Government of Pakistan
PAKISTAN TELECOMMUNICATION AUTHORITY
www.pta.gov.pk

INVITATION TO BID

For the Procurement Next Generation Firewall System

Pakistan Telecom Authority, (a telecommunication regulator in Pakistan) invites sealed bids from the original manufacturers / distributors / suppliers/resellers/ Contractors/partners etc. having Five years of experience and registered with Income Tax and Sales Tax Departments and who are on Active Taxpayers List of the Federal Board of Revenue for procurement, configuration, deployment and maintenance NGFS:

Description	Quantity
Hardware Based NGFS having advance Threat Prevention service, URL Filtering, Application Control, advance Sandboxing with malware protection and analysis service, advance DNS Security Service, with six virtual firewall systems, with client and clientless vpn service, and Dual redundant power supply, Active-Active and Active-passive HA support.	2
10G SFP + (Transceivers) Multimode (same Brand)	08
1G SFP (Transceivers) Multimode (same Brand)	08
Multi-mode Fiber patch cords LC/LC (Duplex) 10 meter or above. (Branded)	16
Firewall Central Management Software (Perpetual License for 25 Firewalls)	01
Next Business Day Warranty , Support/SLA	03 years (24 X 7) Support/SLA

Bidding documents, containing detailed terms and conditions, method of procurement, procedure for submission of bids, bid security, bid validity, opening of bid, evaluation criteria, clarification / rejection of bids, performance guarantee etc. are available at the office of the undersigned. Price of the bidding documents is **Rs. 500/-** (non-refundable- in shape of pay order / bank draft, in favor of PTA). Bidding documents can also be downloaded from (www.pta.gov.pk) free of cost.

The bids, prepared in accordance with the instructions in the bidding documents, must reach at PTA Headquarters F-5/1, Islamabad on or before **3rd April, 2020** upto **10:30 AM**. Technical Bids will be opened on the same day at **(11:00 AM).**

This advertisement is also available on PPRA website at **www.ppra.org.pk**

Muhammad Salman Zafar,
Director (ICT)
PTA HQs, F-5/1, Islamabad
Phone: 051-2878134, Fax Number: 051-9225368
salmanzafar@pta.gov.pk

"Say No to Drugs"

20 x 2

Government of Pakistan
PAKISTAN TELECOMMUNICATION AUTHORITY
HEADQUARTERS F-5/1, ISLAMABAD.
http// www.pta.gov.pk

BIDDING DOCUMENTS

Sealed bids are invited from well reputed dealers/suppliers/distributors/partners having Five years of experience and registered with Sales Tax and Income Tax Department having valid certificate from Original Equipment Manufacturers (OEM) for procurement, configuration, deployment and maintenance NGFS, as per details below:

S.No.	Description	Quantity
	NEXT GENERATION FIREWALLS SYSTEM (NGFS)	
1	Hardware Based NGFS having advance Threat Prevention service, URL Filtering, Application Control, advance Sandboxing with malware protection and analysis service, advance DNS Security Service, with six virtual firewall systems with client and clientless vpn service and Dual redundant power supply. Active-Active and Active-Passive HA support.	2
	10G SFP + (Transceivers) Multimode (same Brand)	08
	1G SFP (Transceivers) Multimode (same Brand)	08
	Multi-mode Fiber patch cords LC/LC (Duplex) 10 meter or above. (Branded)	16
	Firewall Central Management Software (Perpetual License for 25 Firewalls)	01
	Next Business Day Warranty , Support/SLA	03 years (24 X 7) Support-SLA

Detailed specifications of above-mentioned Hardware are provided at **Annex-C** of this document. Notice of the bids issued on PTA's/PPRA's websites is part of the contract document.

Terms and Conditions

1. GENERAL INFORMATION:

a. Bidding documents, duly completed in all respects, will be received on or before **3rdApril, 2020** up to **1030 AM**. The submission and evaluation of bids will be carried out under the "*Single Stage Two Envelop Procedure*". Technical bids will be opened by Technical Evaluation Committee, at PTA HQs on the same day at 1100 AM, in presence of bidder's representative, who may choose to attend.

b. Bid will comprise of single package containing two separate sealed envelopes. One envelop will contain the "Technical Proposal" and the second envelop will contain the "**Financial** Proposal". Technically qualified bidders will be informed the date, time and venue for the opening of financial bids. Financial bids of technically disqualified bidders will be returned un-opened.

c. Bids should be sent to Director (ICT) Pakistan Telecommunication Authority (PTA), Headquarters F-5/*1*, Islamabad.

d. Bidder shall quote only single option, bids with multiple options will be rejected without any right of appeal.

e. Annex-A, Annex-B, Annex-C and Annex-D are integral part of technical and financial proposals, which may be read/filled carefully, signed and stamped by the bidders. Further, details of the annexures are mentioned below:

  i. Annex-A consists of mandatory requirements for bidder(s)

  ii. Annex-B consists of technical capabilities of bidder(s), which has total 100 marks, whereas minimum qualifying marks are 75%.

