RAJASTHAN HIGH COURT, JODHPUR

Corrigendum cum Clarification

No. HC/SK/2025-26/ 694

Dated: 03.02.2026

Ref: NIT No. HC/SK/Procurement/2025-26/40 Date: 19.01.2026

Sub: Bids for the Supply, Installation & Maintenance of 01 number of Server, 01 number of Firewall and 36 number of Assistive listening system at Subordinate Courts of Rajasthan, High Court, Jodhpur and Jaipur Bench, Jaipur under E-Court Project Phase-III

I am directed to issue a corrigendum cum clarification after Pre-bid meeting for the advertisement of Bids for the Supply, Installation & Maintenance of 01 number of Server, 01 number of Firewall and 36 number of Assistive listening system at Subordinate Courts of Rajasthan, High Court, Jodhpur and Jaipur Bench, Jaipur under E-Court Project Phase-III as under:-

S. No	RFP Page No.	RFP Clause Parameter	Sub Section	Clause Details	Response to pre-bid suggestions or query	Change or corrigendum proposed
Item No. 2 Firewall						
1	22	High Availability	**8.**	Active/Active and Active/Passive and should support session state synchronization among firewalls in a high availability cluster.	No change	
2	22		**10.(10)**	The firewall must disallow root access to firewall system all users (including super)	Modified as per new specs received from Hon'ble eCommitte. SCI	The firewall must have the ability to manage firewall policy even if management server is unavailable
			10.(12)	Solution should have machine learning capabilities on the data plane to analyze web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			10.(13)	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood (Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks.	No change	
3	23		**11.(6)**	Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, POP3, FTP, SMB traffic with configurable AV action such as allow, deny, reset, alert etc.	No change	
			11.(7)	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs.	No change	
			11.(8)	Should support inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			11.(9)	The device should support zero day prevention by submitting the executable files and getting the verdict back in five minutes post detection	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
	23		**11.(12)**	The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan	No change	

				while some applications to be included.		
			11.(16)	The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen.	No change	
			11.(17)	Automatically identify and block phishing sites.	No change	
			11.(18)	Prevent users from submitting credentials to phishing sites	No change	
			11.(19)	Prevent the use of stolen credential	No change	
4	23	Advanced Persistent Threat (APT) Protection	12.(1)	There should be provision to enable the APT solution if required in Future with following features. This should be a both on premise and cloud base unknown malware analysis.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			12.(3)	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
	23		12.(4)	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
5	23	URL Filtering feature enabled from day 1	13.(1)	NGFW should protect against evasive techniques such as cloaking, fake CAPTCHAS, and HTML character encoding based attacks	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			13.(3)	NGFW should support policy creation around end user attempts to view the cached results of web searches and internet archives from day 1	Modified as per new specs received from Hon'ble eCommitte. SCI	The solution should support policy creation around end user attempts to view the cached results of web searches and internet archives
6	23	DNS Security Features from day 1	14.(3)	DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control	Modified as per new specs received from Hon'ble eCommitte. SCI	DNS Security should support predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control
	24		14.(4)	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations	Modified as per new specs received from Hon'ble eCommitte. SCI	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains/malicious/phishing/spam
			14.(5)	It should prevent against new malicious domains and enforce consistent protections for millions of emerging domains	Modified as per new specs received from Hon'ble eCommitte. SCI	It should support prevention against new malicious domains and enforce consistent protections for millions of emerging domains
			14.(6)	The solution should support integration and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate with URL Filtering to continuously crawl newfound or un-categorized sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots.	Modified as per new specs received from Hon'ble eCommitte. SCI	The solution should support integration and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate with URL Filtering to continuously crawl newfound or un-categorized sites for threat indicators.

			14.(7)	Should support simple policy formation for dynamic action to block domain generation algorithms and sinkhole DNS queries.	No change	
			14.(8)	Solution should have prevention against DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			14.(9)	The solution should be capable to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers.	Modified as per new specs received from Hon'ble eCommitte. SCI	The solution should support capabilities to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the newly observed domain.
			14.(10)	The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink-holing malicious domains to cut off Command and control.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
7	24	SSL/SSH Decryption	15.(3)	The firewall must have the capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			15.(4)	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections	Deleted as per new specs received from Hon'ble eCommitte, SCI	Deleted
			15.(7)	The firewall supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring).	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
8	24	Routing and Multicast support	18.(6)	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address	Modified as per new specs received from Hon'ble eCommitte. SCI	The solution should also support FQDN besides IP address for static route next hop, policy based forwarding next hop and BGP peer address.
			18.(7)	The firewall must support VXLAN Tunnel content inspection	No change	
			18.(8)	The firewall must support DDNS provides such as DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org and No-IP.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			18.(13)	PIM-SM, PIM-SSM, IGMP v1, v2, and v3	Modified as per new specs received from Hon'ble eCommitte. SCI	PIM-SM, IGMP
9	25	Monitoring, Management and Reporting	20.(1)	Should provide on device as well as centralized management and reporting solution with complete feature parity on firewall administration. The Central Management and Reporting Solution should be a dedicated OEM appliance with	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
			20.(2)	There should be provision to permanently block the export of private keys for certificates that have been generated or imported to harden the security posture in order to prevent rogue administrators from misusing keys.	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
	25		20.(7)	Should be able to create report based on SaaS application usage	Deleted as per new specs received from Hon'ble eCommitte. SCI	Deleted
Additional points for Firewall as per new specs received from Hon'ble eCommitte, SCI						
10		Testing and Certification		The product should be TEC MTCTE certified		New clause added
				The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant		New clause added

