THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY
KENYA DIGITAL ECONOMY ACCELERATION PROJECT
ICTA-PROGRAM IMPLEMENTATION UNIT

Name of Assignment: Supply, Delivery, Installation & Commissioning of Enterprise Cyber Security Tools
RFB Reference No.: RFB No: KE-ICTA-441867-GO-RFB
Loan No./Credit No./Grant No.: IDA 7289-KE and 7290-KE
Country: Kenya
Date: 22nd July,2025

Dear All,

RE: CLARIFICATION OF RFP DOCUMENT THROUGH CLARIFICATION 1

In accordance with the Instructions to Bidders *[Clarification of Bidding Document] and TOR*, the Client is clarifying the following sections of the issued RFB Document

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
1.	We would like to know the information for the following questions. a. Are the Internet Gateway (IGW) firewall and the DMZ firewall located at the same site, or are they deployed in different physical locations? b. If the DMZ firewall is deployed at a different location, could you please confirm the Internet firewall model and vendor currently used at that site c. Is the DMZ intended to be an internal DMZ (within the organization) or an external/public-facing DMZ? d. Is the proposed centralized firewall management solution expected to manage all 6 IGW firewalls and the 2 DMZ firewalls? e. If the firewalls are distributed across different locations, is there WAN or inter-site connectivity between the centralized management system and all	a. IGW firewalls and DMZ firewalls will be deployed in different physical locations. b. The DMZ firewall will breakout to the internet through the IGW firewalls. The IGW firewalls and DMZ firewalls physical locations are part of the same WAN. c. The DMZ is public-facing DMZ for the government network with various external phasing services. d. The proposed centralized firewall management must be able to manage all 6 IGW firewalls and the 2 DMZ firewalls. e. There is a WAN/inter-site connectivity between centralized management system and all firewall locations.

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
	firewall locations? f. Are there any additional firewalls (beyond the 6 IGW and 2 DMZ firewalls) that are expected to be managed under the centralized management platform? g. Is this solution intended to replace existing firewall infrastructure (i.e., a migration), or is it a greenfield deployment? h. Is the Sandboxing with File Sanitization feature expected to use a local on-premises sandbox, or is a cloud-based sandbox acceptable/preferred? i. If local sandboxing is required, is there a specific location where the sandbox appliance will be hosted?	f. At the moment there's no additional firewall beyond the 6 IGW and DMZ firewalls expected to be managed under the centralized management platform. However, the proposed management platform should cater for scalability in case ICT Authority decides to add more firewalls in future due to traffic growth. g. The solution is complementing an existing firewall infrastructure. h. On prem and/or cloud sandbox proposals are both accepted but clarify what the offering proposal is. i. For bidders with local sandbox proposals, ICTA will provide the rack-space required. The design must be clearly articulated in the submission.
2.	Request For Extension Of Tender Closing Date On RFB: Ke-Icta-441867-Go-Rfb – Supply, Delivery, Installation And Commissioning Of Enterprise Security Tools extension of at least 2 weeks	Given the current project schedule and strict timelines, an extension for closing date for this tender will not be granted
3.	Should the Miercom test results be for the exact proposed model or can it be from a related product family?	The Miercom test results should be of the exact proposed model being proposed.
4.	Are the performance figures for a single appliance or for a cluster?	The performance figures are for a single appliance.
5.	Is vendor-native Light Out Management required, or is standard remote KVM/IPMI acceptable?	The light out management must be vendor native.
6.	Must the solution support peer review and real-time collaboration or is sequential editing acceptable?	The solution must support peer review and real-time collaboration.
7.	Can AI-based threat prevention be cloud-integrated or OEM-attached, or must it be native?	The AI-based threat prevention must be OEM attached.
8.	Is a very high threshold acceptable instead of truly unlimited tunnels?	All options are welcome. Please clearly state the number of tunnels supported in your compliance.
9.	Is an internal CA mandatory or can the solution integrate with external certificate authorities?	Both internal CA and external certificate authorities are mandatory.
10.	Is integration with third-party Gen AI acceptable or must it be built-in?	The Gen AI must be built-in the proposed solution.
11.	Can training be conducted online or must it be in-person at OEM offices?	The Expected training Proposals are for in-person training at an OEM offices or OEM approved offices.
12.	Are product datasheets with part numbers sufficient instead of public URLs?	Both product datasheets, with clearly stated pages and categories and public URLs are expected.