  iii. Annex-C consists of technical evaluation of the product and bidder(s) may quote higher specs, however, quoting lower specs shall disqualify the bidder

  iv. Annex-D, comprises of financial bid format, to be followed by all bidders, the bidder should quote its rates clearly, in the financial proposal in both figures and words without any ambiguity.

  v. The bidder must be current dealers/suppliers/distributors/partners of the principal manufacturer.

  vi. License renewals including SLA/Support, Warranty and Security Services of Firewall may be renewed on same terms and conditions as mentioned in the tender document for next three years (After the expiry of three years' warranty, support/SLA etc.), mutually agreed by both parties.

  vii. Draft agreement is also part of the Bid documents.

2. BIDDER's INFORMATION

a. Name of Firm ____
b. Date of establishment of business
c. (documentary proof of registration etc.) _________________________
d. Address ____
e. Telephone No ____________________Fax No. __________________
f. GST Reg. No ____
g. National Tax No ____

3. EVALUATION CRITERIA

a. The bidder should quote its rates clearly in the Financial Proposal in both figures and words.

b. Category A is a turnkey solution, and the bidder shall quote for all items of hardware and Software.

c. Technical bids shall be opened and evaluated by technical evaluation committee in view of Annex-A, Annex- B and Annex-C. Bidder, obtaining at least 75%, shall be eligible for the participation in financial bid opening.

d. Financial bids of technically qualified bidders (bidders compliant of Annex-A, Annex-B and Annex-C) shall be opened and evaluated by procurement committee of PTA i.e. PC-I.

e. Work will be awarded to **financially lowest evaluated bidder.** If two or more bidders quote equal lowest price in financial proposals, then the work will be awarded to the one having higher technical marks, in technical evaluation.

4. Bid Security

a. Bid security will be equal to 2% of the bid amount and will be in the shape of pay order / demand draft in favor of Pakistan Telecommunication Authority, Headquarters, Sector F-5/1, Islamabad. Bid security **shall be attached with the financial proposal otherwise proposal** will not be accepted.

b. Bid security will be forfeited if successful lowest bidder unable to deliver the Hardware with in stipulated time frame.

c. **Bids without Bid security will be rejected without any right of appeal.**

d. **Bid security of successful bidder will be adjusted against the 10% of retention money till warranty period**. However, bid security of unsuccessful bidders will be returned after award of supply order to successful bidder.

e. In case of cancelation of Supply Order due to default of the supplier, the Bid security shall be forfeited in favor of PTA.

f. **Retention money** equal to 10% of total bid amount (after adjusting 2% bid security already deposited by the successful vendor) will be submitted at the time of the hardware delivery. Retention money will be kept against warranty and support and will only be released after completion of warranty period and on issuance of performance certificate from two ICT officers one of which should be the responsible IT Officer and the other should be officer in charge.

g. Retention Money will be forfeited in favor of PTA if the above mentioned officers reported hardware/software or any type of warranty/support issues related to the Firewalls.

h. Retention money shall be submitted in shape of pay order / demand draft in favor of Pakistan Telecommunication Authority, Headquarters, Sector F-5/1, Islamabad.

i. Retention money will be submitted at the time of the delivery of the hardware, Hardware without retention money will not be accepted.

5. PRICES

a. **The bidder should quote its rates clearly in Pak Rupees in the Financial Proposal in both figures and words as per format attached at Annex-D.**

b. The rates quoted shall remain valid for 90 days from the date of bid opening.

c. No currency exchange rate will be applicable and bids with a condition of currency exchange rate applicability will be rejected without any right of appeal.

d. Bid(s) shall be inclusive of all applicable taxes i.e. GST etc.

e. PTA will bear no transportation/carriage charges.

6. PAYMENT PROCEDURE

a. No advance payment shall be made against the supply of software and Hardware mentioned in this bidding document.

b. Payment is subject to successful installation, configuration, testing and commissioning of the HA Firewalls and payment shall be made on provision of invoice/bill, after delivery of the equipment /software at PTA Headquarters and issuance of satisfactory performance certificate by ICT directorate and physical inspection verification certificate issued by PC-I.

c. Payment shall be subject to withholding of applicable taxes as per government rules.

d. Payment will be linked with active taxpayer status of the bidder and no payment will be made until the bidder appears on ATL (Active Taxpayer List) of FBR (Federal Board of Revenue).

e. Payment will be released after verification of Hardware its warranty details from the principle manufacturer via official website, email or letter etc., if deemed necessary.

7. HARDWARE/SOFTWARE

a. The supply of hardware should be arranged through legal channels by clearing all duties/taxes (if any) levied by the Govt.