				for consecutive 5 years		
11		Architecture		The proposed NGFW should have feature for processing of a packet in one go method or it should have a specific security processing unit which should perform functions like networking, user identification, policy lookup, traffic classification with application identification, decoding, signature matching for identifying threats and contents.		New clause added
				Required performance throughput should be available in single unit of proposed solution without HA/ Clustering/ stacking, all the parameters must be validated using publicly available datasheets.		New clause added
	21		4.(2)	The proposed firewall must have min 8 physical cores with x86 processor	Modified as per new specs received from Hon'ble eCommitte, SCI	The proposed firewall must have min 8 physical cores with x64 processor; minimum 24GB RAM from day one and should have 400 GB inbuilt SSD Proposed Firewall can be ASIC based in nature / open architecture.
12	21	Storage	5	The NGFW should have 240 GB or higher solid-state drives for System storage.	This clause is already covered in Architecture clause	Deleted
13	21	Interface Requirement	6.(2)	Minimum 6*1G SFP and Minimum 4x 1/10Gig SFP/SFP+ ports fully populated with SR transceivers from day 1	Modified as per new specs received from Hon'ble eCommitte, SCI	8 x 1/10Gig SFP/SFP+ with minimum 2*SFP+ SR transceivers from day one; 4 x 1 Gig SFP Ports from Day one
			6.(3)	Dedicated 2x HA ports with active optical cable of minimum 5 meter length in addition to requested data ports, OOB, Console Management and USB Port	Modified as per new specs received from Hon'ble eCommitte, SCI	Dedicated HA ports with active optical cable of minimum 5 meter length in addition to requested data ports, Mgmt, Console and USB Port
14		Next Generation Firewall Features		The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment		New clause added
				The firewall must have the ability to manage firewall policy even if management server is unavailable		New clause added
				Firewall appliance must have at least 10 (active from day-1) with each virtual firewall/domains/instances having a separate administrative control OR equivalent, Security zones and VLAN, Associated Licenses, Software and Hardware towards Virtual domains/ Virtual Firewalls/Virtual instances.		New clause added
				The following features must be available in each virtual firewall: domain/instant context environment: Firewall,IPSEC VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy-based routing, DDOS, User and Group management, Logging and Reporting.		New clause added
				Should protect against phishing and JavaScript		New clause added
				Ready for post-quantum threats using NISTapproved algorithms like ML-KEM and emerging algorithms like BIKE, HQC, and Frodo to protect		New clause added

				against harvest-now, decrypt-later attacks		
				File filter capability to block specific file types, including password-protected files from being uploaded/ downloaded		New clause added
				Ability to sanitize Microsoft Office documents and PDF files by stripping harmful active content (hyperlinks, embedded media, JavaScript, macros) while preserving textual content integrity		New clause added
15		Threat Protection		The solution should have File Filter capabilities to block certain files, specifically the password protected files from being uploaded/ downloaded.		New clause added
				To help prevent tampering, the Appliance should have Trusted Platform Module (TPM) chip soldered on the motherboard to reduce the risk of data transaction interceptions from attackers. This is used to protect the passwords and private keys against malicious software and phishing attacks. The dedicated module helps in generating, storing, and authenticating cryptographic keys		New clause added
				Should support more than 15,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS)		New clause added
				Must support various form of user Authentication methods simultaneously, like: Local Database, LDAP server, RADIUS server, TACACS+ server and PKI methods.		New clause added
16		DNS Security capabilities		For Malicious DNS domain database Should take inputs from multiple third-party sources of threat intelligence.		New clause added
17		Certification		Firewall should be IPv6 Certified/IPv6 logo ready		New clause added
				Common Criteria (ISO/IEC 15408) EAL/ EAL4 or higher or NDcPP or ICSA NIAP/CCEVS Protection Profiles certification for the model or family		New clause added
				Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 or EN 61000 or EN 62368 Standards for Safety requirements of Information Technology Equipment		New clause added
Changes Date & Time						
18		Page No. 4.6 (Bid Dates) & Page No. 8 (Key Timelines)		Online Bid (Techno-commercial and Financial) Submission Closing Date and Time	03/02/2026 at 05.:00 PM	11/02/2026 at 05.:00 PM
				Submission of Banker's Cheque/Demand Draft/ Bank Guarantee for Tender Fee, EMD,and Processing Fee*	04/01/2026 at 11.00 AM	12/02/2026 at 11.00 AM
				Bid (Techno-commercial) opening Date and Time	04/01/2026 at 11.30 AM	12/02/2026 at 11.30 AM

Corrigendum cum clarification is also available on Rajasthan High Court website www.hcraj.nic.in and https://sppp.rajasthan.gov.in portal. The rest of contents of NIT will remain same.

By Order,

03/02/26

Registrar (Classification-II)