Bid Number: GEM/2024/B/5589162
Dated: 11-12-2024

Bid Corrigendum

GEM/2024/B/5589162-C3

Following terms and conditions supersede all existing “Buyer added Bid Specific Terms and conditions” given in the bid document or any previous corrigendum. Prospective bidders are advised to bid as per following Terms and Conditions:

Buyer Added Bid Specific Additional Terms and Conditions

1. OPTION CLAUSE: The Purchaser reserves the right to increase or decrease the quantity to be ordered up to 25 percent of bid quantity at the time of placement of contract. The purchaser also reserves the right to increase the ordered quantity by up to 25% of the contracted quantity during the currency of the contract at the contracted rates. Bidders are bound to accept the orders accordingly.
2. Buyer Added text based ATC clauses

   1. The ATC document along with Annexure-I & Annexure-II is attached herewith.

Corrigendum -1

GEM bid No. GEM/2024/B/5589162

–

A. Modification to Technical Specification

Sl. No.	Earlier Item Description	Current Item Description
System Specification:		
4	Should have minimum of 500GB SSD RAID storage in the appliance	Should have minimum of 240GB SSD storage in the appliance
9	Should have at least 4 x 10G SFP+ ports, at least 4 transceivers should be included wit h the appliance	Should have at least 4 x 10G SFP+ ports, among th em at least 4 should be populated with multimode 10G-SR transceivers. At least two such ports shoul d be on LAN side
Performance Parameters:		

12	All functional and security features should s upport atleast 2000 users from day one	Firewall should be capable of serving as the primar y firewall of a reputed academic institutional camp us having more than 2000 users. The appliance sh ould be equipped with enough hardware resources (including but not limited to CPU and RAM) to avoid any hardware contention issues, under its us ual traffic load.
Firewall Features		
8	Gateway level Anti-Virus/Malware solution s hould be appliance based and available fro m day one, The Firewall should scan for thr eats in inbound, outbound and intra-zone tr affic for malware in files (maxsize should b e at least 30Mb) across all ports and TCP st reams by Gateway Anti-Virus/Malware	Gateway level Anti-Virus/Anti-Malware solution sho uld be appliance based and available from day one , The Firewall should scan for threats in inbound, o utbound and intra-zone traffic for malware in files across all ports and TCP streams by the Gateway A nti-Virus/Anti-Malware software. In case there is an y upper limit on size of files, potentially to be scan ned, such upper limit should not be less than 30Mb
	Certifications:	
1	The quoted Firewall model should be TEC c ertified or an equivalent certificate issued b y a competent authority for Cyber Security Products in India needs to be included alon gwith the technical bid	The quoted Firewall model should be TEC certified

B. Modification to OEM,/Bidder Eligibility Criteria

Sl. No.	Earlier Item Description	Current Item Description
11	The OEM of the proposed solution should b e among the top 15 players in last 3 publish ed Firewall/Network Security Appliance rep orts by Gartner/Radicati or an equivalent ra ting by any organization approved by the G overnment of India for Firewall/Network Sec urity Appliance. Website reference of such l ist should be provided as necessary eviden ce(s).	**Clause removed**

14	**New Clause**	The successful bidder may be asked to i nstall the quoted NG-Firewall model for a trial period of up to 30 days, to ensure al l performance parameters are met to the satisfaction of the user, before the final i nvoice is raised and the installation certi ficate is issued. Any issues related to performance bottle neck /throttling/hardware contention (> 50%)/packet drop etc. which may lead to disruption of IT services of user, will be t reated as failure of trial.
15	**New Clause**	The bidder must provide documentary evidence of having supplied at least three similar or lower-spe cification NG-Firewall models to reputable institutio ns such as Government Institutions, CFTIs, or Cent ral Universities (preferably IITs, NITs, etc.), caterin g to a user base of at least 2000 users with traffic c omparable to ISI Kolkata in last five years.

