BID NO: GEM/2025/B/6995790

(NOTICE INVITING TENDER FOR THE SUPPLY, INSTALLATION, CONFIGURATION, TESTING, COMMISSIONING, AND MAINTENANCE OF **NEXT-GENERATION FIREWALL** IN HIGH AVAILABILITY MODE)

Corrigendum cum clarification for GeM Tender No. GEM/2025/B/6995790- based on pre-bid meeting held on 16/02/2026 and other queries received

The clarifications/Replies on queries raised by the bidders is as under:

S.No.	**Ref. No.**	**Actual Clause in the RFP**	**Clarification Sought /Amendment Requested**	**Remark from the vendors**	**Recommended Reply to the queries**
1	ANNEXURE-B, Page No. 15 Point No. 11	The solution must protect from known and brand-new phishing sites by stopping credential phishing in real time.	The solution must protect from known and brand-new phishing sites by blocking the website.	Since every OEM has its own proprietary technology and architecture, we request you to kindly amend this clause to allow participation of multiple OEMs/vendors by accepting equivalent technologies that meet the required functional and performance specifications.	Please refer to Corrigendum - I
2	ANNEXURE-B, Page No. 15 Point No. 13	Solution should support Advance DNS security and prevent DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection.	Solution should support Advance DNS security such as e.g. DNS spoofing, DNS poisoning, DNS hijacking & DNS tunnelling .	Since every OEM has its own proprietary technology and architecture, we request you to kindly amend this clause to allow participation of multiple OEMs/vendors by accepting equivalent technologies that meet the required functional and performance specifications.	Please refer to Corrigendum - I

3	ANNEXURE-B, Page No. 15 Point No. 23	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to IPv6) functionality	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) functionality	As discussed during Prebid meeting, the existing infrastructure primarily supports dual-stack (IPv4/IPv6) and IPv6-to-IPv4 communication. NAT46 support is deemed non-essential and has been removed from the technical specifications.	Please refer to Corrigendum - I
4	ANNEXURE-B, Page No. 16 Point No. 27	SSL/TLS inspection must be supported on any port used for SSL/TLS i.e., inspection must be supported on non-standard port as well, for SSL 3.0, TLS 1.0, 1.1, 1.2 and 1.3	SSL/TLS inspection must be supported on any port used for SSL/TLS i.e., inspection must be supported on non-standard port as well, TLS 1.0, 1.1, 1.2 and 1.3	SSL 3.0 in unsecured and all modern browsers have disabled SSL 3.0, PCI DSS prohibits its use, most enterprise security policies forbid it and Major vendors have removed support from products. Kindly consider this point and remove.	Please refer to Corrigendum - I
5	ANNEXURE-B, Page No. 17 Point No. 42	The proposed OEM shall submit a comprehensive Firewall Performance Benchmark Testing Report for the quoted model. The report must clearly demonstrate the claimed versus independently verified performance metrics. The submitted documentation shall include, - Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) All signatures enabled - Antivirus All signatures enabled - URL Filtering All categories enabled	Remove	Every OEM follows its own internal testing methodology and performance validation criteria. After conducting multiple controlled laboratory tests under defined conditions, the final validated performance results are published in the official product datasheets, which are publicly available. As per our best knowledge and industry verification, leading OEMs such as Fortinet, Palo Alto , Sophos, Cisco , Check Point and SonicWall do not provide detailed comprehensive benchmark testing reports with all security services enabled	Please refer to Corrigendum - I

		- User Identity / Identification - Sandboxing / Advanced Threat Protection - Full Logging and Reporting for all traffic and threats The performance report must correspond to the exact hardware model and software version proposed. Reports based on alternate configurations or higher-tier models shall not be accepted.		simultaneously, beyond what is officially documented in their published datasheets.	
6	ANNEXURE-B, Page No. 17 Point No. 51	Solution must have on-appliance or external (locally available) reporting storage to store logs for a minimum of 180 days as per CERT- IN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity 1 TB, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.	Solution must have on-appliance or external (locally/Cloud available) reporting storage to store logs for a minimum of 180 days as per CERT- IN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity 480 GB, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.	Since every OEM has its own hardware design, we kindly request that this clause be amended to allow participation from multiple OEMs/vendors by accepting equivalent technologies that meet the specified functional requirements and performance specifications.	Please refer to Corrigendum - I
7	ANNEXURE-B, Page No. 17 Point No. 52	Appliance syslog protocol should be compliant to RFC5424.	The proposed appliance must support the Syslog protocol and shall be capable of	Since every OEM has its own proprietary technology and architecture, we kindly request you to amend	Please refer to Corrigendum - I

