Standard Bidding Document

Purchase of Licensed Enterprise Next-Generation Firewall (NGFW) with XDR
(Goods)

National

Single Stage-Two Envelope

November 13, 2026

National Highways & Motorway Police (National Highways & Motorway Police (NHMP)),Assistant Director (Logistics)
Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory
Phone: +92-303-506-7925, Email: logbranch@gmail.com

Table of Contents

REQUEST FOR BIDS 1

Instructions to Bidders 3

Bid Data Sheet 24

Bids Data Sheet (BDS) 25

Eligibility Criteria 30

Evaluation Criteria 32

Items/Lots 33

Related Services of Goods: 34

Items/Lot Specification 35

Price Schedule 58

General Conditions of Contract 60

Special Conditions of Contract 71

Bid Securing Declaration 77

Contract Form 79

Integrity Pact 82

Performance Guarantee Form 84

Annexure 87

Request for Proposal 88

Financial Annexure 91

Procurement Forms 92

Additional Forms and Documents 95

REQUEST FOR BIDS

PROCUREMENT OF GOODS

1. The **National Highways & Motorway Police (National Highways & Motorway Police (NHMP))** has reserved Funds for the procurement planned for FY **2026-27**. The **National Highways & Motorway Police (National Highways & Motorway Police (NHMP))** intends to apply part of the proceeds of this Fund to cover eligible payments under the contract for the " **Purchase of Licensed Enterprise Next-Generation Firewall (NGFW) with XDR**" with the reference of **"P114196"**

2. The **National Highways & Motorway Police (National Highways & Motorway Police (NHMP))** invites sealed Bids from eligible Bidders for procurement of goods described in the bidding documents on **EPADS v2.0**.

3. **Single Stage-Two Envelope** will be used by adopting **Least Cost Based Selection (LCBS)** Technique for the subject procurement, in line with the Public Procurement Rules, 2026 and any Regulations, Regulatory Guides, Procurement Guidelines or Instructions issued by the Authority from time to time.

4. All Bids must be accompanied by a Bid Security amount described in Bid Security Section in Bidding Document in the form of **Pay Order, Banker's Cheque, Call at Deposit, Bank Guarantee, Demand Draft** or all bids must be accompanied by bid securing declaration in the format specified in the Bidding documents

5. E-Bidding documents, containing detailed terms & conditions, specifications and requirements etc. are available on **e-Pak Acquisition and Disposal System (EPADS)** at **https://epads.gov.pk/opportunities/federal/procurements/114196** for all the interested bidders registered on **EPADS v2.0**. Bidders are required to get themselves registered on **EPADS v2.0** to participate in Bidding process.

6. The e-bids, prepared in accordance with the instructions in the e-Bidding Documents, must be submitted through **EPADS v2.0** on or before **Tuesday, December 1, 2026 11:00 AM**. E-bids will be opened using **EPADS v2.0** on

the same day at **Tuesday, December 1, 2026 11:30 AM**. Manual submission of Bids shall not be entertained. Those vendors who have not yet registered on the new version of **EPADS v2.0,** may register themselves on **https://vendors.epads.gov.pk/**. A tutorial to explain the registration process is available at **https://www.youtube.com/watch?v=MNW6T38v7tc**

In terms of Rule 65 of Public Procurement Rules, 2026 Grievance Redressal Committee (GRC) is notified for the subject procurement and notification copy is available on the procuring agency's website and on Authority's website at (**www.ppra.gov.pk**).

National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics)
Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory
+92-303-506-7925
logbranch@gmail.com

Instructions to Bidders

A. Introduction

1.Scope of Bids

1.1 The Procuring Agency (PA), as indicated in the **Bids Data Sheet (BDS)** invites Bids **through EPADS v2.0** for the provision of Goods as specified in the BDS and **in Section V – Evaluation Criteria, Specifications & Schedule of Requirements**. The name, identification, and number of items/deliverables are provided in the **BDS**. The successful Bidders will be expected to provide the goods within the specified period and timeline(s) as stated in the **BDS**.

2. Source of Funds

2.1 Source of funds is referred in Clause-2 I of Invitation for Bids.

3. Eligible Bidders

3.1 A Bidder may be natural person, company or firm or public or semi-public agency of Pakistan or any foreign country**,** or any combination of them with a formal existing agreement (on Judicial Papers) in the form of a joint venture, consortium, or association. In the case of a joint venture, consortium, or association, all members shall be jointly and severally liable for the execution of the Contract in accordance with the terms and conditions of the Contract. The joint venture, consortium, or association shall nominate a Lead Member as nominated in the BDS, who shall have the authority to conduct all business for and on behalf of any and all the members of the joint venture, consortium, or association during the Bidding process, and in case of award of contract, during the execution of the contract.

Verifiable copy of the agreement that forms a joint venture, consortium or association shall be required to be submitted as part of the Bid.

The appointment of Lead Member in the joint venture, consortium, or association shall be confirmed by submission of a valid Power of Attorney to the Procuring Agency.

Any bid submitted by the joint venture, consortium or association shall indicate the part of proposed contract to be performed by each party and each party shall be evaluated (or post qualified if required) with respect to its contribution only, and the responsibilities of each party shall not be substantially altered without prior written approval of the Procuring Agency and in line with any

instructions issued by the Authority.

(The limit on the number of members of JV or Consortium or Association may be prescribed in BDS, in accordance with the guidelines issued by the PPRA).

3.2 The invitation for Bids is open to all prospective suppliers, manufacturers, or authorized agents / dealers subject to any provisions of incorporation or licensing by the respective national incorporating agency or statutory body established for that particular trade or business. Procuring agencies shall specify the registration/licensing requirements for the foreign bidders keeping in view the requirement of that business.

3.3 A Bidder shall not have a conflict of interest. All Bidders found to have a conflict of interest shall be disqualified. A Bidder may be considered to have a conflict of interest with one or more parties in this Bidding process, if they:

1. are 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 Agency to provide consulting services for the preparation of the design, specifications and other documents to be used for the procurement of the Goods to be purchased under this Invitation for Bids.

2. have controlling shareholders in common; or

3. receive or have received any direct or indirect subsidy from any of them; or

4. have the same legal representative for purposes of this Bid; or

5. have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Bids of another Bidder, or influence the decisions of the Procuring Agency regarding this Bidding process; or

6. Submit more than one Bid in this Bidding process.

3.4 A Bidder may be ineligible if –

1. he is declared bankrupt or, in the case of company or firm, insolvent;

2. payments in favor of the Bidder is suspended in accordance with the judgment of a court of law other than a judgment declaring bankruptcy and resulting (in accordance with the national laws) in the total or partial loss of the right to administer and dispose of its property;

3. the Bidder is convicted, by a final judgment, of any offence involving professional conduct;

4. the Bidder is blacklisted locally or by international organizations and hence debarred due to involvement in corrupt and fraudulent practices, or submission of false or misleading information or performance failure or involved in disrupting procurement process or due to breach of bid Securing Declaration.

3.5 As and when required, bidders shall provide to the Procuring Agency evidence of their eligibility, proof of compliance with the necessary legal requirements to carry out the contract effectively.

3.6 Bidders shall submit Bids relating to the nature, conditions and modalities of sub-contracting wherever the sub-contracting of any elements of the contract amounting to more than ten (10) percent of the Bid price is envisaged.

4. Eligible Goods and Related Services

4.1 All goods and related services to be supplied under the contract shall have their origin in eligible source countries, and all expenditures made under the contract will be limited to such goods and services. For purpose of this Bid, ineligible countries are the countries declared ineligible by the Federal Government.

5. One Bid per Bidder

5.1 A bidder shall submit only one Bid, in the same bidding process, either individually as a Bidder or as a member in a joint venture or any similar arrangement.

5.2 **The Bidder shall not engage a subcontractor for any portion of the contract if the value of such subcontracting exceeds thirty percent (30%) of the total contract amount.**

6. Cost of Bidding

6.1 Any cost incurred by the bidder relating to the preparation and submission of its Bid shall be borne by the bidder, and the Procuring Agency shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

B. Bidding Documents

7. Contents of Bidding Document

7.1 The Goods required, Bidding procedures, and terms and conditions of the contract are prescribed in the Bidding Documents. In addition to the Invitation for Bids, the Bidding documents which should be read in conjunction with any addenda issued in accordance with **ITB 10.1** include:

Section I -Invitation to Bids

Section II Instructions to Bidders (ITB)

Section III Bid Data Sheet (BDS)

Section IV Evaluation Criteria, Specifications, Schedule of Requirements

Section V Bid Forms

Section VI General Conditions of Contract (GCC)

Section VII Special Conditions of Contract (SCC)

Section VIII Contract Forms

Section IX Integrity Pact

Section X Declaration of Beneficial Ownership Information.

7.2 The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding documents. Failure to furnish all the information required in the Bidding documents through EPADS v2.0 will be at the Bidder’s risk and may result in the rejection of its Bids.

8. Clarification of Bidding documents

8.1 A prospective Bidder requiring any clarification of the Bidding documents may notify the Procuring Agency through EPADS v2.0**.**

8.2 The Procuring Agency will within two (02) working days after receiving the request for clarification, respond to any request for clarification through EPADS v2.0 provided that such request is received not later than three (03) days, prior to the deadline for the submission of Bids as prescribed in **ITB 22**

8.3 The Procuring Agency's response will be forwarded to all identified Prospective Bidders through EPADS v2.0, including a description of the inquiry,

but without identifying its source.

8.4 Should the Procuring Agency deem it necessary to amend the Bidding document as a result of a clarification, it shall do so following the procedure under **ITB 9.**

8.5 If indicated **in the BDS**, the Bidder's designated representative is invited at the Bidder's cost to attend a pre-Bid meeting at the place, date and time mentioned **in the BDS**. During this pre-Bid meeting, prospective Bidders may request clarification of the schedule of requirement, the Evaluation Criteria or any other aspects of the Bidding document.

8.6 Minutes of the pre-Bid meeting, if applicable, including the text of the questions asked by Bidders, including those during the meeting (without identifying the source) and the responses given, together with any responses prepared after the meeting will be uploaded on EPADS v2.0. Any modification to the Bidding documents that may become necessary as a result of the pre-Bid meeting shall be made by the Procuring Agency exclusively through the use of an Addendum pursuant to ITB 9. Non-attendance at the pre-Bid meeting will not be a cause for disqualification of a Bidder.

9. Amendment of Bidding documents

9.1 Before the deadline for submission of Bids, the Procuring Agency for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder or Pre-Bid meeting may modify the Bidding documents by issuing addenda through EPADS v2.0.

9.2 The Procuring Agency shall promptly publish the addendum through EPADS v2.0.

Any addendum issued including the notice of any extension of the deadline shall also be communicated through EPADS v2.0 to all the bidders who have already submitted their bids. Such bidders shall have the right to withdraw their already submitted bid and re-submit the revised bid prior to the original or extended bid submission deadline.

9.3 To give prospective Bidders reasonable time in which to take an addendum/corrigendum into account in preparing their Bids, the Procuring Agency may, at its discretion, extend the deadline for the submission of Bids through EPADS v2.0:

Provided that the Procuring Agency shall extend the deadline for submission of Bids, if such an addendum is issued within last three (03) days of the Bids submission deadline.

C. Preparation of Bids

10. Language of Bid

10.1 The Bid prepared by the bidder, as well as all correspondence and documents relating to the Bids exchanged by the Bidder and the Procuring Agency shall be written in the English language unless otherwise specified in the BDS**.** Supporting documents and printed literature furnished by the Bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in the English language unless otherwise specified in the **BDS**, in which case, for purposes of interpretation of the Bidder, the translation shall govern.

11. Documents and samples Constituting the Bid

11.1 The Bid prepared by the Bidder shall constitute the documents required in the **BDS**.

Details of sample(s) where applicable and requested in the BDS.

Documentary evidence established in accordance with ITB 13 that the Bidder is eligible and/or qualified for the subject bidding process;

Documentary evidence established in accordance with **ITB 03** that the Bidder has been authorized by the manufacturer to deliver the goods into Pakistan, where required and where the supplier is not the manufacturer of those goods;

Documentary evidence established in accordance with ITB 12 that the goods and related services to be supplied by the Bidder are eligible goods and services, and conform to the Bidding Documents;

Bid security or Bid Securing Declaration furnished in accordance with **ITB ---.**

12. Documents Establishing Eligibility of the Goods and Conformity to Bidding documents

12.1 To establish the conformity of the bidder to the Bidding document, the Bidder shall furnish as part of its Bids the documentary evidence that Goods

provided conform to the technical specifications and standards.

13. Documents Establishing Eligibility and Qualification of the Bidder

13.1 Pursuant to **ITB 10,** the Bidder shall furnish, as part of its Bid, all those documents establishing the Bidder's eligibility to participate in the Bidding process and/or its qualification to perform the contract if its Bid is accepted.

14. Form of Bid

14.1 The Bidder shall fill the Form of Bid furnished in the Bidding document. The Bid Form must be completed without any alterations to its format and no substitute shall be accepted.

15. Bid Prices

15.1 The Bid Prices quoted by the Bidder in the Form of Bid and in the Price Schedules shall conform to the requirements specified below or exclusively mentioned hereafter in the Bidding documents.

15.2 **All items in the Schedule of Requirement must be listed and priced separately in the Price Schedule(s). If a Price Schedule shows items listed but not priced and neither explicitly denied, their prices shall be construed to be included in the prices of other items.**

15.3 In the event that any item(s) in the Price Schedule are not quoted, and such omission is determined by the Procuring Agency not to materially affect the responsiveness of the Bid, the Procuring Agency may, for the sole purpose of bid evaluation and comparison, assign a price to the unquoted item(s) in accordance with the following methodology:

(a) The assigned price shall be the average of the prices quoted for the same item(s) by all substantially responsive bidders; or

(b) In cases where no comparable quotations are available, the Procuring Agency shall apply the corresponding item price from its duly approved cost estimate for evaluation purposes.

The prices so assigned shall be utilized exclusively for bid evaluation and comparison, and shall not, under any circumstances, be incorporated into or form part of the Contract Price.

15.4 The Bid price to be quoted in the Form of Bid in accordance with **ITB 13.1** shall be the total price of the Bid.

15.5 The Bidder shall indicate on the appropriate Price Schedule, the unit prices (where applicable) and total Bid price of the Goods it proposes to provide under the contract.

15.6 Prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and not subject to variation on any account. A Bid submitted with an adjustable price will be treated as non-responsive and shall be rejected.

16. Bids Currencies

16.1 Prices shall be quoted in Pakistani Rupees unless otherwise specified in the BDS in accordance with Rule 42 (2) of the Public Procurement Rules, 2026.

17. Bids Validity Period

17.1 Such extensions may be more than one time but the total period of such extension shall not exceed the original bid validity period.

17.2 Bids shall remain valid for the period specified in the **BDS** after the Bid submission deadline prescribed by the Procuring Agency. A Bid valid for a shorter period shall be rejected by the Procuring Agency as non-responsive**.** The period of Bid validity will be determined from the complementary Bid securing instrument, i.e. the expiry period of Bid Security or Bids Securing Declaration as the case may be.

The procuring agency shall ordinarily be under an obligation to process and evaluate the bid and to issue letter of award within the stipulated bid validity period.

