INDIAN ASSOCITION FOR THE CULTIVATION OF SCIENCE
2A&2B, Raja S.C. Mullick Road, Jadavpur, Kolkata-700032

NIT No.: IACS/CCRES/Firewall/23-24/54 **Date:19/01/2024**

Sealed tender in two bids system (technical bid and price bid) is invited from bonafide, resourceful and eligible manufacturer/exclusive distributor/vendors for **"Procurement (supply, installation, testing and commissioning) of Two New Next Generation Firewall (NGFW) against Buy-back basis with 3 old Firewalls for replacement purpose of old Cisco Firewalls by 'New, Better and Next Generation' Firewalls".**

Part-I (Technical Bid) of the tender should contain technical specifications in detail as well as commercial terms and conditions. Part-II (Price Bid) should clearly indicate item-wise price, if needed, as mentioned in the technical bid. The Technical Bid and Price Bid are to be submitted in separately sealed envelopes, distinctly marked accordingly and both to be put inside another envelope, that should be sealed and super scribed with tender notice no. and due date. The bidders may submit bids duly signed in their own letter heads.

Pre-bid meeting to discuss Technical specifications will be held at Roy Chowdhuri Hall, Centenary Building, 1st Floor, IACS, at 12.00 P.M on 25.01.2024 at IACS.

Completed tender bids should reach to the Dispatch section, IACS on or before the scheduled date and time specified below:

Tender Notice No.	**NIT No. IACS/CCRES/Firewall/23-24/54 Date :19- 01-2024**
Last date and time of submitting Tender	**02.02.2024 at 03:00 P.M.** at Dispatch Section
Pre-bid meeting to discuss Technical specifications	**25.01.2024 at 12:00 P.M. at Roy Chowdhuri Hall, Centenary Building, 1st Floor, IACS.**
Date and time of opening tender	**02.02.2024 at 05:00 P.M.**
Place of opening Tender	I.A.C.S., Kolkata
Contact	Email: ccresrc@iacs.res.in, admap@iacs.res.in Tel.+913324734971 [Ext.1176]

The technical bids will be opened first to judge/evaluate the technical specifications of the said Firewalls and there after the price bids of only technically qualified bidders will be opened.

Technical Bid Evaluation: The technical bids will be opened first to judge/evaluate the technical specifications of the said materials.

Opening of price-bid: The Price Bids of the bidders qualifying the technical bid will only be opened, the date and time of which will be intimated to the short-listed bidders at their email addresses. The rest of the bids will be rejected.

Please note that IACS will not provide any accommodation or reimburse any expenses to any of the bidders for attending opening of technical bid.

Quotations received incomplete or beyond the stipulated time will be summarily rejected.

1. TECHNICAL BID

The technical bid should contain technical specifications and should be kept in a separate sealed envelope duly super scribed as 'TECHNICAL BID' on the outer cover of the envelope as already detailed above. **It should be clearly mentioned on the envelope as "Technical Specification for Next Generation Firewall (NGFW)".**

Bill of materials:

Description	Quantity No
Next Generation Firewall (NGFW)	**2 Nos.**

1.2 Technical specification:

Next Generation Firewall (NGFW):-

Sl. No	Technical Specification of New Proposed Firewall
1	The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall latest report.
2	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.
3	Firewall appliance must have 2 x 10GE SFP+slots, 6 x 1GE SFP slots populated with two nos. MM tranceivers & 10 x 1GE RJ45 interfaces from day one. All these interfaces should be available simultaneously.
4	Firewall Throughput should be at least 20 Gbps.
5	Firewall appliance must have minimum 400GB SSD local storage.
6	Threat Prevention (including FW, IPS, Application Control & Antivirus) throughput must be at least 6 Gbps with real-world / enterprise MIX traffic.
7	NGFW (including FW, IPS, Application Control) throughput must be at least 6 Gbps with real-world / enterprise MIX traffic.
8	NGFW should have IPsec VPN throughput of at least 15 Gbps.
10	NGFW should support more than 400,000 new sessions per second.