8. DELIVERY/COMPLETION PERIOD

a. All IT Equipment shall be delivered within (08) weeks' time after issuance of work order.

b. Configuration, installation and implementation will be the responsibility of the vendor, however technical engineers from ICT directorate will be available to make the process rational.

c. Completion time of the projects shall be two (02) weeks after delivery at H/Qs F-5/1, Islamabad with provision of support mentioned in **section 10.**

9. DEALER/SUPPLIER /PARTNER

Bidder shall be a dealer/supplier/distributor/partner of their respective Firewall Hardware manufacturer.

Both Principal Manufacturer and Vendor are equally responsible for the successful execution of the project and design shall be validated by principal manufacturer.

10. WARRANTY/SUPPORT/TRAINING

a. For Supply and Installation of Next Generation Firewalls System and all other components: Successful bidder will be responsible for three years' warranty and onsite support for three years (24X7-Support/SLA).

b. Vendor will be responsible for Training of two ICT officers Free of Cost. The successful bidder shall provide the necessary trainings prior to product delivery and will give both the participants complete overview of the solution, help them become familiar with its capabilities, and allow them to practice using the solution with day to day operations.

11. PENALTY

a) If the supplier fails to deliver within due time mentioned in the work order, then a penalty of 01% per week of the total value of work Order will be charged up to a maximum of four (04) weeks (Days less than six will be considered as one week). Thereafter, supply order will stand cancelled and Bid security will be forfeited.

b) If the supplier fails to install/configure provided hardware/software within due time mentioned in clause 8(C) of the is document, then a penalty of 01% per week of the retention money will be charged up to a maximum of four (04) weeks (Days less than six will be considered as one week). Thereafter, retention money will be forfeited in favor of PTA, supply will be rejected, and the project will be closed.

c) If the supplier fails to provide warranty / support as per certificate provided as per Annex-B (clause 3) of the bidding document, then a penalty of 01% per week of the retention money will be charged.

d) In case of non-satisfactory performance by the supplier during the warranty period, PTA reserves the right to forfeit the retention money in favor of PTA.

e) If the vendor fails to install, configure, deploy and test the system or unable to provide (i) Warranty (ii) Support and any other technical requirement as identified by PTA ICT team then the penalty, in addition to the forfeiture of the retention money, decided by PTA Authority will be applicable to the bidder as per Agreement.

12. DISQUALIFICATIONS

Proposals will be liable to be rejected if any deviation is found from the instructions as laid down in the bid document i.e.

a. Financial bid is submitted without the required Bid security.

b. Offers are received after specified date and time.

c. Specification and other requirements are not properly adhered to or different from those given in the bidding documents.

d. GST and NTN certificates are not attached and bidder is not is Active payer List of FBR.

e. Service centre of the quoted brand is not in Islamabad/Rawalpindi.

f. Bidder do not have “Valid” certificate from manufacturer.

g. Bidder quoted multiple options, referring **section 1 (d)**.

h. Affidavit on **Judicial Paper** to the effect that the firm has not been black listed by any government/semi government/autonomous body or company isn’t submitted with technical proposal.

i. Warranty/Replacement certificate both on Judicial Paper and vendor letter head for three years.

13. RIGHTS RESERVED

Pakistan Telecommunication Authority Islamabad reserves the rights to cancel the bid, accept or reject any bid as per PPRA rules.

CHECKLIST

a. Bid security in shape of bank draft/pay order. (Yes/No)
(cheques are not acceptable)

b. Relevant documents are attached as per Annexures (Yes/No)

c. List of such projects handled with copies of supply order. (Yes/No)

d. Affidavit on judicial paper for not been black listed. (Yes/No)

e. Specification and other requirements are met. (Yes/No)

f. Service Centre of the quoted brand is in Islamabad/Rawalpindi (Yes/No)

Muhammad Salman Zafar
Director (ICT)

General Evaluation Criteria Annex-A

Part A) Mandatory Requirements *	
1	Firm has to produce Sales Tax and Income Tax Registration.
2	Minimum Five years of relevant experience.
3	Sales and Service Center of the vendor must be in Islamabad / Rawalpindi.
4	Vendor status should be "Active" in Tax Payers List
5	Affidavit on Judicial Paper to the effect that the firm has not been black listed by any government/semi government/autonomous body or company
6.	Non-quoting International Branded items for any of the above hardware item will lead to disqualification.
7.	Firm has to produce valid Authorization Letter and partner Certificate of the principal/manufacturer for Pakistan
8.	Minimum three supply orders for Next Generation Firewalls System.