			simultaneously forwarding logs to a minimum of three (03) external Syslog servers.	this clause to allow participation from multiple OEMs/vendors by accepting equivalent technologies that meet the functional requirements and performance specifications.	
8	ANNEXURE-B, Page No. 18 Point No. 63	Proposed Solution s hould be a on-premises solution wi th management and reporting solution should be placed in premises.	The proposed solution must support on-premises/cloud environments and shall include centralized management and reporting functionality. In case of a cloud-based deployment, the data center location must be within the national geographical boundaries to ensure data sovereignty and regulatory compliance.	Cloud adoption is steadily increasing across industries due to its scalability, flexibility, and cost efficiency. It reduces infrastructure dependencies and significantly lowers the costs associated with data protection, disaster recovery, and business continuity.	No change
9	ANNEXURE-B, Page No. 18 Point No. 64	Solution should not send any logs outside the on-premises network.	Solution should not send any logs outside the on-premises network. In case of a cloud-based deployment, the data centre location must be within the national geographical boundaries to ensure data sovereignty and regulatory compliance.	Cloud adoption is steadily increasing across industries due to its scalability, flexibility, and cost efficiency. It reduces infrastructure dependencies and significantly lowers the costs associated with data protection, disaster recovery, and business continuity.	Please refer to Corrigendum - I
10	ANNEXURE-B, Page No. 19 Point No. 75	Certified ICSA Firewall, NSS lab last report/ VERSION check with 93% and above exploit	Remove	as discussed during Prebid meeting, ICSA and NSS lab both are closed and no longer	Please refer to Corrigendum - I

		protection rate or equivalent Indian certification/report from STQC or other govt agency.		working. So please remove this point.	
11	2	The appliance should have at least 4 x SFP,4*SFP+ ,4 * 1G Copper RJ45 ports populated with 2*10G SFP+ SR,2*10G SFP+ LR,2*1G SFP LR,2*1G SFP SR along with 3 mtr fiber patch codes from Day 1.	The appliance should have at least 4x 25 GE SFP28/SFP+ ,4 x SFP,4*SFP+ ,4 * 1G Copper RJ45 ports populated with 2 * 25G ,2*10G SFP+ SR,2*10G SFP+ LR,2*1G SFP LR,2*1G SFP SR along with 3 mtr fiber patch codes from Day 1.	It is recommanded to asked parameters of the thorougput of the firewall have the 25 GBPS connectivity to avoid the bottlenack and the performance of the firewall.	No change
12	6	Should support 14 Gbps or more threat prevention/protection throughput enable on enterprise mix / app mix (Threat prevention throughput should be measured with Application Control, Antivirus, IPS, Antispyware, Sandboxing, **DNS Security, File blocking, Logging** -all of these enabled utilizing appmix/enterprise mix transactions)	Should support 14 Gbps or more threat prevention/protection throughput enable on enterprise mix / Realworld throughput	Every OEM have it's own ways to publish the performance parameters. Fortinet publish Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.	Please refer to Corrigendum - I
13	9	Firewall should support at least 16 Million or higher concurrent sessions with full features turned on and utilizing HTTP transactions.	Firewall should support at least 16 Million or higher concurrent sessions	Every OEM have it's own way to publish the perfromance parameters while TCP and HTTP transcations	Please refer to Corrigendum - I
14	42	The proposed OEM shall submit a comprehensive **Firewall Performance**	kindly delete this cluase	Request Performance Benchmark Testing Report. All OEM published their datasheet publicly	Please refer to Corrigendum - I

