No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

TENDER DOCUMENT

"UPGRADATION OF IT INFRASTRUCTURE"

FOR

FEDERAL MEDICAL COLLEGE

FY – 2025-26

MINISTRY OF NHSR&C
GOVT. OF PAKISTAN, ISLAMABAD
051-9107724-5

Federal Medical & Dental College, Islamabad
Procurement Section

No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

TENDER NOTICE

Federal Medical College (FMC) invites sealed bids from reputed firms / suppliers / distributer of similar works / assignments and registered with FBR for **"Upgradation of IT Infrastructure"** for Financial Year 2025-26

1. The procurement shall be completed in according with the Public Procurement Rules.

2. All the firms / bidders should submit proposals as per Rule 36 (a) of PPRA Rules, 2004 **(Single Stage Two Envelope Procedure).** Technical Bids will be opened in the presence of bidders and committee members.

3. The tender documents containing detailed information, terms and conditions etc. can be obtained from the undersign on written request along with PKR 5,000 cash.

4. 2% of the bid will be deposited as bid Security in shape of pay order in favor of Federal Medical College, Islamabad which in case of unsuccessful tenders will be released and in case of successful bidders after satisfactory completion of work.

5. The sealed bids /proposals containing (Separate Financial and Technical Bids) will be received before or latest by **12th May, 2026** at **11:00AM** . The technical bid will be opened on the same day at **11:30AM** in the Conference Room of Federal Medical College, in the presence of available bidders or their representatives. After the evaluation of Technical Bids the Financial Bids of technically qualified bidders will be opened.

6. Federal Medical College reserves the right to accept / cancel / reject any or all proposals, as per Rule 33 of PPRA Rules, 2004.

Principal
Federal Medical College

Federal Medical & Dental College, Islamabad
Procurement Section

No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

TABLE OF CONTENTS

Contents

Federal Medical & Dental College, Islamabad
Procurement Section

1. Scope of Work

i) Hardware / software etc installation, configuration and support services will be solely responsibility of the vendor.
ii) Software bidder will be responsible for the installation, configuration and support services.
iii) **In case of any discrepancy** or less items bid will be rejected. Compliance / Checklist sheet with the technical specification must be attached with the Technical proposal.
iv) Product Support Services must be within 24 hours hardware replacement under warranty period as described in detailed specifications.
v) In case of failure or malfunctioning of hardware equipment / component, a free replacement and installation of the device / part will be the responsibility of the vendor and on exchange basis as Free of Cost (FOC) under warranty.
vi) Technical Support services should include resolution of complaints related to equipment.
vii) The drivers / applications support CD / media must be provided for hardware equipment compatible with the OS respectively (if any)
viii) Hardware devices having end of life must be communicated, moreover, nearly end of life hardware devices will not be acceptable.
ix) Vender will be responsible for all types of IT equipment being delivered.
x) 24 x 7 availability of hotline.

Note: *Vendor is solely responsible to provide the support services for the offered product even the support for the same product would have been discontinued by the OEM*

TERMS, CONDITIONS AND INSTRUCTIONS FOR THE BIDDERS
1. (Please Read Carefully)

2.1. Documents Required

i. Company profile with list of its recent clients.
ii. Copy of NTN Certificate of the firm.
iii. Copy of Active Sales Tax Registration Certificate of the firm.
iv. Bid Security 2% of quoted price in the shape of Bank Draft/Pay Order bearing No. ...., Date .... & Rs. ....
v. Compliance sheet for offered product.
vi. Official Authorized Partnership Certificate from sole manufacture along with Product Broachers for ICT infrastructure and IT Equipment.
vii. Proof of after sale Service Centre located in Islamabad / Rawalpindi.

2.2. Opening of Competitive Bids

i. All the firms/ bidders should submit proposals as per Rule 36 (b) of PPR 2004 (**Single Stage – Two Envelope Procedure**)
ii. Bids are required to be submitted lot wise; clearly indicating rates in Pak Rupees and should be valid for 90 days.

2.3. Rejection of the Bid

i. Any offer not compliant with the terms & conditions of the tender enquiry is liable to be rejected under provision of PPRA Rules-2004.
ii. Any offer will not be entertained if:
  - Firm/bidder is black listed/suspended by any Government department.
  - Offer with shorter price/delivery validity than required in the tender enquiry.