17.3 Under exceptional circumstances, prior to the expiration of the initial Bid validity period, the Procuring Agency may request the Bidders' consent to an extension of the period of validity of their Bids through EPADS v2.0,. The Bid Security provided under **ITB 17** shall also be suitably extended. A Bidder may refuse the request without forfeiting its Bid security or causing to be executed its Bid Securing Declaration. A Bidder agreeing to the request will not be required nor permitted to modify its Bid, but will be required to extend the validity of its Bid Security or Bid Securing Declaration for the period of the extension.

18. Bid Security or Bid Securing Declaration

18.1 The Bidder shall furnish as part of its Bid, a Bid Security in accordance with Rule 36 of the Public Procurement Rules, 2026.

18.2 The original Bid Security shall be enclosed within the sealed envelope and to be submitted physically before closing time for submission of bids. Whereas, scanned copy of bid security shall be uploaded electronically through EPADS v2.0 before closing hours for submission of bids.

18.3 The Bidder who failed to submit the original Bids security before the submission deadline shall be disqualified straightaway.

18.4 The Bid Security or Bid Securing Declaration is required to protect the Procuring Agency against the risk of Bidder’s conduct which would warrant the security’s forfeiture, pursuant to **ITB 18.7.**

18.5 The Bid Security shall be denominated in the local currency or in another freely convertible currency, and it shall be in the form specified in the BDS which shall be in any of the following:

a) a bank guarantee, a bank draft, an irrevocable letter of credit issued by a Scheduled bank in the form provided in the Bidding Documents or another form acceptable to the Procuring Agency;

b) a cashier’s or certified cheque; or

c) another security if indicated in the BDS.

The Bid Security shall be valid for twenty-eight (28) days beyond the end of the validity of the Bid. This shall also apply if the period for Bid Validity is extended. In either case, the form must include the complete name of the Bidder.

18.6 The Bid Security shall be payable promptly upon written demand by the Procuring Agency in case any of the conditions listed in **ITB 18.7** are invoked.

18.7 Unsuccessful Bidders' Bid Security will be discharged or returned as promptly as possible, however in no case later than thirty (30) days after the expiration of the period of Bid Validity prescribed by the procuring agency pursuant to **ITB 17.** The Procuring Agency shall make no claim to the amount of the Bid Security, and shall promptly return the Bid Security documents, after whichever of the following that occurs earliest:

a. the expiry of the Bid Security;

b. the entry into force of a procurement contract and the provision of a Performance Guarantee, for the performance of the contract if such a guarantee, is required by the Bid documents;

c. the rejection by the Procuring Agency of all Bids;

d. cancellation of procurement proceedings.

e. the withdrawal of the Bid prior to the deadline for the submission of Bids, unless the Bid document stipulates that no such withdrawal is permitted.

18.8 The successful Bidder's Bid Security will be discharged upon the Bidder signing the contract**,** or furnishing the Performance Guarantee.

18.9 The Bid Security may be forfeited or the Bid Securing Declaration executed:

a. if a Bidder:

b. withdraws its Bid during the period of Bid Validity as specified by the Procuring Agency, and referred by the Bidder on the Form of Bids except as provided for in **ITB 16.2**; or

c. does not accept the correction of errors**;** or

d. in the case of a successful Bidder, if the Bidder fails:

e. to sign the contract; or

f. to furnish Performance Guarantee**.**

19. Withdrawal, Substitution, and Modification of Bid

19.1 Before Bid submission deadline, any Bidder may withdraw, substitute, or modify its Bid after it has been submitted through EPADS v2.0.

20. Format and Signing of Bid

20.1 The Bidder shall prepare and submit Bids with due diligence after carefully reading all the terms and condition before bid submission deadline through EPADS v2.0.

D. Submission of Bids

21. Submission of Bids through EPADS v2.0 before bid submission deadline.

21.1 The Technical and Financial Bids, shall be submitted electronically through EPADS, before bid submission deadline. The bid submission option shall be automatically disabled once the deadline is over.

22. Deadline for Submission of Bids

22.1 Bids shall be received by the Procuring Agency through EPADS v2.0 before bid submission deadline.

22.2 The Procuring Agency may, under exceptional circumstances, extend the deadline for the submission of Bids, after recording reasons in writing and in an equal opportunity manner.

In such case, all rights and obligations of the Procuring Agency and the Bidders that were previously governed by the original deadline shall thereafter be subject to the revised deadline.

E. Opening and Evaluation of Bids

23. Opening of Bids

23.1 The respective Bid Evaluation Committee of the Procuring Agency shall open all Bids through the EPADS v2.0, on the date and time specified in the Bid Data Sheet (BDS).

23.2 The respective Bid Evaluation Committee **shall generate minutes through EPADS v2.0 containing brief details of bid opening process.** The record of the Bid opening shall include, as a minimum: the name of the Bidder, the Bid price if applicable, and the presence or absence of a Bid Security or Bid Securing Declaration.

23.3 The procuring agency shall live broadcast the opening of bids on national media or on their website or digital channels, if the volume of procurement exceeds five hundred million rupees in case of goods and services and one thousand million rupees in case of works.

23.4 In case the date of opening of bid has been declared as public holiday or the procuring agency fails to open bid due to any EPADS v2.0 related issues, the submission and opening of bids shall be shifted to the next working day at the same time.

23.5 In case of Single Stage One Envelope Procedure, the Bidders names, the Bid prices, the total amount of each Bid and, the presence or absence of Bid Security, Bid Securing Declaration and such other details as the Procuring Agency may consider appropriate, will be announced by the Bid respective Evaluation Committee.

23.6 No bid will be rejected at the time of bid openning except for bids whose original bid security has not been provided to the procuring agency before bid submission deadline.

24. Clarification of Bids

24.1 To assist in the examination, evaluation and comparison of Bids of the Bidders, the respective Bid Evaluation Committee may, ask any Bidder for a clarification of its Bid including breakdown of prices.

24.2 The request for clarification and the response shall be sought through EPADS v2.0 before **three days prior to the deadline for submission of bids.** No change in the prices or substance of the Bids shall be sought, offered, or permitted.

24.3 The alteration or modification in the bids which in any way affect the following parameters will be considered as a change in the substance of a Bid:

1. evaluation & qualification criteria;
2. required scope of work or specifications;
3. all securities requirements;
4. tax requirements;
5. terms and conditions of Bidding documents.
6. change in the ranking of the Bidder

24.4 From the time of bid(s) opening to the time of Contract award if any Bidder wishes to contact the Procuring Agency on any matter related to the Bids it should do so through **EPADS v2.0**.

25. Preliminary Examination of Bids

25.1 Prior to the detailed evaluation of Bids, the respective Bid Evaluation Committee will determine whether each Bid:

1. meets the eligibility criteria defined in **ITB 3**;

2. has been prepared as per the format and contents defined by the Procuring Agency in the Bidding documents;

3. is accompanied by the required securities; and

4. is substantially responsive to the requirements of the Bidding documents.

25.2 The respective Bid Evaluation Committee's determination of a Bid's responsiveness will be based on the contents of the Bid itself.

25.3 A substantially responsive Bid is one which conforms to all the terms, conditions, and specifications of the Bidding documents, without material deviation or reservation. A material deviation or reservation is one that: -

1. affects in any substantial way the scope, quality, or performance of the Goods;

2. limits in any substantial way, inconsistent with the Bidding documents, the Procuring Agency's rights or the Bidders obligations under the Contract; or

3. if rectified, would affect unfairly the competitive position of other Bidders presenting substantially responsive Bids.

25.4 If a Bid is not substantially responsive, it will be rejected by the respective Bid Evaluation Committee and may not subsequently be evaluated for complete technical responsiveness.

26. Examination of Terms and Conditions; Technical Evaluation

26.1 The respective Bid Evaluation Committee shall examine the Bids to confirm that all terms and conditions specified in the **GCC** and the **SCC** have been accepted by the Bidder without any material deviation or reservation.

26.2 The respective Bid Evaluation Committee shall evaluate the technical aspects of the Bids submitted, to confirm that all requirements specified in Schedule of Requirements and Technical Specifications of the Bidding documents have been met without material deviation or reservation.

26.3 If after the examination of the terms and conditions and the technical evaluation, the respective Bid Evaluation Committee determines that the Bid is not substantially responsive in accordance with **ITB,** it shall reject the Bid.

27. Correction of Errors

27.1 Bids determined to be substantially responsive will be checked for any arithmetic errors. Errors will be corrected as follows: -

1. if there is a discrepancy between 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, unless in the opinion of the respective Evaluation Committee there is an obvious misplacement of the decimal point in the unit price, in which the total price as quoted shall govern and the unit price shall be corrected;

2. if there is an error in a total corresponding to the addition or subtraction of sub-totals, the sub-totals shall prevail and the total shall be corrected; and

3. where there is a discrepancy between the amounts in figures and in words, the amount in words will govern.

4. Where there is discrepancy between grand total of price schedule and amount mentioned on the Form of Bid, the amount referred in Price Schedule shall be treated as correct subject to elimination of other errors.

27.2 The amount stated in the Bid will be adjusted by the respective Bid Evaluation Committee in accordance with the above procedure for the correction of errors and, with the concurrence of the Bidder, shall be considered as binding upon the Bidder. If the Bidder does not accept the corrected amount, its Bid will then be rejected, and the Bid Security may be forfeited or the Bids Securing Declaration may be executed.

28. Conversion to Single Currency

28.1 For the purposes of comparison of bids quoted in different currencies, the price shall be converted into a single currency in accordance with Rule 42(2) of Public Procurement Rules,2026.

29. Evaluation of Bids

29.1 The Bids, quotations, or proposals shall be evaluated by the respective evaluation committees as per evaluation criteria prescribed in the Bidding Documents in accordance with Rule 11, 12 and 13 of the Public Procurement Rules, 2026.

29.2 While evaluating the bids, the procuring agency shall consider the following:

i. Bids will be evaluated on lump sum bid basis or items wise or Lot wise (contracts), as specified in the BDS; and the Bid Price;

ii. correction of arithmetic errors in accordance with ITB 27;

30. Domestic Preference

30.1 The respective Bid Evaluation Committee shall evaluate and compare bids, allow for preference to domestic bidders, while competing with the international bidders in accordance with the policies of the Federal Government.

The percentage of preference, to be accorded shall be clearly mentioned in the bidding documents under the bid evaluation criteria.

31. Determination of Successful Bid

31.1 **Selection technique will be adopted for determining the Successful Bid in accordance with the criteria referred in the BDS or prescribed in the separate section titled as Evaluation Criteria.**

31.2 **Least Cost Based Selection (LCBS)**
After meeting the requirements of eligibility, qualification and substantial responsiveness, the bid in compliance with all the mandatory (technical) specifications/requirements and/or requisite quality threshold (if any), and having lowest evaluated cost (or financial proposal) shall be considered Successful Bid.

31.3 **Quality and Cost Based Selection (QCBS)**
In such combination, there shall be some specific weightage of both the technical features and financial aspects of the proposal. The financial marks shall be awarded on the basis of inverse proportion calculations. The successful bid shall be declared, on the basis of combined evaluation.

31.4 **Quality Based Selection (QBS)**
After meeting the requirements of eligibility, qualification and substantial responsiveness the bid in compliance with all the mandatory (technical) specifications/requirements and attaining highest marks in the Technical Evaluation considering all other qualitative and/or quantitative parameters (or point rated criteria) for technical proposal(s) such as working methodology, implementation plan, resource allocation, additional functionalities, risk

management approach, knowledge transfer techniques, post implementation methodology etc. shall be treated as highest ranked bid. Later on, the financial proposal of highest ranked bidder shall be opened, however, in case of failure to proceed further with such a bidder, the procuring agency may resort to second highest bidder and so on.

31.5 The Procuring Agency may adopt the Quality & Cost Based Selection Technique due to the following two reasons:

1. Where the Procuring Agency knows about the main features, usage and output of the products; however not clear about the complete features, technical specifications and functionalities of the goods to be procured and requires the bidders to submit their proposals defining those features, specifications and functionalities; or

2. Where the Procuring Agency, in addition to the mandatory requirements and mandatory technical specifications, requires parameters specified in Evaluation Criteria to be evaluated while determining the quality of the goods.

31.6 In such cases, the Procuring Agency may allocate certain weightage to these factors as a part of Evaluation Criteria, and may determine the ranking of the bidders on the basis of combined evaluation in accordance with provisions of Rule 2(1)(xxviii) of the Public Procurement Rules, 2026.

32. Abnormally Low Financial Bids

32.1 An abnormally low bid is a bid that, in light of the Procuring Agency's cost estimate, market conditions, or other received bids, appears to be unrealistically low and may not be sustainable for successfull contract execution.

32.2 **Where the Bid price is considered to be abnormally low, the Procuring Agency shall perform price analysis either during determination of Successful Bids or as a part of the post-qualification process.**

32.3 The Procuring Agency may reject an Abnormally low financial bid in accordance with Rule 43 of the Public Procurement Rules, 2026.

32.4 In order to identify the Abnormally Low Bids (ALB) following approaches can be considered to minimize the scope of subjectivity:

1. Comparing the Bid price with the cost estimate;

2. Comparing the Bid price with the Bid(s) offered by other Bidders submitting substantially responsive Bids; and

3. Comparing the Bids price with prices paid in similar contracts in the recent past either government- or development partner-funded.

32.5 The respective Bid Evaluation Committee will determine to its satisfaction whether the Bidder that is selected as having submitted the successful bid is qualified to perform the contract satisfactorily.

32.6 The determination will take into account the Bidder's financial, technical, and production capabilities. It will be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, as well as such other information as the Procuring Agency deems necessary and appropriate. Factors not included in these Bidding documents shall not be used in the evaluation of the Bidders' qualifications.

32.7 Respective Bid Evaluation Committee may seek "Certificate for Independent Price Determination" from the Bidder and the results of reference checks may be used in determining an award of contract.

Explanation: The Certificate shall be furnished by the Bidder. The Bidder shall certify that the price is determined keeping in view of all the essential aspects such as raw material, its processing, value addition, optimization of resources due to economy of scale, transportation, insurance and margin of profit etc.

32.8 An affirmative determination will be a prerequisite for award of the contract to the Bidder. A negative determination will result in rejection of the Bidder's Bid, in which event the respective Bid Evaluation Committee will proceed to the next ranked Bidder to make a similar determination of that Bidder's capabilities to perform satisfactorily.

F. Award of Contract

33. Criteria of Award

33.1 The Procuring Agency will award the Contract to the Bidder whose Bids has been determined to be substantially responsive to the Bidding documents and who has been declared as Successful Bidder.

34. Negotiations

34.1 In accordance with Rule 52A of Public Procurement Rules, 2026, without changing the cost and scope of work or services, the procuring agency may

negotiate with the successful bidder (with a view to streamline the work or task execution, at the time of contract finalization) on methodology, work plan, staffing and special conditions of the contract.

There shall be no limitation on the successful bidder offering voluntary reduction in bid price without affecting the quality or scope of the procurement.

35. Procuring Agency's Right to reject all bids

35.1 The Procuring Agency reserves the right to reject all bids or proposals at any time prior to the issuance of the Letter of Award, without incurring any liability, in accordance with Rule 45 of the Public Procurement Rules, 2026.

36. Cancellation of Procurement

36.1 The procuring agency reserves the right to cancel the procurement proceedings in accordance with Rule 46 of the Public Procurement Rules, 2026.

37. Procuring Agency’s Right to Vary Quantities at the Time of Award

37.1 The Procuring Agency reserves the right at the time of contract award to increase or decrease the **quantity of** Goods originally specified in these Bidding documents provided this does not exceed **by** 15%, without any change in unit price or other terms and conditions of the Bids and Bidding documents.