C. Modification to Scope of Work

Scope of Work remains unchanged

Revised Technical Specification

(after incorporation of corrigendum)

Sl. No.	Item Description
	System Specification:

1	The firewall should be On-premise, Physical, 1U, 19" Rack Mountable Appliance.
2	Should have x86 based or equivalent multicore processor
3	The appliance should have minimum 4GB of RAM
4	Should have minimum of 240GB SSD storage in the appliance
5	Should be equipped with hot swappable redundant power supplies
6	Should have sufficient no of redundant fans
7	Should have at least 4 WAN Ports
8	Should have at least 8 x 1/2.5 GbE Copper ports
9	Should have at least 4 x 10G SFP+ ports, among them at least 4 should be populated wit h multimode 10G-SR transceivers. At least two such ports should be on LAN side
	Performance Parameters:
1	The overall firewall throughput (mixed traffic) should be at least 25 Gbps
2	Should have Threat Prevention Throughput of at least 12 Gbps. Threat Prevention throughput must be measured with Gateway Anti-Virus/Malware, IPS, Application Visibility and Control (AVC) features enabled
3	Should have Intrusion Prevention Throughput of at least 15 Gbps
4	Should be able to handle minimum 225K new sessions per second
5	Should be able to handle minimum 4M concurrent connections
6	The TLS SSL DPI throughput should be minimum 6Gbps
7	Should support at least concurrent 50 Site to Site IPSec VPN Peers from day one and sho uld have provision for support upto 6000 peers
8	Should support atleast concurrent 500 Client to Site IPSec VPN Peers from day one and s hould have provision for support upto 4000 peers
9	Should support atleast concurrent 200 Client to Site SSL VPN Peers from day one and sh ould have provision for support upto 1500 peers
10	The overall VPN throughput should be minimum 5Gbps

11	The firewall should be able to provide Threat Prevention Throughput of atleast 4 Gbps, w hen simultaneously supporting 20 concurrent Site to Site IPSec VPN sessions and 200 co ncurrent Client to Site SSL VPN sessions.
12	Firewall should be capable of acting as primary firewall for a reputed academic campus h aving more than 2000 users. The appliance should be equipped with enough hardware re sources (including but not limited to CPU and RAM) to avoid any hardware contention iss ues, with usual traffic load
	Firewall Features:
1	Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Rout e-based VPN over OSPF, RIP, BGP
2	Should be IPv6 Ready from day one
3	The Firewall solution should support policy based routing, application based routing and multi-path routing
4	Should support Application Visibility and Control (AVC), User Identity, Next Generation In trusion Prevention System (IPS), Zero Day Protection/Advance Malware protection, HTTP/ HTTPS Web content filtering, along with email filtering for spam and malware
5	The NGFW should support stateful packet inspection and filtering technology with dynam ic user-based NAT with provision to create rules based on source & destination IP addres s, hosts, network, IP range and Geolocation.
6	Should provide policy-based traffic shaping by application. User, Group, IP address and N etwork
7	The Intrusion Prevention System should be integrated with the NGFW solution to enable it to scan packet payloads for vulnerabilities and exploits, covering a b road spectrum of attacks and vulnerabilities, Should automatically update the signatures database from a central database server atleast on a daily basis
8	Gateway level Anti-Virus/Malware solution should be appliance based and available from day one, The Firewall should scan for threats in inbound, outbound and intra-zone traffic for malware in files across all ports and TCP streams by Gateway Anti-Virus/Malware. In c ase there is any upper limit on size of files, potentially to be scanned, such upper limit sh ould not be less than 30Mb
9	Should have the option to automatically update the new virus pattern updates. Gateway level Anti-Virus/Malware should be supported for HTTP,HTTPS, FTP, SMTP, POP3
10	Should Provide advance protection to prevent zero day threats, ransomware and evolvin g malware, Mobile Malware, from day one
11	Should support HTTP/HTTPS Web content filtering.
12	Should support various form of user authentication methods simultaneously, including L ocal Database, LDAP, and RADIUS, for Single Sign On