Federal Medical & Dental College, Islamabad
Procurement Section

- Not compliant with the required specifications, terms & conditions.
- Bid submission after the time and date fixed for its receipt.
- Received without earnest money.
- Tender is received by telegram.
- Tender/offer is un-signed.
- Offer is ambiguous.
- Offer is conditional.
- Bid offering less items as defined in LOT
- Federal Medical College further reserves the right to accept or reject any or all tender(s) without assigning any reason.

2.4. *Performance Guarantee*

i. The qualified bidder / firm will be required to furnish 2% performance guarantee of the total amount of supply order in the shape of CDR / Bank Guarantee / Insurance Guarantee, and released after satisfactory completion of the warranty / guarantee period. The Earnest money will be released upon receipt of performance guarantee, In addition, earnest money can also be retained as a performance guarantee, if vendor desires.

ii. In case, if supplier / contractor fails to complete the given assignment within specified timeframe, the performance guarantee / security deposit will be forfeited.

2.5. *Warranty / Guarantee*

i. The successful bidder shall provide warranty / guarantee as specified in detailed specifications against each hardware item.

ii. The warranty period will start from the date of supplies received in Federal Medical College.

iii. The qualified bidder must warranty the IT Equipment and ensure availability of technical support services as informed through electronic & non-electronic means. Each and every complaint should be completely responded by the competent resource of the firm and visit on-site within 24 hours of its notification.

iv. If any bidder fails to rectify the problem in the provided equipment during warranty period due to any reason, Federal Medical College will be authorized to repair or replace the faulty equipment / component thereof and forfeit the Bank Guarantee / Insurance Guarantee retained value.

v. The security deposit for warranty and guarantee will be released after expiry of the warranty period (one year).

2.6. *Taxes*

i. The rates should be quoted inclusive of all applicable taxes.

ii. The bidder should provide the Income Tax and Sales Tax Registration Certificates.

iii. The project authorities will deduct the taxes at source as per prevailing rules / regulations of the Government.

iv. In case the supplies or part thereof are exempt from levy of any tax, the bidder shall provide an exemption certificate (SRO) to this effect, otherwise taxes will be deducted.

2.7. *Bidding*

i. Rate quoted for the offered product in Pak Rupees.

ii. Installation and commissioning charges of equipment must be included in the quoted rates.

iii. Tender documents must be filled in, stamped and signed by authorized representative of the firm.

iv. Any bid with erasing / cutting / crossing etc. must by properly signed by the authorized person signing the tender. Moreover, all pages of the

Federal Medical & Dental College, Islamabad
Procurement Section

tender must also be properly signed. Offers with any over writing, not authenticated with signatures of authorized person, shall in no circumstances be accepted. Softcopy should also be provided.

v. The participated firm must be an official authorized partner from principal for the quoted brand.
vi. Federal Medical College may increase or decrease quantities of one or more items.
vii. Procurement may be done in phases / partially against original quantities mentioned in the RFP till up to 30th June, 2026. However, bidders are required to quote for total quantities mentioned in the document. Schedule of deliveries will be shared at the time of signing of contract.

2.8. *Timeline of the project:*

Delivery Time / Installation and Configuration within two (02) weeks and agreed by the Vendor / bidder in writing at the time of the technical bid submission on affidavit duly notarized.

2.9. *Bid Evaluation*

i. Bid Must be submitted via EPADS
ii. Bids shall be evaluated in accordance with advertised specifications of equipment, terms & conditions.
iii. Rates offered by the firms.
iv. Supply time, and maintenance of warranty period.
v. Physical compliance with required specifications and quality conformance for the offered product in demonstration session.
vi. Active part inspection will be carried-out visiting the site where offered product installed and operational.
vii. Willingness of the firm to enter into contract agreement with the Federal Medical College for supply of equipment on the rates tendered by the firm / bidder in its financial bid.
viii. The weightage of technical bid will be 80% and financial bid will be 20%.

