DEVELOPMENT BANK OF THE PHILIPPINES
Head Office: Sen. Gil J. Puyat Avenue corner
Makati Avenue, Makati City, Philippines

SUPPLEMENTAL BID BULLETIN NO. 1

10 December 2025

Attention: **All prospective bidders for the project**

BID REFERENCE NO. G-2025-36: SUPPLY, DELIVERY, INSTALLATION, TESTING, AND COMMISSIONING OF A NEXT GENERATION FIREWALL (NGFW) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES (ABC: PhP 118,000,000.00 inclusive of all applicable taxes)

Please be informed of the following:

1. The schedule of bid activities for the above-cited project shall proceed as follows:

ACTIVITY	DATE AND TIME	VENUE
Deadline of Submission of Eligibility, Technical, and Financial Proposals*	**17 December 2025 (Wednesday) ON OR BEFORE 9:00 AM**	6/F BAC Secretariat, DBP Head Office, Makati City
Opening of Eligibility, Technical, and Financial Proposals	**17 December 2025 (Wednesday) 9:30 AM**	12/F Suite 5, DBP Head Office, Makati City

Late submissions shall not be accepted

2. Response to the queries of the bidders:

QUESTIONS	RESPONSE
Bidder No. 1	
For Firewall Management server, can we propose a cloud-based (SaaS) management platform instead of a Hardware-Based form factor?	**No. The "On-Premises" Hardware Base is a requirement.**
As firewalls of different brands have their own firewall architecture, may we request to remove the RAM requirements and just propose model that will suffice how much throughput is required?" If the throughput is low, even with plenty of RAM, the network will experience latency, congestion, and degraded performance since the primary function of the NGFW is to inspect and filter network traffic	**No. The specifications on the RAM, as stated in the TOR, are required.**

QUESTIONS	RESPONSE
in real time. These operations are CPU-intensive and throughput-dependent, not RAM-heavy.	
Can we relax the SDWAN-ready license in the Data Center firewall? Rationale: DC firewall is not positioned for SDWAN deployment.	**No. The requirement to have the option for SDWAN capabilities is required.**
Bidder No. 2	
Under page 111, Hardware Technical Specifications, Item B.1.03 B.1.03. 4 x 10GBASE-T RJ45 ports with 10G copper transceivers, and Spare set of 4 x 10G SFP+ interfaces/slots, with 4 x 10G SFP+ multimode fiber transceivers Question: Does the "spare set of 4 x 10G SFP+ interfaces/slots" means it is just a spare module and we need to include in the proposal additional module with SFP+ transceivers?	**Yes. Spare module and transceivers are required.**
Under page 113, Hardware Technical Specifications, Item B.2.17 B.2.17. The proposed Firewall should support more than 25,000 (excluding custom signatures) IPS signatures. It should support the capability to configure correlation rule where multiple rules/event can be combined together for better efficacy Question: We would like to confirm whether the required minimum of 25,000 IPS signatures includes bot-related signatures and patterns, as anti-bot protection being part of IPS capabilities.	**Yes. Bot-related protections to be counted within the 25,000 minimum IPS signatures, since anti-bot is typically integrated into IPS functionality.**
Under page 112, Hardware Technical Specifications, Item B.1.17 B.1.17. The solution should have the option to enable SDWAN capabilities without a separate additional license Question: Requesting that SD-WAN capabilities mentioned Data Center / Internal firewall be relaxed given that the firewall in question is intended to serve as a Data Center / Internal firewall rather than an edge or branch deployment.	**No. SDWAN capabilities are required.**
Under page 117, Item B.7.02 B.7.02. 1G copper or 10G SFP+ transceiver (both interfaces / Transceiver must be available)	**The device must support both 1G copper and 10G SFP+ interfaces. If it cannot provide both at the same time, the provider must supply the other interface as a spare, ready for module/transceiver exchange, to comply with the availability requirement.**