38. Notification of Award

38.1 Prior to the award of contract, the procuring agency shall announce and publish the result of bid evaluation on EPADS v2.0 in accordance with Rule 48 of the Public Procurement Rules, 2026.

The Bidder whose Bids has been accepted will be notified of the award by the Procuring Agency prior to expiration of the Bids/Bid Validity period. The Letter of Award will state the sum that the Procuring Agency will pay the successful Bidder in consideration for the delivery of Goods as prescribed by the Contract (hereinafter and in the Contract called the "Contract Price).

38.2 The Letter of award will constitute the formation of the Contract, subject to the Bidder furnishing the Performance Guarantee and signing of the contract.

39. Signing of Contract

39.1 Promptly after issuance of Letter of award, Procuring Agency shall send the successful Bidder the draft Contract, incorporating all terms and conditions as agreed by the parties to the contract.

39.2 Immediately after the Redressal of grievance by the GRC (if any), and **after fulfillment of all conditions precedent** of the Contract Form, the successful Bidder and the Procuring Agency shall sign the Contract.

40. Corrupt & Fraudulent Practices

40.1 Procuring Agencies (including beneficiaries of Government funded projects and procurement) as well as Bidders/Contractors under Government financed contracts, observe the highest standard of ethics during the procurement and execution of such contracts, and will avoid engaging in any corrupt and fraudulent practices.

F. Grievance Redressal & Complaint Review Mechanism

41. Constitution of Grievance Redressal Committee

41.1 The Grievance Redressal Committee shall address the grievance, if any submitted by any party, including the bidder, in accordance with Rule 65 of the Public Procurement Rules, 2026 read with Redressal of Grievances Regulations, 2021.

In case if any party or the bidder is not satisfied with the decision of the GRC or if it fails to decide within ten days, the bidder or the party may file an appeal before the Appellate Committee of the Authority in accordance with Rule 65(7) of the Public Procurement Rules, 2026 to be read with Redressal of Grievances Regulations, 2021.

G. Mechanism of Blacklisting

42. Mechanism of Blacklisting

42.1 The Procuring Agency shall initiate blacklisting proceedings against any bidder, supplier, or contractor in accordance with the Rule 25 of the Public Procurement Rules, 2026.

42.2 The blacklisted/debarred bidder may file the review petition before the Authority in accordance with Rule 25 (6) of the Public Procurement Rules, 2026 to be read with Procedure of filing and disposal of Review Petitions Regulations, 2021.

43. Contract Management

43.1 For each procurement, the Procuring Agency shall designate a Contract Manager, who shall be duly responsible for the efficient management and administration of the contract in strict compliance with the provisions set forth under Rules 58, 59, and 60 of the Public Procurement Rules, 2026.

44. Inspection of goods and evaluation of services.

44.1 The Inspection Committee or the Firm shall have the right to conduct inspections of the goods in accordance with Rule 61 of the Public Procurement Rules, 2026.

45. Socio-economic development.

45.1 In accordance with Rule 63 of the Public Procurement Rules, 2026, preference may be granted to small and medium enterprises and marginalized groups in accordance with the policies notified by the Federal Government.

46. Environmental objectives

46.1 As per Rule 64 of the Public Procurement Rules, 2026, the procuring agency may seek to procure goods with a reduced environmental impact throughout their life cycle when compared to goods services with the same primary function that may otherwise be procured.

Bid Data Sheet

Bids Data Sheet (BDS)

The following specific data for the procurement of Goods to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

BDS Clause Number
ITB Number
Amendments of, and Supplements to, Clauses in the Instruction to Bidders

A. Introduction

BDS Clause Number 1
ITB Number 1.1

Name of Procuring Agency: **National Highways & Motorway Police (National Highways & Motorway Police (NHMP))**

The subject of procurement is: **Purchase of Licensed Enterprise Next-Generation Firewall (NGFW) with XDR**

Period for Provision of Goods:

Extension Period (if applicable):

Expected commencement date: **Monday, January 4, 2027**

BDS Clause Number 2
ITB Number 2.1

Source of funds [Enter source of funds]

Financial year for the operations of the Procuring Agency: **2026-27**

Name and identification number of the Contract: **P114196**

Identification Number:

BDS Clause Number 3
ITB Clause Number 3.1

Eligible Bidder [Enter eligibility of bidder]

JV/Consortium or Association Allowed: **No**
Number of JV/Consortium Members: **Nil**
see section of eligibility criteria.

B. Bidding Documents

BDS Clause Number 4

ITB Clause Number 4.1

Eligible goods and related services [Enter requirements for eligible goods and related services, if any]

ITB Number 8.1

The Bidders may seek clarifications through **EPADS v2.0** : Clarification Date: Saturday, November 28, 2026

ITB Number 8.2

The Bidders may seek clarifications through **EPADS v2.0** : Clarification Date: Saturday, November 28, 2026

ITB Number 8.3

The Bidders may seek clarifications through **EPADS v2.0** : Clarification Date: Saturday, November 28, 2026

ITB Number 8.5

Pre-bid meeting will be/will not be held [Tick the appropriate] If yes write down the time, and date of the pre-Bid meeting:
[The meeting should take place not later than one weeks before the deadline for Bid submission.]

C. Preparation of Bids

BDS Clause Number 5
ITB Number 10.1

The Language of all correspondences and documents related to the Bids shall be in: **English**

List of documents required along with the bid:

1. Original Bid Security must be deposited at Logistics Branch, CPO, NHMP, G-11/1, Islamabad and scanned copy of Bid Security in PDF format shall be emailed to logbranch@gmail.com well before closing date and time, otherwise bid will not be considered.

2. The bidder must provide FBR Tax Returns for the last financial year.

BDS Clause Number 6
ITB Number 11.1

Documents required / not required with bid submission [enter list of documents] Samples required / not required with the bid [Enter the names and number of samples]

Items/Lots and their related documents:
See section items and Lots

BDS Clause Number 7
ITB Number 12.1

Items / Lots Specifications:

see section of items specifications.

BDS Clause Number 8
ITB Number 15.6

The price shall be **Fixed**.

BDS Clause Number 9
ITB Number 16.1

Currency of the Bids shall be : **PKR**

BDS Clause Number 10
ITB Number 17.1

The Bids/Bid Validity period shall be: **120 Days**

BDS Clause Number 11
ITB Number 18.1

The amount of Bid Security shall be as defined in Bid Security Section for items and lots given in **BDS 6**
Instrument of Bid Security shall be in the Name of : **IG, National Highways & Motorway Police**

The Bid Security shall be in the form of: **Pay Order, Banker's Cheque, Call at Deposit, Bank Guarantee, Demand Draft**

ITB Number 18.2

The address for submission of original bid security is [Insert the address for bid security submission]

D. Submission of Bids

BDS Clause Number 12
ITB Number 20.1

Bid shall be submitted online on EPADS v2.0 whereas hard copy of the bid security should be submitted to the following;

Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory before bid submission deadline.

Bids that are not submitted on EPADS v2.0 shall be disqualified.

The deadline for Bids submission is: **Tuesday, December 1, 2026 11:00 AM**

Day *:* ***Tuesday***

Date: ***Tuesday, December 1, 2026***

Time *:* ***11:30 AM***

E. Opening and Evaluation of Bids

BDS Clause Number 13
ITB Number 23.1

The Bids opening shall take place on **EPADS v2.0**.

Day *:* ***Tuesday***

Date: ***Tuesday, December 1, 2026***

Time *:* ***11:30 AM***

ITB Number 29.2

The procuring agency shall consider the following:
lump sum bid basis; or
items wise; or

Lot wise (contracts),

ITB Number 30.1

BDS Clause Number 14
ITB Number 31.1

Domestic Preference [applicable / not applicable]

ITB Number 31.2

Selection technique adopted will be:
The Procuring Agency shall use any of the following evaluation techniques for determination of successful bid.

Least Cost Base Selection (LCBS)
Quality and Cost Based Selection (QCBS)
Quality Based Selection (QBS)
[Insert the Evaluation Technique]

Selection technique adopted will be: **Least Cost Based Selection (LCBS)**
see Evaluation Criteria

F. Review of Procurement Decisions

BDS Clause Number 15
ITB Number 41.1

Grievence against this procurement shall be submitted online on EPADS v2.0.

Arbitrator shall be appointed by mutual consent of the both parties.

ITB Number 42.2

The Address of PPRA Grievance Redressal Appellate Committee to submit a copy of grievance:

Grievance Redressal Appellate Committee,
Public Procurement Regulatory Authority
1st Floor, G-5/2, Islamabad, Pakistan
Tel: +92-51-9202254

Eligibility Criteria

All Active Taxpayers shall be eligible to participate in the procurement process, unless expressly excluded or otherwise restricted under the Eligibility Criteria specified by the Procuring Agency.

Required Registration
FBR (NTN) FBR (GSTN)

Eligibility Criteria	Document
The bidder must submit an affidavit on legal stamp paper that the firm is not blacklisted on any ground by any Government (Federal, Provincial), a local body or a public sector organization. On account of submission of any false statement, the bid will be straightway rejected and the decision will be final and non-challengeable.	Yes
Bidder should have local office/presence in Islamabad or Rawalpindi. (Office addresses and locations on the letterhead of the firm)	Yes
Bidder should be an authorized dealer of the proposed firewall OEM. (Valid OEM Manufacturer Authorization Letter is required).	Yes
Bidder should have minimum two (02) years of relevant experience in firewall/NGFW deployment, installation, configuration and support (Documentary evidence such as work orders, contracts or completion certificates).	Yes

Bidder should have maintained an adequate technical support team in Pakistan capable of providing remote and on- site support for installation, configuration, troubleshooting, migration, and maintenance of the proposed firewall solution. (List of technical staff along with their skill set on letterhead of the firm).	Yes
The Bidder must have a minimum annual turnover of PKR 20 million during the last financial year (Income Tax Returns/ Audited Tax Statements).	Yes

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Evaluation Criteria

Eligibile bidder(s) with substantially responsive bid(s) offering **Least Cost Based Selection (LCBS)** shall be consider for the award of contract(s).

Least Cost Based Selection (LCBS)

Weightage

Technical Evaluation %
100

Technical Marks	30
Passing Marks	**30**
Technical Evaluation Criteria	
Company Profile & OEM Authorization (Quantitative)(Doc Required)	5
02 Years Relevant Experience (Quantitative)(Doc Required)	5
Minimum 3 work orders with at least 01 year of support (Quantitative)(Doc Required)	5
Compliance Certificate with Technical Specifications & Proposed Solution on letterhead of the firm alongwith Brochure and Authentic Technical Data Sheet of proposed solution (Quantitative)(Doc Required)	5
Assurance of Implementation, Migration & Technical Support Capability on letterhead of the firm (Quantitative)(Doc Required)	5
Financial Strength for the current financial year (20 Million) (Quantitative)(Doc Required)	5

Items/Lots

Lot Title : New Generation Firewall with XDR

Bid Security : 894000 PKR

Item	UNSPSC	Delivery Schedule	Quantity	Manufacturer / Dealer Authorization	Warranty
Enterprise Next-Generation Firewall (NGFW)	Firewall network security equipment	**Address:** Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory **Schedule:** Immediately after signing of the Agreemenet **Quantity:** 1/Qty	1 / Qty	--	3 Years
Extended Detection & Response (XDR)	Firewall network security equipment	**Address:** Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory **Schedule:** Immediately after signing of the agreemenet **Quantity:** 200/Licences	200 / Licences	--	3 Years

Related Services of Goods:

No

Items/Lot Specification

Lot Title : New Generation Firewall with XDR

Item: Enterprise Next-Generation Firewall (NGFW)

UNSPSC: Firewall network security equipment

Specifications / Requirements:

S.No	Specification Requirement
A. General Requirements	
1	The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 5 years.
2	The proposed NGFW should be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA and NEBS certified.
3	The proposed NGFW should require no reboot for checking and installing security updates.
4	The proposed NGFW should have integrated reporting capabilities requiring no additional hardware to generate reports.
5	The proposed NGFW should identify applications regardless of port, SSL/SSH encryption, or evasive techniques employed.

S.No	Specification Requirement
6	The proposed NGFW should categorize unidentified applications for policy control, threat forensics, or application identification technology development.
7	The proposed NGFW should be a natively engineered security solution (Not an application control blade with underlying stateful inspection firewall).
8	The proposed NGFW should be a natively engineered appliance with a single-pass parallel processing architecture for traffic processing.
9	The proposed NGFW should have integrated traffic shaping functionality (QoS) based on source/destination IP, port, protocol and application.
10	The proposed NGFW must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability.
11	The proposed NGFW should control access and enforce policies for websites and applications, including SaaS applications.
12	The proposed NGFW should have a single OS across all form factors.
13	The proposed NGFW should support creating security policies to prevent credential theft.
14	The proposed NGFW should support enforcing multi-factor authentication to internal applications.
15	The proposed NGFW should support an unfettered open API without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples.
16	The proposed NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.

S.No	Specification Requirement
17	The proposed NGFW must provide visibility and the ability to restrict applications using non-standard ports in a single security policy rule
18	The proposed NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy
19	The proposed NGFW must be able to provide Machine Learning algorithms for advanced protections directly from the NGFW with no external connections needed
20	The proposed NGFW should grant easy OS updates without the need of certain combinations for hotfixes or patches to be in place
21	The proposed NGFW should have a feature of holding multiple OS images to support resilience and easy roll-backs during the version upgrades
22	The proposed NGFW should support enabling any new security offering without impacting the performance of the traffic flowing through it
23	The proposed NGFW should have a feature of identifying what applications are hitting the security policies and migrating these policies into application based policies
B. Architecture, Physical & Performance Specifications	
1	The proposed NGFW should deliver 8.5Gbps of documented firewall throughput (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions)
2	The proposed NGFW should deliver minimum of 4.2Gbps of documented threat prevention throughput (Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, DNS Security, file blocking and logging enabled, utilizing 64 KB HTTP/appmix transactions)

S.No	Specification Requirement
3	The proposed NGFW should deliver minimum of 4.1Gbps or above of IPsec VPN throughput (IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled)
4	The proposed NGFW should support 0.94 Million Max sessions
5	The proposed NGFW should support 100,000 new connections per second (measured with application-override utilizing 1byte HTTP transactions)
6	The proposed NGFW should support the addition of virtual systems for future expansion
7	The proposed NGFW must support minimum of 8 x 1Gigabit Ethernet (RJ45) interfaces, 6 x 1G SFP interface, 4 x 10G SFP+ interfaces.
8	The proposed NGFW should support (1) 10/100/1000 out-of-band management port, (1) 10/100/1000 high availability, (1) 1 Console port, (1) USB Port, Mini USB.
9	The proposed NGFW should offer redundant AC power supplies
10	The proposed NGFW should support Active/Active, Active/ Passive & Clustering deployments
11	The proposed NGFW should support state full session maintenance in the event of a fail-over to a standby unit
12	The proposed NGFW should support the High Availability feature for either NAT/Route or transparent mode
13	The proposed NGFW should support multiple heartbeat links
14	The proposed NGFW should support L3, L2, transparent and tap mode deployments
C. Security Policy Control features	
1	The proposed NGFW should support creating security policies based on Layer 7 applications irrelevant to the TCP/UDP port number (non-profile-based application control)

S.No	Specification Requirement
2	The proposed NGFW should support the management of unknown traffic (unidentified applications) through security policies
3	The proposed NGFW should have a built-in security policies optimization tool which facilitates converting legacy Layer 4 port-based security policies to Layer 7 application-based ones
4	The proposed NGFW should support enforcing security policies based on a schedule
5	The proposed NGFW should simplify rule use tracking via a timestamp for the most recent rule match, a timestamp for the first rule match, and a rule hit counter
D. Advanced Threat Prevention Features	
1	The proposed NGFW should protect networks by providing multiple layers of prevention, confronting threats at each phase of an attack.
2	The proposed NGFW should detect and block threats on any and all ports instead of invoking signatures based on a limited set of predefined ports.
3	The proposed NGFW should benefit from other cloud-delivered security subscriptions for daily updates that stops exploits, malware, malicious URLs, command and control (C2), and spyware.
4	The proposed NGFW should provide protections against unknown threats instantly by embedding ML in the core of the firewall to provide inline signature-less attack prevention.
5	The proposed NGFW should utilize Inline malware protection—through signatures based on payload, not hash.
6	The proposed NGFW should continuously collect telemetry to enable data-intensive ML processes to automatically compute and recommend policy changes.