11	NGFW should support at least 8 Million concurrent sessions.
12	The NGFW solution should support NAT64, NAT46, DNSv6 & DHCPv6.
13	The proposed system should be able to operate in Transparent (Access) mode and NAT/Route mode simultaneously without creating virtual context or virtual firewall.
14	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.
15	The NGFW should support WAN links load balancing and fail-over for at least 4 links
16	The NGFW should support internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,
17	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.
18	The Firewall & IPSEC VPN module should have ICSA (International Computer Security Association) or other equivalent Certification.
19	The NGFW should have both SSL and SSH Inspection capabilities.
20	The system should support 2 forms of site-to-site VPN configurations: a) Route based IPsec tunnel b) Policy based IPsec tunnel
21	The system should support IPSEC site-to-site VPN and remote user IPSec VPN in transparent mode.
22	The system should provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.
23	Solution must support at least 1000 concurrent SSL VPN.
24	The proposed firewall must support at least 6Gbps of SSL Inspection throughput along with IPS feature enabled.
25	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.
26	The NGFW shall be able to support various form of user Authentication methods simultaneously, including: Local Database, LDAP, RADIUS, TACACS+, Windows AD, Citrix & Terminal Server Agent support for Single Sign On.
27	The NGFW should readily available integration with SDN platforms (Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network) - Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix
	Intrusion Prevention System
28	IPS throughput should be at least 8 Gbps or better for Enterprise MIX traffic
29	The IPS should be able to inspect SSL sessions by decrypting the traffic
30	The IPS system should have at least 10,000 signatures
31	In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and NGFW should continue to operate while the IPS problem is being resolved
32	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.
33	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
34	NGFW should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks.
	Application Control Features:
35	The appliance should have at least 4000 application signatures database
36	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.
	Anti-Malware & Advanced Persistent Threat

37	Should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI
38	NGFW should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.
39	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also.
40	Antivirus module should be ICSA certified
41	NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time before passing it to user.
42	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
43	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.
44	Buyer should get access of OEM's cloud portal from where he can view file-analysis status details including file submission time, source IP, destination IP, File name, URL, File size, File type, Suspicious Act etc.
45	The Firewall should provides up-to-date risk and vulnerability data in the context of what is important to the business
46	The firewall should have functionality of security audit checks are updated to match evolving vulnerability exploits and attacks,
	Web & DNS Security Functionalities
47	The NGFW must have in-built Web Filtering Functionality
48	The NGFW must have in-built Web Proxy functionality for HTTP and FTP protocols.
49	The NGFW shall allow administrators to override Web Filtering database ratings with local settings
50	The NGFW should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.
51	The NGFW must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, Dynamic DNS based websites.
52	The NGFW must have capability to filter YouTube videos by using channel ID
53	The NGFW must have option to rate web resource based on their DNS rating
54	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware
55	The NGFW must block Botnet C&C domains request at DNS level itself.
56	The NGFW must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.
	Data Leakage Prevention
57	NGFW should have in-built DLP functionality without requiring any additional hardware or software license
58	NGFW should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.
59	NGFW must detect, protect and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP
60	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.
61	DLP actions should be : Log only, block, quarantine user/IP/Interface
62	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.
	High Availability
63	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component
64	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.

65	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode
66	The NGFW must support both Active-Passive and Active-Active High Availability options.
67	The NGFW must provide Load sharing mode along with redundancy in case multiple virtual firewalls are created on it.
68	The NGFW shall support interface link monitoring failover
69	The NGFW shall support external device ping probe failover
70	The HA solutions should support silent firmware upgrade process that ensures minimum downtime
71	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.
72	The NGFW must have capability to perform security inspection in networks where forward traffic and return traffic follow different paths.
	Administration, Management & Reporting Functionality Feature Requirements
73	Traffic reports : availability, bandwidth usage per application, latency, packet loss, QoS etc.
74	Solution should support for configuration rollback

2. PRICE BID

The financial bid indicating (item-wise) price for the item(s) mentioned in the technical bid should be kept in a separate sealed envelope and should be submitted in the following format duly super scribed as 'PRICE BID' on the outer cover of the envelop as already detailed above. Price bids of only technically qualified bidders will be opened and they will be intimated the date and time of the opening of price-bid at their e-mail ids. Rest of the bidders will stand rejected.

