NATIONAL HEALTH SYSTEMS RESOURCE CENTRE

NIHFW Campus, Baba Gang Nath Marg, Munirka, New Delhi – 110067

TENDER DOCUMENT

TECHNICAL & FINANCIAL BID

UNDER TWO BID SYSTEMS

NAME OF WORK

Procurement of Next Generation Firewall (NGFW)

NATIONAL HEALTH SYSTEMS RESOURCE CENTRE
(NIHFW Campus, Baba Gang Nath Marg, Munirka, New Delhi - 110067)

NATIONAL HEALTH SYSTEMS RESOURCE CENTRE
(NIHFW Campus, Baba Gang Nath Marg, Munirka, New Delhi - 110067)
FILE NO-NHSRC/11-12/Tenders/01/PF (2)

DETAILED NOTICE INVITING FOR LIMITED TENDER

On behalf of the Executive Director, NHSRC, the indenter, tenders are invited for hiring in a two bid from reputed, experienced professional service providers for Procurement of Next Generation Firewall (NGFW) of NHSRC by agencies in Delhi/NCR subject to terms and conditions of the contract notified in the tender document available on the official NHSRC website www.nhsrcindia.org for use in the NHSRC NIHFW Campus, Baba Gang Nath Marg, Munirka, New Delhi-110067.

About NHSRC

The National Health Systems Resource Centre (NHSRC) is a registered Society under the Ministry of Health & Family Welfare, Government of India to provide technical assistance to the central & state government. It was established on 8th December 2006 as a Society under Societies Registration Act XXI of 1860. Its mandate is to assist in policy and strategy development in the provision and mobilization of technical assistance to the states and in capacity building for the Ministry of Health and Family Welfare (MoHFW) at the centre and in the states.

National Health Systems Resource Centre (NHSRC) worked as a technical support wing of the Ministry of Health & Family Welfare, Govt. of India. NHSRC acts as a nodal agency for channelizing the Technical Assistance (TA) to central and state governments for effectively implementing the NHM, with a specific focus on health system strengthening, capacity development & comprehensive Primary Healthcare. The Key technical areas of NHSRC are Community Processes, Healthcare Financing, Healthcare Technology, Human Resources for Health, Public Health Administration, and Quality Improvement in Healthcare.

It has a 23-member Governing Body, chaired by the Secretary, MoHFW, Government of India with the Mission Director, NHM as the Vice Chairperson of Governing Body and the Chairperson of its Executive Committee. Of the 23 members, 14 are ex-officio senior health administrators including four from the states, and 9 are public health experts from academics and civil society with the Executive Director, NHSRC who is the Member Secretary of both the Governing Body and the Executive Committee. NHSRC's governing body meets sanctions on its annual work agenda and its budget.

This Expression of Interest (hereinafter referred to as 'EOI') is being procurement of **Firewall (NGFW).**

The detailed terms and conditions of the tender may be downloaded from the NHSRC website https://nhsrcindia.org/ and the same shall be read as part and parcel of this EoI.

You are requested to confirm your willingness to provide services by your firm with the following information positively by **12-04-2024** to "**The Principal Administrative Officer", NHSRC** at the given office address.

Schedule to be invitation of EoI

Tender - Start Date	1000 Hrs. on 22-March-2024
Tender document download/Sale start date/time	1000 Hrs. on 22-March-2024
Pre-Bid Meeting	1500 Hrs. on 28-March-2024
Last date and time for receipt of bids	1700 Hrs. on 12- April- 2024
Date and time for opening of the Prequalification- cum-technical bid	1430 Hrs. on 15 - April- 2024
Date and time for opening of the Financial Bid	1430 Hrs. on 19 - April- 2024
Service to be provided	Firewall (NGFW)
Validity of tender offers	30 days from the date of opening of prequalification - cum-technical bid
Performance Security Deposit (Only for finalized bidder)	3% of the contract value

1. NHSRC will not be responsible for any delay in receiving the EOI.
2. The Incomplete/unsigned bids may be rejected.

Contents

Instructions for Submitting Proposal

Offline Submission:

1. Part A (Technical Proposal) and Part B (Financial Proposal) must be submitted in separate documents. **Please do not include any price information in Part A.**

2. The cover of the envelope should be clearly named as "**FIREWALL NGFW for NHSRC TECHNICAL PROPOSAL**" and "**FIREWALL NGFW NHSRC FINANCIAL PROPOSAL**" separately. Both envelopes are to be kept together in one **SINGLE SEALED ENVELOPE**.