S.No	Specification Requirement
7	The proposed NGFW should use cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
8	The proposed NGFW should leverage heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
9	The proposed NGFW should support creating custom signatures, which allows tailoring intrusion prevention capabilities to a network’s unique needs.
10	The proposed NGFW should support other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques.
11	The proposed NGFW should employ natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it.
12	The proposed NGFW should inspect and classify traffic as well as detect and block both malware and vulnerability exploits in a single pass.
13	The proposed NGFW should comb each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload.
14	The proposed NGFW should analyze the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques.
15	The proposed NGFW should support protocol decoder-based analysis.
16	The proposed NGFW should provide protocol anomaly-based protection.
17	The proposed NGFW should leverage inline, stream-based detection and prevention of malware hidden within compressed files and web content.

S.No	Specification Requirement
18	The proposed NGFW should provide protections against payloads hidden within common file types, such as Office/Microsoft 365 documents and PDFs.
19	The proposed NGFW should enable the correlation of a series of related threat events (e.g., from Threat Prevention logs) that, when combined, indicate a likely attack.
20	The proposed NGFW should have an option of configuring exception.
21	The proposed NGFW should be able to detect & prevent the malware by scanning different file types.
22	The proposed NGFW should be able to identify malwares coming from incoming files and malwares downloaded from Internet.
23	The proposed NGFW should provide an option to create custom signature for applications.
24	The proposed NGFW should have all major applications signatures and it should able to understand well known application like P2P and voice without any dependency on the port.
25	The proposed NGFW should enforce inline deep learning for real-time enforcement for new and unknown command and control.
26	The proposed NGFW machine learning and deep learning models should be aligned to key protocols, such as SSL, HTTP, unknown UDP, and unknown TCP.
27	The proposed NGFW should use ML-based analysis to identify advanced DNS-based threats.
28	The proposed NGFW should utilize a cloud-based database which contains tens of millions of known malicious domains, enabling the blocking of phishing, malware, and other high-risk categories.
29	The proposed NGFW should provide threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time.

S.No	Specification Requirement
30	The proposed NGFW should enable forging a response to a DNS query for a known malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client to identify infected hosts.
31	The proposed NGFW should allow defining separate policy actions as well as a log severity level for a specific signature type.
32	The proposed NGFW should identify the use of DGAs, which generates random domains on the fly for malware to use as a way to call back to a C2 server.
33	The proposed NGFW should identify DGA (Domain Generation Algorithms) domains based on dictionary words.
34	The proposed NGFW should prevent the use of DNS tunneling, which exploits the DNS protocol to tunnel malware and other data through a client-server model.
35	The proposed NGFW should disrupt ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.
36	The proposed NGFW should leverage predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.
37	The proposed NGFW should prevent fast flux domains.
38	The proposed NGFW should protect against domains surreptitiously added to hacked DNS zones of reputable domains.
39	The proposed NGFW should prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.
40	The proposed NGFW should prevent dangling DNS attacks.

S.No	Specification Requirement
41	The proposed NGFW should prevent attackers from directing users to malicious domains with the use of a wildcard DNS record.
42	The proposed NGFW should prevent techniques that exploit DNS protocol to tunnel malicious payloads into networks.
43	The proposed NGFW should protect users from connecting to domains that can be used to launch DDoS attacks.
44	The proposed NGFW should support traffic static analysis.
45	The proposed NGFW should support traffic dynamic analysis.
46	The proposed NGFW should support advanced file analysis with URL crawling to prevent multistage, multi hop attacks.
47	The proposed NGFW analysis environment should replicate macOS, Android, Windows XP/7/10, and Linux.
48	The proposed NGFW file analysis should support PE files (EXE, DLL, and others), all Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files.
49	The proposed NGFW support protocols should be SMTP, POP3, SMB, FTP, IMAP, HTTP, and HTTPS.
50	The proposed NGFW should generate signatures based on the malware payload of the sample and tested for accuracy and safety.
51	The proposed NGFW should provide protection updates for unknown malware within seconds.
E. Advanced URL Filtering	

S.No	Specification Requirement
1	The proposed NGFW should possess a patented inline real-time web threat prevention capability which uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time
2	The proposed NGFW machine-learning models should get retrained frequently, ensuring protection against new and evolving never before-seen threats (e.g., phishing, exploits, fraud, C2)
3	The proposed NGFW should protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding
4	The proposed NGFW URL database should maintain hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis
5	The proposed NGFW should be allow classifying websites based on site content, features, and safety, and includes more than 70 benign and malicious content categories
6	The proposed NGFW should support risk rating which scores URLs on a variety of factors to determine risk
7	The proposed NGFW should have multi-category support which categorizes a URL with up to four categories, allowing for flexible policy and the creation of custom categories
8	The proposed NGFW should detect and prevent credential theft by controlling sites to which users can submit corporate credentials based on the site’s URL category
9	The proposed NGFW should se ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts
10	The proposed NGFW allow designating multiple policy action types based on URL categories or criteria
11	The proposed NGFW should apply URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies

S.No	Specification Requirement
12	The proposed NGFW should apply URL filtering policies when end users attempt to view the cached results of web searches and internet archives
13	The proposed NGFW should prevent inappropriate content from appearing in users’ search results
14	The proposed NGFW should enable administrators to notify users of a violation using a custom block page
15	The proposed NGFW should support crawling and analysis in 41 languages
F. User Identification & Authentication Features	
1	The proposed NGFW should support identifying user-id by integrating with Active Directory through WinRM and WMI
2	The proposed NGFW should support identifying user-id by integrating with Exchange through WinRM and WMI
3	The proposed NGFW should support identifying user-id by running as syslog receiver
4	The proposed NGFW should support identifying user-id by Integrating through XML APIs with Third Party solutions
5	The proposed NGFW should support identifying user-id through captive portal
6	The proposed NGFW should support Identifying user-id in terminal servers
7	The proposed NGFW should support identifying user-id by running an agent at user machines
8	The proposed NGFW should have direct Multi-Factor Authentication integration with RSA, Okta, PingID and Duo
9	The proposed NGFW should support SSO authentication
10	The proposed NGFW should support multiple server profiles like SAML 2.0, Radius, LDAP, Tacacs+, and Kerberos.
G. Advanced Mobility & Host Information Profiling Features	
1	The proposed NGFW should offer a remote user VPN agent for Windows, MAC, Linux, Chrome, iOS, and Android

S.No	Specification Requirement
2	The proposed NGFW should support app-Level VPN for iOS and Android devices
3	The proposed NGFW should have support portal based and clientless SSL VPN
4	The proposed NGFW should support MFA
5	The proposed NGFW should offer a host information check feature by collecting & reporting device information & attributes, Host Information Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and Plist presence & status
6	The proposed NGFW should support enforcing security policies based on device/host information profiles
7	The proposed NGFW should support the integration with Third Party MDM solutions like AirWatch or MobileIron
8	The proposed NGFW should support split tunneling based on IP addresses, domains and applications
9	The proposed NGFW should support VPN authentication override using cookies
10	The proposed NGFW should support the exclusion of video traffic from main remote user VPN tunnel
11	The proposed NGFW should support trusted root certificates push to remote VPN user devices to help enable features like SSL offload
12	The proposed NGFW should support VPN gateway selection criteria based on source user-id, region, OS and IP address
H. Management, Logging & Reporting Features	
1	The proposed NGFW should offer a Command Line Interface (CLI).

S.No	Specification Requirement
2	The proposed NGFW should offer a built-in web interface, non Java base (GUI).
3	The proposed NGFW should support XML Rest API based management.
4	The proposed NGFW should have a commit-based configuration management.
5	The proposed NGFW should support config-audit by comparing running config against candidate config.
6	The proposed NGFW should offer an interactive graphical summary around the applications, users, URLs, threats, and content traversing the network.
7	The proposed NGFW should offer a customized graph-based network activity for applications using non-standard ports.
8	The proposed NGFW should offer a customized graph-based blocked activities which includes blocked applications activity, blocked users activity, blocked content activity, blocked threats activity, and security policies blocking activity.
9	The proposed NGFW should offer a customized graph-based tunnel activities including tunnel ID/Tag, tunnel application usage, tunnel user activity, and tunnel ip source/destination activity.
10	The proposed NGFW should support custom reporting with the ability to generate a report per user, user group and application.
11	The proposed NGFW should support exporting reports to PDF and sending reports by email.
12	The proposed NGFW should have a dedicated SaaS applications usage report.
13	The proposed NGFW should have dedicated log sets for traffic, threats, URL filtering, data filtering, file control, user id mapping, authentication, configuration, system and alarms.
14	The proposed NGFW should support custom admin roles.

S.No	Specification Requirement
15	The proposed NGFW should allow administrators to work directly on the appliance, and make configuration changes as needed, without having to log in to a central manager.
16	The proposed NGFW should allow central administrators to monitor and view the changes made by local administrators.
17	The proposed NGFW management should be done directly through the appliance without the need of installing any clients or virtual machines.
18	The proposed NGFW should offer the ability to choose which firewall administrator’s configuration changes to be committed on the firewalls.
19	The proposed NGFW should offer the ability to quickly roll back changes from specific users and restore configurations.
20	Solution must be endorsed from Pakistan Security Standard.
21	All required relevant licenses and subscriptions for three (03) years including but not limited to:
	i. Threat prevention subscription.
	ii. Sandboxing subscription.
	iii.Advanced URL Filtering Subscription.
	iv.DNS Security subscription.
	v.SD-WAN Subscription

Item: Extended Detection & Response (XDR)

UNSPSC: Firewall network security equipment

Specifications / Requirements:

S.No	__EMPTY	__EMPTY_1	Specification Requirement
1	Next-Generation Antivirus Requirements		
	Should be able to perform/have following capabilities		
	a.		Machine learning-based local analysis and threat prevention
	b.		Behavior-based threat prevention for dynamic analysis of running processes
	c.		Exploit prevention by exploit technique
	d.		Known threat prevention based on threat intelligence, such as file hashes
	e.		Automated integration with a cloud-based malware prevention service, with analysis reports
	f.		Zero-delay signatures to rapidly deliver protection and share threat intelligence
	g.		Transparent threat detection engine updates
	h.		Security profiles and exceptions
	i.		Ad hoc and scheduled scanning of endpoints
	j.		Protection against malware, ransomware and file-less attacks

S.No	__EMPTY	__EMPTY_1	Specification Requirement
	k.		Single lightweight agent for endpoint protection, detection and response
2	Endpoint Protection Requirements		
	Should have the following features		
	a.		Host firewall
	b.		Disk Encryption
	c.		Device Control
	d.		Customizable prevention rules
3	Investigation Requirements		
	Should have following capabilities		
	a.		Visualization of the chains of execution leading up to an alert
	b.		Timeline analysis view to see all actions and alerts on a timeline
	c.		Querying for indicators of compromise (IOCs), Behavioral IOCs (BIOC) and endpoint behaviors
	d.		Advanced querying language for visualization of data
	e.		In-context wizard that lets you search for information, perform common investigation tasks, or initiate response actions from anywhere in the management console
	f.		Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations
4	Incident Management Requirements		

S.No	__EMPTY	__EMPTY_1	Specification Requirement
	Should have the following capabilities		
	a.		Automated grouping of related alerts from various sources into a single incident
	b.		Listing of notable artifacts from alerts and their threat intelligence information
	c.		Listing of user and hosts involved in incidents to quickly determine the scope of an incident
	d.		End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.)
	e.		Ability to change the severity of an incident
5	Threat Intelligence Requirements		
	Should have the following capabilities		
	a.		Ability to alert on known malicious objects on endpoints with IOC rules
	b.		IOC creation from the management console
	c.		Ability to import multiple IOCs from a CSV file using the management console
	d.		Configurable severity level of an IOC
6	Response Requirements		
	Should have the following capabilities		
	a.		Remote terminal capability
	b.		Full CMD, PowerShell, and Python commands and scripts on Windows 7, 8,10 and Windows 11

S.No	__EMPTY	__EMPTY_1	Specification Requirement
	c.		Full Bash and Python commands on macOS and Linux
	d.		Ability to execute custom Python scripts across multiple endpoints simultaneously on Windows, macOS, and Linux
	e.		Remote isolation of a single endpoint or multiple endpoints
	f.		Remote file deletion of a single endpoint or multiple endpoints
	g.		Automatic and manual collection or retrieval of quarantined files and objects
	h.		Ability to view, suspend, or terminate running processes or download binaries with a graphical task manager for Windows, macOS, and Linux
	i.		Graphical file manager with ability to view, download, rename, or move files for Windows, macOS, and Linux
	j.		Search and destroy to swiftly sweep across endpoint and eradicate threats
	k.		Integration with a security orchestration, automation, and response (SOAR) solution for incident analysis
	l.		Integration with security information and event management (SIEM) solutions
7	Visibility and Detection Requirements		
	Should have the following capabilities		
	a.		Supervised and unsupervised machine learning capabilities
	b.		Predefined and customizable behavior-based detection rules

S.No	__EMPTY	__EMPTY_1	Specification Requirement
	c.		Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services
	d.		Ability to consume threat intelligence feeds from third-party sources
	e.		Detection of attack techniques across the attack lifecycle including discovery, lateral movement, command and control, and exfiltration
	f.		Demonstrated ability to detect attacker tactics and techniques through MITRE ATT&CK Evaluations
	g.		Tagging of MITRE ATT&CK tactics and techniques in alerts and detection rules
8	Data Collection Requirements		
	a.		User information
		-1	Domain and distinguished name
		-2	Email address
		-3	Organizational unit
		-4	Logged-in user
		-5	Typical user of a machine
		-6	User creating the process that initiated communication
		-7	User group and organizational unit from directory services
	b.		Device information

S.No	__EMPTY	__EMPTY_1	Specification Requirement
		-1	MAC address
		-2	Hostname of device
		-3	Domain name
		-4	Distinguished name of host
		-5	Organizational unit
		-6	Operating system and version
	c.		Process information
		-1	Process timestamp
		-2	Path and name
		-3	Process ID
		-4	Loaded modules
		-5	Hash values, such as MD5 and SHA-256
		-6	Command line arguments
		-7	RPC requests and code injection data, if applicable
		-8	Signature state
	d.		File information for file create, write, access, open, rename, or delete
		-1	Timestamp
		-2	Path and name

PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

S.No	__EMPTY	__EMPTY_1	Specification Requirement
		-3	Previous file name and path for file rename events
		-4	Hash values, such as MD5 and SHA-256
		-5	Username
	e.		Network activity, including outgoing connections, failed connections, and incoming connections
		-1	Timestamp
		-2	Source IP address, destination IP address, source port, and destination port
		-3	Bytes sent and received
		-4	Protocol
		-5	Geolocation data
		-6	Connection duration
	f.		Registry activities, such as create key, modify key, delete key, and rename key
		-1	Timestamp
		-2	Key name
		-3	Value and type
		-4	Previous key name for rename events
	g.		System events
		-1	User status change event, such as login and logout

S.No	__EMPTY	__EMPTY_1	Specification Requirement
		-2	Host status change event
		-3	Agent status change event
	h.		Security alerts
		-1	Endpoint threat logs
9	Endpoint Agent System Support and Resource Requirements		
	a.		Support for all recent Windows versions, including Windows Server
	b.		Support for all recent macOS and Mac OS X versions
	c.		Support for Android, iOS and Chrome OS
	d.		Support for all major Linux distributions
	e.		Full auditing for all actions in the system
	f.		Ability to push agent updates from the management console & auto update ability when connected to the internet automatically
	g.		Optional peer-to-peer agent updates
	h.		Granular control of agent controls and notifications, including tray icon visibility, custom end user notifications, and the option to restrict response options such as remote terminal access
10	Deployment, Management and Security		
	a.		Scalable, cloud-based management and agent deployment

S.No	__EMPTY	__EMPTY_1	Specification Requirement
	b.		Single, web-based management console for endpoint security as well as extended detection and response
	c.		Role-based access control (RBAC) for granular permissions
	d.		Multi-factor authentication (MFA) for management
	e.		Ability to fetch required data from the entire database using scripts
11	Data Retention and Coverage Requirements		
	a.		Detection and response for threats involving managed and unmanaged endpoints
	b.		Detection and response for threats involving remote users
	c.		Continuous collection and centralized storage of all security data for behavioral analytics
	d.		Data retention of 180 days
	e.		Optional retention of data for an unlimited length of time
12	License Requirements		
	a.		200 licenses required for endpoints on site deployment
	b.		3 years license & support
	c.		Solution must be endorsed from Pakistan Security Standard (PSS)

Price Schedule

For Individual Items

#	Item Title	Quantity	Unit Price (PKR)	Total Price (PKR)	Delivery Location	Delivery Period / Year	Country of Origin
1							
2							

For Lots

#	Lot Title	Total Lot Price (PKR)	Country of Origin
1	[Lot 1 Title]		

PUBLIC PROCUREMENT REGULATORY AUTHORITY
(PPRA)
EPADS

General Conditions of Contract

A. General

1. Definitions

1.1 Unless the context otherwise requires, the following terms whenever used in this Contract shall have the same meaning and shall be interpreted as indicated

a. “Applicable Law” means the laws and any other instruments having the force of law in the Government’s Country, or in such other country as may be specified in the Special Conditions of the Contract (SC), as they may be issued and in force from time to time;

b. The “Arbitrator” is the person appointed with mutual consent of both the parties, to resolve contractual disputes as provided for in the General Conditions of the Contract GCC Clause 35 hereunder.

c. “Authority” means Public Procurement Regulatory Authority.

d. The “Commencement Date” is the date when the Supplier shall commence execution of the contract as specified in the SCC.

e. “Completion date” means the date of completion of the Contract by the Bidder as certified by the Procuring Agency.

f. “Procuring Agency” means:-

a. any Ministry, Division, Department or any Office of the Government;

b. any authority, corporation, body or organization established by or under a Law or which is owned or controlled by the Government;.

g. “The Contract” means an agreement enforceable by law;

h. “The Contract Price” means the price payable to the Bidder under the Contract for the full and proper performance of its contractual obligations;

i. “Ancillary Services” means those services ancillary to the provision of Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Bidder covered under the Contract;

j. “GCC” means the General Conditions of Contract contained in this section;

k. “SCC” means the Special Conditions of Contract by which the GCC may be amended or supplemented;

l. **“**Day” means calendar day unless indicated otherwise.

m. “Defective Goods” are those goods which are below standards, requirements or specifications stated by the Contract.

n. “Delivery” means the transfer of the goods from the supplier equipment, machinery, and /or other materials which the Supplier is required to supply to the Procuring Agency under Contract.

o. “Effective Date” means the date on which this Contract comes into force and effect.

p. “Force Majeure” means an unforeseeable event which is beyond reasonable control of either Party and which makes a Party’s performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

For the purposes of this Contract, “Force Majeure” means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of a Party, and which makes a Party’s performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances. and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood, epidemics, or other adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by Government agencies.

q. The Bidder” means the individual or corporate body whose Bids to provide the Goods has been accepted by the Procuring Agency;

r. “The Project Site,” where applicable, means the place or places named in Bids Data Sheet and technical Specifications;

s. “Government” means the Government of Pakistan;

t. “Subcontractor” means any entity to which the Bidder subcontracts any part of the Goods.

u. The “Services” means the work to be performed by the Bidder pursuant to this Contract and as prescribed in the Specifications and Schedule of Activities included in the Bidder’s Bids;

v. “Party” means the Procuring Agency or the Bidder, as the case may be, and “Parties” means both of them;

w. “Foreign Currency” means any currency other than the currency of the country of the Procuring Agency;

x. “Completion Date” means the date of completion of the contract by the Bidder as certified by the Procuring Agency;

y. “In Writing” means communicated in written form with proof of receipt;

z. “Local Currency” means the currency of Pakistan;

a. “Origin” means the place where the Goods were mined, grown, or produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, or substantial and major assembly of components, a commercially recognized new produce results that is substantially different in basic characteristics or in purpose or utility from its components.

b. “Specification” means the Specification of the Goods and performance of incidental services in accordance with the relevant standards included in the Contract and any modification or addition made or approved by the Procuring Agency.

c. “Procuring Agency” means: -
any Ministry, Division, Department or any Office of the Federal Government;
any authority, corporation, body or organization established by or under a Federal Law or which is owned or controlled by the Federal Government;

2. Application and Interpretation

2.1 These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of the Contract.

2.2 In interpreting these Conditions of Contract headings and marginal notes are used for convenience only and shall not affect their interpretations unless specifically stated; references to singular include the plural and vice versa; and masculine include the feminine. Words have their ordinary meaning under the language of the Contract unless specifically defined.

3. Applicable Law

3.1 The contract shall be governed and interpreted in accordance with the laws of Pakistan, unless otherwise specified in SCC.

4. Governing Language

4.1 The Contract as well as all correspondence and documents relating to the Contract exchanged between the Bidder and the Procuring Agency, shall be written in the **English language** unless otherwise stated in the **SCC**. Supporting documents and printed literature that are part of the Contract may be in another language provided these are accompanied by an accurate translation of the relevant passages in English, in which case, for purposes of interpretation of the Contract, this translation shall govern.

5. Notices

5.1 Any notice, request, or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the **SCC**.

6. Standard

6.1 The Goods supplied under this Contract shall conform to the standards mentioned in the Technical Specifications, and, when no applicable standard is mentioned, the American Standards (such as ACI, IEEE, ASME, etc.) or the Pakistani standards such as PSQCA Such standards shall be the latest issued by the concerned institution.

7. Delivery/Location

7.1 The Goods shall be delivered to such locations as the Procuring Agency may approve and as specified in SCC.

8. Authorized Representatives / Authority of Member in charge

8.1 Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Procuring Agency or the Bidder may be taken or executed by the officials specified in the **SCC**.

B. Commencement, Completion, Modification, and Termination of Contract

8. Effectiveness of Contract

8.1 This Contract shall come into effect on the date the Contract is signed by both parties and such other later date as may be stated in the SCC.

9. Commencement of the Contract

9.1 The Bidder shall confirm availability of Key Experts and begin carrying out the Services not later than the number of days after the Effective Date specified in the SCC.

10. Program

10.1 Before commencement of the Contract, the Bidder shall submit to the Procuring Agency for approval a Program showing the general methods, arrangements, order and timing for all activities. The Services shall be carried out in accordance with the approved Program as updated.

11. Starting Date/Expiration Date

11.1 The Bidder shall start carrying out the Services Five (05) days after the date the Contract becomes effective, or at such other date as may be specified in the **SCC.**

11.2 Unless terminated earlier pursuant to Clause **GCC 16** hereof, this Contract shall expire at the end of such time period after the Effective Date as specified in the SCC.

12. Entire Agreement

12.1 This Contract contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

13. Modification

13.1 Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any Bids for modification or variation made by the other Party.

13.2 In cases of any modifications or variations, the prior written consent of the Procuring Agency is required.

14. Force Majeure

14.1 Definition

For the purposes of this Contract, "Force Majeure" means an event which is beyond the reasonable control of a Party and which makes a Party's performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

14.2 No Breach of Contract

The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

14.3 Extension of Time

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure. However, such period shall not exceed sixty (60) days.

14.4 Payments

During the period of their inability to perform the Services as a result of an event of Force Majeure, the Bidder shall be entitled to continue to be paid under the terms of this Contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the Services and in reactivating the Service after the end of such period.

15. Termination

15.1 By the Procuring Agency

The Procuring Agency may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause. In such an occurrence the Procuring Agency shall give at least thirty (30) calendar days' written notice of termination to the Bidder in case of the events referred to in (a) through (d); at least sixty (60) calendar days' written notice in case of the event referred to in (e);

a. If the Bidder fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice of suspension;

b. If the Bidder becomes (or, if the Bidder consists of more than one entity, if any of its members becomes) insolvent or bankrupt or enter into any agreements with their creditors for relief of debt or take advantage of any law for the benefit of debtors or go into liquidation or receivership whether compulsory or voluntary;

c. If the Bidder fails to comply with any final decision reached as a result of arbitration proceedings;

d. If, as the result of Force Majeure, the Bidder is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;

e. If the Procuring Agency, in its sole discretion and for any reason whatsoever, decides to terminate this Contract;

15.2 By the Bidder

The Bidder may terminate this Contract, by not less than thirty (30) calendar days' written notice to the Procuring Agency, in case of the occurrence of any of the events specified in paragraphs (a) through (d) of this Clause.

a. If the Procuring Agency fails to pay any money due to the Bidder pursuant to this Contract and not subject to dispute within forty-five (45) calendar days after receiving written notice from the Bidder that such payment is overdue.

b. If, as the result of Force Majeure, the Bidder is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days.

c. If the Procuring Agency fails to comply with any final decision reached as a result of arbitration.

d. If the Procuring Agency is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Bidder may have subsequently approved in writing) following the receipt by the Procuring Agency of the Bidder's notice specifying such breach.

C. Obligations of the Bidder

16. General

16.1 Standard of Performance

1. The Bidder shall deliver the product and carry out the Services with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Bidder shall always act, in respect of any matter relating to this Contract or to the Services, as a faithful adviser to the Procuring Agency, and shall at all times support and safeguard the Procuring Agency's legitimate interests in any dealings with the third parties.

16.2 Law Applicable to Goods

The Bidder shall deliver the goods in accordance with the Contract and in accordance with the Law of Pakistan and shall take all practicable steps to ensure that any of its Experts and Sub-Bidders, comply with the Applicable Law.

17. Conflict of Interests

17.1 Bidder Not to Benefit from Commissions and Discounts.

The remuneration of the Bidder shall constitute the Bidder's sole remuneration in connection with this Contract or the Services, and the Bidder shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Bidder shall use their best efforts to ensure that the Personnel, any Subcontractors, and agents of either of them similarly shall not receive any such additional remuneration.

17.2 Bidder and Affiliates Not to be Otherwise Interested in Project

The Bidder agree that, during the term of this Contract and after its termination, the Bidder and its affiliates, as well as any Subcontractor and any of its affiliates, shall be disqualified from providing Goods for any project resulting from or closely related to the Services.

17.3 Prohibition of Conflicting Activities

Neither the Bidder nor its Subcontractors nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

a. during the term of this Contract, any business or professional activities in the Government's country which would conflict with the activities assigned to them under this Contract;

b. during the term of this Contract, neither the Bidder nor their Subcontractors shall hire public employees in active duty or on any type of leave, to perform any activity under this Contract;

18. Confidentiality

18.1 Except with the prior written consent of the Procuring Agency, the Bidder and the Experts shall not at any time communicate to any person or entity any confidential information acquired in the course of the contract.

19. Insurance to be Taken Out by the Bidder

19.1 The Bidder(a) shall take out and maintain, and shall cause any Subcontractors to take out and maintain, at its (or the Subcontractors', as the case may be) own cost but on terms and conditions approved by the Procuring Agency, insurance against the risks, loss or damage, and for the coverage, as shall be specified in the SCC; and (b) at the Procuring Agency's request, shall provide evidence to the Procuring Agency showing

that such insurance has been taken out and maintained and that the current premiums have been paid.

20. Bidder's Actions Requiring Procuring Agency's Prior Approval

20.1 The Bidder shall obtain the Procuring Agency's prior approval in writing before taking any of the following actions:

(a) appointing such members of the Personnel not provided by the Bidder;

(b) changing the Program of activities; and

(c) any other action that may be specified in the SCC.

21. Reporting Obligations

21.1 The Bidder shall submit to the Procuring Agency the reports and documents in the numbers, and within the periods as prescribed by the Procuring Agency.

22. Liquidated Damages

22.1 If the Supplier fails to deliver any or all of the Goods or to perform the Services within the period(s) specified in the Contract, the Procuring Agency shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to the percentage specified in **SCC** of the delivered price of the delayed Goods or unperformed Services for each week or part thereof of delay until actual delivery or performance, up to a maximum deduction of the performance security (or guarantee) specified in **SCC**. Once the said maximum is reached, the Procuring Agency may consider termination of the Contract pursuant to **GCC Clause 16.**

22.2 Correction for Over-payment

If the Intended Completion Date is extended after liquidated damages have been paid, the Procuring Agency shall correct any overpayment of liquidated damages by the Bidder by adjusting the next payment certificate. The Bidder shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment, at the rates specified in SCC.

22.3 Lack of performance penalty

If the Bidder has not corrected a Defect within the time specified in the Procuring Agency's notice, a penalty for Lack of performance will be paid by the Bidder. The amount to be paid will be calculated as a percentage of the cost of having the Defect corrected, assessed as specified in the SCC.

23. Performance Guarantee

23.1 The Performance Security (or Guarantee) shall be provided to the Procuring Agency no later than the date specified in the Letter of Acceptance and shall be issued in an amount and form acceptable to the Procuring Agency as specified in SCC, and denominated in the types and proportions of the currencies in which the Contract Price is payable as specified in the SCC.

23.2 Within Seven (07) days from the issuance of acceptance letter from the Procuring Agency, the successful Bidder shall furnish the Performance Guarantee in shape of ------- at the discretion of the PA in the amount **specified in SCC.** In case the amount of Bids security is equal or greater than

23.3 The proceeds of the Performance Guarantee shall be payable to the Procuring agency as compensation for any loss resulting from the Supplier's failure to complete its obligations under the Contract.

23.4 The Performance Guarantee shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Procuring agency and shall be in the acceptable form as specified in SCC.