#	Eligibility Criteria	Documents Required	Compliance (Yes / No)	Max Marks
1.	Bidder is an entity duly registered and incorporated under the laws of Pakistan. Bidder has a valid Registration Certificate for Income Tax, Sales Tax and/or other allied agencies / organizations / regulatory authorities	Registration / Incorporation certificate / FBR Certificate		10
2.	Bidder MUST provide written acknowledgment on a Stamp Paper of PKR 100 duly attested by the notary public Federal Medical College may visit the warehouse for inspection of the quoted quantities of hardware Ex-Stock. Delivery of hardware / Software / equipment / Installation / Configuration must be within fifteen (15) days from Purchase Order.			40
3.	Bidder is an Active Taxpayers as per Federal Board of Revenue (FBR)'s database i.e. Active Taxpayers List (ATL)	Active Tax Payer / Income Tax Returns		05

Federal Medical & Dental College Islamabad
Procurement Section

#	Eligibility Criteria	Documents Required	Compliance (Yes / No)	Max Marks
4.	Bidder Affidavit on the Stamp Paper attested by Notary Public which certifies to provide One -years warranty / guarantee after installation for IT equipment's / software.	Stamp Paper		05
5.	Affidavit on the Stamp Paper duly attested by Notary Public that the bidder is not blacklisted by any government / semi government / public Department.	Stamp Paper		05
7.	The bidder shall be authorized distributor / partner / reseller of OEM.	Proof of Partnership with OEM		05
8.	The quoted brand must be having service centers in Islamabad / Rawalpindi.	List of Service Centers		05
9.	Certified Resource of the quoted brand	Certificate must attach		05

2.10. *Supply of Stores*

i. The items mentioned in the list are required to be delivered at Federal Medical College within time period mentioned in the tender document.

ii. The stores are required by the consignee within stipulated date. However, the tender is required to indicate their own guarantee earliest date by which the items / store should be brand new and in original manufacturers packing.

2.11. *Federal Medical College reserve the Rights Within Provision Of PPRA Rules-2004*

- Award contract to more than one bidder.
- Accept or reject any or all tenders
- Increase the quantity of items or may order partial supplies or cancel any or all items.
- Purchase full or part of the store or ignore / scrap / cancel the tender.
- Claim compensation for the loss caused by the delay in the delivery or any other damage pointed out at time of delivery or commissioning or installation or during warranty period.

2.12. *Payment*

The payment for the supplies made within 30 days by the successful bidder shall be released provided that:-

i. The invoice is complete, accurate and to the entire satisfaction of the procuring agency / client.

ii. Supplies are delivered / installed according to the instructions of the Federal Medical College.

iii. Vendor must produce satisfactory inspection with the invoice issued by the Federal Medical College that authenticates the quality conformance, quantity of products delivered and amount of work done successfully.

iv. 2% performance guarantee is provided with the invoice having validity up to the date of Warranty period.

v. The payment against a supply order shall be made on the completion of the delivery of supplies including installation, commissioning, etc. as mentioned in the supply order.

Federal Medical & Dental College Islamabad
Procurement Section

2.13. Arbitration

Any disputed situation / condition between the bidder and the procuring agency regarding this bid or any other matter ancillary thereto whatsoever, the same shall be referred to the sole arbitrator i.e. Grievance Redressed Committee Federal Medical College.

The Arbitrator shall give its award within two months from the date on which it enters upon the reference. The provisions of the Arbitration Act, 1940 shall apply to the arbitration proceeding. Reference to arbitration shall be a condition precedent for any other action at law.

2.14. Penalty

For failure to comply with the supply/work order and the liquidated damages will be levied as under:-

i. 1% of the cost of that items mentioned in the supply order that remain un-delivered /un-finished for each day of non-supply up to maximum of twenty (20) days exceeding the job completion / delivery period.
ii. If the material is not supplied for 20 consecutive days, Federal Medical College reserves the right to cancel the contract and get the full or remaining assignment completed from the other competitive bidders on the equivalent price / amount that will be deducted from the securities deposited by the default firm / supplier.

1- Only registered suppliers, who are on Active Taxpayers List (ATL) of FBR, are eligible to supply goods / services to Government departments.
2- The payment to the registered persons may be linked with the active taxpayer status of the suppliers as per FBR database. If any registered supplier is not in ATL his payment should be stopped till he files his mandatory returns and appears on ATL of FBR.

2.15. Undertaking

We undertake and declare that

i. The prices quoted including of all taxes, transportation and cost of installation etc. The quantity of above items can be increased.
ii. The offered prices must be valid up to **31-12-2026** starting from the date of tender opening.
iii. All products are covered under warranty issued by manufacturer / principal starting from the date of supply / installation and in case of any defect and malfunctioning we shall be responsible for repair / replacement as per guarantee / warranty.
iv. The supplier is responsible to arrange replacement / technical support during warranty / guarantee period.