3. The document shall be sent in a sealed envelope **EITHER** by post to 'The Principal Administrative Officer, National Health Systems Resource Centre, NIHFW, Baba Gangnath Marg, Munirka, New Delhi -110067' **OR** physically kept in the tender box 'RFP for Firewall' placed at NHSRC.

4. Any delay in the timely submission of the proposal through the post, or any other cause, will not be considered by NHSRC and will be deemed rejected.

Both Technical and Commercial proposals shall include a self-declaration as specified under section, "Bidder Declaration".

For Bidders Participating

a) The bidders (both offline and online bidders) or their authorized representatives need to send an e-mail to The Principal Administrative Officer, National Health Systems Resource Centre at "**it.support@nhsrcindia.org"** intimating their confirmation for participation in pre-bid and bid opening meeting. This will ensure that only an authorized person is participating, and accordingly, needful arrangements can be done.

b) National Health Systems Resource Centre is not bound to accept the lowest bidder or any proposal. We also reserve the right to request any, or all, of the Bidders to meet with us to clarify their proposal.

c) The final decision for approval/ rejection of the Bid of the Bidder at any stage of evaluation shall lie solely with NHSRC and NHSRC shall be under no obligation to disclose the reasons for the same to the Bidder.

d) The duly completed sealed tender in the manner prescribed should be submitted to PAO, NHSRC concerned, above-mentioned address up to **1700 Hrs on 11-April-2024** and the Technical Bid shall be opened at **1430 Hrs on 12-April-2024** in the presence of tenderer or their authorized representative (only one) who may wish to be present.

e) The offers shall remain open for acceptance for 45 days from the date of opening of the Technical Bid. Any tenderer not keeping offers open for the prescribed period; the same shall be summarily rejected.

f) If the date of opening of the tender is declared as holiday the tender will be opened on the next working day at the same time and venue.

g) Incomplete offer/offers not conforming strictly to the manner prescribed /offer not

submitted on prescribed tender from or late/delayed tender shall not be considered and stand summarily rejected.

h) The offers submitted would be governed by all the terms & conditions laid down in the prescribed tender form in addition to the terms & conditions indicated herein.

i) NHSRC reserves the right to amend or withdraw any of the terms and conditions contained in the tender document or scrap the tender enquiry at any stage without assigning any reason and NHSRC will not be liable for any costs and consequences incurred by the intending Tenderers.

j) NHSRC reserves the right to accept or reject any or all of the bids in full or in part including the lowest, without assigning any reasons, thereof or incurring any liability thereby.

k) NHSRC shall have the right to changes the terms & conditions /cancel the tendering process at any time, without thereby incurring any liabilities to the affected bidders. Reasons for changing the terms & conditions / cancellation, as determined by NHSRC in its Sole discretion including but are not limited to the following:

Principal Administrative Officer
NHSRC, New Delhi

Instructions To Tenderers

National Health Systems Resource Centre (hereinafter referred to as NHSRC), Principal Administrative Officer invites tenders under two bid system from Professional Service Providers (hereinafter referred as Service Provider) for Next Generation Firewall (NGFW).

If any agency is able to quote in accordance with the requirements of the Tender, they may submit their tender to this office in the prescribed tender form duly sealed and, in the manner, prescribed.

Address For Correspondence

For all purpose of this contract the address of the tenderer mentioned in the tender shall be the address to which all communications to the Service Provider shall be sent, unless the Professional Service Providers has notified a change by a separate letter sent by Registered Post with Acknowledgement-Due. The Professional Service Providers shall be solely responsible for the consequence of an omission to notify a change of address in the manner aforesaid.

Pre-Bid Meeting

A pre-bid meeting will be held in the Conference Room of National Health Systems Resource Centre, Baba Gangnath Marg, Munirka, and New Delhi 110067 at **1500 Hrs. 28-March-2024** for clarifications required on any aspect pertaining to the Tender Document.