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
13.	What level of support is expected during the 12-month warranty period (e.g., NBD, onsite)?	ICTA expects onsite support for the local bidders and direct remote support through OEM's TAC for "breakfix" scenarios.
14.	**The Technical Specifications have the following requirement:** **Specific Experience:** The Bidder shall demonstrate that it has successfully completed at least Three (3) contracts within the last Five (5) years prior to bid submission deadline, each with a value of at least Kes. 310 Million or equivalent that have been successfully and substantially completed and that are similar in nature and complexity to the Goods and Related Services under the Contract. For a joint venture, this requirement may be met by all members combined. **Kindly confirm whether** the contract references provided must be specifically for the proposed solution, or if we may submit references for any ICT-related services contracts, provided they meet the required value and complexity criteria?	The references are for any ICT security related services contracts that are similar in nature and complexity to the Goods and related Services under this RFB.
15.	**The Technical Specifications have the following requirement:** The partner must have Engineers certified to high level of security certifications for the proposed solutions (Palo Alto PCNSE, Cisco CCIE Security, Checkpoint CCSE, Checkpoint CCTE, Checkpoint CCSM, Fortinet NSE 7 etc.) Composition of qualified technical Staff (One Mark Each per resource profile shared that has certified copies of expertise Certification) No Points for Resource without certifications) **Kindly confirm the following:** 1. Is it mandatory to attach certifications specifically related to the proposed solution, or can we attach any of the listed certifications (PCNSE, CCIE Security, CCSE, CCTE, CCSM, NSE 7), regardless of the proposed brand? 2. Is it required that each category of technical personnel (e.g., Cybersecurity Engineers, Integration Engineers, Network Engineers) hold the respective high-level certifications, or is it acceptable for the certifications to be distributed across the technical team as long as the requirement is met?	The bidders can attach equivalent certification to those stipulated in the tender, provided for any brand provided the Certifications should be related in level and match to the solution they are proposing. 2. The certifications to be distributed across the technical team as long as the requirement is met.
16.	Could we consider allowing firewall vendors who are recognized as leaders by other well-known global analysts like Forrester Wave, SE Labs, or NetSec Open, instead of only those listed as leaders in the Gartner Magic Quadrant?	Please refer to the specification as defined in the tender requirements.
17.	For the firewalls requested, if the Intrusion Prevention System (IPS) throughput is the same, should we also consider the firewall's overall throughput? Since the firewall will likely be used in Next-Generation Firewall (NGFW) mode with IPS enabled, can we focus only on the combined NGFW and IPS performance instead?	Please refer to the specification as defined in the tender requirements.
18	Could we consider configuring a cluster of DMZ firewalls to collectively handle the required throughput, thereby ensuring the performance demands are met effectively? This approach would allow multiple firewalls to work together, increasing capacity and providing redundancy for better network security and reliability.	The performance in the DMZ firewalls is for a single appliance. The ICT Authority will deploy the firewalls in A/S set up.