Sr. No	Item	Quantity	Make/Model	HSN/SAC Code	Base price	Total Price(Without GST)	GST@	GST Value	Total price with GST
1	Next Generation Firewall (NGFW)	2							
2	Buy-back value of Present Firewall	1	Cisco, Model ASA 5545						
3	Buy-back value of Present Firewall	1	Cisco, Model ASA 5550						
4	Buy-back value of Present Firewall	1	Cisco, Model ASA 5516						

	Total GST:	**Total Price:**

3. SCOPE OF WORK:

i. The NGFW will replace the existing Cisco make Firewalls in the IACS Data centres. It consists of supply, installation , testing and commissioning of the Firewalls as per IACS requirement and maintenance of the same for a period of 5 years in terms of onsite comprehensive warranty. Any Software or hardware updates released by the OEM should be installed by the vendor free of cost within the warranty period. The Vendor should provide onsite skill support (by deputing own representative at IACS, JADAVPUR Campus|) for the networking Firewall for the entire warranty period of 5 years.

4. WARRANTY:

ii. The Comprehensive Warranty shall be for a period of 5 years from the date of satisfactory installation, testing, commissioning and handing over the equipment which covered under warranty in working order. During the Warranty period the replacement of any part(s) of the equipment or rectification of the defective product will be free of cost. During the warranty period, the Vendor should do a precautionary visit twice a year to do Health Check-up of the device to ensure smooth functioning of the network.

iii. If, the tender is required to replace the rejected equipment and/ or other articles, he will replace them forthwith, but not later than a period of 14 (fourteen) days from the date of rejection. The tenderer shall bear all cost of such replacement, including freight, if any, of such replacement or repaired equipment and/ or other articles but without being entailed to any extra payment on that or any otheraccount.

iv. Vendor shall make necessary arrangements for keeping the sufficient spares at site to minimize the down time.

v. Software or hardware updates released by the OEM should be installed by the vendor free of cost within the warranty period.

vi. Warranty should be offered directly by the OEM.

vii. Single point of contact for all communication related with after sales and support.

5. BID SECURITY : (Declaration vide order no. F.9/4/2020-PPD dtd. November 12, 2020)

a. An Account payee Demand Draft/Pay Order of Nationalized Bank for Rs. 2,50,000/- (Rupees 2.5 Lakhs only) drawn in favor of "Indian Association for the Cultivation of Science (State Bank of India, Jadavpur University Branch, A/CNo.11079699211, IFSC:SBIN000093, MICR Code:700002048)" is to be furnished by the bidders except those who are registered with the Central Purchase Organizations, National Small Industries Corporation or the concerned Ministry or Department, as Bid Security money or Earnest Money Deposit (EMD). Alternatively, the Bidder shall have the option to furnish the EMD in the format of Bank Guarantee (BG).

b. The Demand Draft for the Bid-Security should have at least about 90 (ninety) days validity period of opening of the bids.

c. In case of non-award of the work the Bid Security money would be returned to the unsuccessful Bidders.

6. PERFORMANCE SECURITY:

An Account Payee Demand Draft on any commercial bank of India of 5% of the order value in the name of "Indian Association for the Cultivation of Science" is to be furnished by the successful bidder as Performance security. Performance Security may be furnished in the form of Fixed Deposit Receipt or Bank Guarantee from a Commercial Bank. Performance security money should remain valid for a period of 60 days beyond the date of completion of all contractual obligations of the supplier including warranty obligations. Bid security money or EMD will be refunded to successful bidder on receipt of the Performance security money.

7. TERMS OF PAYMENT:

Payment will be made 100% on successful delivery of the Firewalls as well as execution of orders (supply, installation, testing and commissioning). Partial payment against supply within scheduled delivery period will not be admissible. The vendors should quote CIF Kolkata for the said items.

8. ELIGIBILITY CRITERIA AND DOCUMENTS REQUIRED:

The following shall be the minimum eligibility criteria for selection of bidders technically

1. The Bidder should be an Original Equipment Manufacturer (OEM) or an authorized firm of reputation having sufficient expertise and experience in the subject tender with sound warranty/service support capability and authorization from Manufacturer.
2. Either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product.
3. If an agent submits bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same tender for the same item/product.
4. The tenderer should clearly mention whether they are the OEM or authorized dealer/agent of the

Manufacturers. In the case of dealer/distributor/agent, latest letter of authorization from the OEM specifically for this tender should be submitted along with the Technical Bid.

5. Submission of duly filled in and signed compliance certificate from Bidder are must with the Technical Bid.
6. Equipment offered must be supported with printed catalogue & description on OEM website.
7. Manufacturers / exclusive distributors / vendors should have history of supplying this type of Firewalls to this or other scientific organizations. Availability of a list in this regard would be preferred.
8. Bidder should submit their past experience for supplying and successful installation of similar units to other research Institute/Universities/other organization in India. Please provide documentary proofs of such successful installation and project completion. Also, a compliance table (see below) must be prepared and submitted along with the technical bid.