Scope / Objective / Deliverables

A. Eligibility Criteria The firm should

I. Be a registered one under Company's Act and should have an experience in the field of maintenance of Firewall.

II. Be registered with Sales and Service Tax Authorities with respective State Government /Government of India (As applicable).

III. Agency submit authorization letter of OEM.

IV. If the firm meets the above technical requirements, they may apply in the technical bid proforma placed as Appendix-I, with photocopies of all the documents in proof of the Registration, Experience, Financial Strength, OEM Certificate & Hardware details for verification.

V. RATE / FINANCIAL BID:

The Professional Service Provider shall quote as per "B" Financial Bid as per format given in Appendix II. Conditional Financial Bid shall be summarily rejected. Service tax, if applicable shall be paid extra. Tax deduction at source (TDS) shall be governed as per prevailing rules.

B. Scope of Work

S. No.	Item	Description of Work
1.	Installation & Configuration of Firewall	1. Configuration of Network LAN & WAN 2. Create the policy for inbound & outbound. 3. NAT Policy 4. Web filtering policy 5. User-based authentication 6. App-based policy 7. Location-based policy 8. Creation of different groups 9. Quality of service implementation 10. VPN Set-up 11. Set up for logging & reporting. 12. Load Balancing set-up 13. Configure Access Control Lists (ACLs) 14. Establish Firewall Zones and an IP Address Structure

Technical Specifications for the Firewall

S. No.	Item Description	Technical Specification	Compliance	Remark
1	**Make**	To be mentioned by the bidder/ Vendor		
2	**Model No.**	To be mentioned by the bidder/ Vendor		
3	**Country of Origin**	To be mentioned by the bidder/ Vendor		
4	**Hardware Architecture**	The proposed hardware-based firewall should not consume more than 1RU Rack-mountable space		
		Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core CPU's based architecture to protect latest security threats.		
5	**Performance & Scalability**	Appliance must have one Console port, dedicated one management Port, two USB port and redundant power supply		
		The device should have 6 x 10G (SFP+); 16 x 1GbE from day 1.		
		Appliance should have 128 GB or more Built in Storage from day 1 and should be expandable to 1 TB		
		Appliance should support 16 Gbps or more Firewall throughput & 8 Gbps or more IPS throughput.		
		Appliance should		

		support 9 Gbps or more Threat Protection throughput		
		The device should have Concurrent Sessions: 4 million or higher & New connection/Sec: 100,000 or higher		
		Firewall Should support at least 9 Gbps or more IPSec VPN throughput and 3000 IPSec Site-to-Site VPN tunnels & 2000 IPSec VPN clients.		
		Firewall Should support at least 4 Gbps or more TLS/SSL inspection & decryption throughput and 1000 SSL VPN clients.		
6	**General Firewall Features**	Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy-based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic.		
		Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2).		
		Should have Layer 2 bridge or transparent mode, Wire mode,		

		Sniffer mode /Tap mode. Solution should support policy-based routing, Application based routing and also Multi Path routing.		
		Application Control: The proposed system shall have the ability to detect, log and take action against network traffic based on over 3000+ application signatures from day1		
		The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.		
		Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found. The Firewall should Support for TLS 1.3 to improve overall security on the firewall. This should be implemented in Firewall Management, SSL VPN and DPI.		
		Firewall should support clientless SSL VPN technology or an easy to manage IPSec client for easy access to email, files, computers, intranet		

		sites and applications from a variety of platforms.		
		Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate-based authentication connection tunnel.		
		Solution should support User identification and activity available through seamless AD/LDAP Services SSO integration combined with extensive information obtained through Deep Packet Inspection.		
7	**Firewall Security Features**	Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats		
		Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations, and can be applied on		

		common protocols as well as raw TCP streams.		
		Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture		
		Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 7000+ IPS Signatures and 50 million Could AV signatures.		
		Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify. URL database should have at least 15-20 million sites and 50 + categories.		
		Firewall should support HTTP Request tempering protection, Directory traversal prevention, SQL injection Protection, Cross-site scripting Protection (XSS) & DNS security		