Bidders not fulfilling the above mentioned Mandatory requirements will stand disqualified

Technical Capabilities of Bidder- Part-B Annex-B

Part B) General Evaluation*				
Sr. #	**Attributes**	**Max. Score**	**Points Earned**	**Criteria**
1	Detail of Offices	10		Firm has sales and services offices at four (4) provincial headquarters. Two and half (2.5) points for each p.h.q.
2	Spare Parts Availability	10		Firm has Spare Parts of the quoted model Depot/facility at Islamabad / Rawalpindi.
3	Replacement time for faulty parts under warranty equipment/parts (**Certificate has to be produced)** (Clause 11(c) referred)	15	15	Next Business Day (NBD)
4	Total strength of relevant Technical Staff at **Rawalpindi / Islamabad**(List shall be attached with name, designation, qualification and related experience).	20	20	Firm has ten(10) or more relevant technical staff in Islamabad / Rawalpindi.
			15	Firm has more than seven (7) or more up to nine (9) relevant technical staff in Islamabad / Rawalpindi
			5	Firm has five (5) or more upto six(6) relevant technical staff in Islamabad / Rawalpindi
5	Firm Experience (minimum Five years' experience required)	20		(4) points will be given for each year of experience, beyond 5 years of mandatory requirement.
6	Projects completed of similar nature (documentary proof be provided i.e. Supply Orders etc.)	25		Five points will be awarded for each project of same nature on provision of supply order/certificate i. Supply of (2) or above NGFS in Single Supply Order. Max Five Supply orders, Minimum (3)
Sub Total		**100**		
***Minimum qualifying marks are 75% in above table whereas Annex "C" shall be compulsory.* All supporting Documents to be attached for all relevant pages of Annex-B.**				

(To be included in Technical Proposal-Mandatory Requirements)

Detailed Specifications of Next Generation Firewall (Qty =2) with Central Management Software for 25 devices		
1.1	**Mandatory System Performance and scaling requirements:**	Compliance
1.1.1	The Bidder shall propose 2 Next Generation Firewalls, with three years of below subscription and support services (SLA) with 24X7 Technical Support with 8x5xNBD RMA	
a	Application Visibility	
b	Advanced Intrusion Prevention System	
c	Full/Extended Antivirus Database, Anti-Spyware	
d	URL Filtering	
e	Advanced DNS Security	
f	Advance Malware Prevention	
g	File Blocking and Filtering	
h	Quality of Service	
i	At least 6 Virtual Contexts	
1.1.2	The Next Generation Firewall must deliver at least 5 Gbps of application firewall throughput with Application Visibility and User Identification enabled utilizing 64K HTTP transactions, using real-world enterprise traffic mix.	
1.1.3	When enabled below threat features, Firewall should deliver at least 2.2 Gbps throughput utilizing 64K HTTP transaction using real-world enterprise traffic mix:	
a	Advanced/Extended Intrusion Prevention System with all signatures/anomalies and severities	
b	Full/Extended Antivirus Database Scan	
c	Anti-Spyware	
d	Anti-botnet	
e	URL Filtering (including user notification, safe search enforcement etc.)	
f	DNS Security (including detection of DNS tunneling, DAGs, etc.)	
g	File-blocking and File-filtering (DLP)	
h	Sandboxing for all supported file types	
i	Application Identification	
j	User Identification (agentless)	
k	Logging enabled	
1.1.4	Proposed solution will be subject to stress testing to validate the technical compliance of the solution if required. Failure to satisfy above parameters will lead to negative impact	
1.1.5	NGFW Performance must not be affected when enabling any of the below features and must still commit to the minimum throughputs required in section 1.2.3:	
a	Logging and storing it on local HDD.	
b	All management features like SSH, HTTPS, SNMP, etc	
c	Scheduled threat prevention DB updates up to the level of checking every 1 minute to ensure best security coverage.	
d	Multiple alert systems like Syslog, SNMP and others at the same time.	
e	All applications inspections.	
f	Changing the order of the security rules.	
g	Using all IPS signatures for all supported applications with extended packet captures for critical to high severity alerts.	

