GOVERNMENT ENGINEERING COLLEGE, Kozhikode	
NOTICE INVITING E-TENDER	
No.GECK/898/24-P1	Dated : 23-10-2025
Tender No.	P1/03/2025-26
Subscription	Purchase and Installation of INTERNET FIREWALL for this institution.
Last date and time of receipt of tender	20/11/2025 3 PM On the website (www.etenders.kerala.gov.in)
Date and time of opening of tender	21/11/2025 3 PM
Bid Validity	120 days
Bidding Fee	₹.2,100/- + GST 378/-
E.M.D required	₹.14,168/-

Conditions:

Price: Should include all charges and taxes which specifically stated.

Payment: Will be made only after the successful supply, installation of the items as per supply order.

Delivery F.O.R: Govt. Engineering College, Kozhikode.

Agreement: Preliminary Agreement in **Kerala Stamp Paper worth ₹.220/-**(Preliminary Agreement shall be uploaded without fail otherwise bid will not be considered)

Delivery Condition: Within 4 to 6 weeks from the Supply Order Guarantee/Warrantee: 3 year security subscription with warranty. Specified in the specification of items list.

Date of opening: In case the proposed date declared as holiday, the tender will be opened on the next working day in the same time.

Special Conditions

- The bidder must furnish name of institutions (under this department and others) in Kerala where the same items were supplied.
- Proforma Report/Original Pamphlet/Warranty Certificate/Preliminary Agreement in Kerala stamp Paper

worth ₹.220/- are required

- The demonstration of the item/equipment will have to be arranged by the bidder before the evaluation committee during technical evaluation and if any of the items/equipment is not found suitable and/or up-to-the mark by the Committee, the same shall be liable to be rejected.
- The firm must have proven knowledge and expertise in standard system installation, commissioning and providing training.
- The price must be quoted in INR ₹

After E-tendering the hard copies of all the tender documents except BOQ/Schedule should be submitted to the Principal, Government Engineering College, Kozhikode and cover should be superscribed with the tender id, closing date and opening date of the tender.

NB: The tender procedure will be made as per Rules mentioned in the Revised Store Purchase Manual. The bidders should participate this tender through E-tendering System. Tender cost and EMD should be submitted only through online. For more details contact phone number 0495 2383220.

E A Jasmin
PRINCIPAL, EC

Signed by
E A Jasmin
Date: 23-10-2025 12:49:35

Specification

The detailed specification of the proposed firewall is as follows.

Sl. No.	Description	Qty	UoM
1	Firewall supporting 1000 Users, 8xGbE copper ports, 2 x 10 GbE SFP+ slot, inbuit HDD supporting logs	1	Nos
1.1	3 year Security Subcription with warranty	1	Nos

Sr No	General Specification for Firewall
1	General Requirement
1.1	Device should be based on 64-bit hardware platform & based on Multi-Core Architecture with Optimization for excellent throughput for all your key processes
1.2	The Proposed solution should have option for visibility into encrypted traffic flows, support for TLS 1.3 without downgrading the performance.
1.3	The device should be having security functions like Firewall, VPN (IPsec Site to Site &SSL Client VPN), Gateway level antivirus, Category-based web and application filtering, Intrusion prevention system, Traffic shaping, Cloud Sandboxing, DoS/DDoS.
1.4	Solution should offer Zero day Protection with advanced Sandboxing engine with static and dynamic analysis.
1.5	Sandboxing solution should log all the files scanned and should provide screenshot of dynamic file execution.
1.6	Solution should support multi factor authentication on appliance or by using external authentication server for minimum 500 VPN users and same MFA should also be applicable for user portal, and Web admin from day one.
1.7	Solution should support Multiple WAN link balancing multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules, should support more than two ISP
1.8	Solution should support Threat Response capability integrating with same OEM XDR to automatically isolate active adversaries and threats on the network and prevent lateral movement or communication.
1.9	Solution should have Policy test simulator tool for firewall rule and web policy simulation and testing by user, IP, and time of day.
2	Hardware & Performance Requirement

