



BID BULLETIN NO. 01

Date: **22 September 2023**

ITB No.: **bac-23-0920c**

Project Name: **Supply, Delivery and Configuration of Various ICT Equipment - PLP (Rebid)**

ABC: Php 2,720,000.00

To all prospective bidders:

This Bid Bulletin is issued to clarify, supplement, modify and/or revise the particular sections in the Bid and Contract Documents as stipulated in the Bidding Documents issued on 20 September 2023. The Bidders shall take note of the following items carefully and consider them in the preparation of their bid proposals, as they shall form part of the CONTRACT DOCUMENTS.

Item	Previous Specification/ Clarification/Request to Consider	Amendment/Response to Clarification
ADDENDUM:		
Kindly see attached "ANNEX A" for the Terms of Reference"		

Bidders who have already submitted bids are hereby informed that they are allowed to modify or withdraw their bids, if necessary, before the scheduled opening of bid envelopes.

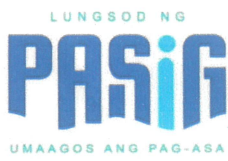
For modifications in your original submitted bid, kindly submit new bidding documents (sealed and marked as "Modified Bid") and have these received at the Office of the Bids and Awards Secretariat. Bid modifications received after the deadline shall not be considered and shall be returned to the bidder unopened.

Conforme:


Bitto Ulanern

END-USER REPRESENTATIVE
Signature Over Printed Name


ATTY. JOSEPHINE C. LATI-BAGAOISAN
Chairperson



TERMS OF REFERENCE

"ANNEX A"

SUPPLY, DELIVERY AND CONFIGURATION OF COMPUTER SERVER AND FIREWALL FOR PAMANTASAN NG LUNGSOD NG PASIG

TO: All Prospective Bidders
Members of the Bids and Awards Committee
Other Concerned

I. Technical Specifications

Below are the minimum requirements for the Computer Server, UPS and Firewall of the Pamantasan ng Lungsod ng Pasig.

Hardware Specifications:

Table with 2 columns: Item No. 1 and SERVER Hardware Specifications. It lists requirements for Processor, Memory, Storage, Storage Controller, Network Connectivity, and Form Factor.



	<p>I/O Ports</p> <p>Front Ports</p> <ul style="list-style-type: none"> • 1 x Dedicated for management and monitoring of server • 1 x USB 2.0 • 1 x VGA <p>Rear Ports</p> <ul style="list-style-type: none"> • 1 x USB 2.0 • 1 x Serial (optional) • 1 x USB 3.0 • 2 x RJ-45 • 1 x VGA (optional for liquid cooling configuration) <p>Internal Ports</p> <ul style="list-style-type: none"> • 1 x USB 3.0
	<p>Supported Operating System</p> <p>Canonical Ubuntu, Citrix Hypervisor, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi</p>
	<p>Power Supply</p> <p>At least 1400W Dual, Hot-Plug Redundant, Mixed Mode Power Supply with Power Cord - 2.8m, 15A/100-250V, C13 to C14 Jumper Cord</p>
	<p>Warranty</p> <p>Three (3) years warranty with 24x7x4 support</p>

Item 2	FIREWALL Hardware Specifications
1	NGFW hardware appliance with the following technical specifications:
2	The proposed Next Generation Security Platform shall also provide exactly 4.8 gigabits per second of threat prevention throughput of Extensive (i.e. all threat signatures and heuristics rated as Low, Medium, High, and Critical Severity enabled.) Threat Prevention Capabilities.
3	The NGFW shall have a security-specific Operating System (OS) built as an appliance (not on generic hardware) and shall handle traffic in a single-pass manner for efficient performance.
4	Must support a dual redundant power supply
5	The NGFW must support at least the following interfaces:
a	10/100/1000 out-of-band management port (1) HSCI 10 gigabit high availability (1) RJ-45 console port (1) USB port (1) Micro USB console port (1)
b	4x 10/100/1000
c	4 x 1G/2.5G/5G
d	4x 1G/2.5G/5G /PoE,
e	2x 1G SFP slots
f	8x 1G/10G SFP/SFP+ slots with optional transceiver modules