23.5 The Performance Guarantee will be discharged by the Procuring agency and returned to the Supplier not later than thirty (30) days following the date of completion of the Supplier's performance obligations under the Contract, including any warranty obligations, unless otherwise **specified in SCC.**

23.6 The bid security of the successful bidder shall not be substituted with the Performance Guarantee.

24. Fraud and Corruption

24.1 The Procuring Agency requires the Supplier to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the Bidding process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

25. Sustainable Procurement

25.1 The Bidder shall conform to the sustainable procurement contractual provisions, if and as specified in the SCC.

D. Bidder's Personnel

26. Description of Personnel

26.1 The titles, agreed job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the Services of the Bidder's Key Personnel. The Key Personnel listed by title as well as by name are hereby approved by the Procuring Agency.

27. Removal and/or Replacement of Personnel

27.1 Except as the Procuring Agency may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Bidder, it becomes necessary to replace any of the Key Personnel, the Bidder shall provide as a replacement a person of equivalent or better qualifications.

27.2 If the Procuring Agency finds that any of the Personnel have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Bidder shall, at the Procuring Agency's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the Procuring Agency.

27.3 The Bidder shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.

E. Obligations of the Procuring Agency

28. Assistance and Exemptions

28.1 The Procuring Agency shall use its best efforts to ensure that the Government shall provide the Bidder such assistance and exemptions as specified in the SCC.

29. Change in the Applicable Law

29.1 If, after the date of this Contract, there is any change in the Applicable Law with respect to taxes and duties which increases or decreases the cost of the related Services rendered by the Bidder, then the remuneration and reimbursable expenses otherwise payable to the Bidder under this Contract shall be increased or decreased accordingly by agreement between the Parties, and corresponding adjustments shall be made to the amounts referred in the SCC.

30. Services and Facilities

30.1 The Procuring Agency shall make available to the Bidder and the Experts, for the purposes of the Services and free of any charge, the services, facilities and property described , at the times and in the manner specified in the SCC or terms of reference.

30.2 In case that such services, facilities and property shall not be made available to the Bidder, the Parties shall agree on (i) any time extension that it may be appropriate to grant to the Bidder for the performance of the Services, (ii) the manner in which the Bidder shall procure any such services, facilities and property from other sources, and (iii) the additional payments, if any, to be made to the Bidder as a result thereof.

F. Payments to the Bidder

31. Contract Price

31.1 The price payable shall be in Pakistani Rupees unless otherwise specified in the SCC. Prices charged by the Supplier for Goods delivered under the Contract shall not vary from the prices quoted by the Supplier in its Bid.

32. Terms and Conditions of Payment

32.1 Payments will be made to the Bidder according to the payment schedule stated in the SCC and as per actual invoice submitted by the Bidder.

32.2 Unless otherwise stated in the SCC, the advance payment shall be made against the provision by the Bidder of a bank guarantee for the same amount, and shall be valid for the period stated in the SCC. Any other payment shall be made after the conditions listed in the SCC for such payment have been met, and the Bidder have submitted an invoice to the Procuring Agency specifying the amount due.

33. Currency of Payment

33.1 Any payment under this Contract shall be made in the currency(ies) specified in the SCC.

G. Quality Control

34. Identifying Defects

34.1 The principle and modalities of Inspection of the Goods by the Procuring Agency shall be as indicated in the SCC. The Procuring Agency shall check the Bidder’s performance and notify him of any Defects that are found. Such checking shall not affect the Bidder’s responsibilities. The Procuring Agency may instruct the Bidder to search for a Defect and to uncover and test any service that the Procuring Agency considers may have a Defect. Defect Liability Period is as defined in the SCC.

35. Correction of Defects, and

Lack of Performance Penalty

35.1 The Procuring Agency shall give notice to the Bidder of any Defects before the end of the Contract. The Defects liability period shall be extended for as long as Defects remain to be corrected.

35.2 Every time notice a Defect is given, the Bidder shall correct the notified Defect within the length of time specified by the Procuring Agency's notice.

35.3 If the Bidder has not corrected a Defect within the time specified in the Procuring Agency's notice, the Procuring Agency will assess the cost of having the Defect corrected, the Bidder will pay this amount, and a Penalty for Lack of Performance.

36. Taxes and Duties

36.1 A Supplier shall be entirely responsible for all taxes, duties, fees, etc., incurred until delivery of the contracted Goods to the Procuring Agency.

H. Settlement of Disputes

37. Alternate Dispute Resolution

37.1 Upon the commencement of the Procurement Contract, any disputes arising between the contracting parties shall be resolved in accordance with Rule 66 of the Public Procurement Rules, 2026.

37.2 The procuring agency may refer the matter to the Chief Justice Islamabad High Court or Managing Director PPRA or the Secretary Ministry of Law & Justice for appointment of Arbitrator.

37.3 The fee for the Arbitrator shall be specified in Pak Rupees as determined by the appointing authority which shall be borne and shared equally by the contracting parties.

38. Change Orders

The Procuring Agency may at any time, by a written order given to the Supplier, make changes within the general scope of the Contract in any one or more of the following:

a)Drawings, designs, or specifications, where Goods to be furnished under the Contract are to be specifically manufactured for the Procuring Agency;
b)The method of shipment or packing;
c)The place of delivery; and/or
d)The Services to be provided by the Supplier.

39. Contract Amendenments

39.1 Subject to GCC Clause 32, no variation in or modification of the terms of the Contract shall be made except by written amendment signed by the parties.

40. Sub-Contracts

40.1 The Supplier shall consult the Procuring Agency in the event of subcontracting under this contract if not already specified in the Bid. Subcontracting shall not alter the Supplier's obligations.

Special Conditions of Contract

SECTION VIII. SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the Conditions of Contract. The corresponding clause number of the GCC is indicated in parentheses.

Number of GC Clause

Amendments of, and Supplements to, Clauses in the General Conditions of Contract

Number of GC Clause 1

Definitions

The Procuring Agency is: **National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics) Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory**

The Supplier is:

The title of the subject procurement is: **Purchase of Licensed Enterprise Next-Generation Firewall (NGFW) with XDR**

Number of GC Clause 3

Applicable/Governing Law:

The Contract shall be interpreted in accordance with the laws of Islamic Republic of Pakistan

Number of GC Clause 4

Language:

The language of the Contract, all correspondence and communications to be given, and all other documentation to be prepared and supplied under the Contract shall be in **English.**

Number of GC Clause 5

Notices:

The addresses for the notices are:

The Authority:

National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics)
Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory
+92-303-506-7925
logbranch@gmail.com

Contractor/ Bidder:

[Name, address and telephone number].

The Contractor/ Bidder's Representative(s)

[Name, address, telephone number and e-mail address]

Number of GC Clause 7.1

The Authorized Representatives are:

For the Procuring Agency:

National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics)
Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory
+92-303-506-7925
logbranch@gmail.com

For the Bidder:

Name: ……

Designation: ……..

Address: ……..

Number of GC Clause 8

Effectiveness of the contract

Number of GC Clause 9

Commencement of Contract:

Number of GC Clause 11.2

Expiration of Contract:

Number of GC Clause 15

Termination

In the event of termination of the contract due to any reason as already defined in the General Conditions of Contract, the Bidder shall be responsible for providing to the Authority the Goods till the time of alternate arrangements.

Number of GC Clause 17

Conflict of Interest:

The Procuring Agency reserves the right to determine on a case-by-case basis whether the Bidder should be disqualified from providing goods or services due to a conflict of a nature described in Clause GCC 17**.**

Number of GC Clause 22

Liquidated Damages

If the Bidder fails to provide services as required under the contract or in case of any data loss/data breach or any incident compromising the data security or other such failures related to any services, the Bidder shall pay to the Procuring Agency as Liquidated Damages at a rate of **0.20%** to **10.00%** of the Contract value, in accordance with the extent of performance failure & the cost of investigating such incidents as judged by the Authority.

Number of GC Clause 23

Performance Guarantee:

Instrument of Performance Guarantee shall be in the Name of : **IG, National Highways & Motorway Police**

The amount of performance guarantee shall be **10.00%** of the contract price in acceptable form of **Pay Order, Banker's Cheque, Call at Deposit, Bank Guarantee, Demand Draft**

Number of GC Clause 32

Payment terms:

Payment will be made to the Bidder against the procured Goods and services according to the actual invoice or running bills submitted by the Bidder against the services provided within the time given in the conditions of the contract.

Number of GC Clause 33

Currency of Payment:

All the payment to be released to the contractor/Bidder shall be in Pakistani Rupees.

Number of GC Clause 34

Identifying Defects:

The Authority reserves the right at any time to inspect the premises of the provider to inspect the goods and monitor the goods being provided.

Inspections & Tests Requirements

For being Brand New, bearing relevant reference numbers of the equipment (Certificate from supplier)

For Physical Fitness having No Damages (Certificate from supplier)

For the Country of Origin as quoted by the Supplier (Certificate from manufacturer)

Solution must be endorsed from Pakistan Security Standard (PSS)

Delivery & Documents

Copies of the Supplier’s invoice showing Goods’ description, quantity, unit price, and total amount;

Original and two copies of the usual transport document (for example, a negotiable bill of lading, a non-negotiable sea waybill, an inland waterway document, an air waybill, a railway consignment note, a road consignment note, or a multimodal transport document) which the buyer may require to take the goods;

Copies of the packing list identifying contents of each package;

Insurance Certificate;

Manufacturer's or Supplier's Valid Warranty Certificate;

Inspection Certificate issued by the Nominated Inspection Agency (if any), and the Supplier's Factory Inspection Report;

Certificate of Origin.

The above documents would be required even if the equipment has already been imported and is available with the supplier ex-stock

Number of GC Clause 37

Following is the guidance for Dispute Resolution

(a) For Contracts to be entered with foreign Contractor/ Service Provider:

All disputes arising in connection with the present Contract shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with said Rules.

(b) For Contracts to be entered with nationals of Pakistan:

i. If any dispute of any kind whatsoever shall arise between the Authority and the Bidder in connection with or arising out of the Contract, including without prejudice to the generality of foregoing, any question regarding its existence, validity, termination and the execution of the Contract – whether during developing phase or after their completion and whether before or after the termination, abandonment or breach of the Contract – the parties shall seek to resolve any such dispute or difference by mutual diligent negotiations in good faith within 14 (fourteen) days following a notice sent by one Party to the other Party in this regard.

ii. At future of negotiation the dispute shall be resolved through mediation and mediator shall be appointed with the mutual consent of the both parties.

iii. At the event of failure of mediation to resolve the dispute relating to this contract such dispute shall finally be resolved through binding Arbitration in accordance with GCC clause 38.

iv. The cost of the mediation and arbitration shall be shared by the parties in equal proportion however the both parties shall bear their own costs and lawyer's fees regarding their own participation in the mediation and arbitration. However, the Arbitrator may make an award of costs upon the conclusion of the arbitration making any party to the dispute liable to pay the costs of another party to the dispute.
v. Arbitration proceedings as mentioned in the above clause regarding resolution of disputes may be commenced prior to, during or after completion of the contract.

Notwithstanding any reference to the arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree that the Authority shall pay the Bidder any monies due to the Bidder.

Rules of procedure for arbitration proceedings:

Any dispute between the Authority and a Bidder who is a national of the Islamic Republic of Pakistan arising in connection with the present Contract shall be referred to adjudication or arbitration in accordance with the laws of the Islamic Republic of Pakistan including Arbitration Act 1940, however above provision shall prevail in referring the case to the Arbitrator.

Place of Arbitration and Award:

The arbitration shall be conducted in English language and place of arbitration shall be at Islamabad. The award of the arbitrator shall be final and shall be binding on the parties.

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Bid Securing Declaration

Form 9: Bid Securing Declaration

Date: *[insert date (as day, month and year)]*

Bid No.:***P114196***

Alternative No.: **[insert identification No if this is a Bid for an alternative]**

To: **National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics) Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory**

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid Securing Declaration.

We accept that we will be blacklisted and henceforth cross debarred for participating in respective category of public procurement proceedings for a period of (not more than) six months, if fail to abide with a bid securing declaration, however without indulging in corrupt and fraudulent practices, if we are in breach of our obligation(s) under the Bid conditions, because we:

1. have withdrawn or modified our Bid during the period of Bid Validity specified in the Form of Bid;

2. Disagreement to arithmetical correction made to the Bid price; or

3. having been notified of the acceptance of our Bid by the Procuring Agency during the period of Bid Validity, (i) failure to sign the contract if required by Procuring Agency to do so or (ii) fail or refuse to furnish the Performance Security or to comply with any other condition precedent to signing the contract specified in the Bidding Documents.

We understand this Bid Securing Declaration shall expire if we are not the successful

Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight (28) days after the expiration of our Bid.

Signed: [insert signature of person whose name and capacity are shown] In the capacity of
[insert legal capacity of person signing the Bid Securing Declaration]

Name: [insert complete name of person signing the Bid Securing Declaration]

Duly authorized to sign the Bid for and on behalf of: [insert complete name of Bidder]

Dated on day of , [insert date of signing]
Corporate Seal (where appropriate)

Contract Form

SECTION IX: CONTRACT FORMS

THIS AGREEMENT made the _____ day of _____ 20_____ between **National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics) Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory**

(hereinafter called "the Procuring Agency") of the one part and *[name of Bidder]* of *[city and country of Bidder]* (hereinafter called "the Bidder") of the other part:

WHEREAS the Procuring Agency invited Bids for provision of goods, viz., **Purchase of Licensed Enterprise Next-Generation Firewall (NGFW) with XDR (*P114196*)** and has accepted a Bids by the Bidder for the provision of Goods in the sum of *[contract price in words and figures]* (hereinafter called "the Contract Price").

NOW THIS CONTRACT WITNESSETH AS FOLLOWS:

1. In this Contract 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 Contract, In the event of any ambiguity or conflict between the Contract Documents listed below, the order of precedence shall be the order in which the Contract Documents are listed below:-

1. This form of Contract;
2. the Form of Bids and the Price Schedule submitted by the Bidder;
3. the Schedule of Requirements;
4. the Technical Specifications;
5. the Special Conditions of Contract;
6. the General Conditions of the Contract;
7. the Procuring Agency's Letter of Acceptance; and
8. [*add here: any other documents*]

3. In consideration of the payments to be made by the Procuring Agency to the Bidder as hereinafter mentioned, the Bidder hereby covenants with the Procuring Agency to provide the Goods related services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Procuring Agency hereby covenants to pay the Bidder in consideration of the provision of Goods and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

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

Signed, sealed, delivered by _____the _____ (for the Procuring Agency)

Witness to the signatures of the Procuring Agency:

……

Signed, sealed, delivered by _____the _____ (for the Procuring Agency)

Witness to the signatures of the Bidder: ……

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Integrity Pact

Integrity Pact

DECLARATION OF FEES, COMMISSION AND BROKERAGE ETC. PAYABLE BYTHE SUPPLIERS OF GOODS, SERVICES & WORKS IN CONTRACTS WORTH RS.10.00 MILLION OR MORE

Contract Number: Contract Value: Contract Title:

Dated:

[Name of Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing [Name of Supplier] represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[Name of Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

[Name of Supplier] accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [Name of Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by [Name of Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

Performance Guarantee Form

Performance Guarantee Form

To: **National Highways & Motorway Police (National Highways & Motorway Police (NHMP)), Assistant Director (Logistics) Plot no. 29 & 48, Street no. 01, NHMP Central police Office, Mauve Area, G-11/1, Islamabad Capital Territory**

WHEREAS *[name of Bidder]* (hereinafter called "the Bidder") has undertaken, in pursuance of Contract No. *[reference number of the contract]* dated *[insert date]* for provision of Goods*(*hereinafter called "the Contract").