Sr. No	Item	Tender specification	Your offered instrument specification	Extent of compliance
1	**Next Generation Firewall (NGFW)**			

9. Attested copy of Registration certificates of the firm/company and GST details should also be submitted.
10. Manufacturers or Bidder are requested to provide ISO9001:2015.

11. Bidder should enclose copy of following documents:
    i. Trade license.
    ii. Company Registration certificate.
    iii. Bid specific OEM Authorization certificate is mandatory.
    iv. GST registration certificate.
    v. PAN GST certificate to be submitted.
    vi. Similar 3 Purchase Orders copy.
    vii. Income Tax Return (for the last 3 years).
    viii. Audited Balance Sheet (for the last 3 years).
    ix. A list of clients where these type of NGFW has been installed should also be provided.
    x. Documentary proof of Servicing facility and service engineer stationed at Kolkata.
    xi. Documentary proof of the vendor/bidder working in this field for at least last 3years.
    xii. Annexure-I in letter head with company seal and sign.

12. **Technical Supporting Staff**–The bidder should have trained and qualified customer support staff with ample experience in the required field. Complete details of service centres and support staff should be provided. They should have service centre in Kolkata with proper address. The details of the service centres should be provided.

13. Documentary proof of Servicing facility and service engineer stationed at Kolkata.
14. Documentary proof of the vendor/bidder working in this field for at least last 3 years.
15. Annexure-I in letter head with company seal and sign.
16. All network components should be from same OEM.
17. The OEM of the active network product should have well established manufacturing plant/Research & Development Lab in India or abroad.
18. All active network devices quoted by the bidder should be from a single OEM only.
19. The OEM of active network devices to be quoted by the bidder should have local Technical Assistance Centre (TAC) support in India through a toll-free number and Returned Materials Authorization (RMA) depot in India.
20. The OEM of active network devices to be quoted by the bidder should be present in the country from at least past 10 years.
21. Products (active) being quoted should be available as on date with the OEM and should be publicly available.
22. All active material to be procured should be from an OEM, which has not been acquired by other business entities for the period of last 3 years, this is to ensure dependable and continuous support as per warranty requirements and life cycle of the network.

9. GENERAL INSTRUCTIONS

1. Validity of tender: Tender submitted should remain valid for at least six months from the date of opening the tender. Validity beyond six months from the date of opening of the tender shall be lapsed by mutual consent.
2. Incomplete and conditional tenders as well as tenders received after the due date will be summarily rejected without assigning any reasons thereof.
3. The existing old Firewalls which are being currently used in IACS network will be returned to the lowest bidder only after successful installation of the new one since it is a buy-back for replacement purpose of old Firewalls by 'New, Better and Next Generation Firewall' version.
4. All contracts related to this tender will be interpreted under the Indian Law.
5. At any time prior to the bid due date, IACS may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder during pre-bid meeting, modify the bidding documents. The amendment(s) will be notified on the institute website. Prospective bidders are advised to occasionally to visit the website (www.iacs.res.in) for any amendment.
6. Service facility: In Kolkata, supplier should mention their details of service setup and man powers that are responsible for after sales support. Response time should be within 24hrs.
7. Delivery should be made within 90 days of the receipt of the Purchase Order by the Vendor. IACS reserves the right to impose penalty in the form of Liquidated damage (LD) as per GoI rules in case of delayed delivery.
8. Guarantee certificate, users manuals etc. are to be handed over to the user after successful commissioning of the system.
9. In the event of date being declared a closed holiday for purchaser's office, the due date for submission of bids and opening of the technical bids will be the following working day at the appointed time.
10. In case of any dispute, the decision of IACS authority shall be final and binding on the bidders.

11. Once the pre-bid meeting is over and issues are clarified, no query or objection or complain shall be entertained in connection with the tender. Absence of any vendors in pre-bid conference shall not be considered as justification for making query or objection thereto. Also, non-attendance in the pre-bid meeting is not a disqualification for participating in the tender process.
12. For any clarification regarding technical specifications, information etc., please send your queries to ccresrc@iacs.res.in and admap@iacs.res.in.
13. The authority of IACS reserves the right to reject any or all of the tenders received without assigning any reason thereof.

Registrar