6	Must support at least 9.5 Gbps firewall throughput with application control and logging enabled
7	Must support at least 140,000 new sessions per second
	General Requirements
9	The Management Plane (handling Admin Consoles, Reporting, etc.) and the Data Processing Plane (handling Firewall Policies, IPS, Anti-Virus, Anti-Spyware Scanning, etc.) must be separated such that when the Management Plane was to hang, it could be separately restarted without disrupting the on-going traffic data processing functions
10	The NGFW must have visibility into applications regardless of ports or protocols
11	The proposed Enterprise Security Platform must have been in the Leaders Quadrant in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for the last 10 years
13	The proposed solution must have the capability to generate a Report where it benchmarked with Vendor and Third-party best practices (ie: NIST) unlimited-ly without any additional charges, or special license required.
14	The proposed Enterprise Security Platform must have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis without the need of any additional software subscription/licenses or hardware components.
	NGFW Functionality
15	The proposed Next Generation Security Platform shall support all the following authentication services: Directory services: Microsoft Active Directory, Microsoft Exchange, OpenLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.
16	The proposed Enterprise Security Platform must support the identification of the traversing applications, regardless of port or protocol, even if the traffic is tunneled in GRE, GTP and NULL-IPSec, uses evasive tactics, or is encrypted without the need of additional software/hardware.
17	The proposed Enterprise Security Platform shall allow the administrator to review any policy impact for new or modified application signatures included in a content release version. This WebGUI feature will enable the administrator to simultaneously update the security policies and install new content, and allows for a seamless shift in policy enforcement.
18	The proposed Enterprise Security Platform shall be able to block source IP addresses performing DoS attacks on the hardware INGRESS level even before consuming any CPU or packet buffer resource without any user configuration
19	Must have a Policy Optimizer which is able filter rules who are used or unused in specific time frames such as 30 days, 90 days, etc., with an external management device



20	The proposed Enterprise Security Platforms shall be able to decrypt, inspect and control both inbound and outbound SSL and SSH connections to prevent unwanted activities or malicious content on the same proposed hardware, also serve as the decryption broker to other security devices
22	The proposed Enterprise Security Platform shall have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.
23	The proposed Enterprise Security Platform shall include individual user activity report shows applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware modules
24	Must have “indicators of compromise” (IOCs) tagging for alerting organization when a specific threat has been observed in the organization or similar industry. The tags must be searchable, allowing the user to instantly pivot to associated malicious samples.
	Advanced Threat Prevention
25	Must Support a Protocol anomaly-based protection that detects non-RFC-compliant protocol usage, such as an overlong URI or FTP login.
26	Must Support a Protocol decoder-based analysis that statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits.
27	Must Support Heuristic-based analysis that detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
28	Must have integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.
29	The proposed solution shall deliver inline machine learning (ML) at the network level and should block unknown threats in real time instead of waiting for a sandbox- integrated directly on the NGFW
30	The ML capability of the proposed solution shall prevent unknown weaponized files, credential phishing, and malicious scripts instantly without holding files or web pages and without compromising business productivity.
	Advanced URL Filtering



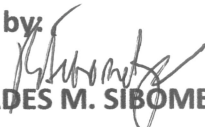
31	<p>Must Support Real-Time Credential Theft Protection which detects and prevents credential theft by controlling sites to which users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites in real-time while still allowing users to only submit credentials to corporate and sanctioned sites with Zero false positives.</p>
32	<p>Must support Inline Real-Time Web Threat Prevention by using cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).</p>
33	<p>Must support Phishing Image Detection with ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.</p>
34	<p>Must support Translation Site Filtering that applies Advanced URL Filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.</p>
35	<p>Must have multilingual functionality that supports web crawling and analysis in 41 languages.</p>
	<p>Advanced Wildfire</p>
36	<p>Must provide flexible support for Snort and Suricata rule conversion, providing easy-to-configure custom signatures. This support completely eliminates the need for standalone IPS or IDS solutions</p>
37	<p>Must prevent highly evasive malware via stealthy observation n to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.</p>
38	<p>Must support uncovering malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis to prevent malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing.</p>
39	<p>Must support an intelligent Runtime Memory Analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed.</p>



Vendor Requirements	
1	The bidder must submit a Manufacturer's certificate stating that the bidder is an authorized distributor of the Server and Firewall Solution.
2	The bidder must submit a list of local sales and technical offices in the Philippines for guaranteed support.
3	The bidder must submit a list of at least two (2) installed bases of both server and firewall solutions with addresses and contact details.
4	The bidder must submit a list of locally based certified personnel including copies of unexpired certifications - 3 Certified Technology Architect Specialists of the Server Solution - 3 Certified Accredited Engineers of the proposed Firewall Solution
5	The bidder must submit a Resume/Curriculum Vitae as proof that the technical engineer is LOCALLY (Phils) base and employed by the vendor/bidder
6	The bidder must provide a Project Manager to oversee the project. The bidder must submit Project Management training or certifications as his/her credentials with a CV/resume
7	The bidder must submit the Helpdesk escalation procedure with a flowchart. The local helpdesk will provide 24x7 technical assistance
8	Training, Implementation, Installation, and configuration of the Firewall and server shall be provided by the supplier.

Item 3	Uninterruptable Power Supply Hardware Specifications
1	SMART-UPS SRT 6000VA /6000W 230V, SMART UPS ON-LINE LCD PF1.0 5U

Prepared by:


MELQUIADES M. SIBOMET JR. Ed. D.
MIS Head

Noted:


Mr. Roberto A. Osorio
Head, Project Management Division, MISO


Mr. Jerry V. Obico
Head, Infrastructure Division, MISO


Mr. John Carlo F. Fatallo
OIC, MIS Office Pasig City