearly give the contact persons GDC should reach out to during the project implementation and support for one year after commissioning. *(4 Marks)* c) Provide Evidence of **Support Center** including evidence of service desk management system and ticketing solution by the vendor in the event of downtime *(4 Marks)* d) Attach a sample SLA offered by the firm during system deployment for a period of 1 year, other than the online support from the manufacturer. *(4 Marks)* *e)* Completeness and accuracy of the proposal *(Attach a*	**2**0mks

	technical write up indicating how the proposed solution meets or exceeds GDC set out requirements clearly defining the devices to be supplied, licensed modules, perpetual licenses and renewable licenses. Indicate any deviation from the provided GDC specifications - 4 Marks	
6	**Proof of Resource Qualifications** Bidder should have the following resources for the proposed OEM:- *i)* One (1) Expert/Architect and two (2) professional level Engineers trained/certified on the proposed OEM Solution *(3 Marks for each certified engineer)* ii) A Project Manager certified in Project Management with a minimum of 3 years' experience in handling IT projects *(3 Marks)* iii) A Security expert with a certification in Network Security/Information Security/ Cyber Security. *(4 Marks)* iv) Network engineers/administrator: He/She should hold an Industry Standard Certification in CISCO & Avaya products *(4 Marks)* ***NOTE: Please attach the relevant evidence for the achievement of the above qualifications.***	20
	Total Marks	**100**

NB: *The minimal qualifying technical score will be 75 points. Only bidders that meet the minimum score will have their financial proposals evaluated.*

Evaluation criteria points should be clearly outlined in the bid response/ clearly referenced in the evaluation criteria pages.

SECTION: VII PRICE SCHEDULE FOR SUPPLY AND INSTALLTION OF PERIMETER NETWORK FIREWALL

The bidders are required to provide their price breakdown as per schedules below;

Price Schedule for Year One (1)						
SNO	**Component**	**Quantity**	**Implementation period**	**Unit Price in Kshs**	**16% VAT**	**Total Prices in Kshs**
1.	Nairobi Kawi Gateway Firewall	1	Year 1			
2.	Nakuru Gateway Firewall	1	Year 1			
3.	Menengai and Paka Gateway Firewall	2	Year 1			
4.	Kapkerwa Gateway Firewall	1	Year 1			
5.	Central Management Appliances	2	Year 1			
6.	Training for 8 Engineers with Certification Vouchers	8 Pax	Year 1			
7.	Installation and Commissioning charges for year One (1)	1 LOT	Year 1			
8.	Bidder Maintenance Support for year one (1)	Annual	Year 1			
Total Cost in Kshs inclusive of 16% VAT for year One (1) transferred to summary price schedule						

NOTE:

1. **Prices quoted MUST be inclusive of ALL TAXES where applicable.**

Tenderer's Name (Company) _____

Signature & Rubber stamp: _____

Date: _____

Delivery Period: _____

Price Schedule for Year Two (2)						
SNO	**Component**	**Quantity**	**Implementation period**	**Unit Price in Kshs**	**16% VAT**	**Total Prices in Kshs**
1.	Suswa Gateway Firewall	1	Year 2			
2.	Kabarak Gateway Firewall	1	Year 2			
3.	Installation and Commissioning charges for year two (2)	1(Lot)	Year 2			
4.	Bidder Maintenance Support for year two (2)	Annual	Year 2			
Total Cost in Kshs inclusive of 16% VAT for year two (2) transferred to summary price schedule						

NOTE:

1. **Hardware specifications for Suswa and Kabarak offices in Year 2 are similar to hardware specifications for Kapkerwa Gateway Firewall.**
2. **Prices quoted MUST be inclusive of ALL TAXES where applicable.**

Tenderer's Name (Company) _____

Signature & Rubber stamp: _____

Date: _____

Delivery Period: _____

SUMMARY PRICE SCHEDULE

No	**Particulars**	**Total Cost in Kshs**
1.	Total Cost in Kshs inclusive of 16% VAT for year one (1)	
2.	Total Cost in Kshs inclusive of 16% VAT for year two (2)	
Grand Total Cost in Kshs inclusive of 16% VAT for year one (1) and two (2) transferred to FORM OF TENDER.		