2.1	The appliance should support 8xGbE copper ports ,2 x 10 GbE SFP+ slot
2.2	Firewall must Support SSL scanning Throughput of minimum 2.3 Gbps
2.3	Firewall must support at least 12 million concurrent connections
2.4	Firewall must support at least 180,000 new sessions per second of processing.
2.5	Firewall should support min 100 GB SATA-SSD build in HW
2.6	Firewall should support integrated IPS throughputs of minimum 10 Gbps.
2.7	Device should have a minimum Firewall throughput of 45 Gbps.
2.8	Firewall should have a minimum Threat Protection throughput 2 Gbps.
2.9	Firewall should have a minimum NGFW throughput of 9 Gbps.
2.10	Firewall should have a minimum IPsec VPN throughput of minimum 22 Gbps
3	General Features
3.1	Firewall should support CLI and GUI based access to the firewall modules.
3.2	Should support Local authentication and integration with third party authentication solutions like, Active Directory, LDAP Server, RADIUS, TACACS+, eDirectory and Kerberos
3.3	Centralized, daily updates, automatic and manual updates or offline update.
3.4	Firewall should have Advance Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
4	Web Filtering
4.1	Firewall should support minimum of at least 90+ predefined categories.
4.2	Should have flexibility to create network, user, Web and app-based traffic shaping (QoS) policy.
4.3	Exceptions based on network objects defined.
4.4	Notification of custom messages or URL redirection.
5	Intrusion Prevention System
5.1	IPS should protect for 5,000+ Signatures database.
5.2	Firewall should block attacks such as DoS- SYN, IP/ICMP/TCP/UDP related attacks.
5.3	Solution should have IPS deep packet inspection engine
5.4	IPS should have option to create custom signature
5.5	Firewall should block attacks such as DNS cache poisoning, FTP bounce, improper commands.
6	Application Control
6.1	Firewall should have feature to identify, allow, block or limit usage of applications beyond ports and protocols.
6.2	Firewall should provide protection against Block potentially unwanted Applications
6.3	Application signature database of minimum 3500+ Applications for Application Control
7	SD WAN

7.1	Should have inbuild SD WAN technology with application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications
7.2	The Solution should support performance-based SLAs to automatically select the best WAN link based on jitter, latency, or packet-loss
7.3	Should support multiple WAN link options including VDSL, DSL, cable, LTE/cellular, and MPLS
7.4	Should provide real-time insights into latency, jitter and packet loss for all WAN links
7.5	Should maintain application sessions when link performance falls below thresholds and should make a transition to a better performing WAN link
7.6	Should have a centralized SDWAN management platform to create Multiple site-to-site VPN tunnels between network locations using an optimal architecture like hub-and-spoke, full mesh, or some combination.
7.7	Centralized management should have wizards for easy and quick creating of SDWAN Connections
8	Logging & Reporting
8.1	Firewall logs must contain information about the firewall policy rule that triggered the log
8.2	Firewall must provide at a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.
8.3	Firewall should have support to log (in detail) all connections which are blocked or pass through the firewall.
8.4	Firewall should have support to generate performance statistics on real-time basis.
8.5	Solution should have Reporting with minumum 6 months of storage from Same OEM
8.6	Should Support 100+ drilled down reports on the appliance
9	OEM Criteria
9.1	Proposed solution should have Common Criteria EAL4+
9.2	Proposed solution should have Manufacturer Authorization (MAF)
9.3	Proposed solution should have MTCTE certification from TEC
9.4	Proposed solution should be Make In India
9.5	OEM should have ISO 27001 Certification
9.6	Solution should be listed in Latest Gartner Magic Quadrant for Network Firewalls
9.7	OEM Should be SOC2 Type 2 compliant
9.8	OEM should be exisiting in the industry for Past 15 years or More
10	Licenses & Warranty
10.1	Three Year Subscription licenses for Firewall, Advanced Threat Protection, Intrusion Prevention System (IPS), Anti-malware, Web and App visibility control, Cloud Sandboxing , 24x7 OEM support, security and software updates.

GOVT. ENGINEERING COLLEGE * GOVT. OF KERALA * DEPT. OF TECH. EDN. * KOZHIKODE *

PRINCIPAL
GOVT. ENGINEERING COLLEGE
WEST HILL, KOZHIKODE
KERALA - 673 005

9/6/25
SUMESH. E
PEN : 632457
Computer Programmer (HG)
Govt. Engineering College, Kozhikode