13	The Firewall should support deep packet SSL to decrypt HTTPS traffic for Scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found
14	Should have at least 5000 IPS Signatures ,3000+ application Signature and 80+ URL categories
15	Should support device configuration and management through Web Console, CLI , SNMP and API integration
16	Should support TCP/UDP protocols for syslog collection
	High Availability:
1	The Firewall should be configured in an Active-Passive High Availability mode with real-time switch-over without any session being reset in case of malfunction
	Certifications:
1	The quoted Firewall model should be TEC certified
2	Should have atleast Common Criteria (India or Global)/NDPP/NSS/ICSALabs certification.
	Warranty and Licensing:
1	The Firewall appliance (both active and passive units) including any additional hardware module associated to it supplied by the OEM at the time of installation must be covered under 3 years Onsite Comprehensive Warranty with Advanced RMA
2	OEM should have 24x7 TAC support with Toll Free number and R&D center in India. Refer to the service assurance terms mentioned under Scope of Work, specifically point no. 5
3	License for all the software modules purchased with the appliance must be appliance based with minimum 3 years support
4	Crucial services like VPN (SSL and IPSec), networking, and Access & NAT rules should continue to work without any requirement for active license in an event of any license subscription of a software/hardware module getting expired
5	License for NGFW high availability with next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, DNS protection, advanced threat protection, cloud sandboxing and reporting etc., should be included from day one
6	In case of a dispute in terms of performance parameters during commissioning and testing, the testing equipment e.g. traffic generator to test and verify the performance parameters should be provided by the bidder

7	The solution should not go out of service in next 5 years starting from the date of purcha se

Revised Scope of Work

(Unchanged)

1. To supply, install, configure, integrate, commission and provide suppor t of NG-Firewall appliance to meet the requirements of Indian Statistical I nstitute (ISI) Kolkata for 3 years post installation.
2. The solution shall be implemented at CSSC, 4th Floor, SN Bose Bhavan, ISI Kolkata - 700108.
3. The supplied system should be integrated with the existing security ap pliances and network infrastructure of the Institute.
4. Bidder should ensure engagement of OEM during the implementation and maintenance period and should submit proof of warranty and 24x7 e nterprise support with the OEM agreement executed in the name of ISI K olkata exclusively for this project. There shall be no limitations on the ent erprise support.
5. Bidder should undertake to conduct Quality Assurance testing and assi st ISI Kolkata to perform User Acceptance Testing.
6. Bidder should provide post-implementation training to ISI Kolkata offici als for regular management and operation purpose.
7. Bidder should deliver all the relevant documents, SOPs required for the smooth implementation and operation of the project before final accepta nce. The documents and design should be vetted by the respective OEMs .
8. Bidder should provide post-implementation support for the offered syst ems by trained support engineers.
9. The selected vendor is expected to close all the vulnerabilities/weakne ss identified by ISI Kolkata in a time bound manner during implementatio n and warranty period.
10. The selected vendor is expected to comply with all the security policies of ISI Kolkata before acceptance of final solution.
11. Full documentation and SOPs of the project are to be included in the de liverables by the successful vendor.

12. The selected vendor should integrate with ISI Kolkata’s existing NTP server for setting the global time settings.

13. The successful vendor will be expected to provide all the necessary software licenses, implement, train and handover the solution to ISI Kolkata officers. The bidder would subsequently provide support through bug fixes, updates, upgrades, troubleshooting, configuration changes, etc., by providing onsite support as and when required.

14. All the supplied systems must be covered under enterprise level onsite comprehensive warranty for 3 years post installation.

15. The selected bidder must perform migration of data including all rules and policies from the existing Cisco ASA 5585 Firewall to the new one.

16. ISI Kolkata may further extend the quantity to additional user licenses for all the proposed products/ solutions at the same rate as and when required during the contract period.

17. In case of any conflict between the GeM defined Catalogue Specification/Terms & Conditions & those mentioned in ATC specified by the procuring entity, the details given in ATC will prevail. Technical Evaluation will be done as per the conditions of ATC document.

Revised Bidder Eligibility Criteria

(after incorporation of corrigendum)

1. The offered product specification should be as per the specification mentioned in Annexure-I and no deviation from it will be accepted. Compliance of BoQ specification as per Annexure-I must be submitted.

2. The Bidder/OEM should be neither blacklisted by any Government Department, nor is any criminal case registered/pending against the bidder or its owner/partners anywhere in India.

3. The bidder must provide complete technical compliance documentation in accordance with the specified technical requirements. Furthermore, the technical compliance documentation should be accompanied by a product datasheet or brochure, which should be publicly accessible on the OEM's website for verification purposes. Website link of the product line and datasheets, which may provide necessary evidence(s), must be provided.