h	Virtual Context should not impact the firewall performance	
1.1.6	Administrators must not have to apply any tradeoff between security and performances, choosing to use in any security profile different versions of signature databases, for IPS with reduced numbers of element.	
1.1.7	Administrators must not have to apply any tradeoff between security and performances, choosing to use in any security profile different versions of signature databases, for Antivirus and malware scanning with reduced numbers of element.	
1.1.8	The proposed firewalls shall support at least 1,000,000 concurrent sessions with all threat prevention enabled features and at least 57,000 new sessions per second.	
1.1.9	The proposed firewalls shall deliver at least 2.5 Gbps IPSEC VPN throughput based on 64K HTTP Transaction Size	
1.1.10	The proposed firewalls shall deliver at least 3,500 IPSEC site-to-site tunnels if required.	
1.1.11	Dedicated high availability ports (preferably 1G ports).	
1.1.12	High Availability, Active / Active with Asymmetrical Routing support and Active/Passive	
1.1.13	Proposed Solution must support QoS (marking and/or traffic shaping) for multiple classes at the same time and must be able to make policy as below:	
a	QoS Policy-based traffic shaping (priority, guaranteed, maximum)	
b	QoS Policy-based diffserv marking	
c	QoS Policy-based on application category, users/groups or any combination	
1.1.14	The proposed firewalls must have at least network ports as follow:	
i	(4) 1Gbps SFP/SFP+ interfaces	
ii	(4) 1G/10G SFP/SFP+ interfaces	
iii	(12) 10/100/1000 copper interfaces.	
1.1.15	Reporting: Solution should provide granular reporting (with query builder)	
1.1.16	Reporting: Network Log storage for 45 days	
1.1.17	Reporting: The proposed firewall shall support real time interactive graphical dashboard to highlight high risky applications, suspicious app-centric content and users	
1.1.18	Reporting: The proposed firewall has the ability to schedule PDF report generation and send it over email	
1.1.19	Data Filtering: The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.1.20	Data filtering: Social Security Numbers, Credit Card Numbers any regex pattern	
1.1.21	Data filtering: Custom Data Patterns	
1.2	**Functional Requirements**	
1.2.1	Unlimited Concurrent User License for IPSEC, Remote, & SSL Client Based VPNs.	
1.2.2	Proposed Firewalls should be able to decrypt TLS 1.2 Traffic with RSA-AES256-GCM-SHA384 with 2K keys at server response packet size of 1500 bytes	
1.2.3	Possibility to support internally developed applications with application ID customized manually by the customer	
1.2.4	The NGFW platform shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode L1, layer 2 and layer 3	
1.2.5	The NGFW platform shall support multiple virtual routers to run different set of routing protocols (Interfaces can be binded to different virtual routers)	
1.2.6	Anti-Virus should not reduce the IPS inspection throughput and should be able to give full threat prevention capabilities	
1.2.7	Anti-Spyware should not reduce the IPS inspection throughput and should be able to give full threat prevention capabilities	
1.2.8	Advanced malware protection to prevent unknown modern targeted attacks and APTs	
1.2.9	Support IPSec VPN, and dynamic site-to-site VPN support with LSVPN.	

1.2.10	Identify users, not just IP addresses. Leverage information stored in Active Directory for visibility, policy creation, reporting, and forensic investigation.	
1.2.11	Inspect content in real-time. Protect the network against attacks and malware embedded in application traffic at low-latency, high throughput speeds, with all signatures applied at the same time	
1.2.12	Policy-based control by application and/or application category (non-port based) - as a policy matching criteria	
1.2.13	The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before	
1.2.14	The proposed solution should be able decrypt ssh/ssl/tls 1.2 protocols and extend Advance Malware Protection to all file types over HTTP, HTTPS, POP3, IMAP, FTP, SMTP and SMB	
1.2.15	The proposed firewalls shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, brute force attack, “SYN cookie”, “IP spoofing” and malformed packet protection.	
1.2.16	The proposed firewalls shall support transparent and tap mode within the appliance.	
1.2.17	The proposed firewalls shall support 802.1Q Virtual Local Area Networks (VLANs) tagging (in tap, transparent, layer 2 and layer 3).	
1.2.18	The proposed firewalls shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode, layer 2 and layer 3.	
1.2.19	The proposed firewalls shall support standards-based link aggregation (IEEE 802.3ad) to achieve higher bandwidth.	
1.2.20	The proposed firewalls shall support policy-based forwarding based on zone, source or destination address, source or destination port, application and users/groups imported from Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups.	
1.2.21	Should support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic	
1.2.22	The proposed firewalls shall support IPv6 routing for virtual routers.	
1.2.23	Should provide hot swap fans and redundant power supplies	
1.2.24	Should support XML API that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	
1.2.25	Should support Syslog Receiver feature that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	
1.2.26	Firewall should support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)	
1.2.27	The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.2.28	The firewall should take decision based on different matching parameters not based on layer4 parameters. It should be based on applications, URL categories, device state, IP addresses, security zones, username/group(s)	
1.2.29	Policies based on port-and-protocol And Application as the match criteria (application decision should not be done separately)	
1.2.30	Support Geographical Location policy in a security rule, where connections going to a country or countries can be blocked	
1.3	**Threat Prevention: Next Generation IPS**	
1.3.1	Block viruses, spyware, malware and network worms and vulnerability exploits within content of application content	
1.3.2	File blocking by type and application	
1.3.3	Anonymous Botnet Detection	
1.3.4	Blocks application vulnerabilities	