		The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc.		
		Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X		

		and multi-browser environments.		
		Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined.		
		The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration. Firewall Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.		
8	**High-Availability Features**	The proposed solution should support active passive / standby high availability with stateful synchronization.		
		The device should support stateful session failover to a standby appliance in the event of a hardware failure without any manual		

		intervention.		
9	**Visibility and Monitoring**	Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network.		
		The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status.		
		Solution should support granular network visibility of network topology along with host info.		
		Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats.		
10	**Management & Reporting Feature**	The management platform must be accessible via a web-based interface and without any additional client software		
		The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre		

		on-prem. The Centralize management platform should support multidevice firmware upgrade, certificate management, global policy template to push config across multiple firewalls in single click.		
		The on prem Centralize management platform should support closed network deployment with High Availability		
		The solution should store syslog in local storage or remote appliance. OEM can offer individual solution for logging and reporting based architecture to meet the requirements.		
		Firewall should have reporting facility to generate reports on virus dedicated over different protocols, top sources for viruses, destination for viruses, top viruses etc.		
		Analytics platforms support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem		
		The solution should support Cloud-based configuration backup.		
		The solution should support Application Visualization and Intelligence - should		

		show historic and real-time reports of what applications are being used, and by which users. Reports should be completely customizable using intuitive filtering and drill-down capabilities.		
		Should have reporting facility to generate reports on virus dedicated over different protocols, top sources for viruses, destination for viruses, top viruses etc.		
		The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.		
11	**Certification, Warranty, Installation, Testing and Commissioning**	The Firewall solution must be ICSA certified (Till Q3 2022) for Network Firewall, Anti-virus, Advanced Threat Defense & IPv6/USGv6 - Certification etc.		
		The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019).		
		Proposed Solution should support 24x7x365 telephone, email and web-based technical support.		
		OEM should have		

		TAC and R&D center in INDIA.		
		Manufacturer's warranty should be mentioned minimum 3 (three) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection, ATP, Patch & Firmware upgrade.		
		Bidder must carry out on site installation, testing and commissioning.		
12	**User Support**	Firewall should support 700 concurrent users' login		

APPENDIX-II

(To be kept on Cover Subscribed 'B' - Financial Bid)

FINANCIAL BID

I/we hereby quote rates as under;

S. No.	Item	Make & Model	Quantity	Rate (in Rs)
1.	Hardware Price			
2.	Software (License) Price			
3.	Installation, Commissioning, Configuration (As per Scope of work)			
Sub Total (in Rupees)				
Taxes (in Rupees)				
Total(in Rupees)				

* The cost quoted shall not be liable to change and shall be firm and final.
* Goods supplied shall be as manufacturer specifications and have a guarantee period of 1 Year and be accompanied with relevant certificates as applicable.
*Service tax, if applicable shall be paid extra.

Specific Terms and Conditions

1. Service & Support

(a) Authorised Service Centre within the state of Delhi, along with a dedicated contact person with telephone number for technical solution in a fast-track basis at this institution as and when required basis.

(b) **Availability of Service Centres**: Bidder/OEM must have a Functional Service Centre in the State of each Consignee's Location in case of carry-in warranty. (Not applicable in case of goods having on-site warranty). If service center is not already there at the time of bidding, successful bidder / OEM shall have to establish one within 30 days of award of contract. Payment shall be released only after submission of documentary evidence of having Functional Service Centre.

(c) **Dedicated /toll Free Telephone No. for Service Support**: BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.

(d) **Escalation Matrix For Service Support**: Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.

(e) In case hardware fault, alternate hardware must be provided on the same date.

(f) In the event of the failure of the vendor to repair the equipment within the stipulated five working days, organization will be free to get the equipment repaired from some other source and the firm shall be liable to pay for the entire expenditure incurred by the organization for the repair/replacement of the equipment and transportation in addition to above financial compensation. The compensation along with the repair charges of the equipment from any other firm shall be deducted directly from the amount of payment to be made by the organization to the tenderer.

2. Warranty

(a) Bidder / OEM must give an undertaking that after expiry of warranty period, it will provide AMC Service for next 3 years for the offered products at the rate not more than 10 % of contract price per annum.