We understand that:-

Federal Medical College reserves the right to accept or reject our bid and we undertake not to question the decision in this regard.

The earnest money submitted by us is liable to forfeiture in case our firm fails to abide by the terms and conditions given in the advertisement referred to above

Federal Medical & Dental College Islamabad
Procurement Section

<u>Signature & Stamp Of Authorized Agent</u>

No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

Scope of Bid

Federal Medical College Invites sealed bids for supply and installation of following lot /Goods as specified in detail in the Schedule of Requirements along with Technical Specifications in Turn key lot:

Sr. No	Item	Qty	Specification	
1	Next Generation Firewall with 3 years Support and Subscription.	1	Annexure A	Lot
2	24 Port Port Switch	3	Annexure B	
3	Wireless Access Point along with controller	20	Annexure C	
4	UPS 5 KVA	1	Annexure D	
5	Passive Complete Networking	35	Annexure E	
6	Server Room Establishment	1 Job	Annexure F	
7	Rack Mount Server	1	Annexure G	
8	Extended Detection and Response for 3 year's subscription and Support	350	Annexure H	
9	Network Attached Storage	1	Annexure I	

Bidder must quote for the complete LOT, Bidder offering less items as defined in LOT will be disqualified.

Next Generation Firewall with 3 years Support and Subscription **Annexure A**

Requirement	Compliance
The proposed NGFW firewall throughput (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions) Throughput 8.5Gbps	
The proposed NGFW minimum threat prevention throughput (Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, Sandboxing, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions) Throughput 4.5Gbps	
The proposed NGFWof IPsec VPN throughput (IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled) Throughput 4.1Gbps	
Max sessions 0.945 Million	
New connections per second (measured with application-override utilizing 1byte HTTP transactions) 100,000	
Interfaces 8 x 10/100/1000. 6 x 1G SFP. 4 x 1G/10G SFP/SFP+. 4 x 1G/2.5G/5G POE. 1 x 10/100/1000 out-of-band management port. 1x RJ 45 Console port, 1 x USB Port, Mini USB	
NG Firewalls with redundant AC power supplies	
Advance Threat prevention subscription 3-year term, Sandboxing subscription 3 years term, Advanced URL Filtering Subscription, 3-year, DNS Security subscription 3-year term, SD-WAN Subscription 3 years term 1500 x Client VPN must be with supported and included in the solution.	
Rack mount kit/ Power Cord and other accessories	

Federal Medical & Dental College Islamabad
Procurement Section

No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

Technical Specifications

	General Requirements	Compliance
1	The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 10 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	
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	
24	The proposed NGFW should offer redundant AC power supplies	
25	The proposed NGFW should support Active/Active, Active/ Passive deployments	

Federal Medical & Dental College Islamabad Procurement Section

26	The proposed NGFW should support state full session maintenance in the event of a fail-over to a standby unit	
27	The proposed NGFW should support the High Availability feature for either NAT/Route or transparent mode	
28	The proposed NGFW should support multiple heartbeat links	
29	The proposed NGFW should support L3, L2, transparent and tap mode deployments	

	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	
	Advanced Threat Prevention Features	
1	The proposed NGFW should protects 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 signatureless 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	

Federal Medical & Dental College Islamabad Procurement Section

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	
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	
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	

Federal Medical & Dental College Islamabad Procurement Section

46	The proposed NGFW should support advanced file analysis with URL crawling to prevent multistage, multihop 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	

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	

Federal Medical & Dental College, Islamabad
Procurement Section

	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.	
	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	

	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	

Federal Medical & Dental College Procurement Section

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	

24 Port Port Switch **Annexure B**

General requirements
• Switch must be covered with official warranty of the manufacturer on the territory of Pakistan for a period of not less than 1 years
• The switch must be equipped with 10/100/1000BaseT ports, not less than 24
• The switch must be equipped with SFP ports, not less than 8 x 1/10Gb SFP+ uplink ports (includes 2 x Stacking ports) • MACsec-capable switch must support fabric technology
• The switch must be equipped with out-of-band 10/100BaseT Ethernet port for management
• The switch must be able to mount in 19" Rack. Required rackmount kit must be included.
Performance
• The switching bandwidth must be not less than 208 Gbps
• The switch should have non-blocking architecture. All ports must operate on highest possible speed simultaneously
• The maximum number of stored MAC addresses in the switching table the switch shall be not less than 32,000
• The routing table of the switch must store not less 16,000 IPv4 routes
• The switch must support 6,000 or more Multicast groups