		Benchmark Testing Report for the quoted model. The report must clearly demonstrate the claimed versus independently verified performance metrics. The submitted documentation shall include, - Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) – **All signatures enabled** - Antivirus – **All signatures enabled** - URL Filtering – **All categories enabled -** User Identity / Identification - Sandboxing / Advanced Threat Protection - Full Logging and Reporting for all traffic and threats The performance report must correspond to the exact hardware model and software version proposed. Reports based on alternate configurations or higher-tier models shall not be accepted.		available which published all the perfromance parameters that can be submitted. The ask is specific report which is specific to OEM.	
15	43	Shall include at least FIVE (05) years warranty for the appliance along with license & all required subscriptions for Gateway Antivirus/Antimalware/spyware/NGFW, Web / URL/Content	Shall include at least FIVE (05) years warranty for the appliance along with license & all required subscriptions for Gateway Antivirus/Antimalware/spyware/NGF	It is highly recommanded to ask for the HA (Active-Passive , Active -Active in normal even in Virtual Firewall scenario). Even the virtual firewall support suggested to aks which major OEM is	No changes

		filtering, application filtering, IPS, and HA (as applicable). Licensing for VPN and two-factor authentication provision for 5000 users shall be provided. Required licenses for HA (active-passive) shall also be provided. The license period will be counted from date of installation and activation. The subscription must include 24X7X365 TAC support for FIVE (05) years from day 1.	W, Web / URL/Content filtering, application filtering, IPS, and HA and Virtual Firewall minimum 5 nos (as applicable). Licensing for VPN and two-factor authentication provision for 5000 users shall be provided. Required licenses for HA **(active-passive & Active-Active Both in normal and Virtual Firewall configuraiton)** . The subscription must include 24X7X365 TAC support for FIVE (05) years from day 1.	having features. 5000 users VPN and MFA request to revalidate this count as this will add the cost for solution where seems no use cases in education users where studnet laptops are not in control of IT.	
16	47	Solution should have a GUI and CLI-based management console, user threat level mapping, cloud application usage visibility, SDWAN based on jitter/latency/packet loss, reporting analyzer function, ability to identify risky users based on browsing behavior, integration provision with managed services, IPv6 certified, malicious file reports with screenshot, and dashboard file release capability.	Solution should have a GUI and CLI-based console, user threat level mapping, cloud application usage visibility, SDWAN based on jitter/latency/packe t loss, reporting analyzer function, ability to identify risky users based on browsing behavior, integration provision with managed services, OS Or proposed mdoel OR Fmaiy must IPv6 certified, malicious file reports with screenshot, and	every OEM have it's own way to publish the perfromance parameters while TCP and HTTP transcations	Please refer to Corrigendum - I

			dashboard file release capability.		
17	51	Solution must have on-appliance or external (locally available) reporting storage to store logs for a minimum of 180 days as per CERTIN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity 1 TB, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.	Solution must have **on-appliance (Hardware OR Software) from same OEM reporting** storage to store logs for a minimum of 180 days as per CERTIN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity 1 TB, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.	Recommanded to ask the logs and reporting dedicated tool from same OEM for the better integration and enhance analytics capability. Third party tool having many time multiple challages and limited capabilites.	Please refer to Corrigendum - I
18	53	Solution should have group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group.	kindly delete this cluase	Not relevant for single firewall cluster. For manage the multiple firewall seprate management solution recommanded	Please refer to Corrigendum - I
19	75	Certified ICSA Firewall, NSS lab last report/ VERSION check with 93% and above exploit protection rate or equivalent Indian certification/report from STQC or other govt agency.	Certified ICSA OEM , NSS lab last report/ VERSION/ OEM model check with 99% and above exploit protection rate or equivalent Indian certification/report from STQC or other govt agency.	93% seems to be lower ask it shall suppot minimum 99% as NSS publish report in 2019 where other OEM claims 99% or higher securtiy efficiancy in terms of exploit blok rate . This is better to ask for your organization so prooven solution help to your organization	No change

20	76	The proposed Firewall / Firewall Operating System shall be tested and certified for EAL/ NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.	The proposed Firewall / Firewall Operating System shall be tested and certified for EAL4+ and NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions with proposed model or It's Operating System OR Family or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.	better to ask EAL 4+ certification with including NDPP /NDcPP certification. Also certifcation is not done on all the model. It may be on the OS or it's family or the proposed model . So requested to support in this cluase	Please refer to Corrigendum - I
21	80	After login, the user should be able to change their passwords without administrator's approval and should also be able to log out from any or all the devices from which it is logged in.	kindly delete this cluase	Other OEM do support force a password change at next login for the user in their solution. Request for relax this cluase	Please refer to Corrigendum - I