4. Manufacturer Authorization Certificates from the OEM mentioning the specific Bid Number should be submitted for the proposed solution, failing which the bid will be rejected.

5. The OEM of the proposed solution should be an established and reputable company with a minimum of 10 years of experience within the cybersecurity sector. Bidder should submit a publicly verifiable list of such products which may show presence of the OEM for said amount of time.

6. OEM should be a reputed Firewall vendor with a market presence in India for at least 3 years, with hardware appliance-based solutions. OEM must have 24x7 online Technical Support available (details to be provided). OEM should have supplied at least 5 NG-Firewall solutions having similar or higher specifications in the last 5 years in India and PO copies with contact information of such clients should be provided with the bid.

7. The OEM must also have a proven track record in effectively identifying vulnerabilities within software systems. Documentary evidence of list of such publicly available reports may be provided as necessary evidence(s).

8. To demonstrate their expertise in threat research, the OEM should maintain a research team that has published a minimum of 20 technical documents in the past two years, specifically in areas related to cybersecurity. Documentary evidence of list of such publicly available documents may be provided as necessary evidence(s).

9. Additionally, the OEM should receive data feeds from its own threat intelligence platform, ensuring reasonable visibility and presence in the global digital landscape. Documentary evidence mentioning the name of the platform along with website link and publicly available datasheets/ reports which may be provided as necessary evidence(s).

10. The Bidder must have a registered office in Kolkata. Documentary evidence issued by any Govt. agency to this effect must be submitted.

11. ~~The OEM of the proposed solution should be among the top 15 players in last 3 published Firewall/Network Security Appliance reports by Gartner/Radicati or an equivalent rating by any organization approved by the Government of India for Firewall/Network Security Appliance. Website reference of such listshould be provided as necessary evidence(s).~~

12. Bidder must have been engaged in IT-related services at least for the last 3 years and must have supplied at least 2NG-Firewall solutions in the last 3 years. PO copy to be submitted.

13. The bidder must submit the Make In India Declaration as per the Annexure - II enclosed herewith.

14. The successful bidder may be asked to install the quoted NG-Firewall model for a trial period of up to 30 days, to ensure all performance parameters are met to the satisfaction of the user, before the final invoice is raised and the installation certificate is issued. Any issues related to performance bottleneck/throttling/hardware contention (>50%)/packet drop etc which may lead to disruption of IT services of user, will be treated as failure of trial.

15. The bidder must provide documentary evidence of having supplied at least three similar or lower-specification NG-Firewall models to reputable institutions such as Government Institutions, CFTIs, or Central Universities (preferably IITs, NITs, etc.), catering to a user base of at least 2000 users with traffic comparable to ISI Kolkata in last five years.

—

.

3. Buyer uploaded ATC document Click here to view the file.

Disclaimer

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bid. If any clause(s) is / are incorporated by the Buyer regarding following, the bid and resultant contracts shall be treated as null and void and such bids may be cancelled by GeM at any stage of bidding process without any notice:-

1. Definition of Class I and Class II suppliers in the bid not in line with the extant Order / Office Memorandum issued by DPIIT in this regard.
2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.
3. Publishing Custom / BOQ bids for items for which regular GeM categories are available without any Category item bunched with it.
4. Creating BoQ bid for single item.
5. Mentioning specific Brand or Make or Model or Manufacturer or Dealer name.
6. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
7. Floating / creation of work contracts as Custom Bids in Services.

8. Seeking sample with bid or approval of samples during bid evaluation process. (However, in bids for attached categories, trials are allowed as per approved procurement policy of the buyer nodal Ministries)
9. Mandating foreign / international certifications even in case of existence of Indian Standards without specifying equivalent Indian Certification / standards.
10. Seeking experience from specific organization / department / institute only or from foreign / export experience.
11. Creating bid for items from irrelevant categories.
12. Incorporating any clause against the MSME policy and Preference to Make in India Policy.
13. Reference of conditions published on any external site or reference to external documents/clauses.
14. Asking for any Tender fee / Bid Participation fee / Auction fee in case of Bids / Forward Auction, as the case may be.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

*This document shall overwrite all previous versions of Bid Specific Additional Terms and Conditions.

This Bid is also governed by the General Terms and Conditions