Federal Medical College, Islamabad
Procurement Section

Stacking
• The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps
• The failure of any switch in the stack should not cause stack outage more than 20ms.
• The switch must support the joint failover configuration with another identical switch to connected devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms.
• The failover configuration must be supported for two separate switches and two separate stacks of switches.
Ethernet L2
• The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z.
• The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols
• The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching.
• The switch must support 802.1w, 802.1s, PVST+ protocols
• The switch must support Link Aggregation Group (LAG). Number of ports in one LAG must be not less than 8
• The switch must support the following mechanisms for traffic balancing in LAG: The combination of the MAC addresses of source and destination; The combination of IP addresses of source and destination; The combination of IP addresses of source and destination, and numbers of TCP and UDP port numbers; The combination of IPv6 source and destination and numbers of the protocols of the 4th layer of the OSI model.
• The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA
Routing IPv4/IPv6
• The switch must support Policy-based Routing
• The switch must support BFD for static routing and dynamic routing protocols OSPFv2/OSPFv3
L2/L3 Multicast
• Then switch must support Multicast VLAN registration (MVR) protocol
• The switch must support IGMPv1 / v2 / v3 protocols;
• The switch must support protocols: IGMPv1 / v2 / v3 snooping (IGMPv1 / v2 / v3 snooping);
• The switch must support the protocol PIM Snooping;
User authorization and QoS
• Each interface for connecting user devices must support at least 8-x hardware queues.
• Access control lists that are configured on the switch port must operate at line speed available on port.
• The switch must support the IEEE 802.1x protocol.
• The switch should provide dynamic assignment of user access policies L2-L4 on ports
Management
• The switch must support standard SNMP versions 2c and 3, Syslog.
• The switch must support NTP
• Switch must support on Prem management and cloud management

Wireless Access Points **Annexure C**

Indoor AP with 2.03 Gbps wireless throughput and 2 Giga Ports, offers 4x4:4 MU-MIMO technology on the 5G band and 2x2:2 MU-MIMO on the 2.4G band. Self-Power adaptation upon auto detection of PoE or PoE+ with Up to 175-meter coverage, Support 200+ concurrent Wi-Fi clients, Advanced QoS, Anti Hacking secure boot, along with Controller

UPS **Annexure D**

5KVA
True Online Double Conversion Pure Sinewave UPS
Single Phase IN / Single Phase OUT
Frequency: 50 Hz, +/- 5% Hz
Power factor: 0.9
Power bypass system: Built in maintenance
Frequency: 50Hz, +/-0.5 Hz
Crest factor: 3:1
SNMP / Web browser Connectivity Slot.
USB Port option.
High instantaneous overload Capacity.
Backup time – must be **10-15 minutes** with Sealed lead Acid Maintenance Free Battery

Passive Complete Networking **Annexure E**

Passive Work including ducting, copper/ Power Cable/ fiber laying, termination and fluke testing.

i. Giga Cable UTP CAT6
ii. CAT 6 Patch Panel
iii. CAT6 I/O
iv. Faceplate Single / dual Shutter
v. Patch Cords CAT 6, 1 meter
vi. Optical Distribution Frame.
vii. Dura Duct, Pipe and Accessories
viii. Centralized Power to all racks from UPS

CAT 6 Cable

Cat 6 Cable, UTP, PVC, 4 pairs, 305 meter / Box Gigabit original copper cable Category 6 U/UTP Cable (with cross-shaped separator) offer the possibility to deploy unshielded Category 6/Class E systems when installed with Cat-6 RJ45 Jacks.