QUESTIONS	RESPONSE
Question: We would like to confirm if we can 1G can suffice the requirement since the statement uses OR. For clarity, remove the parenthetical note.	
Under page 115, Hardware Technical Specifications, Item B.5.05 B.5.05. Operates seamlessly as both gateway and management control. Question: To clarify, the requirement for the DR Firewall will function as a firewall and will be a capability to locally manage its own configuration and operation. Is this correct?	**Yes. The DR Firewall must function as a Gateway-Firewall and with capability for local management.**
Under page 117, Hardware Technical Specifications, Item B.6.09 B.6.09. Must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant segment Question: For clarity, may we confirm if this requirement pertains to a firewall's ability to segment the rule base into a sub-policy structure that enforces a "parent-and-child rule" association, rather than creating a separate policy outside of the parent-and-child relationship? In this context, does the enforcement of a sub-policy mean that relevant traffic is forwarded from the parent rule to its associated sub-policy?	**Yes. The requirement is the firewall's ability to enforce a hierarchical parent-child rule structure, where traffic flows from the parent rule into its associated sub-policy for further filtering, rather than creating standalone policies.**
Under page 117, Hardware Technical Specifications, Item B.6.11 B.6.11. Management GUI shall have the ability to easily get to IPS signature definition from the IPS logs Question: May we confirm if this requirement pertains to a firewall management's ability to directly click on an IPS log entry and immediately view the corresponding IPS protection/signature definition displaying critical details such as severity/criticality, confidence level, attack name and information, and industry references/common vulnerability exploits (CVE) all within the same tab?	**Yes. The requirement pertains to a seamless workflow where relevant IPS signature details are accessible directly from the log entry, rather than requiring separate navigation or external lookup.**
Under page 117, Hardware Technical Specifications, Item B.6.12 B.6.12. Must combine policy configuration and log analysis in a single pane, in order to avoid	**Yes. The intent is for administrators to configure policies and analyze logs side by side in one view, allowing immediate correlation of rule changes with events, instead of switching to a separate log viewer.**

QUESTIONS	RESPONSE
mistakes and achieve confidence of the change. Question: May we confirm our understanding of the requirement regarding the capability of the firewall management solution to provide a unified interface where administrators can configure security policies and simultaneously view the corresponding logs and events in a single view without the need to open another dashboard or tab reducing errors in policy changes? Will DBP require also filter/search log along with instant log view or analysis?	
Under page 117, Hardware Technical Specifications, Item B.6.13 B.6.13. Must provide lookup of all references to any given network object in all of its policies and settings. Question: May we confirm our understanding of DBP's requirement specific to this item - "look of all reference", means the ability of the firewall management to provide a comprehensive lookup function allowing DBP to instantly view all references to a selected network object across all policies and settings?	**Yes. The firewall management solution must allow administrators to instantly view all references to a selected network object across all policies and settings.**
Bidder No. 3	
Specification: The proposed Firewall should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. Question: Instead of Dynamic, can it be highly efficient and low-risk configuration management for IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.)	**No. Dynamic tuning implies automated, adaptive adjustments by the firewall itself.**
Specification: The proposed management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows Question: Can we leverage its own vulnerability information?	**Yes. Firewall solution's own vulnerability information can be used as baseline, but it should still be capable of integrating third party vulnerability information or sources with the solution's threat policy adjustment workflows to meet the existing requirement**
Specification: The proposed management platform should have the capability to centrally manage workload attribute feeds obtained from multiple public and private cloud environments, to enable firewalls to adapt to changes	**Yes. This feature means the management platform can centrally collect workload information from different cloud environments and automatically adjust firewall policies in real time, so security rules**

QUESTIONS	RESPONSE
instantaneously. This enables the firewall policy to adapt in real-time to the changes in public and private cloud workloads. Question: Do we need to support public cloud even if the proposed solution is an on-premise solution?	**always match the current state of workloads without manual updates**
Specification: Multifactor Authentication Question: Can we leverage third-party authentication system to enable multi-factor authentication (MFA)?	**Yes. The solution shall support Multifactor Authentication (MFA) either natively or through integration with third-party authentication systems, without incurring additional expense to DBP.**
Bidder No. 4	
From page 111, Form 9 (page 2 of 17) B.2 Perimeter Firewall B.2.01. Not more than 2RU appliances with airflow ducts available from front to back. Question: We respectfully request, if we can relax for at least 3RU appliance with front-to-back airflow.	**No. The requirements defined in the TOR are retained pursuant to our internal setup.**
From page 112, Form 9 (page 3 of 17) B.2 Perimeter Firewall B.2.08. Throughput Capacity at least NGFW 45 Gbps + Threat Protection and RAM of at least 128GB Question/Clarification: We respectfully request, if we can remove the RAM specification. The proposed system has: 198 / 197 / 140 Gbps Throughput. There's no explicit reference for the RAM specifications of the model as Fortinet does not disclose it with their FortiGate Models. But the technology that Fortinet uses which is a purpose-built ASICs called Security Processing Units (SPUs).	**No. We retain the required RAM specification to guarantee that the hardware can support both the high-speed data path and all security functions without sacrificing performance.**
From page 113, Form 9 (page 4 of 17) B.3 VPN Concentrator B.5.02. 8 x 1/10G copper Question/Clarification: We respectfully request, if we can relax the copper ports to the following 16 x GE RJ45 Ports 8 x GE SFP Slots 4 x 10GE/GE SFP+/SFP Slots 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots	**No. We retain the specified Interfaces as they are critical for alignment with our internal infrastructure.**