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

AND WHEREAS we have agreed to give the Bidders guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Bidder, 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 Bidder 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: *[insert date]*

Signature and seal of the Guarantors

_____

[name of bank or financial institution]

_____

[address]

_____

[date}

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Annexure

Request for Proposal

1. **INVITATION FOR BIDS**

National Highways & Motorway Police (NHMP) invites sealed proposals from reputed, financially sound and technically competent firms/authorized partners for the supply, installation, configuration, integration, testing, commissioning and three-year support of an Enterprise Next-Generation Firewall (NGFW) solution, including associated security licenses, VPN licenses, SFP+ modules, Extended Detection & Response (XDR) licenses and other accessories as specified in this RFP.

The proposed solution shall provide enterprise-grade network security, threat prevention, secure remote access, application visibility and control, SSL/TLS inspection, web/content filtering, VPN, logging, reporting, high availability, integration with the existing NHMP IT infrastructure and scalable with future expansion.

The procurement shall be made in accordance with applicable Government procurement rules and NHMP procurement procedures.

1. **OBJECTIVE OF THE PROCUREMENT**

The objective of this procurement is to establish a robust, enterprise-grade perimeter and network security infrastructure for NHMP capable of:

1. Protecting NHMP's critical IT infrastructure, applications, servers and network resources from cyber threats
2. Providing Next-Generation Firewall (NGFW) functionality with integrated IPS, anti-malware/antivirus, application control and URL/content filtering
3. Providing secure remote-access and site-to-site VPN capabilities
4. Providing SSL/TLS encrypted traffic inspection
5. Supporting high availability, stateful failover and redundant power
6. Providing centralized monitoring, logging, reporting and security visibility
7. Supporting integration with existing network, Active Directory/NMS/Syslog and endpoint security infrastructure
8. Supporting future network expansion and higher bandwidth requirements
9. Providing a scalable and centrally manageable security platform for NHMP

1. **SCOPE OF WORK**

The successful bidder shall be responsible for the complete supply and implementation of the proposed solution, including but not limited to:

1.

1.1. **Supply**

The bidder shall supply:

1. Enterprise Next-Generation Firewall appliance
2. Required security subscriptions and licenses
3. Secure Remote Access VPN licenses
4. Extended Detection & Response (XDR) licenses
5. SFP+ modules
6. Rack mounting accessories
7. Redundant power supply modules
8. All required cables, accessories, transceivers and mounting hardware
9. Any other component required for complete and operational deployment

3.2 Installation and Configuration

The successful bidder shall:

1. Install the firewall at NHMP's designated server room
2. Rack-mount and physically install the appliance
3. Configure interfaces, VLANs, routing, security zones and policies
4. Configure NAT, access-control policies and application control
5. Configure IPS, anti-malware, URL filtering and other security services
6. Configure SSL/TLS inspection in accordance with NHMP requirements
7. Configure VPN services
8. Configure logging, monitoring and reporting
9. Configure integration with Active Directory and other approved authentication services
10. Configure Syslog/SNMP/NMS integration
11. Configure high-availability and stateful failover functionality as applicable and when required
12. Integrate the solution with the existing NHMP network infrastructure
13. Carry out testing and commissioning

3.3 Migration and Integration

The successful bidder shall ensure migration of existing firewall/network security policies and shall ensure minimum disruption to NHMP operations.

The bidder shall prepare an implementation & migration plan, obtain prior approval from NHMP competent authority before making changes to the production environment.

3.4 Testing and Commissioning

The bidder shall conduct comprehensive testing covering:

1. Firewall throughput
2. Threat protection
3. IPS functionality
4. SSL/TLS inspection
5. VPN connectivity
6. Application control
7. URL/content filtering
8. Failover and recovery
9. Routing
10. VLAN connectivity
11. Logging and reporting
12. Authentication and Multi Factor Authentication
13. Network management integration
14. Security policy enforcement

A formal User Acceptance/Commissioning Test shall be conducted before final acceptance.

4. OPERATIONAL REQUIREMENTS

The proposed solution shall be capable of operating as the primary enterprise security gateway for NHMP's Central Police Office/data-centre environment.

The solution shall:

1. Support 24/7 operation
2. Provide centralized policy and security management
3. Provide real-time threat detection and prevention
4. Support secure segmentation of network traffic
5. Support application-aware security policies
6. Provide visibility into users, applications, traffic and threats

7. Provide secure remote access for authorized personnel
8. Support integration with existing network infrastructure
9. Provide detailed logs for security monitoring and forensic analysis
10. Support future expansion without requiring immediate replacement of the appliance

Information (Read-Only)

See Form Under Additional Forms and Documents: **Request for Proposal** (page number: 96)

Financial Annexure

Financial Annexure must be filled as per format for a bid to be considered.

Financial Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Financial Annexure** (page number: 114)

Procurement Forms

PUBLIC PROCUREMENT REGULATORY AUTHORITY
(PPRA)
EPADS

PUBLIC PROCUREMENT REGULATORY AUTHORITY
(PPRA)
EPADS

Additional Forms and Documents

National Highways & Motorway Police
Central Police Office, G-11/1, Islamabad

REQUEST FOR PROPOSAL (RFP)
ENTERPRISE NEXT-GENERATION FIREWALL
Procurement, Installation, Configuration, Integration and Support of Enterprise Next-Generation Firewall (NGFW)

1. INVITATION FOR BIDS

National Highways & Motorway Police (NHMP) invites sealed proposals from reputed, financially sound and technically competent firms/authorized partners for the supply, installation, configuration, integration, testing, commissioning and three-year support of an Enterprise Next-Generation Firewall (NGFW) solution, including associated security licenses, VPN licenses, SFP+ modules, Extended Detection & Response (XDR) licenses and other accessories as specified in this RFP.

The proposed solution shall provide enterprise-grade network security, threat prevention, secure remote access, application visibility and control, SSL/TLS inspection, web/content filtering, VPN, logging, reporting, high availability and integration with the existing NHMP IT infrastructure.

The procurement shall be made in accordance with applicable Government procurement rules and NHMP procurement procedures.

2. OBJECTIVE OF THE PROCUREMENT

The objective of this procurement is to establish a robust, enterprise-grade perimeter and network security infrastructure for NHMP capable of:

1. Protecting NHMP's critical IT infrastructure, applications, servers and network resources from cyber threats.
2. Providing Next-Generation Firewall (NGFW) functionality with integrated IPS, anti-malware/antivirus, application control and URL/content filtering.
3. Providing secure remote-access and site-to-site VPN capabilities.
4. Providing SSL/TLS encrypted traffic inspection.
5. Supporting high availability, stateful failover and redundant power.
6. Providing centralized monitoring, logging, reporting and security visibility.
7. Supporting integration with existing network, Active Directory/NMS/Syslog and

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

endpoint security infrastructure.

8. Supporting future network expansion and higher bandwidth requirements.
9. Providing a scalable and centrally manageable security platform for NHMP.

3. SCOPE OF WORK

The successful bidder shall be responsible for the complete supply and implementation of the proposed solution, including but not limited to:

3.1. Supply

The bidder shall supply:

1. Enterprise Next-Generation Firewall appliance.
2. Required security subscriptions and licenses.
3. Secure Remote Access VPN licenses.
4. Extended Detection & Response (XDR) licenses.
5. SFP+ modules.
6. Rack mounting accessories.
7. Redundant power supply modules.
8. All required cables, accessories, transceivers and mounting hardware.
9. Any other component required for complete and operational deployment.

3.2 Installation and Configuration

The successful bidder shall:

1. Install the firewall at NHMP's designated server room.
2. Rack-mount and physically install the appliance.
3. Configure interfaces, VLANs, routing, security zones and policies.
4. Configure NAT, access-control policies and application control.
5. Configure IPS, anti-malware, URL filtering and other security services.
6. Configure SSL/TLS inspection in accordance with NHMP requirements.
7. Configure VPN services.
8. Configure logging, monitoring and reporting.
9. Configure integration with Active Directory and other approved authentication services.
10. Configure Syslog/SNMP/NMS integration.
11. Configure high-availability and stateful failover functionality as applicable and when required.

12. Integrate the solution with the existing NHMP network infrastructure.
13. Carry out testing and commissioning.

3.3 Migration and Integration

The successful bidder shall ensure migration of existing firewall/network security policies and shall ensure minimum disruption to NHMP operations.

The bidder shall prepare an implementation & migration plan, obtain prior approval from NHMP competent authority before making changes to the production environment.

3.4 Testing and Commissioning

The bidder shall conduct comprehensive testing covering:

1. Firewall throughput.
2. Threat protection.
3. IPS functionality.
4. SSL/TLS inspection.
5. VPN connectivity.
6. Application control.
7. URL/content filtering.
8. Failover and recovery.
9. Routing.
10. VLAN connectivity.
11. Logging and reporting.
12. Authentication and Multi Factor Authentication.
13. Network management integration.
14. Security policy enforcement.

A formal User Acceptance/Commissioning Test shall be conducted before final acceptance.

4. OPERATIONAL REQUIREMENTS

The proposed solution shall be capable of operating as the primary enterprise security gateway for NHMP's Central Police Office/data-centre environment.

The solution shall:

1. Support 24/7 operation.
2. Provide centralized policy and security management.
3. Provide real-time threat detection and prevention.
4. Support secure segmentation of network traffic.

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

5. Support application-aware security policies.
6. Provide visibility into users, applications, traffic and threats.
7. Provide secure remote access for authorized personnel.
8. Support integration with existing network infrastructure.
9. Provide detailed logs for security monitoring and forensic analysis.
10. Support future expansion without requiring immediate replacement of the appliance.

5. MINIMUM TECHNICAL SPECIFICATIONS

Annexure A and B as Turnkey lot

The offered firewall shall meet or exceed the following minimum specifications.

Sr.	Item Code	Item Description	Qty	Specification	
1	NGFW	Next Generation Firewall with 3 years support and subscription	1	Annexure A	Turnkey Lot
2	XDR	Extended Detection and Response (XDR) with 3 years license	200	Annexure B	

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Specification

Next Generation Firewall - Solution

Technical Specifications

A. General Requirements

1. The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 5 years.
2. The proposed NGFW should be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA and NEBS certified.
3. The proposed NGFW should require no reboot for checking and installing security updates.
4. The proposed NGFW should have integrated reporting capabilities requiring no additional hardware to generate reports.
5. The proposed NGFW should identify applications regardless of port, SSL/SSH encryption, or evasive techniques employed.
6. The proposed NGFW should categorize unidentified applications for policy control, threat forensics, or application identification technology development.
7. The proposed NGFW should be a natively engineered security solution (Not an application control blade with underlying stateful inspection firewall).
8. The proposed NGFW should be a natively engineered appliance with a single-pass parallel processing architecture for traffic processing.
9. The proposed NGFW should have integrated traffic shaping functionality (QoS) based on source/destination IP, port, protocol and application.
10. The proposed NGFW must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability.
11. The proposed NGFW should control access and enforce policies for websites and applications, including SaaS applications.
12. The proposed NGFW should have a single OS across all form factors.
13. The proposed NGFW should support creating security policies to prevent credential theft.
14. The proposed NGFW should support enforcing multi-factor authentication to internal applications.
15. The proposed NGFW should support an unfettered open API without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples.

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

16. The proposed NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.
17. The proposed NGFW must provide visibility and the ability to restrict applications using non-standard ports in a single security policy rule
18. The proposed NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy
19. The proposed NGFW must be able to provide Machine Learning algorithms for advanced protections directly from the NGFW with no external connections needed
20. The proposed NGFW should grant easy OS updates without the need of certain combinations for hotfixes or patches to be in place
21. The proposed NGFW should have a feature of holding multiple OS images to support resilience and easy roll-backs during the version upgrades
22. The proposed NGFW should support enabling any new security offering without impacting the performance of the traffic flowing through it
23. The proposed NGFW should have a feature of identifying what applications are hitting the security policies and migrating these policies into application based policies

B. Architecture, Physical & Performance Specifications

1. The proposed NGFW should deliver 8.5Gbps of documented firewall throughput
   (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions)
2. The proposed NGFW should deliver minimum of 4.2Gbps of documented threat prevention throughput (Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, DNS Security, file blocking and logging enabled, utilizing 64 KB HTTP/appmix transactions)
3. The proposed NGFW should deliver minimum of 4.1Gbps or above of IPsec VPN throughput
   (IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled)
4. The proposed NGFW should support 0.94 Million Max sessions
5. The proposed NGFW should support 100,000 new connections per second (measured with application-override utilizing 1byte HTTP transactions)
6. The proposed NGFW should support the addition of virtual systems for future

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

expansion

7. The proposed NGFW must support minimum of 8 x 1Gigabit Ethernet (RJ45) interfaces, 6 x 1G SFP interface, 4 x 10G SFP+ interfaces.
8. The proposed NGFW should support (1) 10/100/1000 out-of-band management port, (1) 10/100/1000 high availability, (1) 1 Console port, (1) USB Port, Mini USB.
9. The proposed NGFW should offer redundant AC power supplies
10. The proposed NGFW should support Active/Active, Active/ Passive & Clustering deployments
11. The proposed NGFW should support state full session maintenance in the event of a fail-over to a standby unit
12. The proposed NGFW should support the High Availability feature for either NAT/Route or transparent mode
13. The proposed NGFW should support multiple heartbeat links
14. The proposed NGFW should support L3, L2, transparent and tap mode deployments

C. Security Policy Control features

1. The proposed NGFW should support creating security policies based on Layer 7 applications irrelevant to the TCP/UDP port number (non-profile-based application control)
2. The proposed NGFW should support the management of unknown traffic (unidentified applications) through security policies
3. The proposed NGFW should have a built-in security policies optimization tool which facilitates converting legacy Layer 4 port-based security policies to Layer 7 application-based ones
4. The proposed NGFW should support enforcing security policies based on a schedule
5. The proposed NGFW should simplify rule use tracking via a timestamp for the most recent rule match, a timestamp for the first rule match, and a rule hit counter

D. Advanced Threat Prevention Features

1. The proposed NGFW should protect networks by providing multiple layers of prevention, confronting threats at each phase of an attack.
2. The proposed NGFW should detect and block threats on any and all ports instead of invoking signatures based on a limited set of predefined ports.
3. The proposed NGFW should benefit from other cloud-delivered security subscriptions for daily updates that stops exploits, malware, malicious URLs,

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

command and control (C2), and spyware.

4. The proposed NGFW should provide protections against unknown threats instantly by embedding ML in the core of the firewall to provide inline signature-less attack prevention.
5. The proposed NGFW should utilize Inline malware protection—through signatures based on payload, not hash.
6. The proposed NGFW should continuously collect telemetry to enable data-intensive ML processes to automatically compute and recommend policy changes.
7. The proposed NGFW should use cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
8. The proposed NGFW should leverage heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
9. The proposed NGFW should support creating custom signatures, which allows tailoring intrusion prevention capabilities to a network's unique needs.
10. The proposed NGFW should support other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques.
11. The proposed NGFW should employ natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it.
12. The proposed NGFW should inspect and classify traffic as well as detect and block both malware and vulnerability exploits in a single pass.
13. The proposed NGFW should comb each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload.
14. The proposed NGFW should analyze the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques.
15. The proposed NGFW should support protocol decoder-based analysis.
16. The proposed NGFW should provide protocol anomaly-based protection.
17. The proposed NGFW should leverage inline, stream-based detection and prevention of malware hidden within compressed files and web content.
18. The proposed NGFW should provide protections against payloads hidden within common file types, such as Office/Microsoft 365 documents and PDFs.
19. The proposed NGFW should enable the correlation of a series of related threat events (e.g., from Threat Prevention logs) that, when combined, indicate a likely attack.
20. The proposed NGFW should have an option of configuring exception.
21. The proposed NGFW should be able to detect & prevent the malware by scanning

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

different file types.