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
19.	**Firewall Analyst Reports:** The mandatory evaluation criteria for the IGW Firewalls (Item 1, Part 1, Section 1) state that the proposed solution must be in the Leaders Quadrant of the Gartner Magic Quadrant for Enterprise Network Security. We would like to inquire if solutions recognized as leaders by other reputable industry analysts such as Forrester, SE Labs, or NetSec Open would also be considered compliant.	Please refer to the specification as defined in the tender requirements.
20.	**DMZ Firewall Throughput:** The specifications for the High-Performance Internal (DMZ) Firewalls (Item 2) list required throughputs, including 500 Gbps for firewall throughput and 150 Gbps for NGFW throughput. Could you please clarify if proposing a clustered configuration of multiple firewalls that collectively meets or exceeds these performance requirements would be an acceptable solution?	The DMZ firewall performance numbers are for a single appliance.
21.	**Throughput Evaluation (IPS vs. Firewall):** The tender lists separate performance requirements for Firewall throughput, IPS throughput, and NGFW throughput. Considering that the firewalls will likely be deployed in NGFW mode with IPS functionality continuously active, could you please clarify the evaluation weighting of these metrics? Specifically, if a proposed solution meets the required IPS and NGFW throughputs, will the standalone firewall throughput figure be considered of lesser importance?	ICTA has use-cases as to why the performance metrics are stipulated as they are in the requirements. Please work with the tender requirements.
22	Is Miercom firewall rating a mandatory requirement: On the test summary report page the rating company mentions "NOTE that the vendors did not get an opportunity to configure their own products as per the percentages described on the specifications" "Vendor must share latest Miercom firewall security results highlighting the below expected outputs; Must have at least 90% Zero Day Malware Prevention Efficacy Must have less than 5% missed phishing and malicious URL missed detection rate Must have at most 0.2% False Positive Malware Detection Rate Must have at least 90% of exploits blocked by Intrusion prevention system." See link to access the document on page6 where the configuration issue is highlighted. https://miercom.com/wp-content/uploads/2025/02/Miercom-Check-Point-NGFW-CONFIDENTIAL-SR241113M-3FEB2025.pdf	Miercom testing is an independent testing and certification lab that conducts product evaluations, for third-party validation. Their "Performance Verified" label is used by vendors to showcase test results under specific conditions. In regard to this test rating being mandatory to this tender, our response is that it is. It is the benchmark to which we have based the expected performance of the expected firewalls that have been independently validated and confirmed. The test is mandatory as it's a lab test based in real life use cases enabling ICT Authority to evaluate vendors and proposals based on the said use cases. Testing in a lab, Malware efficacy, Vulnerability Efficacy and Phishing Efficacy align with cyber threats that the ICT Authority faces in its day to day operations.
22 a.	There is mention of check point firewall on pg139 under inspection and testing, reference "Checklist for implementing a Check Point Next-Generation Firewall (NGFW)." and "e) Verify security blades needed to be enabled and review the licensing and subscription requirements". Does it mean the firewalls to be supplied should only be check point or alternatives can be proposed ?	All firewall solutions are welcome and will be evaluated in accordance to the evaluation criteria and functional requirements as guided in the RFP.
22 b.	There is mention of check point firewall training on pg 140 under post implementation "e) Provide training for administrators on managing and troubleshooting Check Point NGFW". Does it mean the firewalls to be supplied should only be check point ?	All firewall solutions are welcome and will be evaluated in accordance to the evaluation criteria and functional requirements as guided in the RFP. Bidders should provide similar and equivalent training certification from their preferred OEM solution provided. All

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
		solutions are welcome and will be evaluated based on the criteria and functional requirements as guided in the RFP.
22 c.	There is mention of "Network Security Blade Firewall" on page 114. This are Check point security modular features does it mean the requirements is tied to check point only or we can propose alternatives ?	All firewall solutions are welcome and will be evaluated in accordance to the evaluation criteria and functional requirements are as guided in the RFP.
22d.	On pg49 under item number1 and pg. 107 under Part 2: SYSTEM REQUIREMENTS Hardware performance in enterprise testing conditions as follows: • Pg49 Firewall throughput: - 240 Gbps,pg107 Must support at least 200 Gbps of firewall throughput the requirement is confusing. • Pg49 Item 2,pg107 Must support at least 100 Gbps IPS Throughput the requirement is confusing Hardware performance in enterprise testing conditions as follows: • On pg49 Item 2 Firewall throughput - 500 Gbps, on pg 119 Must support at least 400 Gbps of Firewall Throughput. The requirement is confusing. • On pg 49 NGFW (Including Firewall, Application control and IPS enabled) Throughput – 150 Gbps,on pg 119 Must support at least 50 Gbps Threat Prevention Throughput.	There are two sets of Firewalls being procured. High Performance Internet Gateway (IGW) Firewalls and High Performance Internal (DMZ) Firewalls. The ratings are mapped to each set of firewalls. In this tender, ICTA has clearly stipulated the performance requirement for each set of firewall, highlighting MINIMUM requirements for evaluation under ITEM 1 Mandatory pass evaluation in Pg 106 for high performance internet gateways (IGW) firewalls and Mandatory pass Evaluation in Pg 121 high performance Internal (DMZ) firewalls as follows : **ITEM 1** Mandatory Pass Evaluation for High Performance Internet Gateway IGW Firewalls Pg 106 1. Must support at least 200 Gbps of firewall throughput 2. Must support at least 100 Gbps IPS Throughput 3. Must support at least 100 Gbps and inspection NGFW Throughput. NGFW must include Firewall, Application Control and IPS with logging Enabled. **ITEM 2** Mandatory Pass Evaluation for High Performance Internal (DMZ) Firewalls Pg 119` **1.** Must support at least 150 Gbps of NGFW throughput and scalable to at least 700 Gbps of NGTP throughput. **NGFW must include Firewall, Application Control and IPS with logging Enabled.** The proposed solution by bidders must have the capability to capability to scale up-to 700 Gbps for NGTP throughput without "ripping and replacing" the already deployed solutions. Bidders should demonstrate how this can be achieved with their proposed solutions. NGTP must include Firewall, App Control, URLF, IPS, Anti Malware (Bot,