QUESTIONS	RESPONSE
From page 114, Form 9 (page 5 of 17) B.4 Test/UAT Firewall Throughput Capacity at least NGFW 10 Gbps + Threat Protection and RAM of at least 64 GB Question/Clarification: We respectfully request, if we can remove the RAM specification. The proposed system complies the requirement with 11.5 Gbps NGFW throughput and 10.5 Gbps Threat Protection throughput, though available documentation does not confirm at least 16 GB of RAM	**No. We retain the required RAM specification to guarantee that the hardware can support both the high-speed data path and all security functions without sacrificing performance.**
From page 115, Form 9 (page 6 of 17) B.5. Disaster Recovery Firewall B.5.02. 8 x 1/10G copper Question: We respectfully request, if we can relax the copper ports to the following 16 x GE RJ45 Ports 8 x GE SFP Slots 4 x 10GE/GE SFP+/SFP Slots 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots	**No. We retain the specified Interfaces as they are critical for alignment with our internal infrastructure.**
From page 115, Form 9 (page 6 of 17) B.5. Disaster Recovery Firewall B.5.07. 24 million concurrent sessions and also provide application visibility to allow for the detection or blocking of specific application traffic Question: We respectfully request, if we can relax for at least 16 million concurrent sessions	**No. We retain the specified concurrent sessions to guarantee the full operational integrity and security functionality.**
From page 117, Form 9 (page 8 of 17) B.6. Firewall Management Appliance B.6.09. Must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant segment Question: We respectfully request, if we can relax for at least focused solely on analytics and logging, The proposed system is a platform focused solely on analytics and logging, distinct from firewalls like FortiGate that handle real-time traffic segmentation and policy enforcement. Its functions are restricted to analyzing existing traffic logs, offering policy optimization	**No. We require a solution that manages the live firewall policy and enables traffic flow segmentation as specified.**

QUESTIONS	RESPONSE
suggestions, and logically dividing administrative data via ADOMs, without physically governing network traffic forwarding. While the proposed system cannot directly segment the rule base for traffic forwarding, it does provide related functions: - Log Filtering - Policy Optimization - Administrative Domains	
From page 117, Form 9 (page 8 of 17) B.7. Sandboxing Facility B.7.05. Redundant power supply with Power Cables - C13-C14 Question/Clarification: We respectfully request, if we can relax the power supply to single fixed.	**No. The Facility is a critical security component, redundancy is required to ensure the component is always live and operational.**
Bidder No. 4	
Can we add transceivers to meet the required number of interfaces (convert other slots to the desired ports using transceivers)?	**No. We retain the specified Interfaces as they are critical for alignment with our internal infrastructure, unless otherwise stated in the TOR.**
For dedicated multi-factor authentication (MFA), do they prefer an on-premises solution or a virtual machine (VM)?	**We require MFA Facility that will work seamlessly with your proposed on premise VPN Firewall solution.**

3. The BAC shall no longer entertain any question/request for clarification after the issuance of this Bid Bulletin.

4. The Eligibility and Technical Documents, and Financial Proposals must be properly tabbed for easy reference and must be submitted in sequence/order per Checklist of Requirements.

5. Please refer to Section III. Bid Data Sheet (BDS) of the Philippine Bidding Documents for the detailed procedure and options for the payment of bidding documents and the submission of bids. As indicated in the Invitation to Bid, bidders must settle the required payment for the bidding documents before the deadline of the submission and receipt of bids.

6. **Bidders are encouraged to submit their bid proposals (either manual or online submission) at least one day prior to the deadline to avoid late submissions. Bidders may attend the bid opening through Zoom Meeting App.**

   For online submission of bids, bidders are reminded to email the BAC Secretariat of their intent to submit electronically at least one day prior to the deadline of bid submission. This is to give ample time for the Secretariat to prepare and generate the link wherein bidders will upload their proposals.

7. Please be advised that bids submitted after the deadline shall only be marked for recording purposes, shall not be included in the opening of bids, and shall be returned to the bidder unopened.

For the guidance and information of all concerned.

(SIGNED)
The DBP Bids and Awards Committee