



Phone : 0484-2541193
: 0484-6533184
Fax : 0484-2556863
: 0484-2558741
Email : ercmpu@milma.com
GSTIN : 32AAAAE0621L2Z8

Ernakulam Regional Co-operative Milk Producers' Union Ltd No. E 150 (D)

Head Office: PB No. 2212, Edappally, Cochin - 682 024
(An ISO 9001:2015 & ISO 22000:2018 Certified Company)

No. EU/PUR/10/COMP/2025-26 / 494

22.01.2026

QUOTATION NOTICE

Sealed quotations are invited from reputed firms for the supply, installation, and 5-year comprehensive support of a Next Generation Firewall (NGFW) system at ERCMPU, Head Office, Edappally, Kochi.

1. Terms and Conditions

1. **Estimated Cost:** Total ₹2.00 Lakhs (approx.) for a 5-year period.
2. **Period of Contract:** 5 years, effective from **01.02.2026**.
3. **EMD: Rs. 5,000/-** (EMD of the successful bidder will be released only after completion of contract period.).The quotation should be accompanied by a crossed Demand Draft for **Rs.5,000/-** drawn in favour of Managing Director, ERCMPU LTD., payable at Ernakulam towards the Earnest Money Deposit (non-interest bearing). EMD of unsuccessful bidders shall be refunded without interest after final selection of the party only.
4. **Payment Terms:** Payment will be processed within 15 days of successful installation, activation, and submission of the original invoice.
5. Successful bidder should execute an agreement within 7 days from the date of purchase order in non-judicial stamp paper (Kerala) worth ₹ 200/- for satisfactory completion of work. **If the successful bidder does not complete the assigned work or discontinues the work in between the damage / expenses incurred to ERCMPU shall be recovered from the belongings of the bidder.**
6. The successful Bidder shall obtain membership with ERCMPU by paying a nominal membership fee of Rs. 90.00.
7. **Submission Deadline:** Quotations must reach this office on or before **30.01.2026 by 1:00 PM**. Quotations will be opened at **01:30 PM** on the same day.

Scope of Work

1. **Subscription & Support:** Provision of a **Full Bundle 24x7 Support Subscription for 5 years**, including all security patches, firmware updates, and real-time threat intelligence.
2. **Comprehensive Maintenance:** Total maintenance of both Hardware and Software, including regular preventive health checks.
3. **On-Site Repairs & Continuity:** All repairs must be conducted **on-site** without interrupting internet services.
 - No parts shall be removed from the premises without prior written sanction and formal acknowledgement.
 - If a unit is not repairable immediately, a **substitute unit** of equal or higher configuration must be provided at the Supplier's cost and risk to **ensure zero downtime**.

4. **Incident Response:** Any reported malfunction or system alert must be attended to and cleared immediately to ensure network security and uptime.
5. The Technical specification of firewall is attached herewith .
6. For further clarification you may please contact MIS Section at Head Office Edappally during the office hours. (Ph No. 0484 2986049)

Eligibility Criteria

1. The bidder must have a minimum of **3 years of experience** in maintaining NGFW systems (Hardware & Software) for Central/State Government Departments, PSUs, or reputed Private Sector companies.
2. The bidder must have successfully provided similar services of equivalent capacity to **at least 2 organizations** (Government/PSU/Private) within the last 3 years.
3. The firm must have adequate local physical infrastructure and a dedicated technical team to provide prompt on-site support.
4. Copies of Work Orders and the **Manufacturer Authorization Form (MAF)** must be submitted along with the quotation to prove eligibility.

The **Managing Director, ERCMPU**, reserves the right to accept or reject any or all offers or to cancel the tendering process at any time prior to the award of the contract without incurring any liability.

To

All Notice Boards. Website
Copy to: Head(Fin)/Head (MIS/Systems),Mf/oc


Managing Director

Attachment: Technical Specification (Description & Additional Features)



Technical Specification of Firewall for Head Office

Make :

Model :