CORRIGENDUM -1

GeM Tender No. GEM/2025/B/6995790

Sl. No.	Ref	Existing Entry	To be read as
1.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 11	The solution must protect from known and brand-new phishing sites by stopping credential phishing in real time.	The solution must protect from known and brand-new phishing sites by stopping credential phishing in real time **or by blocking the website.**
2.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 13	Solution should support Advance DNS security and prevent DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection.	**Solution should support Advance DNS security such as DNS spoofing, DNS poisoning, DNS hijacking & DNS tunnelling.**
3.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 23	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to IPv6) functionality	**Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) functionality**
4.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 27	SSL/TLS inspection must be supported on any port used for SSL/TLS i.e., inspection must be supported on non-standard port as well, for SSL 3.0, TLS 1.0, 1.1, 1.2 and 1.3	**SSL/TLS inspection must be supported on any port used for SSL/TLS i.e., inspection must be supported on non-standard port as well, TLS 1.0, 1.1, 1.2 and 1.3**
5.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 42	The proposed OEM shall submit a comprehensive Firewall Performance Benchmark Testing Report for the quoted model. The report must clearly demonstrate the claimed versus independently verified performance metrics. The submitted documentation shall include, - Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) All signatures enabled - Antivirus All signatures enabled - URL Filtering All categories enabled	**{Removed}**

		- User Identity / Identification - Sandboxing / Advanced Threat Protection - Full Logging and Reporting for all traffic and threats The performance report must correspond to the exact hardware model and software version proposed. Reports based on alternate configurations or higher-tier models shall not be accepted.	
6.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 51	Solution must have on-appliance or external (locally available) reporting storage to store logs for a minimum of 180 days as per CERT- IN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity 1 TB, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.	Solution must have on-appliance or external (locally available) reporting storage to store logs for a minimum of 180 days as per CERT- IN Guidelines and historical various types of reports, including bandwidth usage, application usage, web usage, Threat Protection, and compliance reports. Minimum hard drive capacity **more than 900GB**, expendable upto 4 TB. Capable for supporting logs for 5000 users over a period of 180 days.
7.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 52	Appliance syslog protocol should be compliant to RFC5424.	Appliance syslog protocol should be compliant with RFC5424 **or better, or the latest.**
8. .	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 64	Solution should not send any logs outside the on-premises network.	Solution should not send any **user data** outside the on-premises network
9.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 75	Certified ICSA Firewall, NSS lab last report/ VERSION check with 93% and above exploit protection rate or equivalent Indian certification/report from STQC or other govt agency.	**{Removed}**
10.	ANNEXURE-B Detailed Technical Specifications section on	Should support 14 Gbps or more threat prevention/protection throughput enable on enterprise mix / app mix (Threat prevention throughput should be measured with Application Control, Antivirus, IPS, Antispyware, Sandboxing,	Should support 14 Gbps or more threat prevention/protection throughput enable on enterprise mix / app mix **/ Realworld throughput with full features turned on.**

	Page No. 15, Point No. 6	**DNS Security, File blocking, Logging** -all of these enabled utilizing appmix/enterprise mix transactions)	
11.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 9	Firewall should support at least 16 Million or higher concurrent sessions with full features turned on and utilizing HTTP transactions.	Firewall should support at least 16 Million or higher concurrent sessions with full features turned on.
12.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 47	Solution should have a GUI and CLI-based management console, user threat level mapping, cloud application usage visibility, SDWAN based on jitter/latency/packet loss, reporting analyzer function, ability to identify risky users based on browsing behavior, integration provision with managed services, IPv6 certified, malicious file reports with screenshot, and dashboard file release capability.	Solution should have a GUI and CLI-based management console, user threat level mapping, cloud application usage visibility, SDWAN based on jitter/latency/packet loss, reporting analyzer function, ability to identify risky users based on browsing behavior, integration provision with managed services, IPv6 **compatible**, malicious file reports with screenshot, and dashboard file release capability.
13.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 53	Solution should have group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group.	Solution should **support** group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group.
14.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 76	The proposed Firewall / Firewall Operating System shall be tested and certified for EAL/ NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.	The proposed Firewall / Firewall Operating System shall be tested and certified for EAL and NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions **with proposed model or It's Operating System OR Family** or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.
15.	ANNEXURE-B Detailed Technical Specifications section on Page No. 15, Point No. 80	After login, the user should be able to change their passwords without administrator's approval and should also be able to log out from any or all the devices from which it is logged in.	Users should be able to change their passwords without administrator approval.

- **All other terms and conditions, along with the last date of submission of the bids of the bid document, remain unchanged.**