1.3.5	Block known network and application-layer vulnerability exploits	
1.3.6	Block buffer overflow attacks	
1.3.7	Block DoS/DDoS attacks; it shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, reconnaissance attacks, brute force attack, “SYN cookie”, “IP spoofing” and malformed packet protection.	
1.3.8	Supports attack recognition for IPv6 & IPv4	
1.3.9	Stream-based protection and scanning for Anti-Virus & Antispyware	
1.3.10	Built-in Signature and Anomaly based IPS engine	
1.3.11	Ability to create custom user-defined signatures	
1.3.12	Supports CVE-cross referencing where applicable	
1.3.13	Supports automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)	
1.3.14	All Threats should be part of application context	
1.3.15	The platform should be capable to enforce various threat prevention profiles on different applications running on same L4 session	
1.4	**Advanced Malware Prevention**	
1.4.1	Identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques	
1.4.2	Should support anti-evasion capability which is tested against advance evasion technique.	
1.4.3	Cloud-based detection architecture or self-contained on-premises Sandboxing system	
1.4.4	Malware analysis should support files from Windows, Linux, Mac OS and Android platform	
1.4.5	Drive-by Download Detection & Protection	
1.4.6	Dynamic Analysis should include but not limited to: changes made to hosts, suspicious network traffic, anti-analysis detection plus more potentially malicious behaviors	
1.5	**Antivirus/Anti-Spyware:**	
1.5.1	Per-application antivirus or anti spyware scanning options	
1.5.2	Per-category scanning options	
1.5.3	Phone-home detection/blocking	
1.5.4	Malware site blocking	
1.5.5	DNS-based botnet signatures	
1.5.6	DNS Sink holing for Malicious and fast-flux domains	
1.6	**URL Filtering:**	
1.6.1	Multi-category filtering	
1.6.2	Customizable allow and block lists	
1.6.3	Customizable block page & coaching pages	
1.6.4	Custom categories	
1.6.5	Database located locally on the device	
1.6.6	Supports block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)	
1.7	**DNS Security:**	
1.7.1	Neutralize DNS tunneling	
1.7.2	Predict and stop DGA-leveraging malware with real-time domain query analysis	
1.7.3	DNS threat detection methods using the modular and infinitely extensible DNS Security cloud-based service	

1.8	**Data Filtering:**	
1.8.1	Files should be identified by file types or by signature	
1.8.2	The firewall should be capable of identifying and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	
1.8.3	Compressed information stored in zipped files should be able to be unpacked and filtered per policy	
1.8.4	The firewall should be capable of identifying and optionally preventing the transfer of files containing sensitive information (i.e. credit card numbers) via regular expression	
1.8.5	Should not have any file size limitation in checking content for keywords	
1.8.6	The platform should be capable to enforce file blocking on different applications running on same L4 session	
1.8.7	Control Drive-By Download (Files which are downloaded/transferred via web applications without knowledge of the user - it might have an exploit that can attack end-user's workstation)	
1.9	**User Identification:**	
1.9.1	Should support the following authentication services for user-identification: -	
a	Active Directory	
b	Exchange, LDAP, eDirectory, Radius, Kerberos	
C	Client Certificate	
D	Captive Portal	
E	Terminal Server	
F	Supports the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP	
G	Users from Citrix and terminal services environments should be supported in policy and logs	
H	Populate all logs with user identity (traffic, IPS, URL, data, etc.)	
I	Logged user-identification correlated in real-time	
J	Should support REST XML API that would allow the firewall to be integrated with any known NAC, and WLAN controllers for user identification	
K	Should support built in syslog server for collecting user identification logs from unix, and any network controller (WLAN, NAC) for user identification	
1.10	**Networking**	
1.10.1	Tap Mode, Layer 2, and Layer3 (should be supported in the same virtual system at the same time)	
1.10.2	Can be deployed as virtual wire (Layer 1 with no change to MAC nor Ip addresses). Bump in the wire technology	
1.10.3	RIPv2, OSPFv2 and BGP	
1.10.4	Policy based routing	
1.10.5	Policy based routing with application as matching criteria	
1.10.6	5 minutes Automatic Signature generation after malware analysis	

Any inferior Specifications will be rejected

Multiple options are not allowed; vendor should Quote only one option. Quoting multiple option will lead to disqualification.

Annex-D

Financial Proposal (Bid Format) NGFS (with 3 years' warranty)

Date _______________

Company Name ____

Required Specification	**Quoted Specification (With Brand Name)**	**Unit Price** ***Inclusive of Applicable Taxes***	**Qty**	**Total Price Inclusive of** ***Applicable Taxes***
Next Generation Firewall System with Dual redundant power supply.			2	
Three years Security Software subscriptions including Advance Threat Prevention service, URL Filtering, Application Control, advance Sandboxing with malware protection, advance DNS Security Service with six virtual firewall systems with client and clientless vpn service. Three years Warrant and Support/SL			1 job	
10G SFP + (Transceivers) Multimode (same Brand)			08	
1G SFP (Transceivers) Multimode (same Brand)			08	
Multi-mode Fiber patch cords LC/LC (Duplex) 10 meter or above. (Branded)			16	
Firewall Central Management Software (for 25 Firewalls)			01	

Amount in words: (Rupees……………………………………………………………………….)

Any inferior specifications will be rejected

FINANCIAL PROPOSAL not accompanied with Bid security will be rejected without any right of appeal.

