Enhancing Urban Mobility

Kenya Urban Roads Authority

Barabara Plaza Mazao Road, Off Airport South Road
P.O BOX 41727-00100 Nairobi, Kenya
0717 105 233 / 020 801 3844/ 020 272 2222
info@kura.go.ke www.kura.go.ke

Ref. No KURA/EO/SCM/3/Vol 31(7) Date: 1st December, 2022

To All Bidders

RE: PROCUREMENT OF ICT FIREWALL, LICENSES, CONFIGURATION AND TRAINING
TENDER NO: KURA/RMLF/HQ/339/2022-2023

CLARIFICATIONS NO.1

Reference is made to the above subject matter.

This is to notify all bidders that clarifications has been issued for the above tender as attached:

The closing/opening date remain the same as per the tender notice on **8th December, 2022 at 10.00am.** at **Supply Chain Management Office on Ground floor Barabara Plaza, Block D.**

Details of the clarification can be accessed on our **Website on** www.kura.go.ke.

Saadia Haji Adankhalif
FOR: DIRECTOR GENERAL

CLARIFICATION FOR

PROCUREMENT OF ICT FIREWALL, LICENSES, CONFIGURATION AND TRAINING, TENDER NO: KURA/RMLF/HQ/339/2022-2023

Line Item N°	Page No.	Description of Goods	Clarification
1	54	Hardware plus 24x7 Care and Guard Unified Threat Protection bundle (UTP) **(24x7 Care and protection 1 year license:** (Firmware and General Upgrades, UTP Services Bundle (IPS, AV, Botnet IP/Domain, Mobile Malware, Botnet, Cloud Sandbox including Virus Outbreak Protection and Content Disarm & Reconstruct, Application Control service, Web & Video Filtering and Antispam Service))	One (1) year
2	55	Annual support and Maintenance- KURA HQ and 10 regional offices	Firewall equipment to be installed at Head Quarter offices
3	56	2. Technical Specifications	See attached document for clarification
4	59	2. Technical Specifications	This is a detailed firewall specification. NB: Both Specifications shall be used to quote for the firewall

2. Technical Specifications

Summary of Technical Specifications: The Goods and Related Services shall comply with following Technical Specifications and Standards

NO.	ITEM	DESCRIPTION	COMPLIANCE – (F, P, N)	BIDDERS RESPONSE
	Threat Prevention	Prevent Known and Zero-day Threats - Zero-day protection offering network security with evasion-resistant malware detection and complete protection from the most advanced attacks, ensuring quick delivery of safe content to users.		
	Featured in Latest Gartner Report	The proposed firewall must be featured as a Leader in the latest Gartner **Magic** Quadrant for Network Firewalls		
	Security solutions	Threat Prevention and Sandblast must be included		
	Security management	Integrated central unified management.		
	Remote Management and Monitoring	Must support adding a Lights-Out-Management (LOM) expansion card providing out-of-band management to remotely diagnose, start, restart and manage the appliance from a remote location.		
	Required security blades	Should include: • Firewall, • VPN • Mobile access • Context awareness • Application Control, • URL Filtering, • Intrusion Prevention System & IDS, • Antivirus, • Anti-Bot • Threat emulation – Sand Blast Zero-Day Protection with logging enabled.		

	RFC Performance	Supported Concurrent connections with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection with logging enabled **: 2M concurrent connections**		
		Emulation OS Support for Windows 7, 8.1, 10 & current		
	Local management abilities	The firewall solution must include Security Management Container (for managing up to 5 gateways), Network Policy Management and Logging Status.		
	Applications	The system should be application aware with over 8,500+ pre-defined application identification templates and with an ability for admins to customize their own applications templates.		
		Should accept, prevent, schedule, and apply traffic-shaping for specific applications.		
	Required Hardware Configuration	The required specifications are: • 8 on board 1GbE copper interfaces. • 2x10 GbE fiber ports with Short Range (SR) transceivers and 2*5M LC-LC Om4 fiber cables. • 2*240GB SSD		

	Dynamic User-based Policy	• Must be configured and integrated with Microsoft AD or LDAP or RADIUS, or Terminal Servers and with 3rd parties via a Web API • The firewall should enforce consistent policies for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms.		
	Network connectivity	Must support 802.3ad passive and active link aggregation		
		Must provide both Layer 2 (transparent) and Layer 3 (routing) modes.		
	High Availability features required	Active/Active L2, Active/Passive L2 and L3		
		Session failover for routing change, device and link failure		
	Unicast and Multicast Routing	OSPFv2 and v3, BGP, RIP support		
		Static routes, Multicast routes		
		Support for Policy-based routing		
	VPN Licenses	The solution should include Basic Threat Protection for 1 years Web Protection, forensics Access and Data protection – qty 10		
	Log Management -Perpetual License required	The firewalls must include Next Generation Security Management Log dedicated appliance.		
	Support warranty	The firewall solution should come with three years OeM Enterprise Support- 7 days x 24 hours for both HW & SW components.		

	Professional Services	Installation and configuration scope, User training, documentation. - Bidders will be required to perform: • The installation and configuration of the supplied firewalls and integrate them to the existing DC & DR network environments. • Knowledge transfer to ICT admin staff on the proposed solution. • Certification training & exam fee on the proposed NGFW technology at OEM's training facility – 2 Delegates. • One Year Support and maintenance services provided by the bidder.		