Government of West Bengal

Government of west Bengal
Office of the Administrator Forensic Science Laboratory
37/1/2, Belgachia Road, Kolkata - 700 037.

No. 1083**/FSL/Corr/ET-14/2026-27** **Dated: 31.08.2026**

Corrigendum

Amendment of Technical Specification & Extension of Date for Submission of e-tender

The **Technical specification** for procurement of Procurement of Fortinet Firewall 120G series (UTM) for Network Security with 1 year License for FSL, HQ, Kolkata vide e-Tender vide Tender ID: 2026_WBFSL_1038192_1 and Tender Reference Number: SFSL/KOL/ET-14/2026-27 has been **amended** hereunder for better participation-

Accordingly, the last date of submission of bid has been scheduled on 07.09.2026 at 16:00 hours and the opening date will be 10:00 hrs.

Amended Specifications of Firewall (UTM):

Hardware Architecture	The proposed hardware-based firewall should not consume more than 1RU Rack-mountable space.
	Appliance must have one Console port, dedicated one GbE management Port, at least one USB 3.0 for WWAN USB card support (5G/LTE/4G/3G) and should support AC power supplies provide 1+1 redundancy.
	The device should have 16 × 1G Copper ports, 4 × 10G SFP+ ports.
	Appliance should have minimum 256 GB SSD Storage for log retention.
Performance & Scalability	Appliance shall support 5 Gbps or more Firewall throughput & 2.8 Gbps or more IPS throughput.
	Appliance shall support 2.8 Gbps Threat Protection throughput with Gateway AV, Anti-Spyware, IPS and Application Control enabled.
	The device shall support Concurrent Sessions: 2 Million or higher & New connection/Sec: 20,000 or higher.
	Firewall shall support at least 2 Gbps or more IPSec VPN throughput and 2000 IPSec Site-to-Site VPN tunnels. Firewall shall support 1000 or more IPSec VPN clients.
	Should support BGP, OSPF, RIP v1/v2 routing protocol and IPv4 & IPV6 functionality (Both phase 1 and Phase2).
	Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration.
	Should have Layer 2 bridge or transparent mode, Sniffer mode.
	Solution should support policy based routing, Application based routing and also Multi Path routing.

	Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback. Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly rerouting traffic between endpoints through alternate routes.
	Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Route-based VPN over OSPF, RIP, BGP.
	Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Proposed Appliance should support SD WAN features without adding any additional hardware components & necessary licenses, if required, need to be provisioned from day 1.
	Should have support to enable guest users to use their credentials from social networking services to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should act as Wireless LAN Controller from day 1.
	Firewall should have NAT and Routing rule which helps in finding real-time statistics.
Firewall Security Features	Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files.
	The firewall should have low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol.
	Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
	Should support deep packet SSL to decrypt HTTS traffic for Scanning (IPs, Gateway Antivirus, content Filtering, Web filtering, Application Control) transparently for future requirement and then re-encrypt and send to destination if no threat found.
	The firewall must support integratation with appliance based Sandbox technology from the same as the Firewall and OEM must have own Advanced Threat Protection solutions.
	The appliance Sandbox should support technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware.
	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.
High Availability	Proposed solution should support failover in case of primary hardware failure without session loss and manual intervention.
	Proposed solution should support Active/Passive with State Sync or Active/Active.
Visibility and	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.

Monitoring	The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services status.
	Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats.
Management & Reporting	The management platform must be accessible via a web-based interface and without any additional client software.
	Firewall should support management via Cli, SSH ,GUI and support for SNMPv2/3. The solution should support Centralize management which includes configuration, logging, monitoring, and reporting are performed by the Management Centre on-prem.
	The on-prem Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator.
	The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address.
	Analytics platform 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 IPFIX or Net Flow protocols for real time and historical monitoring and reporting.
Certification, Warranty, Installation, Configuration Testing and Commissioning	Proposed Solution should support 24x7x365 telephone, email and web-based technical support.
	Manufacturer's warranty should be mentioned minimum 01 (one) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection, Advance Threat Protection and 01 (one) year for hardware malfunctioning.
	Bidder must carry out on site installation, configuration, testing, and commissioning.

The Tender Inviting Authority reserves the right to cancel the N.I.T. at any time due to unavoidable circumstances and no claim in this respect will be entertained.

1/9/26

Administrator
Forensic Science Laboratory
West Bengal