Authorized Signature of bidder with seal stamp

AGREEMENT

(To be executed on Rs.100/- Judicial paper)

THIS Supply & Service Agreement (the "Agreement") is made on this day __________ 2020;

By and Between

Pakistan Telecommunication Authority, a statutory body established under Pakistan Telecommunication (Re-organization) Act, 1996, having its principle office at PTA H/Q, F-5/1, Islamabad (hereinafter referred to as "**Client**" which expression shall where the context admits include its administrators and assigns) of the One Part

And

M/s_________________________________

through Mr.……………………………………………………………….

bearing CNIC……………………..……………………..….

having place of business at………………………………………..……………………

(hereinafter referred to as "**the Contractor,**" which expression shall where the context so allows include his/its successors-in-interest, executors, administrators, heirs and permitted assigns) of the **Other Part**

(If when and where applicable the Party of the One Part and Party of Other Part shall hereinafter be collectively referred to as 'Parties' and individually as 'Party' as the context of this Agreement requires).

WHEREAS;

A. Client is desirous of procuring & installation of **Next Generation Firewall System** (hereinafter referred to as "**NGFS**") for its HQs Building at F-5/1, Islamabad and have them **delivered/supplied and installed and subsequently maintained** by the Supplier in accordance with the terms of this Agreement;
B. The Supplier is a ____ (*details of incorporation*) being engaged in the business of supplying electrical, electronic equipment including but not limited to integrated security technologies, and has agreed to **supply, deliver, install/configure and thereafter provide maintenance services (hereinafter referred as Services)** of the **NGFS** at Client HQs Building on the terms and subject to the conditions as set forth hereunder.
C. The Supplier represent that;
    i. It has the relevant expertise and holds valid and subsisting licenses/permissions, authorizations/approvals required from the Government of Pakistan and;
    ii It has the requisite expertise and resources to provide top quality of requisite Services of **NGFS** as per Bill of Quantity ("BoQ") to the Client in accordance with highest industry standards and satisfaction of the Client. The Supplier

undertakes that the Services shall be provided only through the staff/labour/workforce that has the requisite expertise and experience in this regard.

D. Upon the basis of the representations and warranties of the Supplier contained herein, the Client wishes to appoint the Contractor to Supply and provide the Services *at HQ Building premises under this Agreement*;

NOW THEREFORE, for the consideration provided herein the representation and warranties, covenants, conditions and promises contained herein below and intending to be legally bound, the Client and Contractor hereby agree as follows:

1. **Scope of Agreement**

Subject to the terms and conditions of this Agreement the Supplier agrees to provide Services *as* per requirements prescribed under **Bidding Documents and its attached Annexure-A, B, C, D;**

2. **Agreement Documents**

2.1 The following documents shall be deemed to form, and be read and construed as, part of this Agreement:

a) Invitation to bid
b) Bidding documents along with its Annexures
c) Bill of Quantity (BoQ)
d) Special Stipulations (if any).
e) Addenda and Corrigenda, if any, issue by the Clients and duly accepted by the Contractor at the signing of the Contract.
f) Bid security/ Tender Guarantee
g) Form of Agreement/ Contract Agreement
h) Clients order to commence the work.
i) Limit of Bid security.
j) Any Correspondence by the Clients/Supplier mutually accepted by the Client and the Contractor.

3. **Term**

3.1 Upon signing of this Agreement the Supplier shall be obligated to start the work on specified location by Client within ____________and complete it within projected time _________________calendar days.

3.2 However, in case of any unavoidable/unforeseen delay (i.e Force Majeure) incurred either by the Contractor or the Client, necessary timeline extension would be agreed mutually between both parties, however, it has to be communicated to each other during the occurrence of Force Majeure as per clause 11.

4. **Termination**

4.1 Notwithstanding anything herein contained the Client shall be exclusively entitled to terminate this Agreement

a. without advance notice, in case the Supplier is in breach of any of the terms of this Agreement, or in case the Client is not satisfied with the Services.
b. Without cause, by giving three (03) days advance written notice to the Supplier.
c. If the *Services* do not meet the specifications, terms & conditions mentioned in the **Annexure-A, B, C, D of Bidding documents.**

4.2 In case of such termination, the Supplier shall not be paid for any Services actually rendered up to the date of termination and any advance payment by the Client in respect of the *Services* not performed or in respect of period falling after the effective date of termination shall be refunded by the Supplier, to the Client. The Client, shall not, because of expiration or termination of this Agreement, be liable to the Supplier for any compensation, reimbursement, or damages because of the loss or prospective profit or because of expenditures or commitments incurred in connection with the business of the Supplier.

5. Deliverables

5.1 The work should be of best quality and as per technical specifications mentioned in the Annexure C and D of Bidding documents.

6. Charges

6.1 In consideration of rendition of Services, all amounts paid to the Supplier are inclusive of all taxes, levies, duties, and any other deduction related thereto etc. and are acknowledged by the Supplier to be adequate and sufficient consideration for the rendition of Services.

6.2 All payments to be made by the Client to the Supplier shall be subject to such deductions and withholding as are required by prevailing laws which shall be to the account of the Supplier.