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
		Virus & Spam) and DNS Security with logging enabled). 2. Must support at least 50 Gbps Threat Prevention Throughput. Threat prevention throughput must **include Firewall, App Control, URLF, IPS, Anti Malware (Bot, Virus & Spam), DNS Security , Zero-Phishing and Sandboxing (Including content disarm and reconstruction) with logging enabled).** 3.Must support at least 400 Gbps of Firewall Throughput. **Reference to Pg 49 G. Evaluation of Technical Bids** **Please note Specified performance requirements:** This section will evaluate the extent to which the specific Hardware and solution performance, capacity or functionality **meets or exceeds** the specified performance/functional requirements. ICTA will use this section as a guide for evaluation as commented above. The solutions proposed will be evaluated to the extent of its performance, ICTA has highlighted the performance as "best-to-have", which will correspond to maximum scoring points. **ITEM 1** High Performance Internet Gateway (IGW) Perimeter Firewalls' performance/functional requirements 1. Firewall Throughput – 240 Gbps 2. IPS Throughput – 140 Gbps 3. NGFW (Including Firewall, Application control and IPS enabled) Throughput -100 Gbps. **ITEM 2** High Performance Internal (DMZ) Firewalls' performance/functional requirements 1. Firewall Throughput – 500 Gbps 2. IPS Throughput – 230 Gbps 3. NGFW (Including Firewall, Application control and IPS

S/NO	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE
		enabled) Throughput -150 Gbps. **The above clarification therefore makes correction of any part of the tender document that may have been documented in error specific to this section of the document.**
22 e.	For the CENTRAL MANAGEMENT APPLIANCE it's not clear if it is Virtual or Physical appliance please clarify ?	The Central Management Appliance must be physical appliances.
22 f	Hardware performance in enterprise testing conditions as follows: • On pg49 Item 2 Firewall throughput - 500 Gbps, on pg. 119 Must support at least 400 Gbps of Firewall Throughput. The requirement is confusing • 0n pg. 49 NGFW (Including Firewall, Application control and IPS enabled) Throughput – 150 Gbps, on pg. 119 Must support at least 50 Gbps Threat Prevention Throughput.	Please refer to ICTA's Response 22d above under Item 1
23	For the Internal DMZ/Internal DC Firewalls that will be deployed at KONZA the specifications are hardware and based on my knowledge KONZA is on private cloud that is virtualized, should the requirement be virtual or physical ?	Internal DMZ/DC Firewalls must be physical appliances
24	Kindly clarify if the below requirement is mandatory and if non-compliance would lead to automatic disqualification: The Bidder must provide ISO/IEC 27001:2022 for Information Security Management Practices	The requirement is mandatory. The Bidder must provide ISO/IEC 27001:2022 for Information Security Management Practices

This Clarification 1 forms part of the issued RFB document. All other terms and conditions of the issued RFB document remain unchanged.

Zilpher Owiti, OGW Chief
Ag. Chief Executive Officer,
ICT Authority