(b) Buyer reserves the right to enter into an AMC agreement (covering preventive maintenance and servicing) with the Successful Bidder / OEM after expiry of the Warranty period at rate as mentioned above and the payment for the AMC charges would be made Quarterly after rendering of the AMC Services of the relevant AMC period. Performance Security of the successful bidder shall be forfeited if it fails to accept the AMC contract when called upon by the buyer. The original Performance Security of contract will be returned only after submission and verification of AMC Performance Security for 3% of total AMC value valid up to AMC period plus 2 months (if there is no other claim). (Undertaking of acceptance to be uploaded with bid).

(c) Warranty period of the supplied products shall be 3 years from the date of final acceptance of goods or after completion of installation, commissioning & testing of goods (if included in the scope

of supply), at consignee location. OEM Warranty certificates must be submitted by Successful Bidder at the time of delivery of Goods. The seller should guarantee the rectification of goods in case of any break down during the guarantee period. Seller should have well established Installation, Commissioning, Training, Troubleshooting and Maintenance Service group in INDIA for attending the after sales service. Details of Service Centres near consignee destinations are to be uploaded along with the bid.

(d) Successful bidder will have to ensure that adequate number of dedicated technical service personals / engineers are designated / deployed for attending to the Service Request in a time bound manner and for ensuring Timely Servicing / rectification of defects during warranty period, as per Service level agreement indicated in the relevant clause of the bid.

3. Scope of Supply

(a) Scope of supply (Bid price to include all cost components): Supply Installation Testing Commissioning of Goods and Training of operators and providing Statutory Clearances required (if any)

(b) Delivery: Hardware with all the licenses must be delivered within 7 working days post issuance of Purchase Order. In case non-delivery of items within 7 working s days, NHSRC reserves right to cancel the order.

4. Penalty:

(a) Penalty clause will operate for complaints, which are not attended within the stipulated time, indicated as below;

Sl. No.	Description	Response Time	Resolution Time	Rate of Penalty Beyond Resolution Time
1.	Hardware problem	4 hours	2 working days.	Rs.500/- per working day / per call basis

(b) As far as possible, the repairs would be carried out on-site itself. In case the equipment is taken to the workshop, the Vendor will have to provide standby equipment, till the equipment is repaired and delivered at NHSRC. In such case penalty clause will not operate provided the original equipment is returned within period of 2 working days from the date of breakdown or matching replacement has been provided.

5. Indemnification

- The Bidder hereby undertakes that NHSRC shall not be liable for or in respect to any damages or compensation payable to any of its employee, associate, agent or contractor or sub-contractor. The Bidder shall indemnify and keep indemnified the NHSRC against all such damages and compensation, all claims, proceedings, damages, costs, charges and expenses whatsoever in respect thereof or in relation thereto.
- The Bidder shall indemnify and keep indemnified NHSRC for any losses/ penalties as may be levied upon the Bidder, by any judicial/ statutory/ administrative authorities/ Court of law, on

account of violation of any law/ rule/ regulation/ condition etc. attributable to the Bidder/ its agents/ or any other person in its employment of or any of its contractors/sub-contractors.

The Bidder shall indemnify and keep indemnified NHSRC for any losses/ penalties as may be levied for any losses/ penalties as may be levied upon it, by any judicial/ statutory/ administrative authorities/ Court of Law, on account of violation of any law/ rule/ regulation/ condition/ infringement of Intellectual Property Rights, etc. attributable to the Bidder/ its agents/ its Affiliates or any other person in its employment or any of its contractors/ sub-contractors, while providing its services herein.

6.Regular Inspection of Website

Prospective bidders are advised to visit NHSRC website https://nhsrcindia.org/. on regular basis for any change in schedule like amendment / corrigendum in Tender Document including technical requirement and pre-bid minutes etc.

7. Amendments To Tender Enquiry (TE) Documents

At any time, prior to the deadline for submission of tender, NHSRC may, for any reason deemed fit by it, modify the Tender Enquiry document by issuing suitable amendment(s) to it. The amendment will be uploaded on NHSRC website only. NHSRC will be under no obligation to inform the Bidders of such amendment on individual basis.

In order to provide reasonable time to the prospective bidders to take necessary action in preparing their tenders as per the amendment, NHSRC may, at its discretion extend the deadline.