7. Invoice

7.1 The Supplier shall submit its Invoice in accordance with the rates/charges specified in **Annexure-D** of Bidding document.

7.2 The Supplier shall be solely responsible for all payments, liabilities and all other obligations of whatsoever nature pertaining to its staff/workers who shall be deputed for the Services at the Client's Building.

7.3 The Supplier undertakes to fully indemnify and hold harmless the Client against any claims, losses, damages, or expenses in relation to injury or death to any persons or loss or damage to property arising out of the performance of supply and installation Services.

7.4 The Supplier and its staff /employees shall be bound to obey safety rules and other regulations prescribed by the Client on its premises. Any losses/damages suffered by the Client due to omission on the part of the Supplier, its staff/employees to abide by this condition shall be the sole liability of the Supplier and it may result in termination of the Agreement by the Client at its sole discretion.

8. Confidentiality

The Supplier, its/his staff, workers, employees, personnel, agents or any other person acting for him and/or on his behalf shall hold in confidence and complete confidentiality and all documents and other information supplied to the Supplier and his Employees personnel, agents etc. by or behalf of the Client or which otherwise came/come into its/his/their knowledge and relates to the Client or any of its project.

9. Indemnification

The Supplier shall indemnify and hold harmless the Client, its Chairman, Directors, Member Offices, Employees and other Personnel against any and all claims, damages, liabilities, losses, and expenses, whether direct or indirect, or personal injury or death to persons or damage to property arising out of (i) any negligence or intentional act or omission by the Supplier or his employees, personal , agents, etc. in connection with the Agreement, or (ii) arising out of or in connection with the performance of his obligations under this Agreement.

10. Resolution of Disputes

10.1 All disputes arising under this Agreement, whether during the term of this Agreement or after the termination or expiry of this Agreement shall be referred to (i) Purchase Committee-I (PC-I) of the Client for amicable settlement /resolution of the dispute at first stage. (ii) In case of failure in settlement, at the second stage the case will be referred to the Authority of the Client through Director (Administration). The decision of the Authority to settle the issue amicably will be final and will not be challenged at any forum including court of Law. (iii) In the event of failure of amicable settlement of dispute as above, either party may refer the dispute to Arbitration under the provision of Arbitration Act, 1940 and the rules issued thereunder, at Islamabad, Pakistan.

10.2 No All variations amendments and in or modification to the terms of this Agreement shall be made, except in writing and shall be binding only if duly agreed and signed by both the parties or their duly authorized representatives.

11. Force Majeure Event

11.1. Neither Party shall be held responsible for any loss or damage or failure to perform all or any of its obligations hereunder resulting from a Force Majeure event.

11.2 For the purpose of this Agreement a “Force Majeure Event” shall mean any cause(s) which render(s) a Party wholly or partly unable to perform its obligations under this Agreement and which are neither reasonably within the control of such Party nor the result of the fault or negligence of such Party, and which occur despite all reasonable attempts to avoid, mitigate or remedy, and shall include acts of God, war, riots, civil insurrections, cyclones, hurricanes, floods, fires, explosions, earthquakes, lightning, storms, chemical contamination, epidemics or plagues, acts or campaigns of terrorism or sabotage, blockades or acts of Governmental Authority after the date of this Agreement.

11.3 The Party initially affected by a Force Majeure shall promptly but not later than seven (07) days following the Force Majeure event notify the other of the estimated extent and duration of its inability to perform or delay in performing its obligations (**"Force Majeure Notification"**). Failure to notify within the afore-said period shall disentitle the Party suffering the Force Majeure from being excused for non-performance for the period for which the delay in notification persists.

11.4 Upon cessation of the effects of the Force Majeure the Party initially affected by a Force Majeure shall promptly notify the other of such cessation.

12. Governing Law

The provisions of this Agreement and the rights and obligations hereunder shall be governed by and construed in accordance with the prevailing laws of Pakistan.

13. Waiver

A party's failure to exercise or delay in exercising any right, power or privilege under this Agreement shall not operate as a waiver; nor shall any single or partial exercise of any right, power or privilege preclude any other or further exercise thereof.

14. Severability

The invalidity or unenforceability of any provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

15. Amendment

All addition amendments and variations to this agreement shall be binding only if in writing and signed by the Parties or their duly authorized representatives.

16. Assignment

This Agreement may not be assigned by either party to other than by mutual agreement between the Parties in writing.

-

IN WITHNESS WHEREOF, the parties hereto set their hands the day, month and year first above written.

For and Behalf of Client.

By: ____________________________
Name: __________________________
Title :
____

For and on Behalf of: Supplier

By: ______________________
Title: _____________________
Name: _____________________
Signature: ________________

Signature: ______________________

Date : ____________________________

Date : ___________________

Witnesses

1.__________________________

Name: _______________________

CNIC: ________________________

2. _________________________

Name: ______________________

CNIC: ______________________