- Conductor Diameter: AWG 24 (Ø 0.525 +/- 0.015mm)
- Insulation Diameter: PE Ø 0.95 +/- 0.05 mm
- Cable assemblies: pairs
- Sheath material: PVC

Mechanical Features:

Maximum cable diameter (mm) 5.40 +/- 0.30
Bending Radius (mm)
Dynamic (installation) / Static (installed) ≥ 8x outer diameter / ≥ 4x outer diameter
Temperature Range In service / Installation, Transport and Storage -20°C +60°C / 0°C +50°C

Standards Cables

IEC 61156-5 ed. 2
ANSI/TIA 568-C.2
ISO/IEC11801 ed.2

Federal Medical & Dental College, Islamabad
Procurement Section

Fire Rating
LSZH: IEC 60332-1
PVC: IEC 60332-1

Patch Panel
1U 19" panels must be available to take a minimum of 24 copper fully shuttered jacks. Other connection densities must be available:
The panels must be designed for keystone fitting of the fully shuttered jacks/sockets. For efficiency of the termination and performance tool less terminate able keystone jacks must be used.
The copper panel panels must have cable management and tie down points (where required) for copper cable. Panels must have the facility to label each fully shuttered socket/jack.

CAT6 I/O
RJ45 K6 Jack, Cat 6, UTP, Shuttered (tool-less termination),
Category 6/Class E system, fully compliant with Category 6 ISO/IEC, EN and TIA standards for hardware performance, confirmed by independent laboratory certifications (Delta, GHMT).

The jacks have the following features:
- Category 6 UTP
- Keystone fixing;
- Tool less assembly (mandatory)
- Capable of being wired to both 568B and 568A
- three cable entry points
- Integral shutter/shuttered jack
- Jacks must be reusable i.e it must support multiple termination.

Applications
- IEEE 802.3 1GBASE-T
- PoE – IEEE 802.3at

Standards
- ISO/ IEC 11801 Edition 2, Am 1-2
- ISO/ IEC 60603-7-5
- EN 50173-1
- ANSI/ TIA/ EIA-568-C.2-2009
- IEC 60512-99-001

Server Room Establishment **Annexure F**

1	Vinyl Flooring. Anti-Static
2	False Ceiling
3	Room lights work
4	Industrial sockit
5	Room paint color
6	1.5 Ton Wall Mount AC
7	Glass Work
8	Bio Matric Door Access
9	42 U Rack 800 x 1000 along with PDUs and Fans
10	7/29 Cable Black and Red
11	Installation/Commissioning

Federal Medical & Dental College Procurement Section

No.F.1-8/Tender/2025-26/FMC
Federal Medical College (FMC)
Hanna Road G-8/4, Islamabad

Rack Mount Server **Annexure G**

1 x Intel Xeon Silver 4514Y 16C 150W 2.0GHz Processor
5 x 2.5" 5400 PRO 960GB Read Intensive SATA 6Gb HS SSD
1 x Broadcom 5719 1GbE RJ45 4-port OCP Ethernet Adapter
1 x 1100W 230V Titanium Hot-Swap Gen2 Power Supply
1 x 2.8m, 10A/100-250V, C13 to C14 Jumper Cord
1 x V3 2U Standard Fan Option Kit
1 x 64GB TruDDR5 5600MHz (2Rx4) RDIMM
Windows Server 2025

Extended Detection and Response **Annexure H**

1.	**Next-Generation Antivirus / XDR Requirements**		**Compliance**
	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	
	l.	Integration with next-generation firewalls for complete Layer 7 visibility, including application name	
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	

Federal Medical & Dental College, Islamabad
Procurement Section

	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	
	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 all latest Windows.	
	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	

Federal Medical & Dental College Procurement Section

	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		
	h.	Asset management with rogue device discovery		
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	
		(7)	Host inventory with detailed user, system, and application information	
	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	
		(7)	Transaction-level data and enhanced information about key protocols, such as DNS, HTTP, DHCP, RPC, ARP, and ICMP	

Federal Medical & Dental College, Islamabad
Procurement Section

	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	
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		
	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/alerts retention of 180 days		
	e.	Optional retention of data for an unlimited length of time		
12.	**License Requirements**			
	a.	350 licenses required for endpoints (on site deployment)		
	b.	3 years license & support		

Network Attached Storage **Annexure I**

Drive Bays: 4 + 2 x 4 TB SSD
Drive Compatibility: 3.5" & 2.5" SATA HDD/SSD
Processor: Quad-Core with AES-NI Hardware Encryption
Memory: DDR4 (Upgradeable)
M.2 Slots: NVMe SSD Slots for Cache
Network: 2 x Gigabit LAN
USB Ports: USB 3.2 Gen1
RAID Support: RAID 0, 1, 5, 6, 10, JBOD, Basic
Maximum Storage Expansion: Up to Large Multi-TB Capacity

Federal Medical & Dental College, Islamabad
Procurement Section