22. The proposed NGFW should be able to identify malwares coming from incoming files and malwares downloaded from Internet.
23. The proposed NGFW should provide an option to create custom signature for applications.
24. The proposed NGFW should have all major applications signatures and it should able to understand well known application like P2P and voice without any dependency on the port.
25. The proposed NGFW should enforce inline deep learning for real-time enforcement for new and unknown command and control.
26. The proposed NGFW machine learning and deep learning models should be aligned to key protocols, such as SSL, HTTP, unknown UDP, and unknown TCP.
27. The proposed NGFW should use ML-based analysis to identify advanced DNS-based threats.
28. The proposed NGFW should utilize a cloud-based database which contains tens of millions of known malicious domains, enabling the blocking of phishing, malware, and other high-risk categories.
29. The proposed NGFW should provide threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time.
30. The proposed NGFW should enable forging a response to a DNS query for a known malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client to identify infected hosts.
31. The proposed NGFW should allow defining separate policy actions as well as a log severity level for a specific signature type.
32. The proposed NGFW should identify the use of DGAs, which generates random domains on the fly for malware to use as a way to call back to a C2 server.
33. The proposed NGFW should identify DGA (Domain Generation Algorithms) domains based on dictionary words.
34. The proposed NGFW should prevent the use of DNS tunneling, which exploits the DNS protocol to tunnel malware and other data through a client-server model.
35. The proposed NGFW should disrupt ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.
36. The proposed NGFW should leverage predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

37. The proposed NGFW should prevent fast flux domains.
38. The proposed NGFW should protect against domains surreptitiously added to hacked DNS zones of reputable domains.
39. The proposed NGFW should prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.
40. The proposed NGFW should prevent dangling DNS attacks.
41. The proposed NGFW should prevent attackers from directing users to malicious domains with the use of a wildcard DNS record.
42. The proposed NGFW should prevent techniques that exploit DNS protocol to tunnel malicious payloads into networks.
43. The proposed NGFW should protect users from connecting to domains that can be used to launch DDoS attacks.
44. The proposed NGFW should support traffic static analysis.
45. The proposed NGFW should support traffic dynamic analysis.
46. The proposed NGFW should support advanced file analysis with URL crawling to prevent multistage, multi hop attacks.
47. The proposed NGFW analysis environment should replicate macOS, Android, Windows XP/7/10, and Linux.
48. The proposed NGFW file analysis should support PE files (EXE, DLL, and others), all Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files.
49. The proposed NGFW support protocols should be SMTP, POP3, SMB, FTP, IMAP, HTTP, and HTTPS.
50. The proposed NGFW should generate signatures based on the malware payload of the sample and tested for accuracy and safety.
51. The proposed NGFW should provide protection updates for unknown malware within seconds.

E. Advanced URL Filtering

1. The proposed NGFW should possess a patented inline real-time web threat prevention capability which uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time
2. The proposed NGFW machine-learning models should get retrained frequently, ensuring protection against new and evolving never before-seen threats (e.g.,

phishing, exploits, fraud, C2)

3. The proposed NGFW should protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding
4. The proposed NGFW URL database should maintain hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis
5. The proposed NGFW should be allow classifying websites based on site content, features, and safety, and includes more than 70 benign and malicious content categories
6. The proposed NGFW should support risk rating which scores URLs on a variety of factors to determine risk
7. The proposed NGFW should have multi-category support which categorizes a URL with up to four categories, allowing for flexible policy and the creation of custom categories
8. The proposed NGFW should detect and prevent credential theft by controlling sites to which users can submit corporate credentials based on the site's URL category
9. The proposed NGFW should se ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts
10. The proposed NGFW allow designating multiple policy action types based on URL categories or criteria
11. The proposed NGFW should apply URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies
12. The proposed NGFW should apply URL filtering policies when end users attempt to view the cached results of web searches and internet archives
13. The proposed NGFW should prevent inappropriate content from appearing in users' search results
14. The proposed NGFW should enable administrators to notify users of a violation using a custom block page
15. The proposed NGFW should support crawling and analysis in 41 languages

F. User Identification & Authentication Features

1. The proposed NGFW should support identifying user-id by integrating with Active Directory through WinRM and WMI
2. The proposed NGFW should support identifying user-id by integrating with Exchange through WinRM and WMI

3. The proposed NGFW should support identifying user-id by running as sy slog receiver
4. The proposed NGFW should support identifying user-id by Integrating through XML APIs with Third Party solutions
5. The proposed NGFW should support identifying user-id through captive portal
6. The proposed NGFW should support Identifying user-id in terminal servers
7. The proposed NGFW should support identifying user-id by running an agent at user machines
8. The proposed NGFW should have direct Multi-Factor Authentication integration with RSA, Okta, PingID and Duo
9. The proposed NGFW should support SSO authentication
10. The proposed NGFW should support multiple server profiles like SAML 2.0, Radius, LDAP, Tacacs+, and Kerberos.

G. Advanced Mobility & Host Information Profiling Features

1. The proposed NGFW should offer a remote user VPN agent for Windows, MAC, Linux, Chrome, iOS, and Android
2. The proposed NGFW should support app-Level VPN for iOS and Android devices
3. The proposed NGFW should have support portal based and clientless SSL VPN
4. The proposed NGFW should support MFA
5. The proposed NGFW should offer a host information check feature by collecting & reporting device information & attributes.
   Host Information Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and Plist presence & status
6. The proposed NGFW should support enforcing security policies based on device/host information profiles
7. The proposed NGFW should support the integration with Third Party MDM solutions like AirWatch or MobileIron
8. The proposed NGFW should support split tunneling based on IP addresses, domains and applications
9. The proposed NGFW should support VPN authentication override using cookies
10. The proposed NGFW should support the exclusion of video traffic from main remote

user VPN tunnel

11. The proposed NGFW should support trusted root certificates push to remote VPN user devices to help enable features like SSL offload
12. The proposed NGFW should support VPN gateway selection criteria based on source user-id, region, OS and IP address

H. Management, Logging & Reporting Features

1. The proposed NGFW should offer a Command Line Interface (CLI).
2. The proposed NGFW should offer a built-in web interface, non Java base (GUI).
3. The proposed NGFW should support XML Rest API based management.
4. The proposed NGFW should have a commit-based configuration management.
5. The proposed NGFW should support config-audit by comparing running config against candidate config.
6. The proposed NGFW should offer an interactive graphical summary around the applications, users, URLs, threats, and content traversing the network.
7. The proposed NGFW should offer a customized graph-based network activity for applications using non-standard ports.
8. The proposed NGFW should offer a customized graph-based blocked activities which includes blocked applications activity, blocked users activity, blocked content activity, blocked threats activity, and security policies blocking activity.
9. The proposed NGFW should offer a customized graph-based tunnel activities including tunnel ID/Tag, tunnel application usage, tunnel user activity, and tunnel ip source/destination activity.
10. The proposed NGFW should support custom reporting with the ability to generate a report per user, user group and application.
11. The proposed NGFW should support exporting reports to PDF and sending reports by email.
12. The proposed NGFW should have a dedicated SaaS applications usage report.
13. The proposed NGFW should have dedicated log sets for traffic, threats, URL filtering, data filtering, file control, user id mapping, authentication, configuration, system and alarms.
14. The proposed NGFW should support custom admin roles.
15. The proposed NGFW should allow administrators to work directly on the appliance, and make configuration changes as needed, without having to log in to a central manager.
16. The proposed NGFW should allow central administrators to monitor and view the changes made by local administrators.

17. The proposed NGFW management should be done directly through the appliance without the need of installing any clients or virtual machines.
18. The proposed NGFW should offer the ability to choose which firewall administrator's configuration changes to be committed on the firewalls.
19. The proposed NGFW should offer the ability to quickly roll back changes from specific users and restore configurations.
20. Solution must be endorsed from Pakistan Security Standard.
21. Three (03) years license:
    i. Threat prevention subscription.
    ii. Sandboxing subscription.
    iii. Advanced URL Filtering Subscription.
    iv. DNS Security subscription.
    v. SD-WAN Subscription

PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA) EPADS

Annexure B

Specification

XDR - Solution

Requirements

1.	**Next-Generation Antivirus Requirements**	
	Should be able to perform/have following capabilities	
	a.	Machine learning-based local analysis and threat prevention
	b.	Behavior-based threat prevention for dynamic analysis of running processes
	c.	Exploit prevention by exploit technique
	d.	Known threat prevention based on threat intelligence, such as file hashes
	e.	Automated integration with a cloud-based malware prevention service, with analysis reports
	f.	Zero-delay signatures to rapidly deliver protection and share threat intelligence
	g.	Transparent threat detection engine updates
	h.	Security profiles and exceptions
	i.	Ad hoc and scheduled scanning of endpoints
	j.	Protection against malware, ransomware and file-less attacks
	k.	Single lightweight agent for endpoint protection, detection and response
2.	**Endpoint Protection Requirements**	
	Should have the following features	
	a.	Host firewall
	b.	Disk Encryption
	c.	Device Control
	d.	Customizable prevention rules
3.	**Investigation Requirements**	
	Should have following capabilities	
	a.	Visualization of the chains of execution leading up to an alert
	b.	Timeline analysis view to see all actions and alerts on a timeline
	c.	Querying for indicators of compromise (IOCs), Behavioral IOCs (BIOC) and endpoint behaviors
	d.	Advanced querying language for visualization of data
	e.	In-context wizard that lets you search for information, perform common investigation tasks, or initiate response actions from anywhere in the management console
	f.	Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations
4.	**Incident Management Requirements**	
	Should have the following capabilities	
	a.	Automated grouping of related alerts from various sources into a single incident
	b.	Listing of notable artifacts from alerts and their threat intelligence information
	c.	Listing of user and hosts involved in incidents to quickly determine the scope of an incident

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

	d.	End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.)	
	e.	Ability to change the severity of an incident	
5.	**Threat Intelligence Requirements**		
	Should have the following capabilities		
	a.	Ability to alert on known malicious objects on endpoints with IOC rules	
	b.	IOC creation from the management console	
	c.	Ability to import multiple IOCs from a CSV file using the management console	
	d.	Configurable severity level of an IOC	
6.	**Response Requirements**		
	Should have the following capabilities		
	a.	Remote terminal capability	
	b.	Full CMD, PowerShell, and Python commands and scripts on Windows 7, 8,10 and Windows 11	
	c.	Full Bash and Python commands on macOS and Linux	
	d.	Ability to execute custom Python scripts across multiple endpoints simultaneously on Windows, macOS, and Linux	
	e.	Remote isolation of a single endpoint or multiple endpoints	
	f.	Remote file deletion of a single endpoint or multiple endpoints	
	g.	Automatic and manual collection or retrieval of quarantined files and objects	
	h.	Ability to view, suspend, or terminate running processes or download binaries with a graphical task manager for Windows, macOS, and Linux	
	i.	Graphical file manager with ability to view, download, rename, or move files for Windows, macOS, and Linux	
	j.	Search and destroy to swiftly sweep across endpoint and eradicate threats	
	k.	Integration with a security orchestration, automation, and response (SOAR) solution for incident analysis	
	l.	Integration with security information and event management (SIEM) solutions	
7.	**Visibility and Detection Requirements**		
	Should have the following capabilities		
	a.	Supervised and unsupervised machine learning capabilities	
	b.	Predefined and customizable behavior-based detection rules	
	c.	Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services	
	d.	Ability to consume threat intelligence feeds from third-party sources	
	e.	Detection of attack techniques across the attack lifecycle including discovery, lateral movement, command and control, and exfiltration	
	f.	Demonstrated ability to detect attacker tactics and techniques through MITRE ATT&CK Evaluations	
	g.	Tagging of MITRE ATT&CK tactics and techniques in alerts and detection rules	
8.	**Data Collection Requirements**		
	a.	**User information**	
		(1)	Domain and distinguished name
		(2)	Email address

		(3)	Organizational unit
		(4)	Logged-in user
		(5)	Typical user of a machine
		(6)	User creating the process that initiated communication
		(7)	User group and organizational unit from directory services
	b.	**Device information**	
		(1)	MAC address
		(2)	Hostname of device
		(3)	Domain name
		(4)	Distinguished name of host
		(5)	Organizational unit
		(6)	Operating system and version
	c.	**Process information**	
		(1)	Process timestamp
		(2)	Path and name
		(3)	Process ID
		(4)	Loaded modules
		(5)	Hash values, such as MD5 and SHA-256
		(6)	Command line arguments
		(7)	RPC requests and code injection data, if applicable
		(8)	Signature state
	d.	**File information for file create, write, access, open, rename, or delete**	
		(1)	Timestamp
		(2)	Path and name
		(3)	Previous file name and path for file rename events
		(4)	Hash values, such as MD5 and SHA-256
		(5)	Username
	e.	**Network activity, including outgoing connections, failed connections, and incoming connections**	
		(1)	Timestamp
		(2)	Source IP address, destination IP address, source port, and destination port
		(3)	Bytes sent and received
		(4)	Protocol
		(5)	Geolocation data
		(6)	Connection duration
	f.	**Registry activities, such as create key, modify key, delete key, and rename key**	
		(1)	Timestamp
		(2)	Key name
		(3)	Value and type
		(4)	Previous key name for rename events
	g.	**System events**	
		(1)	User status change event, such as login and logout
		(2)	Host status change event
		(3)	Agent status change event
	h.	**Security alerts**	
		(1)	Endpoint threat logs

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026

	h.	Granular control of agent controls and notifications, including tray icon visibility, custom end user notifications, and the option to restrict response options such as remote terminal access
10.	**Deployment, Management and Security**	
	a.	Scalable, cloud-based management and agent deployment
	b.	Single, web-based management console for endpoint security as well as extended detection and response
	c.	Role-based access control (RBAC) for granular permissions
	d.	Multi-factor authentication (MFA) for management
	e.	Ability to fetch required data from the entire database using scripts
11.	**Data Retention and Coverage Requirements**	
	a.	Detection and response for threats involving managed and unmanaged endpoints
	b.	Detection and response for threats involving remote users
	c.	Continuous collection and centralized storage of all security data for behavioral analytics
	d.	Data retention of 180 days
	e.	Optional retention of data for an unlimited length of time
12.	**License Requirements**	
	a.	200 licenses required for endpoints on site deployment
	b.	3 years license & support
	c.	Solution must be endorsed from Pakistan Security Standard (PSS)

PUBLIC PROCUREMENT REGULATORY AUTHORITY PPRA EPADS

FINANCIAL ANNEXURE

Breakup of Financial Quotation for the Proposed Solution

Sr.	Item Code	Item Description	Qty	Price (inclusive of all Taxes) in PKR		
				Unit	Total	Lot
1	NGFW	Next Generation Firewall with 3 years support, subscription and Licenses including all accessories and allied services	1			
2	XDR	Extended Detection and Response (XDR) with 3 years license including all allied services	200			

e-Pak Acquisition and Disposal System (EPADS) generated document | © 2026