Notes on standard forms

1. The tenderer shall complete and submit with its tender the form of tender and price schedules pursuant to instructions to tenderers clause 9 and in accordance with the requirements included in the special conditions of contract.

2. When requested by the appendix to the instructions to tenderers, the tenderer should provide the tender security, either in the form included herein or in another form acceptable to the procuring entity pursuant to instructions to tenderers clause 12.3

3. The contract form, the price schedules and the schedule of requirements shall be deemed to form part of the contract and should be modified accordingly at the time of contract award to incorporate corrections or modifications agreed by the tenderer and the procuring entity in accordance with the instructions to tenderers or general conditions of contract.

4. The performance security and bank guarantee for advance payment forms should not be completed by the tenderers at the time of tender preparation. Only the successful tenderer will be required to provide performance/entity and bank guarantee for advance payment forms in accordance with the forms indicated herein or in another form acceptable to the procuring entity and pursuant to the – conditions of contract.

5. The principal’s or manufacturer’s authorization form should be completed by the principal or the manufacturer, as appropriate in accordance with the tender documents.

8.1 **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 of which is hereby duly acknowledged, we, the undersigned, offer to provide. *[description of services]* in conformity with the said tender documents for the sum of. [*total tender amount in words and figures]* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Tender.

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 tender guarantee in a sum equivalent to _____ 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.

Dated this _____ day of_____ 20
[signature] [In the capacity of]
Duly authorized to sign tender for and on behalf of_____

8.2 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 materials and spares. Viz…….. [brief description of materials and spares] and has accepted a tender by the tenderer for the supply of those materials and spares in the spares in the sum of …… [contract price in words and figures]

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 materials and spares 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 materials and spares 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_____.

8.3 **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.....
Branch.....

	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……..

8.4 TENDER SECURITY FORM

Whereas ……...[name of the tenderer]

(hereinafter called "the tenderer") has submitted its tender dated……...[date of submission of tender] for the provision of ……..

[name and/or description of the services]

(hereinafter called "the Tenderer") ……...

KNOW ALL PEOPLE by these presents that WE……

Of……having registered office at

[name of procuring entity] (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]

(Amend accordingly if provided by Insurance Company)

8.5 **PERFORMANCE SECURITY FORM**

To: …….

[name of the 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 services] (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]

(Amend accordingly if provided by Insurance Company)

8.6 MANUFACTURER'S AUTHORIZATION FORM

To [*name of the Procuring entity]* ……..

WHEREAS …… [*name of the manufacturer]* who are established and reputable manufacturers of …….. [*name and/or description of the goods]* having factories at …… [*address of factory]* do hereby authorize …… [*name and address of Agent]* to submit a tender, and subsequently negotiate and sign the Contract with you against tender No. ……. [*reference of the Tender]* for the above goods manufactured by us.

We hereby extend our full guarantee and warranty as per the General Conditions of Contract for the goods offered for supply by the above firm against this Invitation for Tenders.

_____

[*signature for and on behalf of manufacturer]*

Note: This letter of authority should be on the letterhead of the Manufacturer and should be signed by a person competent.

8.7 DECLARATION OF UNDERTAKING

We underscore the importance of a free, fair and competitive procurement process that precludes abusive practices. In this respect we have neither offered nor granted directly or indirectly any inadmissible advantages to any public servant or other person nor accepted such advantages in connection with our bid, nor will we offer or grant or accept any such incentives or conditions in the present procurement process or, in the event that we are awarded the contract, in the subsequent execution of the contract. We also declare that no conflict of interest exists in the meaning of the kind described in the Public Procurement & Disposal Act 2015

We also underscore the importance of adhering to the law in the implementation of the project.

We will inform our staff about their respective obligations and about their obligation to fulfil this declaration of undertaking and to obey the laws of the country. We also declare that our company/sub-contractors/ all members of the consortium has/have not been debarred to engage in procurement/ included in the list of sanctions.

We acknowledge that, the client is entitled to terminate the contract immediately if the statements made in the Declaration of Undertaking were objectively false or the reason for exclusion occurs after the Declaration of Undertaking has been issued.

Dated this _____ day of _____ 20 _____

(Name of company)
(Signature(s)