Sno	Description	Value	Compliances (Yes/No)
1	Type	NGFW	
2	Form Factor (RU)	Desktop	
3	Features	Layer 3 - Layer 4, NAT, VPN, Application Visibility and Control (AVC), User Identity, Next Generation Intrusion Prevention System (IPS), Zero Day Protection / Advance Malware protection, Web Security Essentials / URL Filtering/ DNS Filtering	
4	Traffic handled	TCP,UDP,HTTP/TCP,TCP/UDP	
5	Packet Size (Byte)	1518	
6	Throughput with all features enabled (Under Test Condition) (Mbps)	1,000	
7	Throughput (Real World/Prod Performance)(Under Test Condition) (Mbps)	3,000	
8	Concurrent Session/Concurrent Connection	9,00,000	
9	New session/Connection per second	9,000	
10	Type of Interface Supported	GE Copper	
11	Number of GE Copper interface	8	
12	TLS/SSL inspection and decryption throughput (Mbps)	500	
13	IPSec VPN throughput (Mbps)	1,300	
14	Maximum DPI-SSL Connections	30,000	
15	Number of Ipsec VPN Peers supported (Site to Site)	100	
16	Number of Ipsec VPN Peers supported (Client to Site)	200	
17	Number of SSL VPN Peers supported (Client to Site)	100 (Should Support Atleast 50 Nos From Day 1)	
18	Storage Capacity (GB)	128	
19	Type of Processor	X86 or better	
20	Firewall Policies - License	Yes	
21	Details of the Firewall Policies for the Firewall provided with the License	Web Security Essentials / URL Filtering, IPS License,Application Visibility License, APT (Advance Persistant Threat) License (Anti Malware Protection , C& C attacks, Geo IP Protection, Zero Day Threat Protection), Gateway Anti virus, Gateway Anti spam.	
22	NGIPS Sigature supported	10,000	
23	Security Intelligence	IP,URL,Domain	
24	Certification	Common Criteria, NSS Labs (latest), ICSA Labs for Firewall & Anti Virus & FIPS 140-2	
25	IPv6 Ready from day 1	Yes	
26	On Site OEM Warranty (Year)	5	
Additional Features:			
1	The Firewall should Support for TLS 1.3 to improve overall security on the firewall. Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found. Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams. Firewall should scan for threats in both inbound and outbound and intra-zone traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV. The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats. Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture. The firewall should support DNS Filtering, DNS Sinkhole service and DNS Tunnel detection.		

2	Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify. URL database should have at least 15-20 million sites and 85 + categories. Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 10,000 IPS signatures or 20,000 DPI signatures, 3000 Anti-Spyware signatures and minimum 60 million Cloud AV signatures. The solution should have Granular content filtering allowing customer to block content using the predefined categories or any combination of categories. Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. The Solution must have full API support for management & SAML support for authentication.	
3	Solution should support both on premise and cloud based Multi-engine Sandboxing for preventing zero day threats. The on-premise sandboxing support should be from the same OEM. The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc. Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. 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.	
4	Should have secure SD-WAN that enables organizations to build, operate and manage secure, high-performance networks across remote sites for sharing data, applications and services using low-cost internet services without adding any additional components or hardware. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1.	
5	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 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. The solution should support Wireguard to allow remote users to securely access applications remotely from any device or network.	
6	The proposed solution should support active-passive high availability. The device should support stateful session failover to a standby appliance in the event of a hardware failure without any manual intervention. To achieve Active-Passive HA, the solution should use only one subscription license for two appliances in HA. Should support Zero-Touch registration & provisioning using mobile App.	
7	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. The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status. Solution should support granular network visibility of network topology along with host info. Solution should have real-time visibility of infected hosts, critical attacks, encrypted traffic information & observed threats. The Central Management platform should be on-premise and should have necessary resource allocation for smooth functioning of the management and analytics. Analytics platform should have Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem	
8	The Centralize management platform should support multidevice firmware upgrade, certificate management, global policy template to push config across multiple firewall in single click.	
9	The Management platform shall be appliance/VM based including log storage/ Management and shall support analysis and reporting of firewall logs. Should have Multi Tenant and Device Group level management.	
10	The solution should support Application Visualization and Intelligence - should show historic and real-time reports of what applications are being used, and by which users. Reports should be completely customizable using intuitive filtering and drill-down capabilities.	
11	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.	
12	The Firewall solution offered must be ICSA certification for Network Firewall and Anti Virus & Common Criteria certification	
13	The firewall should have FIPS 140-2 and IPv6/USGv6 certifications from day 1.	
14	Firewall OEM should have TAC/R&D center in INDIA. The product should have TEC Certificate recommended by MeitY.	
15	Proposed Solution should support 24x7x365 telephone, email and web-based technical support.	
16	Manufacturer's warranty should be mentioned minimum 06 (six) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, Bot protection, ATP, Patch & Firmware upgrade. The Firewall should also cover embedded Cyber Warranty upto \$100,000, including compensation for covered losses that lead to business interruption from a) Non-volumetric DDOS attack & b) Unauthorized remote access.	
17	Proposed solution should have Manufacturer authorization (MAF).	